Seguridad de la plataforma de Apple

Mayo de 2022

Contenido

Seguridad de la plataforma de Apple

Introducción a la seguridad de la plataforma de Apple

Apple diseña sus plataformas considerando la seguridad como su núcleo. Aprovechando su experiencia al crear el sistema operativo móvil más avanzado del mundo, Apple ha diseñado arquitecturas de seguridad que atienden los requerimientos únicos de los equipos de escritorio, móviles y de casa, así como de los relojes.

Todos los dispositivos Apple combinan *hardware*, *software* y *servicios* diseñados para funcionar juntos y lograr la máxima seguridad y transparencia en la experiencia del usuario, con el objetivo final de mantener segura la información personal. Por ejemplo, el hardware de seguridad y el silicio diseñados por Apple impulsan funcionalidades de seguridad críticas. Además, las protecciones del software funcionan para mantener la seguridad del sistema operativo y de las apps de terceros. Por último, los servicios ofrecen un mecanismo para actualizaciones de software oportunas y seguras, impulsan un ecosistema de apps protegido y facilitan comunicaciones y pagos seguros. Como resultado, los dispositivos Apple no sólo protegen el dispositivo y los datos, sino todo el ecosistema, incluido todo lo que los usuarios hacen de forma local, en redes y con servicios clave de Internet.

Al igual que diseñamos nuestros productos para que sean simples, intuitivos y compatibles, también los diseñamos para que sean seguros. Las funciones clave de seguridad, como la encriptación del dispositivo basada en hardware, no se pueden desactivar de forma accidental. Otras funciones, como Face ID y Touch ID, mejoran la experiencia del usuario al facilitar la protección del dispositivo y hacerla más intuitiva. Además, como muchas de estas funciones están activadas de forma predeterminada, ni los usuarios ni los departamentos de TI tienen que realizar extensas configuraciones.

Esta documentación proporciona información detallada sobre la implementación de la tecnología y las funciones de seguridad en las plataformas de Apple. También ayuda a las organizaciones a combinar la tecnología y las funciones de seguridad de la plataforma de Apple con sus propios procedimientos y políticas con el fin de satisfacer sus necesidades de seguridad específicas.

El contenido se divide en los siguientes temas:

- **Seguridad del hardware y elementos biométricos:** el silicio y el hardware que forman la base de la seguridad en los dispositivos Apple, incluido el Apple Chip, Secure Enclave, los motores criptográficos, Touch ID y Face ID.

- **Seguridad del sistema:** las funciones integradas de hardware y software que brindan seguridad durante el arranque, las actualizaciones y la operación continua de los sistemas operativos de Apple.
- **Encriptación y protección de datos:** la arquitectura y el diseño que se encargan de proteger los datos del usuario en caso de pérdida o robo del dispositivo, o si una persona o un proceso no autorizados intentan utilizarlo o modificarlo.
- **Seguridad de las apps:** el software y los servicios que brindan un ecosistema seguro para las apps, y que les permiten ejecutarse de forma segura sin comprometer la integridad de la plataforma.
- **Seguridad de los servicios:** los servicios de Apple para la identificación, la administración de contraseñas, los pagos, las comunicaciones y la localización de dispositivos perdidos.
- **Seguridad de la red:** los protocolos de red estándar del sector que proporcionan la autenticación segura y la encriptación de los datos durante la transmisión.
- **Seguridad de los kits para desarrolladores:** los "kits" de infraestructuras para la administración segura y privada del hogar y de la salud, así como extensiones de las funcionalidades de los dispositivos y servicios de Apple para apps de terceros.
- **Administración segura de dispositivos:** los métodos que permiten administrar dispositivos Apple, ayudar a prevenir el uso no autorizado de estos o activar el borrado remoto en caso de pérdida o robo.

Compromiso con la seguridad

Apple se compromete a proteger a los clientes mediante tecnologías de privacidad y seguridad de vanguardia, diseñadas para salvaguardar la información personal, así como mediante amplios métodos que ofrecen protección a los datos corporativos en entornos empresariales. Apple recompensa a los investigadores por su trabajo al descubrir vulnerabilidades mediante el programa de recompensas de seguridad de Apple. Puedes consultar detalles del programa y las categorías de recompensas en https://developer.apple.com/security-bounty/.

Disponemos de un equipo de seguridad experto que ofrece soporte para todos los productos Apple. El equipo realiza auditorías de seguridad y pruebas de los productos, tanto para los que están bajo desarrollo como para los que ya se lanzaron. Además, el equipo de Apple proporciona herramientas de seguridad y capacitación, y supervisa activamente si hay reportes de problemas y amenazas de seguridad. Apple es miembro del Forum of Incident Response and Security Teams (FIRST; Foro de Equipos de Seguridad y Respuesta ante Incidentes).

Apple continúa desafiando los límites de lo posible en cuanto a seguridad y privacidad, y utiliza chips personalizados en toda su línea de productos, desde el Apple Watch, el iPhone y el iPad, hasta las Mac con el chip de seguridad T2 o Apple Chip, para alimentar no sólo el procesamiento eficiente, sino también la seguridad. Por ejemplo, Apple Chip forma la base del arranque seguro, Face ID, Touch ID y la protección de datos. Además, las funciones de seguridad en los dispositivos con Apple Chip, como la protección de integridad del kernel, los códigos de autenticación del puntero y las restricciones de permisos rápidas, ayudan a frustrar tipos comunes de ciberataques. Por lo tanto, si el código del atacante logra ejecutarse de alguna manera, el daño que este puede causar se reduce drásticamente.

Para aprovechar al máximo las amplias funciones de seguridad integradas en nuestras plataformas, invitamos a que las organizaciones revisen sus políticas de TI y de seguridad para asegurarse de que se estén beneficiando totalmente de las capas de tecnología de seguridad que ofrecen estas plataformas.

Para obtener más información sobre cómo reportar problemas a Apple y sobre la suscripción a las notificaciones de seguridad, consulta Reportar una vulnerabilidad de seguridad o de privacidad.

Apple cree que la privacidad es un derecho humano fundamental y cuenta con numerosos controles y opciones integradas que permiten a los usuarios decidir cómo y cuándo las apps usan su información, así como qué información se utiliza. Para obtener más información sobre el enfoque de Apple en cuanto a privacidad, los controles de privacidad de los dispositivos Apple y la política de privacidad de Apple, consulta https://www.apple.com/la/privacy**.**

Nota: a menos que se indique lo contrario, esta documentación cubre las siguientes versiones de sistemas operativos: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 y watchOS 8.5.

Seguridad del hardware y elementos biométricos

Descripción general de la seguridad del hardware

Para que el software sea seguro, debe basarse en un hardware que tenga seguridad integrada. Es por eso que los dispositivos Apple, que funcionan con iOS, iPadOS, macOS, tvOS y watchOS, tienen funcionalidades de seguridad integradas en el propio silicio. Entre ellas se incluye un CPU que impulsa las funcionalidades de seguridad del sistema, así como un silicio adicional dedicado a las funciones de seguridad. El hardware centrado en la seguridad sigue el principio de admitir funciones limitadas y definidas de forma discreta con la finalidad de minimizar la superficie de ataque. Estos componentes incluyen una ROM de arranque, que forma una raíz de confianza de hardware para un arranque seguro, motores AES dedicados para un encriptado y un desencriptado seguros y eficientes, y el Secure Enclave. El *Secure Enclave* es un sistema en chip (SoC) que se incluye en todos los dispositivos iPhone, iPad, Apple Watch, Apple TV y HomePod recientes, así como en las computadoras Mac con Apple Chip y las que cuentan con el chip de seguridad T2 de Apple. El Secure Enclave en sí sigue el mismo principio de diseño que el SoC, que contiene su propia ROM de arranque discreta y su propio motor AES. El Secure Enclave también proporciona la base para la generación y el almacenamiento seguros de las claves necesarias para encriptar los datos en reposo, y protege y evalúa los datos biométricos de Face ID y Touch ID.

La encriptación de almacenamiento debe ser rápida y eficiente, pero al mismo tiempo no debe exponer los datos (o el *material de codificación*) que usa para establecer relaciones de claves criptográficas. El motor de hardware AES resuelve este problema al realizar encriptado y desencriptado rápidos en línea *a medida que se escriben o leen archivos*. Un canal especial del Secure Enclave proporciona el material de codificación necesario para el motor AES sin exponer esta información al procesador de aplicaciones (o CPU) o al sistema operativo en general. Esto ayuda a garantizar que la protección de datos de Apple y las tecnologías FileVault protejan los archivos de los usuarios sin exponer las claves de encriptación de larga duración.

Apple diseñó el arranque seguro para proteger los niveles más profundos del software contra la manipulación, y para permitir que sólo se cargue el software del sistema operativo de confianza de Apple durante el arranque. El arranque seguro comienza con el código inmutable llamado ROM de arranque, el cual se coloca durante la fabricación del SoC de Apple y se le conoce como la *raíz de confianza del hardware*. En computadoras Mac con el chip T2, la confianza del arranque seguro de macOS comienza con el chip T2 en sí (tanto el chip T2 como el Secure Enclave ejecutan sus propios procesos de arranque seguro utilizando sus propias ROM de arranque separadas; esto es un análogo exacto de cómo los chips de la serie A y la familia M1 arrancan de forma segura).

El Secure Enclave también procesa datos faciales y de huellas dactilares de los sensores de Face ID y Touch ID en los dispositivos Apple. Esto proporciona una autenticación segura a la vez que mantiene la privacidad y la seguridad de los datos biométricos del usuario. Esto también permite a los usuarios beneficiarse de la seguridad de contar con contraseñas más largas y complejas junto con la conveniencia de una autenticación instantánea al acceder o comprar.

Seguridad de los SoC de Apple

El silicio diseñado por Apple forma una arquitectura común en todos los productos de Apple e impulsa la Mac, así como los iPhone, iPad, Apple TV y Apple Watch. Por más de una década, el equipo de diseño del silicio de clase mundial de Apple ha estado construyendo y mejorando los sistemas en chip (SoC) de Apple. El resultado es una arquitectura escalable diseñada para todos los dispositivos que lidera la industria en funcionalidades de seguridad. Esta base común para las funciones de seguridad sólo es posible en una empresa que diseña su propio silicio para que funcione con su software.

El silicio de Apple está diseñado y fabricado específicamente con la finalidad de permitir las funcionalidades de seguridad descritas a continuación.

Funcionalidad	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Familia M1
Protección de la integridad del kernel	✓	✓	✓	✓	✓	✓
Restricciones rápidas de permisos		✓	✓	✓	✓	✓
Protección de la integridad del coprocesador del sistema			✓	✓	✓	✓
Códigos de autenticación con puntero			✓	✓	✓	✓
Capa de protección de página		✓	✓	✓	✓	Ver nota a continuación.

Nota: la capa de protección de página (PPL) requiere que la plataforma *sólo* ejecute código firmado y de confianza; este modelo de seguridad no aplica en macOS.

Los chips diseñados por Apple también habilitan específicamente las funcionalidades de protección de datos descritas a continuación.

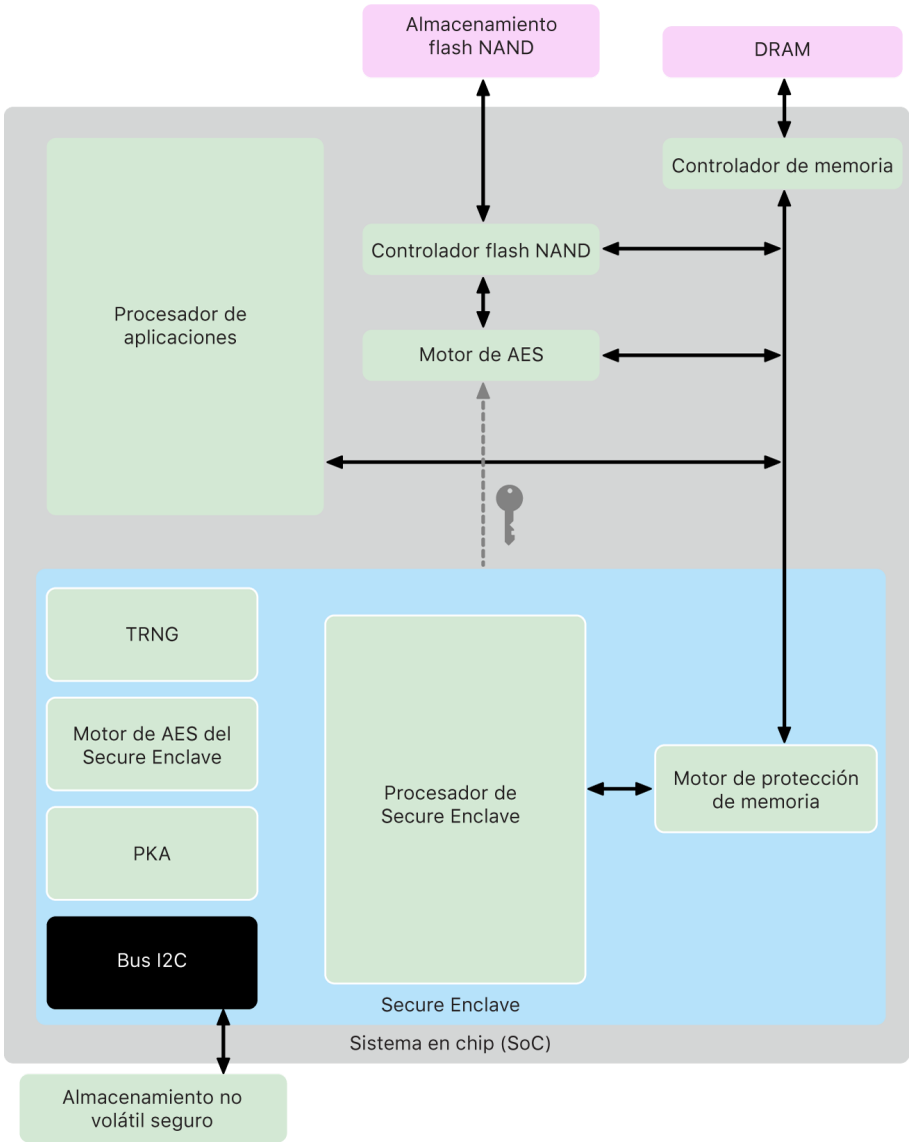
Funcionalidad	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, familia M1
Protección de claves selladas (SKP)	✓	✓	✓	✓	✓
recoveryOS: todas las clases de protección de datos están protegidas.	✓	✓	✓	✓	✓
Modos de arranque alternativos DFU, diagnóstico y actualización: las clases A, B y C están protegidas.			✓	✓	✓

Secure Enclave

El Secure Enclave es un subsistema seguro dedicado que está disponible en las versiones más recientes de iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch y HomePod.

Descripción general

El Secure Enclave es un subsistema seguro dedicado que está integrado en los sistemas en chip (SoC) de Apple. El Secure Enclave se encuentra aislado del procesador principal para brindar una capa adicional de seguridad, y está diseñado para mantener seguros los datos confidenciales del usuario incluso cuando se transgrede el kernel del procesador de aplicaciones. Sigue los mismos principios que el SoC: una ROM de arranque que establece una raíz de confianza del hardware, un motor AES para realizar operaciones criptográficas eficientes y seguras, y memoria protegida. Aunque el Secure Enclave no incluye almacenamiento, cuenta con un mecanismo que permite almacenar información de forma segura en un almacenamiento adjunto separado del almacenamiento flash NAND utilizado por el procesador de aplicaciones y el sistema operativo.



El Secure Enclave es una característica del hardware de la mayoría de las versiones de iPhone, iPad, Mac, Apple TV, Apple Watch y HomePod, en concreto:

- iPhone 5s o modelos posteriores
- iPad Air o modelos posteriores
- Computadoras MacBook Pro con Touch Bar (2016 y 2017) que cuentan con el chip T1 de Apple
- Computadoras Mac basadas en Intel que cuentan con el chip de seguridad T2 de Apple
- Computadoras Mac con Apple Chip
- Apple TV HD o modelos posteriores
- Apple Watch Series 1 o modelos posteriores
- HomePod y HomePod mini

Procesador Secure Enclave

El procesador Secure Enclave proporciona la potencia informática principal del Secure Enclave. Para proporcionar el aislamiento más potente, el procesador Secure Enclave se utiliza exclusivamente para el Secure Enclave. Esto ayuda a prevenir ataques de canal lateral que dependen de software malicioso que comparte el mismo núcleo de ejecución que el software que se ataca.

El procesador Secure Enclave ejecuta una versión personalizada de Apple del microkernel L4 y está diseñado para funcionar de manera eficiente a una velocidad de reloj más baja, lo que ayuda a protegerlo contra ataques de energía y reloj. El procesador Secure Enclave, a partir del A11 y el S4, incluye un motor de memoria protegida y una memoria encriptada con funcionalidades antirreproducción, arranque seguro, un generador de números aleatorios dedicado y su propio motor AES.

Motor de protección de memoria

El Secure Enclave opera desde una sección dedicada de la memoria DRAM del dispositivo. La memoria protegida del Secure Enclave se encuentra aislada del procesador de aplicaciones mediante varias capas de protección.

Cuando el dispositivo arranca, la ROM de arranque del Secure Enclave genera una clave de protección de memoria efímera y aleatoria para el motor de protección de memoria. Siempre que el Secure Enclave escribe en su sección de memoria dedicada, el motor de protección de memoria encripta el bloque de memoria usando AES en el modo XEX (xor-encrypt-xor) de la Mac y calcula una etiqueta de autenticación CMAC (código de autenticación de mensajes basado en encriptado) para la memoria. El motor de protección de memoria almacena una etiqueta de autenticación junto con la memoria encriptada. Cuando el Secure Enclave lee la memoria, el motor de protección de memoria verifica la etiqueta de autenticación. Si la etiqueta coincide, el motor de protección de memoria desencripta el bloque de memoria; si no coincide, el motor avisa de un error al Secure Enclave. Si ocurre un error de autenticación de memoria, el Secure Enclave deja de aceptar solicitudes hasta que el sistema se reinicie.

A partir de los SoC A11 y S4 de Apple, el motor de protección de memoria agrega protección de reproducción para la memoria del Secure Enclave. Para ayudar a evitar la reproducción de datos críticos para la seguridad, el motor de protección de memoria almacena un número único e irrepetible, llamado *valor único*, para el bloque de memoria junto con la etiqueta de autenticación. El valor único se utiliza como una modificación adicional para la etiqueta de autenticación de CMAC. Los valores únicos de todos los bloques de memoria están protegidos mediante un árbol de integridad establecido en una SRAM dedicada dentro del Secure Enclave. Para la escritura, el motor de protección de memoria *actualiza* el valor único y cada nivel del árbol de integridad hasta llegar a la SRAM. Para la lectura, el motor de protección de memoria *verifica* el valor único y cada nivel del árbol de integridad hasta llegar a la SRAM. Las discrepancias de los valores únicos se manejan de forma similar a las discrepancias de las etiquetas de autenticación.

En los SoC A14, A15, los de la familia M1 y modelos posteriores de Apple, el motor de protección de memoria admite dos claves de protección de memoria efímeras. La primera se usa para los datos privados a los que no accede el Secure Enclave, y la segunda es para los datos que se comparten con el motor neuronal seguro.

El motor de protección de memoria funciona de forma transparente y alineado con el Secure Enclave. El Secure Enclave lee y escribe en la memoria como si fuera una DRAM regular sin encriptar, mientras que un observador fuera del Secure Enclave sólo ve la versión encriptada y autenticada de la memoria. Esto ofrece una protección robusta de la memoria sin necesidad de afectar el rendimiento o aumentar la complejidad del software.

ROM de arranque del Secure Enclave

El Secure Enclave incluye una ROM de arranque dedicada para el Secure Enclave. Parecida a la ROM de arranque del procesador de aplicaciones, la ROM de arranque del Secure Enclave es un código inmutable que establece la ruta de confianza del hardware para el Secure Enclave.

Durante el arranque del sistema, iBoot asigna una región dedicada de la memoria para el Secure Enclave. Antes de usar la memoria, la ROM de arranque del Secure Enclave inicializa el motor de protección de memoria para ofrecer protección criptográfica a la memoria protegida del Secure Enclave.

Entonces, el procesador de aplicaciones envía la imagen sepOS a la ROM de arranque del Secure Enclave. Después de copiar la imagen sepOS en la memoria protegida del Secure Enclave, la ROM de arranque del Secure Enclave revisa el hash criptográfico y la firma de la imagen para verificar que el sepOS tenga autorización para ejecutarse en el dispositivo. Si la imagen sepOS cuenta con la firma adecuada para ejecutarse en el dispositivo, la ROM de arranque del Secure Enclave transfiere el control al sepOS. Si la firma no es válida, la ROM de arranque del Secure Enclave está diseñada para impedir cualquier uso posterior del Secure Enclave hasta el siguiente reinicio del chip.

En los SoC A10 y modelos posteriores de Apple, la ROM de arranque del Secure Enclave bloquea un hash del sepOS en un registro dedicado a este fin. El acelerador de claves públicas utiliza este hash para claves vinculadas al sistema operativo.

Monitor de arranque del Secure Enclave

En los SoC A13 y modelos posteriores de Apple, el Secure Enclave incluye un monitor de arranque diseñado para garantizar una integridad más sólida en el hash del sepOS arrancado.

Durante el arranque del sistema, la configuración de la protección de la integridad del coprocesador del sistema (SCIP) del procesador del Secure Enclave ayuda a evitar que este ejecute cualquier código que no sea la ROM de arranque del Secure Enclave. El monitor de arranque ayuda a evitar que el Secure Enclave modifique la configuración de SCIP directamente. Para hacer que el sepOS cargado sea ejecutable, la ROM de arranque del Secure Enclave envía al monitor de arranque una solicitud con la dirección y el tamaño del sepOS cargado. Al recibir la solicitud, el monitor de arranque restablece el procesador del Secure Enclave, aplica un hash al sepOS cargado, actualiza la configuración del SCIP para permitir la ejecución del sepOS cargado, e inicia la ejecución dentro del código recién cargado. A medida que el sistema arranca, este mismo proceso se utiliza cada vez que hay código nuevo disponible para ejecutarse. Cada vez, el monitor de arranque actualiza un hash en ejecución del proceso de arranque. El monitor de arranque también incluye parámetros de seguridad críticos en el hash en ejecución.

Cuando se completa el arranque, el monitor de arranque finaliza el hash en ejecución y lo envía al acelerador de claves públicas para usarlo con las claves vinculadas al sistema operativo. Este proceso está diseñado de tal forma que la vinculación de la clave al sistema operativo no se puede omitir incluso con una vulnerabilidad en la ROM de arranque del Secure Enclave.

Generador de números aleatorios verdaderos

El generador de números aleatorios verdaderos (TRNG) se usa para generar datos aleatorios seguros. El Secure Enclave usa el TRNG cada vez que genera una clave criptográfica aleatoria, una semilla aleatoria de clave u otra entropía. El TRNG se basa en varios osciladores de anillo posprocesados con CTR_DRBG (un algoritmo basado en encriptados de bloque en modo contador).

Claves criptográficas de raíz

El Secure Enclave incluye una clave criptográfica raíz de identificador único (UID). El UID es único para cada dispositivo y no está relacionado con ningún otro identificador de este.

Un UID generado de forma aleatoria se vincula al SoC al momento de su fabricación. A partir de los SoC A9, el TRNG del Secure Enclave genera el UID durante la fabricación y este se escribe en los fusibles mediante un proceso de software que se ejecuta completamente en el Secure Enclave. Este proceso protege el UID para que no sea visible fuera del dispositivo durante la fabricación y, por lo tanto, que no esté disponible para su acceso o almacenamiento por parte de Apple o de ninguno de sus proveedores.

El sepOS usa el UID para proteger secretos específicos del dispositivo. El UID permite vincular los datos a un dispositivo determinado mediante encriptación. Por ejemplo, la jerarquía de claves que protege el sistema de archivos incluye el UID, de modo que si el almacenamiento SSD interno se traslada físicamente de un dispositivo a otro, no será posible acceder a los archivos. Otros elementos secretos protegidos específicos del dispositivo incluyen los datos de Face ID o Touch ID. En una Mac, sólo el almacenamiento completamente interno vinculado al motor AES recibe este nivel de encriptado. Por ejemplo, ni los dispositivos de almacenamiento externo conectados mediante USB ni el almacenamiento basado en PCIe agregado a la Mac Pro (2019) se encriptan de esta manera.

El Secure Enclave también tiene un ID de grupo de dispositivos (GID) que es común a todos los dispositivos que usan un SoC determinado (por ejemplo, todos los dispositivos que usan el SoC A15 de Apple comparten el mismo GID).

Los UID y GID no están disponibles a través del grupo de acción de pruebas conjuntas (JTAG) u otras interfaces de depuración.

Motor AES del Secure Enclave

El motor AES del Secure Enclave es un bloque de hardware que se utiliza para realizar criptografía simétrica basada en el encriptado AES. Este motor está diseñado para resistir la fuga de información a través de la sincronización y el análisis de potencia estática (SPA). A partir del SoC A9, el motor AES también incluye medidas para contrarrestar el análisis dinámico de potencia (DPA).

El motor AES admite claves de hardware y software. Las claves de hardware derivan del UID o GID del Secure Enclave. Estas claves permanecen dentro del motor AES y no se hacen visibles ni siquiera para el software sepOS. Aunque el software puede solicitar operaciones de encriptado y desencriptado con claves de hardware, no puede extraer las claves.

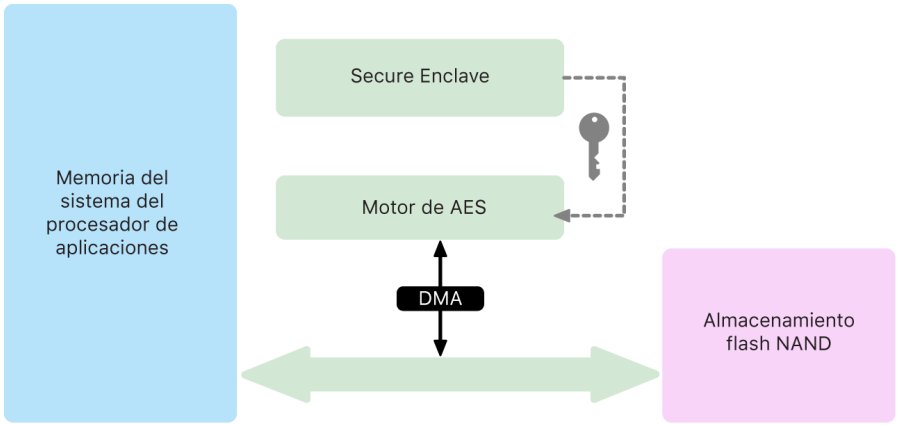
En los SoC A10 y modelos posteriores de Apple, el motor AES incluye bits semilla bloqueables que diversifican las claves derivadas del UID o GID. Esto permite que el acceso a los datos esté condicionado al modo de funcionamiento del dispositivo. Por ejemplo, los bits semilla bloqueables se usan para denegar el acceso a datos protegidos por contraseña cuando se arranca en el modo de actualización del firmware del dispositivo (DFU). Para obtener más información, consulta Códigos y contraseñas.

Motor AES

Todos los dispositivos Apple con Secure Enclave también cuentan con un motor criptográfico AES256 (el "motor AES") integrado directamente en la ruta de acceso directo a memoria (DMA), entre el almacenamiento flash NAND (no volátil) y la memoria del sistema principal. Esto permite conseguir una encriptación de archivos muy eficiente. En los procesadores A9 y modelos posteriores de la serie A, el subsistema de almacenamiento flash se encuentra en un bus aislado que sólo tiene acceso a la memoria que contiene los datos del usuario mediante el motor de encriptado DMA.

En el momento del arranque, sepOS genera una clave de encapsulación efímera usando el TRNG. El Secure Enclave transmite esta clave al motor AES mediante cables dedicados diseñados para evitar que cualquier software fuera del Secure Enclave acceda a ella. El sepOS puede usar la clave de encapsulado efímera para encapsular las claves de archivo para que las utilice el controlador del sistema de archivos del procesador de aplicaciones. Cuando el controlador del sistema de archivos lee o escribe un archivo, envía la clave encapsulada al motor AES, que desencapsula la clave. El motor AES nunca expone la clave desencapsulada al software.

Nota: el motor AES es un componente independiente del Secure Enclave y del motor AES del Secure Enclave, pero su funcionamiento está estrechamente vinculado al Secure Enclave, como se muestra a continuación.



Acelerador de claves públicas

El acelerador de claves públicas (PKA) es un bloque de hardware utilizado para realizar operaciones de criptografía asimétrica. El PKA admite algoritmos de encriptado y firma RSA y ECC (criptografía de curva elíptica). El PKA está diseñado para resistir la filtración de información a través de ataques de tiempo y de canal lateral como SPA y DPA.

El PKA admite claves de software y hardware. Las claves de hardware derivan del UID o GID del Secure Enclave. Estas claves permanecen dentro del PKA y no se hacen visibles ni siquiera para el software sepOS.

A partir de los SoC A13, se ha demostrado mediante técnicas de verificación formales que las implementaciones de encriptado de PKA son matemáticamente correctas.

En los SoC A10 y modelos posteriores de Apple, el PKA admite claves vinculadas al sistema operativo, a lo que se le conoce también como protección de claves selladas (SKP). Estas claves se generan mediante una combinación del UID del dispositivo y el hash del sepOS que se ejecuta en el dispositivo. El hash lo proporciona la ROM de arranque del Secure Enclave, o bien el monitor de arranque del Secure Enclave en el caso de los SoC A13 y modelos posteriores de Apple. Estas claves también se utilizan para verificar la versión del sepOS cuando se realizan solicitudes a algunos servicios de Apple, y también se utilizan para mejorar la seguridad de los datos protegidos con código al ayudar a prevenir el acceso al material de codificación si se realizan cambios críticos en el sistema sin la autorización del usuario.

Almacenamiento no volátil seguro

El Secure Enclave está equipado con un dispositivo de almacenamiento seguro no volátil dedicado. El almacenamiento seguro no volátil se conecta al Secure Enclave mediante un bus I2C dedicado, de modo que sólo el Secure Enclave puede acceder a él. Todas las claves de encriptado de datos de usuario tienen su raíz en la entropía almacenada en el almacenamiento no volátil del Secure Enclave.

En los dispositivos con los SoC A12, S4 y modelos posteriores de Apple, el Secure Enclave está enlazado con un componente de almacenamiento seguro para el almacenamiento de entropía. El componente de almacenamiento seguro está diseñado con un código de ROM inmutable, un generador de números aleatorios de hardware, una clave criptográfica única por dispositivo, motores de criptografía y detección de manipulación física. El Secure Enclave y el componente de almacenamiento seguro se comunican mediante un protocolo encriptado y autenticado que ofrece acceso exclusivo a la entropía.

Los dispositivos lanzados por primera vez en el otoño de 2020 y los modelos posteriores están equipados con un componente de almacenamiento seguro de segunda generación. Este componente agrega cajas de seguridad de conteo. Cada caja de seguridad de conteo almacena un valor de sal de 128 bits, un verificador de código de 128 bits, un contador de 8 bits y un valor máximo de intento de 8 bits. El acceso a las cajas de seguridad de conteo se realiza mediante un protocolo encriptado y autenticado.

Las cajas de seguridad de conteo contienen la entropía necesaria para desbloquear los datos de usuario protegidos con código. Para acceder a los datos del usuario, el Secure Enclave enlazado debe derivar el valor de entropía del código correcto a partir del código del usuario y el UID del Secure Enclave. El código del usuario no se puede obtener mediante los intentos de desbloqueo enviados desde una fuente que no sea el Secure Enclave enlazado. Si se excede el límite de intentos de ingreso de código (por ejemplo, 10 intentos en el iPhone), el componente de almacenamiento seguro borra por completo los datos protegidos con código.

Para crear una caja de seguridad de conteo, el Secure Enclave envía al componente de almacenamiento seguro el valor de entropía de código y el de intento máximo. El componente de almacenamiento seguro genera el valor de sal utilizando su generador de números aleatorios; después, deriva un valor de verificación de código y un valor de entropía de caja de seguridad a partir de la entropía de código proporcionada, la clave criptográfica única del componente de almacenamiento seguro y el valor de sal. El componente de almacenamiento seguro inicializa la caja de seguridad de conteo con un recuento de 0, el valor de intento máximo, el valor de verificación de código derivado y el valor de sal. El componente de almacenamiento seguro entonces devuelve el valor de entropía de caja de seguridad generado al Secure Enclave.

Para obtener posteriormente el valor de entropía de una caja de seguridad de conteo, el Secure Enclave envía la entropía de código al componente de almacenamiento seguro. El componente de almacenamiento seguro primero incrementa el contador de la caja de seguridad. Si el contador incrementado excede el valor de intentos máximo, el componente de almacenamiento seguro borra completamente la caja de seguridad de conteo. Si no se ha alcanzado el conteo de intentos máximo, el componente de almacenamiento seguro intenta derivar el valor de verificación de código y el valor de entropía de caja de seguridad con el mismo algoritmo utilizado para crear la caja de seguridad del conteo. Si el valor de verificación de código derivado coincide con el valor almacenado, el componente de almacenamiento seguro devuelve el valor de entropía de caja de seguridad al Secure Enclave y restablece el contador a 0.

Las claves que se utilizan para acceder a los datos protegidos con contraseña se basan en la entropía almacenada en las cajas de seguridad de conteo. Para obtener más información, consulta Descripción general de la protección de datos.

El almacenamiento seguro no volátil se utiliza para todos los servicios antirreproducción en el Secure Enclave. Los servicios antirreproducción en el Secure Enclave se utilizan para la revocación de datos sobre eventos que marcan los límites de la antirreproducción, entre los que se incluyen:

- Cambiar el código
- Activar o desactivar Face ID o Touch ID
- Agregar o eliminar una cara de Face ID o una huella de Touch ID
- Restablecer Face ID o Touch ID
- Agregar o eliminar una tarjeta de Apple Pay
- Borrar todo el contenido y la configuración

En arquitecturas que no cuentan con un componente de almacenamiento seguro, la EEPROM (memoria de sólo lectura programable y borrable eléctricamente) se utiliza para ofrecer servicios de almacenamiento seguro para el Secure Enclave. Al igual que los componentes de almacenamiento seguro, la EEPROM se adjunta y se puede acceder sólo desde el Secure Enclave, pero no contiene funcionalidades de seguridad de hardware dedicadas ni garantiza el acceso exclusivo a la entropía (aparte de sus características de conexión física) ni la funcionalidad de la caja de seguridad de conteo.

Motor neuronal seguro

En dispositivos con Face ID, el motor neuronal seguro convierte imágenes 2D y mapas de profundidad en representaciones matemáticas de la cara del usuario.

En los SoC del A11 al A13, el motor neuronal seguro se encuentra integrado en el Secure Enclave. El motor neuronal seguro utiliza acceso directo a memoria (DMA) para obtener un alto rendimiento. Una unidad de administración de memoria de entrada-salida (IOMMU) bajo el control del kernel del sepOS limita este acceso directo a las regiones de memoria autorizadas.

A partir del SoC A14 y la familia M1, el motor neuronal seguro se implementa como un modo seguro en el motor neuronal del procesador de aplicaciones. Un controlador de seguridad de hardware dedicado cambia entre el procesador de aplicaciones y las tareas del Secure Enclave, lo que restablece el estado del motor neuronal en cada transición para mantener seguros los datos de Face ID. Un motor dedicado aplica el encriptado, autenticación y control de acceso de la memoria. Al mismo tiempo, utiliza una clave criptográfica y un rango de memoria separados para limitar el motor neuronal seguro a las regiones de memoria autorizadas.

Monitores de energía y reloj

Todos los componentes electrónicos están diseñados para funcionar dentro de un voltaje y una envolvente de frecuencia limitados. Cuando se opera fuera de esta envolvente, los componentes electrónicos pueden fallar y luego podrían anularse los controles de seguridad. Para ayudar a garantizar que el voltaje y la frecuencia permanezcan en un intervalo seguro, el Secure Enclave está diseñado con circuitos de monitoreo. Estos circuitos están diseñados para tener una envolvente operativa mucho mayor que el resto del Secure Enclave. Si los monitores detectan un punto de funcionamiento ilegal, los relojes del Secure Enclave se detienen automáticamente y no se reinician hasta el próximo reinicio del SoC.

Resumen de funciones del Secure Enclave

Nota: los productos A12, A13, S4 y S5 lanzados por primera vez en el otoño de 2020 tienen un componente de almacenamiento seguro de segunda generación, mientras que los productos anteriores basados en estos SoC tienen un componente de almacenamiento seguro de primera generación.

SoC	Motor de protección de memoria	Almacenamiento seguro	Motor AES	PKA
A8	Encriptado y autenticación	EEPROM	Sí	No
A9	Encriptado y autenticación	EEPROM	Protección DPA	Sí
A10	Encriptado y autenticación	EEPROM	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo

SoC	Motor de protección de memoria	Almacenamiento seguro	Motor AES	PKA
A11	Encriptado, autenticación y prevención de reproducciones	EEPROM	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
A12 (dispositivos Apple lanzados antes del otoño de 2020)	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 1)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
A12 (dispositivos Apple lanzados después del otoño de 2020)	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 2)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
A13 (dispositivos Apple lanzados antes del otoño de 2020)	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 1)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque
A13 (dispositivos Apple lanzados después del otoño de 2020)	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 2)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque
A14, A15	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 2)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque
S3	Encriptado y autenticación	EEPROM	Protección DPA y bits semilla bloqueables	Sí
S4	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 1)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
S5 (dispositivos Apple lanzados antes del otoño de 2020)	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 1)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
S5 (dispositivos Apple lanzados después del otoño de 2020)	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 2)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
S6, S7	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 2)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
T2	Encriptado y autenticación	EEPROM	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
Familia M1	Encriptado, autenticación y prevención de reproducciones	Componente de almacenamiento seguro (generación 2)	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque

Face ID y Touch ID

Seguridad de Face ID y Touch ID

Los códigos y las contraseñas son elementos esenciales para la seguridad de los dispositivos Apple. Pero al mismo tiempo, los usuarios necesitan una forma de acceso a sus dispositivos conveniente, a menudo más de cien veces al día. La autenticación biométrica ofrece una forma de conservar la seguridad de tener un código —o incluso fortalecer el código o contraseña, ya que no requiere un ingreso manual— a la vez que proporciona la conveniencia de desbloquear el dispositivo con presionar con el dedo o mirarlo. Face ID and Touch ID no reemplazan el uso de un código o contraseña, pero en la mayoría de los casos, permite un acceso más rápido y sencillo.

La arquitectura de seguridad biométrica de Apple se basa en una estricta separación de responsabilidades entre el sensor biométrico y el Secure Enclave, y una conexión segura entre ambos. El sensor captura la imagen biométrica y la transmite de forma segura al Secure Enclave. Durante la inscripción, el Secure Enclave procesa, encripta y almacena los datos de plantilla de Face ID y Touch ID correspondientes. Durante la coincidencia, el Secure Enclave compara los datos entrantes del sensor biométrico con las plantillas almacenadas para determinar si debe desbloquear el dispositivo o responder que una coincidencia es válida (para Apple Pay, dentro de apps y otros usos de Face ID y Touch ID). La arquitectura admite dispositivos que incluyen tanto el sensor como el Secure Enclave (como iPhone, iPad y muchos sistemas Mac), así como la capacidad de separar físicamente el sensor en un periférico que luego se enlaza de forma segura con el Secure Enclave en una Mac con Apple Chip.

Seguridad de Face ID

Con una simple mirada, Face ID desbloquea de forma segura los dispositivos Apple compatibles. Esta tecnología proporciona autenticación intuitiva y segura mediante el sistema de la cámara TrueDepth, el cual utiliza tecnologías avanzadas para registrar con precisión la geometría de la cara del usuario. Face ID utiliza redes neuronales para determinar la atención, verificar la coincidencia e impedir los engaños para que el usuario pueda desbloquear su teléfono sólo con una mirada, incluso cuando se lleva cubrebocas si se usa un dispositivo compatible. Face ID se adapta automáticamente a los cambios en la apariencia y protege cuidadosamente la privacidad y seguridad de los datos biométricos del usuario.

Face ID está diseñado para confirmar la atención del usuario, proporcionar funciones avanzadas de autenticación con un bajo índice de errores de coincidencia y reducir el robo de identidad tanto físico como digital.

La cámara TrueDepth busca automáticamente la cara del usuario cuando activa su dispositivo Apple compatible con Face ID al levantarlo o tocar la pantalla, así como cuando el dispositivo intenta autenticar la identidad del usuario para mostrar una notificación o cuando las apps compatibles solicitan autenticación mediante Face ID. Cuando se detecta una cara, Face ID confirma la atención e intenta realizar el desbloqueo al detectar que los ojos del usuario están abiertos y dirigen su atención al dispositivo; para ofrecer mejor accesibilidad, la comprobación de atención de Face ID se desactiva cuando VoiceOver está activado y, opcionalmente, se puede desactivar por separado. Siempre que se usa Face ID con cubrebocas se requiere la detección de la atención.

Después de que la cámara TrueDepth confirma la presencia de una cara que pone atención al dispositivo, proyecta y lee miles de puntos infrarrojos para formar un mapa de profundidad de la cara, junto con una imagen infrarroja en 2D. Estos datos se usan para crear una secuencia de imágenes en 2D y mapas de profundidad, los cuales se firman digitalmente y envían al Secure Enclave. Para contrarrestar el robo de identidad tanto digital como físico, la cámara TrueDepth aleatoriza la secuencia de imágenes en 2D y el mapa de profundidad, y proyecta un patrón aleatorio específico del dispositivo. Parte del motor neuronal seguro, protegido dentro del Secure Enclave, trasforma estos datos en una representación matemática y la compara con los datos faciales registrados. Los datos faciales registrados son en sí una representación matemática de la cara del usuario capturada a través de varias poses.

Seguridad de Touch ID

Touch ID es el sistema de detección de huellas digitales que hace posible acceder a los dispositivos Apple compatibles de forma segura, rápida y sencilla. Esta tecnología lee los datos de huella digital desde cualquier ángulo y almacena continuamente más información sobre la huella del usuario, ya que el sensor amplía el mapa de huella digital con cada uso a medida que identifica más nodos superpuestos.

Los dispositivos Apple con sensor Touch ID se pueden desbloquear usando una huella digital. Touch ID no reemplaza la necesidad de que el dispositivo o el usuario tenga una contraseña, la cual se seguirá solicitando después de arrancar, reiniciar o cerrar sesión (en la Mac). En algunas apps, Touch ID también se puede utilizar en lugar del código del dispositivo o la contraseña del usuario, por ejemplo para desbloquear las notas protegidas con contraseña en la app Notas, para desbloquear los sitios web protegidos por el llavero, y para desbloquear las contraseñas de las apps compatibles. Sin embargo, algunos escenarios requerirán siempre el código del dispositivo o la contraseña de usuario (por ejemplo, para cambiar el código existente del dispositivo o la contraseña del usuario, o para crear o eliminar registros de huellas digitales).

Cuando un sensor de huella digital detecta el toque de un dedo, activa la matriz avanzada de imágenes para escanear el dedo y envía el escaneo al Secure Enclave. El canal utilizado para asegurar esta conexión varía, dependiendo de si el sensor Touch ID está integrado en el dispositivo con el Secure Enclave o si está ubicado en un periférico separado.

Mientras se vectoriza la imagen escaneada de la huella digital para su análisis, los datos ráster se almacenan temporalmente en la memoria encriptada dentro del Secure Enclave y luego se descartan. El análisis utiliza el mapeo de los ángulos del patrón de arrugas subdérmico, que es un proceso con pérdidas que descarta “datos detallados del dedo” que serían necesarios para reconstruir la huella real del usuario. Durante la inscripción, el mapa de nodos resultante se almacena en un formato encriptado que solamente el Secure Enclave puede leer como una plantilla para comparar con futuras coincidencias, pero sin ninguna información de identidad. Estos datos nunca salen de tu dispositivo. No se envían a Apple ni se incluyen en los respaldos del dispositivo.

Seguridad del canal integrado de Touch ID

La comunicación entre el Secure Enclave y el sensor Touch ID integrado se lleva a cabo a través de un bus de interfaz de periféricos en serie. El procesador envía los datos al Secure Enclave, pero este no puede leerlos, ya que se encuentran encriptados y autenticados mediante una clave de sesión que se negocia utilizando una clave compartida proporcionada de fábrica para cada sensor Touch ID y su Secure Enclave correspondiente. Para cada sensor Touch ID, la clave compartida es segura, aleatoria y diferente. En el intercambio de claves de sesión, se utiliza la encapsulación de claves AES y ambas partes proporcionan una clave aleatoria que establece la clave de sesión y que utiliza la encriptación de transporte que ofrece tanto autenticación como confidencialidad (mediante AES-CCM).

Magic Keyboard con Touch ID

El Magic Keyboard con Touch ID (y el Magic Keyboard con Touch ID y teclado numérico) incluye un sensor Touch ID en un teclado externo que puede utilizarse con cualquier Mac con Apple Chip. El Magic Keyboard con Touch ID cumple la función de sensor biométrico; no almacena plantillas biométricas, realiza coincidencias biométricas ni aplica políticas de seguridad (por ejemplo, tener que ingresar la contraseña después de 48 horas sin un desbloqueo). El sensor Touch ID del Magic Keyboard con Touch ID debe enlazarse de forma segura con el Secure Enclave de la Mac antes de que se pueda usar, para que después el Secure Enclave pueda realizar las operaciones de inscripción y coincidencia, y aplica las políticas de seguridad de la misma manera que lo haría para un sensor Touch ID integrado. Apple realiza el proceso de enlace desde la configuración de fábrica para los Magic Keyboard con Touch ID que se envían con una Mac. El usuario también puede realizar en elace en caso de ser necesario. Un Magic Keyboard con Touch ID se puede enlazar de forma segura solo con una Mac a la vez, pero una Mac puede mantener enlaces seguros con hasta cinco Magic Keyboard diferentes con Touch ID.

El Magic Keyboard con Touch ID y los sensores Touch ID integrados son compatibles. Si un dedo que se registró en un sensor Touch ID integrado en una Mac se coloca en el sensor de un Magic Keyboard con Touch ID, el Secure Enclave de la Mac procesa correctamente la coincidencia, y viceversa.

Para admitir el enlace seguro y, por lo tanto, la comunicación entre el Secure Enclave de la Mac y el Magic Keyboard con Touch ID, el teclado está equipado con un bloque de acelerador de clave pública (PKA) de hardware, que proporciona certificación, y con teclas físicas que permiten realizar los procesos criptográficos necesarios.

Enlace seguro

Antes de poder utilizar un Magic Keyboard con Touch ID para operaciones que requieren Touch ID, es necesario emparejarlo de forma segura con la Mac. Para esto, el Secure Enclave de la Mac y el bloque PKA del Magic Keyboard con Touch ID intercambian claves públicas, arraigadas en la CA de confianza de Apple, y utilizan claves de certificación en hardware y claves ECDH efímeras para certificar su identidad de forma segura. En la Mac, estos datos están protegidos por el Secure Enclave; mientras que en el Magic Keyboard con Touch ID, estos datos están protegidos por el bloque PKA. Después de realizar el enlace seguro, todos los datos de Touch ID comunicados entre la Mac y el Magic Keyboard con Touch ID se encriptan mediante AES-GCM, con una clave de 256 bits, y claves ECDH efímeras utilizando la curva NIST P-256 basada en las identidades almacenadas (el tecleo normal se transmite usando la seguridad de Bluetooth de la misma manera que lo hace cualquier teclado Bluetooth).

Intención segura para realizar enlaces

Para realizar algunas operaciones de Touch ID por primera vez, como registrar una nueva huella digital, el usuario debe confirmar físicamente su intención de usar un Magic Keyboard con Touch ID con la Mac. La intención física se confirma presionando dos veces el botón de encendido de la Mac cuando lo indique la interfaz de usuario, o cuando se realiza una coincidencia correcta de una huella digital que se haya registrado previamente en la Mac. Para obtener más información, consulta Intención segura y conexiones con el Secure Enclave.

Las transacciones de Apple Pay se pueden autorizar con una coincidencia de Touch ID o al ingresar la contraseña del usuario de macOS y presionar dos veces el botón Touch ID en el Magic Keyboard con Touch ID. Este último permite al usuario confirmar la intención física incluso sin una coincidencia de Touch ID.

Seguridad del canal del Magic Keyboard con Touch ID

Para ayudar a garantizar un canal de comunicación seguro entre el sensor Touch ID en el Magic Keyboard con Touch ID y el Secure Enclave en la Mac enlazada, se requiere lo siguiente:

- El enlace seguro entre el bloque PKA del Magic Keyboard con Touch ID y el Secure Enclave como se describe anteriormente
- Un canal seguro entre el Magic Keyboard con sensor Touch ID y su bloque PKA

El canal seguro entre el Magic Keyboard con sensor Touch ID y su bloque PKA se establece en la configuración de fábrica mediante el uso de una clave única compartida entre los dos (esta es la misma técnica utilizada para crear el canal seguro entre el Secure Enclave en la Mac y su sensor integrado, en computadoras Mac con Touch ID incorporado).

Face ID, Touch ID, códigos y contraseñas

Para usar Face ID o Touch ID, el usuario debe configurar su dispositivo para que se solicite un código o una contraseña al desbloquearlo. Cuando Face ID o Touch ID detectan una coincidencia, el dispositivo del usuario se desbloquea sin solicitar el código o la contraseña del dispositivo. De este modo, el usuario no tiene que ingresar el código o la contraseña muy a menudo y puede utilizar uno más largo y complejo. Face ID y Touch ID no reemplazan el código o la contraseña del usuario, sino que proporcionan acceso fácil al dispositivo dentro de unos límites y restricciones de tiempo razonables. Esto es importante, ya que los códigos o contraseñas seguras son la base de la protección criptográfica de los datos del usuario en dispositivos iPhone, iPad, Mac o Apple Watch.

Cuándo se solicita la contraseña o el código de un dispositivo

Los usuarios pueden usar sus códigos o contraseñas en cualquier momento en lugar de Face ID o Touch ID, pero hay situaciones en las que no se permiten las autenticaciones biométricas. Las siguientes operaciones siempre requieren que se ingrese una contraseña o código, por cuestiones de seguridad:

- Actualización del software
- Borrado del dispositivo
- Visualización y modificación de la configuración del código
- Instalación de perfiles de configuración
- Desbloqueo del panel Seguridad y privacidad de Preferencias del Sistema en la Mac
- Desbloqueo del panel Usuarios y grupos de Preferencias del Sistema en la Mac (si FileVault está activado)

También se requiere un código o contraseña si el dispositivo está en cualquiera de los siguientes estados:

- Cuando el dispositivo se acaba de encender o reiniciar.
- Cuando el usuario ha cerrado sesión en la cuenta de su Mac (o no ha iniciado sesión todavía).
- Cuando el usuario no ha desbloqueado su dispositivo por más de 48 horas.
- Cuando el usuario no ha usado su código o contraseña para desbloquear su dispositivo por 156 horas (seis días y medio), y no ha usado un método biométrico para desbloquearlo en 4 horas.
- Cuando el dispositivo ha recibido un comando de bloqueo remoto.
- Cuando el usuario sale de la pantalla de apagado/emergencia SOS al mantener presionado cualquiera de los botones de volumen y el de reposo/activación simultáneamente por 2 segundos y luego elige Cancelar.
- Cuando ha habido cinco intentos fallidos de coincidencia biométrica (aunque para facilitar el uso, el dispositivo podría ofrecer la posibilidad de ingresar una contraseña o código en lugar de usar los datos biométricos después de unos pocos intentos fallidos).

Cuando se activa Face ID con cubrebocas en un iPhone, está disponible por las siguientes 6.5 horas después de una de las siguientes acciones del usuario:

- Coincidencia correcta de Face ID (con o sin máscara)
- Validación del código del dispositivo
- Desbloqueo del dispositivo con el Apple Watch

La realización de cualquiera de esas acciones prolonga el periodo por 6.5 horas adicionales.

Cuando Face ID o Touch ID está activada en un iPhone o iPad, el dispositivo se bloquea inmediatamente cuando se presiona el botón de reposo/activación, y cada vez que el dispositivo entra en modo de reposo. Face ID y Touch ID requieren una coincidencia (o, de forma opcional, el uso del código) cada vez que se activa el dispositivo.

La probabilidad de que una persona al azar de la población pueda desbloquear el iPhone o el iPad de un usuario es inferior a 1 entre 1 000 000 con Face ID, incluso cuando Face ID con cubrebocas está activada. En el caso de un usuario de iPhone, iPad o Mac con Touch ID y dispositivos enlazados con un Magic Keyboard, es inferior a 1 en 50 000. Esta probabilidad aumenta cuando se registran varias huellas digitales (hasta 1 en 10 000 con cinco huellas) o caras (hasta 1 en 500 000 con dos caras). Como medida de protección adicional, tanto Face ID como Touch ID permiten sólo cinco intentos de coincidencia fallidos, y después será necesario ingresar el código o contraseña para obtener acceso a la cuenta o al dispositivo del usuario. Con Face ID, la probabilidad de una coincidencia incorrecta es mayor en los siguientes casos:

- gemelos o hermanos parecidos al usuario
- niños menores de 13 años (porque sus facciones distintivas aún no se han desarrollado por completo).

La probabilidad aumenta aún más en ambos casos cuando se usa Face ID con cubrebocas. Si a un usuario le preocupa una coincidencia incorrecta, Apple recomienda utilizar un código como forma de autenticación.

Seguridad de la coincidencia facial

La coincidencia facial se realiza dentro del Secure Enclave utilizando redes neuronales programadas específicamente para tal propósito. Apple desarrolló las redes neuronales de coincidencia facial utilizando más de mil millones de imágenes, incluyendo imágenes infrarrojas (IR) y de profundidad recopiladas en estudios realizados con el consentimiento informado de los participantes. Apple trabajó con participantes de todo el mundo para incluir un grupo de personas representativo, tomando en cuenta su género, edad, identidad étnica y otros factores. Se realizaron estudios adicionales según fuera necesario con la finalidad de ofrecer un alto grado de precisión a una gran diversidad de usuarios. Face ID está diseñado para funcionar con sombreros, bufandas, lentes, lentes de contacto y muchos tipos de lentes obscuros. A partir del iPhone 12 y iOS 15.4, Face ID también es compatible con el desbloqueo con cubrebocas. Además, está diseñado para funcionar en interiores, exteriores e incluso en total oscuridad. Una red neuronal adicional programada para detectar y rechazar intentos de robo de identidad impide el desbloqueo del dispositivo mediante fotos o máscaras. Los datos de Face ID, incluyendo las representaciones matemáticas de la cara del usuario, están encriptados y sólo el Secure Enclave puede acceder a ellos. Estos datos nunca salen de tu dispositivo. No se envían a Apple ni se incluyen en los respaldos del dispositivo. Los siguientes datos de Face ID se almacenan de forma encriptada para uso exclusivo del Secure Enclave durante el funcionamiento normal:

- Las representaciones matemáticas de la cara del usuario calculadas durante el registro.
- Las representaciones matemáticas de la cara del usuario calculadas durante algunos intentos de desbloqueo cuando Face ID las considera útiles para mejorar las futuras verificaciones de coincidencias.

Las imágenes faciales capturadas durante el uso normal no se guardan, sino que se desechan inmediatamente después de que se calcula la representación matemática, ya sea para el registro o para la comparación con los datos de Face ID registrados.

Mejorar la coincidencia de Face ID

Para mejorar el rendimiento del desbloqueo y mantenerse al día con los cambios naturales en una cara y apariencia, Face ID aumenta con el paso del tiempo las representaciones matemáticas que tiene almacenadas. Después de una coincidencia exitosa, Face ID puede usar las representaciones matemáticas recién calculadas —si su calidad es suficiente— para un número finito de coincidencias adicionales antes de descartar dichos datos. En cambio, si Face ID no logra reconocer una cara, pero la calidad de la coincidencia es mayor que un límite específico y el usuario ingresa su código inmediatamente después del intento fallido, Face ID toma otra captura y aumenta sus datos de Face ID registrados usando esa representación matemática recién calculada. Estos nuevos datos de Face ID se descartan si el usuario deja de coincidir con ellos o después de un número finito de coincidencias; los nuevos datos también se descartan cuando se selecciona la opción para restablecer Face ID. Estos procesos de aumento permiten a Face ID reconocer cambios considerables de vello facial o uso de maquillaje y, a la vez, minimizar falsos positivos.

Usos de Face ID y Touch ID

Desbloquear el dispositivo o la cuenta de un usuario

Si Face ID o Touch ID están desactivados, al momento en el que un dispositivo o cuenta se bloquea, se descartan las claves de la clase de protección de datos más alta, las cuales se almacenan en el Secure Enclave. No se podrá acceder a los archivos y elementos del llavero de dicha clase hasta que el usuario desbloquee el dispositivo o la cuenta con su código o contraseña.

Con Face ID o Touch ID activados, cuando se bloquea el dispositivo o la cuenta, no se descartan las claves, sino que se encapsulan con una clave que se proporciona al subsistema de Face ID o Touch ID en el Secure Enclave. Durante un intento de desbloqueo del dispositivo o de la cuenta, si el dispositivo encuentra una coincidencia, proporcionará la clave para desencapsular las claves de protección de datos, y el dispositivo o la cuenta se desbloquearán. Para desbloquear el dispositivo, el proceso proporciona protección adicional al solicitar la cooperación entre la protección de datos y los subsistemas de Face ID o Touch ID.

Cuando el dispositivo se reinicia, las claves requeridas para que Face ID o Touch ID desbloqueen el dispositivo o la cuenta se pierden, pues el Secure Enclave las descarta después de que se cumple alguna condición que requiera ingresar el código o la contraseña.

Seguridad de las compras con Apple Pay

El usuario también puede usar Face ID y Touch ID con Apple Pay para realizar compras de manera fácil y segura en tiendas, apps y en la web:

- *Mediante Face ID en tiendas:* para autorizar una compra dentro de una app con Face ID, el usuario primero debe presionar el botón lateral dos veces para confirmar que quiere realizar el pago. Esta presión doble captura la intención del usuario usando un gesto físico directamente relacionado con el Secure Enclave y es resistente a la falsificación por un proceso malicioso. A continuación, el usuario debe autenticarse usando Face ID antes de colocar el dispositivo cerca del lector de tarjetas sin contacto. Después de autenticarse con Face ID en Apple Pay, el usuario puede seleccionar un método distinto de pago; esto requerirá volver a autenticarse, pero el usuario no tendrá que volver a presionar dos veces el botón lateral.
- *Mediante Face ID en apps y en la web:* para realizar un pago dentro de las apps y en Internet, el usuario debe presionar dos veces el botón lateral para confirmar su intención de pagar y debe autenticarse usando Face ID para autorizar el pago. Si la transacción de Apple Pay no se ha completado 60 segundos después de presionar dos veces el botón lateral, el usuario tendrá que volver a presionarlo dos veces para volver a confirmar que quiere realizar el pago.
- *Mediante Touch ID:* en el caso de Touch ID, la intención de pagar se confirma usando el gesto de activación del sensor de Touch ID combinado con la coincidencia exitosa de la huella del usuario.

Usar API proporcionadas por el sistema

Las apps de terceros pueden usar las API proporcionadas por el sistema para solicitar al usuario que se autentique utilizando Face ID o Touch ID, un código o una contraseña. Además, las apps compatibles con Touch ID automáticamente admiten Face ID sin necesidad de modificaciones. Cuando se usa Face ID o Touch ID, a la app sólo se le informa si la autenticación se realizó correctamente o no, pero no se le proporciona acceso a Face ID, Touch ID o los datos asociados con el registro del usuario.

Protección de los elementos del llavero

Los elementos del llavero también se pueden proteger con Face ID o Touch ID, de modo que el Secure Enclave sólo los pueda desbloquear cuando hay una coincidencia correcta o mediante el código del dispositivo o la contraseña de la cuenta. Los desarrolladores de apps tienen API a su disposición para verificar que el usuario ha establecido un código o una contraseña antes de requerir Face ID, Touch ID, un código o una contraseña para desbloquear los elementos del llavero. Los desarrolladores de apps pueden hacer lo siguiente:

- Requerir que las operaciones API de autenticación no recurran a las alternativas de utilizar la contraseña de una app o el código del dispositivo. Consultar si un usuario está registrado, lo que permite que se utilice Face ID o Touch ID como un segundo factor en apps en las que la seguridad es muy importante.
- Generar o usar claves de criptografía de curva elíptica (ECC) dentro del Secure Enclave que pueden protegerse mediante Face ID o Touch ID. Las operaciones que usan estas claves siempre se realizan dentro del Secure Enclave después de que se autoriza su uso.

Realizar y aprobar compras

Los usuarios también pueden configurar Face ID o Touch ID para aprobar compras de iTunes Store, App Store, Apple Books y más, de modo que no tengan que ingresar su contraseña del Apple ID. Cuando se realizan compras, el Secure Enclave verifica que se haya producido una autorización biométrica y luego libera las claves ECC utilizadas para firmar la solicitud de la tienda.

Intención segura y conexiones con el Secure Enclave

La intención segura proporciona una forma de confirmar la intención de un usuario sin ninguna interacción con el sistema operativo o el procesador de aplicaciones. La conexión es un enlace físico, desde un botón físico hasta el Secure Enclave, que está disponible en los siguientes dispositivos:

- iPhone X o modelos posteriores
- Apple Watch Series 1 o modelos posteriores
- iPad Pro (todos los modelos)
- iPad Air (2020)
- Computadoras Mac con Apple Chip

Con este enlace, los usuarios pueden confirmar su intención de completar una operación de una manera diseñada de tal forma que ni el software que se ejecuta con privilegios de root o dentro del kernel pueda falsificarla.

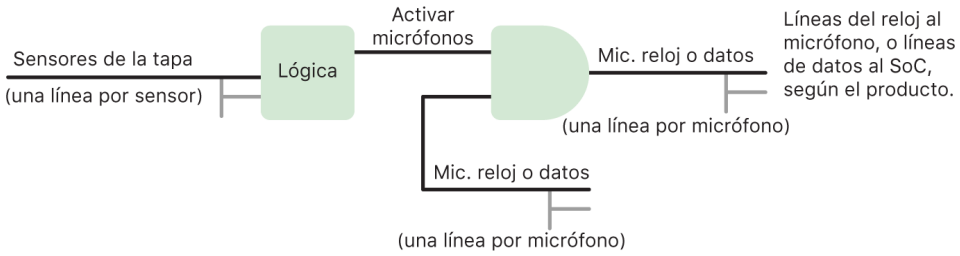
Esta función se utiliza para confirmar la intención del usuario durante las transacciones de Apple Pay y al finalizar el enlace del Magic Keyboard con Touch ID a una Mac con Apple Chip. La intención del usuario se confirma mediante una presión doble en el botón correspondiente (en el caso de Face ID) o mediante la lectura de la huella digital (en el caso de Touch ID) que debe llevarse a cabo cuando la interfaz lo solicite. Para obtener más información, consulta Seguridad de las compras con Apple Pay. Un mecanismo similar, basado en el firmware del chip T2 y del Secure Enclave, es compatible con los modelos de MacBook con el chip de seguridad T2 de Apple que no tienen Touch Bar.

Desconexión del micrófono de hardware

Todas las computadoras portátiles Mac con Apple Chip o basadas en Intel que cuentan con el chip de seguridad T2 de Apple tienen la función de desconexión de hardware que desconecta el micrófono cada vez que se cierra la pantalla. En las computadoras MacBook Air y MacBook Pro de 13 pulgadas que tienen el chip T2, las computadoras portátiles MacBook con el chip T2 lanzadas en 2019 y modelos posteriores, y las computadoras portátiles Mac con Apple Chip, esta desconexión se implementa sólo en el hardware y está diseñada para evitar que cualquier software (incluso el que tenga privilegios de acceso a la raíz o al kernel en macOS, el software del chip T2, u otro firmware) manipule el micrófono cuando la pantalla está cerrada (la cámara no se desconecta del hardware, debido a que su campo de visión está completamente obstruido cuando se cierra la cubierta).

Los modelos de iPad a partir de 2020 también incluyen la posibilidad de desconectar el micrófono de hardware. Cuando se utiliza una funda compatible con MFi (incluidas las vendidas por Apple) con el iPad y esta se cierra, se desconecta el micrófono. Esto está diseñado para evitar que los datos de audio del micrófono estén disponibles para cualquier software, incluso con privilegios de raíz o kernel en iPadOS o cualquier firmware de dispositivo.

Las protecciones de este apartado se implementan directamente con la lógica del hardware, según el siguiente esquema:



En cada producto con corte de micrófono de hardware, uno o más sensores de la tapa detectan el cierre físico de la tapa o estuche usando alguna propiedad física (por ejemplo, un sensor de efecto Hall o de ángulo de bisagra) de la interacción. Para los sensores que requieren calibración, los parámetros se establecen durante la producción del dispositivo, y el proceso de calibración incluye un bloqueo de hardware no reversible que impide cualquier cambio posterior a los parámetros del sensor. Estos sensores emiten una señal de hardware directa que pasa a través de un conjunto simple de lógica de hardware no reprogramable. Esta lógica proporciona funciones de antirrebote, histéresis o una demora de hasta 500 ms antes de desactivar el micrófono. Dependiendo del producto, esta señal se puede implementar al desactivar las líneas que transportan datos entre el micrófono y el SoC, o bien al deshabilitar una de las líneas de entrada al módulo del micrófono que le permiten estar activo; por ejemplo, la línea del reloj o un control similar.

Tarjetas express con reserva de energía

Incluso cuando iOS no se está ejecutando porque la batería del iPhone necesita cargarse, es probable que aún haya carga suficiente para realizar transacciones con tarjetas express. Los dispositivos iPhone compatibles permiten automáticamente esta función con lo siguiente:

- Una tarjeta de transporte público o pago designada como tarjeta de transporte público express
- Las tarjetas de identificación de estudiantes con el modo express activado
- Llaves de auto con el modo express
- Llaves de casa con el modo express
- Tarjetas de acceso de empresas corporativas y del sector turístico con el modo express activado

Al presionar el botón lateral (o, en iPhone SE de segunda generación, el botón de inicio), se muestra el ícono de batería baja así como un mensaje que indica que hay tarjetas express disponibles para su uso. El controlador NFC realiza transacciones con tarjetas express bajo las mismas condiciones que cuando iOS se está ejecutando, excepto que las transacciones se indican sólo con una notificación de vibración (no se muestra una notificación visible). En iPhone SE (segunda generación), las transacciones completadas podrían tardar unos segundos en aparecer en la pantalla. Esta función no está disponible cuando el usuario apaga el dispositivo manualmente.

Seguridad del sistema

Descripción general de seguridad del sistema

Sumándose a las capacidades únicas del hardware de Apple, la seguridad del sistema es responsable de controlar el acceso a los recursos del sistema en dispositivos Apple sin afectar su usabilidad. La seguridad del sistema abarca el proceso de arranque, las actualizaciones de software y la protección de los recursos del sistema computacional, como CPU, memoria, discos, programas de software y datos almacenados.

Las versiones más recientes de los sistemas operativos de Apple son las más seguras. Una parte importante de la seguridad de Apple es el *arranque seguro*, que protege el sistema de infecciones de malware durante el arranque. El arranque seguro comienza en el hardware y construye una cadena de confianza a lo largo del software, en donde cada paso está diseñado para asegurarse de que el siguiente funcione adecuadamente antes de entregar el control. Este modelo de seguridad, además de ser la base para el arranque predeterminado de los dispositivos Apple, es la base para los diversos modos de recuperación y actualización oportuna de los dispositivos Apple. Los subcomponentes como el chip T2 y el Secure Enclave también realizan su propio arranque seguro para ayudar a garantizar que sólo se arranque código que Apple ya considera como de confianza. El sistema de actualización está diseñado para ayudar a prevenir ataques de regresión, por lo que los dispositivos no pueden regresar a versiones anteriores del sistema operativo (que los atacantes saben cómo vulnerar) para robar los datos del usuario.

Los dispositivos Apple también incluyen protecciones de arranque y de tiempo de ejecución que mantienen su integridad durante el funcionamiento continuo. Los chips diseñados por Apple para iPhone, iPad, Apple Watch, Apple TV, HomePod y computadoras Mac con Apple Chips proporcionan una arquitectura común para proteger la integridad del sistema operativo. macOS también incluye un conjunto ampliado y configurable de funcionalidades de protección que apoyan su modelo informático distintivo, así como funciones compatibles con todas las plataformas del hardware de las Mac.

Arranque seguro

Proceso de arranque para dispositivos iOS y iPadOS

Todos los pasos del proceso de arranque contienen componentes firmados criptográficamente por Apple que permiten revisar la integridad con el fin de llevar a cabo el arranque únicamente después de haber verificado la cadena de confianza. Estos componentes incluyen los gestores de arranque, el kernel, las extensiones del kernel y el firmware de banda base celular. Esta cadena de arranque seguro está diseñada para verificar que no se manipulen los niveles más profundos del software.

Cuando se enciende un dispositivo iOS o iPadOS, su procesador de aplicaciones ejecuta inmediatamente el código de la memoria de sólo lectura (conocido como ROM de arranque). Este código inmutable, también conocido como *raíz de confianza de hardware*, se establece durante la fabricación del chip y, de forma implícita, es de confianza. El código de la memoria ROM de arranque contiene la clave pública de la autoridad de certificación (CA) raíz de Apple, que se utiliza para verificar que los gestores de arranque iBoot tengan la firma de Apple antes de permitir que se carguen. Este es el primer paso de la cadena de confianza, en la que cada paso verifica que el siguiente esté firmado por Apple. Cuando el iBoot termina sus operaciones, verifica y ejecuta el kernel de iOS o iPadOS. Para dispositivos con un procesador A9 o modelos anteriores de la serie A, existe un gestor de arranque de bajo nivel (LLB) adicional que se carga y verifica con la ROM de arranque, que a su vez carga y verifica iBoot.

Los intentos fallidos de carga o verificación de las siguientes fases se manejan de formas distintas según el hardware:

- *La ROM de arranque no puede cargar los gestores de arranque de bajo nivel (LLB) (dispositivos antiguos):* modo de actualización del firmware del dispositivo (DFU)
- *LLB o iBoot:* modo de recuperación

En cualquier caso, el dispositivo debe estar conectado al Finder (macOS 10.15 o versiones posteriores) o a iTunes (macOS 10.14 o versiones anteriores) mediante USB y restaurado a la configuración predeterminada de fábrica.

El Secure Enclave utiliza el registro del proceso de arranque (BPR) para limitar el acceso a los datos del usuario en diferentes modos y este se actualiza antes de ingresar a los siguientes modos:

- *Modo de actualización del firmware del dispositivo (DFU):* establecido por la ROM de arranque en dispositivos con el SoC A12 de Apple o modelos posteriores.
- *Modo de recuperación:* establecido por iBoot en dispositivos con los SoC A10 y S2 de Apple o modelos posteriores.

En el caso de los dispositivos que disponen de acceso a datos celulares, el subsistema realiza un proceso de arranque seguro adicional con software firmado y claves verificadas por el procesador de banda base celular.

El Secure Enclave también realiza un arranque seguro que verifica que su propio software (sepOS) cuente con la verificación y firma de Apple.

Implementación de iBoot de forma segura para la memoria

En iOS 14 y iPadOS 14, Apple modificó la cadena de herramientas del compilador C utilizado para construir el gestor de arranque iBoot y mejorar su seguridad. La cadena de herramientas modificada implementa código diseñado para evitar problemas relacionados con la memoria y el tipo de seguridad que se presentan comúnmente en los programas C. Por ejemplo, ayuda a impedir la mayoría de las vulnerabilidades en las siguientes clases:

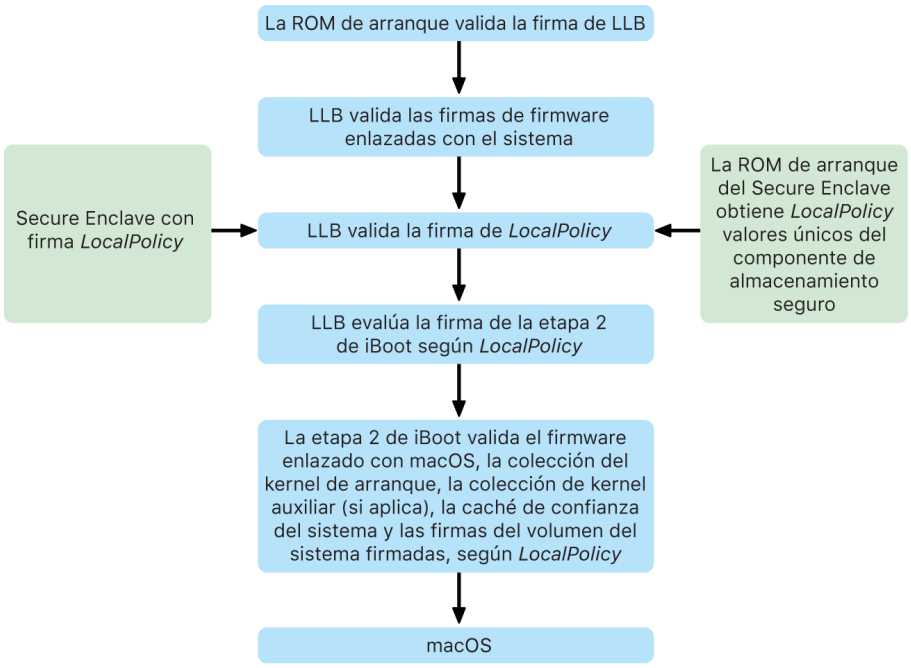
- Desbordamientos del búfer, al asegurarse de que todos los punteros lleven información enlazada que se verifica al acceder a la memoria.
- Explotación de captura, al separar los datos de captura de sus metadatos y detectar de forma precisa condiciones de error como errores de corrupción.
- Confusión de tipo, al garantizar que todos los punteros lleven información de tipo de arranque que se verifica durante las operaciones de cast de los punteros.
- Confusión de tipo, causada por errores del tipo use-after-free, al segregar todas las asignaciones de memoria dinámica por tipo estático.

Esta tecnología está disponible en iPhone con el chip A13 Bionic de Apple o modelos posteriores, y en iPad con el chip A14 Bionic.

Computadoras Mac con Apple Chip

Proceso de arranque en una Mac con Apple Chip

Al encender una computadora Mac con Apple Chip, se realiza un proceso de arranque muy similar al de un iPhone o iPad.



El chip ejecuta código desde la ROM de arranque en el primer paso de la cadena de confianza. El arranque seguro de macOS en una Mac con Apple Chip verifica no sólo el código del sistema operativo en sí, sino también las políticas de seguridad e incluso las kexts (lo cual es compatible, aunque no se recomienda) configuradas por usuarios autorizados.

Cuando se ejecuta el gestor de arranque de bajo nivel (LLB), este verifica las firmas y carga firmware vinculado con el sistema para núcleos intra-SoC, como el almacenamiento, la pantalla, la administración del sistema y los controladores Thunderbolt. El LLB también es responsable de cargar LocalPolicy, que es un archivo firmado por el procesador Secure Enclave. El archivo LocalPolicy describe la configuración que el usuario seleccionó para las políticas de seguridad de ejecución y arranque del sistema. LocalPolicy tiene el mismo formato de estructura de datos que los demás objetos de arranque, pero está firmado de forma local mediante una clave privada, la cual está disponible sólo dentro del Secure Enclave de una computadora en particular, en lugar de estar firmado por un servidor central de Apple (tal como en las actualizaciones de software).

Para ayudar a evitar la reproducción de cualquier LocalPolicy anterior, LLB debe buscar un valor único en el componente de almacenamiento seguro adjunto al Secure Enclave. Para hacer esto, utiliza la ROM de arranque del Secure Enclave y se asegura de que el valor único en el archivo LocalPolicy coincida con el valor único del componente de almacenamiento seguro. Esto ayuda a evitar que se le vuelva a aplicar al sistema un LocalPolicy anterior, que podría tener una configuración de seguridad menor, después de que se ha actualizado la seguridad. El resultado es que el arranque seguro en una Mac con Apple Chip ayuda a proteger no sólo contra el retroceso a versiones del sistema operativo anteriores, sino también contra la reducción de la política de seguridad.

El archivo LocalPolicy captura si el sistema operativo está configurado para seguridad máxima, reducida o permisiva.

- *Máxima seguridad:* el sistema se comporta como iOS y iPadOS, y durante el arranque sólo permite software que tenga la versión más reciente que estaba disponible al momento de la instalación.
- *Seguridad reducida:* LLB recibe la instrucción de confiar en firmas "globales" que se incluyen con el sistema operativo. Esto permite al sistema ejecutar versiones anteriores de macOS. Debido a que las versiones anteriores de macOS inevitablemente tienen vulnerabilidades sin parches, este modo de seguridad se describe como *Seguridad reducida*. Este es también el nivel de política necesario para admitir el arranque de extensiones del kernel (kexts).
- *Seguridad permisiva:* el sistema se comporta del mismo modo que Seguridad reducida, en el sentido de que usa la verificación de firmas global para iBoot y más, pero también le indica a iBoot que debe aceptar algunos objetos de arranque firmados por el Secure Enclave con la misma clave usada para firmar LocalPolicy. Este nivel de política admite que los usuarios creen, firmen y arranquen sus propios kernels XNU personalizados.

Si LocalPolicy le indica a LLB que el sistema operativo seleccionado se está ejecutando en Máxima seguridad, LLB evalúa la firma personalizada para iBoot; y si se ejecuta en seguridad reducida o permisiva, evalúa la firma global. Cualquier error de verificación de firma ocasionará que el sistema se inicie en recoveryOS para ofrecer opciones de reparación.

Después de que se pasa de LLB a iBoot, se carga el firmware vinculado con macOS, como el del motor neural seguro, el procesador siempre activo y otros. iBoot también analiza la información sobre LocalPolicy que le entrega LLB. Si LocalPolicy indica que debe existir una colección del kernel auxiliar (AuxKC), iBoot la busca en el sistema de archivos, verifica que esté firmada por el Secure Enclave mediante la misma clave que LocalPolicy y comprueba que su hash coincida con un hash almacenado en el archivo LocalPolicy. Si se verifica la AuxKC, iBoot la coloca en la memoria junto con la colección del kernel de arranque, antes de bloquear la región completa de la memoria que cubre la colección del kernel de arranque y la AuxKC con la protección de la integridad del coprocesador del sistema (SCIP). Si la política indica que debería haber una AuxKC presente pero no se encuentra, el sistema continúa arrancando en macOS sin ella. iBoot también es responsable de verificar el hash de raíz para el volumen del sistema firmado (SSV) con la finalidad de revisar que el sistema de archivos que montará el kernel tenga una integridad completa verificada.

Modos de arranque en una Mac con Apple Chip

Una Mac con Apple Chip tiene los modos de arranque descritos a continuación.

Modo	Combinación de teclas	Descripción
macOS	Desde el estado de apagado, presiona y **suelta** el botón de encendido.	1. La ROM de arranque entrega a LLB. 2. LLB carga el firmware vinculado con el sistema y el archivo LocalPolicy para el macOS seleccionado. 3. LLB bloquea en el registro del proceso de arranque (BPR) una indicación para señalar que se está arrancando en macOS, y le entrega el proceso a iBoot. 4. iBoot carga el firmware vinculado con macOS, la caché de confianza estática, el árbol de dispositivos y la colección del kernel de arranque. 5. Si LocalPolicy lo permite, iBoot carga la colección del kernel auxiliar (AuxKC) de las kexts de terceros. 6. Si LocalPolicy no lo desactiva, iBoot verifica el hash de la firma raíz para el volumen de sistema firmado (SSV).
recoveryOS vinculado	Desde el estado de apagado, **mantén presionado** el botón de encendido.	1. La ROM de arranque entrega a LLB. 2. LLB carga el firmware vinculado con el sistema y el archivo LocalPolicy para recoveryOS. 3. LLB bloquea en el registro del proceso de arranque una indicación para señalar que se está arrancando en recoveryOS vinculado, y le entrega el proceso a i Boot para recoveryOS vinculado. 4. iBoot carga el firmware vinculado con macOS, la caché de confianza, el árbol de dispositivos y la colección del kernel de arranque. 5. Si el arranque del recoveryOS vinculado falla, se intenta arrancar en el recoveryOS de respaldo. *Nota:* no se permite reducir la seguridad de la política local, LocalPolicy, del volumen recoveryOS vinculado.
recoveryOS de respaldo	Desde el estado de apagado, **presiona dos veces y mantén presionado** el botón de encendido.	1. La ROM de arranque entrega a LLB. 2. LLB carga el firmware vinculado con el sistema y el archivo LocalPolicy para recoveryOS. 3. LLB bloquea en el registro del proceso de arranque una indicación para señalar que se está arrancando en recoveryOS vinculado, y le entrega el proceso a i Boot para recoveryOS. 4. iBoot carga el firmware vinculado con macOS, la caché de confianza, el árbol de dispositivos y la colección del kernel de arranque. *Nota:* no se permite reducir la seguridad de la política local, LocalPolicy, del volumen recoveryOS vinculado.
Modo seguro	Arranca en recoveryOS como se indica anteriormente y luego mantén presionada la tecla **Mayúsculas** mientras seleccionas el volumen de arranque.	1. Arranca en recoveryOS como se indica anteriormente. 2. Mantener presionada la tecla Mayúsculas mientras se selecciona un volumen hace que la app Boot Picker apruebe macOS para el arranque, como de costumbre, y establece una variable `nvram` que le indica a iBoot que no cargue la AuxKC en el próximo arranque. 3. El sistema se reinicia y arranca en el volumen de destino, pero iBoot no carga la AuxKC.

Restricciones de recoveryOS vinculado

En macOS 12.0.1 o versiones posteriores, cada nueva instalación de macOS también instala una versión vinculada de recoveryOS en el grupo de volúmenes APFS correspondiente. Este diseño es familiar para los usuarios de computadoras Mac basadas en Intel, pero en una Mac con Apple Chip esto proporciona garantías adicionales de seguridad y compatibilidad. Como cada instalación de macOS tiene ahora un volumen de recoveryOS vinculado y dedicado, esto ayuda a garantizar que sólo ese volumen de recoveryOS vinculado y dedicado pueda realizar operaciones relacionadas con la actualización de la seguridad. Esto ayuda a proteger las instalaciones de las versiones más nuevas de macOS de las manipulaciones iniciadas desde versiones más antiguas de macOS, y viceversa.

Las restricciones de vinculación se aplican de la siguiente manera:

- Todas las instalaciones de macOS 11 están vinculadas con el volumen de recoveryOS. Si se selecciona una instalación de macOS 11 para arrancar de forma predeterminada, para arrancar su volumen de recoveryOS se debe mantener presionada la tecla de encendido en el momento del arranque en una Mac con Apple Chip. El volumen de recoveryOS puede degradar la configuración de seguridad de cualquier instalación de macOS 11, pero no de una instalación de macOS 12.0.1.
- Si se selecciona una instalación de macOS 12.0.1 o versiones posteriores para arrancar de forma predeterminada, para arrancar su volumen de recoveryOS vinculado se debe mantener presionada la tecla de encendido cuando la Mac arranca. El volumen de recoveryOS vinculado puede degradar la configuración de seguridad de la instalación de macOS vinculada, pero no de cualquier otra instalación de macOS.

Para arrancar en un volumen de recoveryOS vinculado con cualquier instalación de macOS, es necesario seleccionar esa instalación como predeterminada, lo cual se puede hacer desde el panel Disco de arranque de Preferencias del Sistema, o iniciando cualquier volumen de recoveryOS y manteniendo presionada la tecla Opción mientras se selecciona un volumen.

Nota: el volumen de recoveryOS de respaldo no puede degradar ninguna instalación de macOS.

Control de la política de seguridad del disco de arranque para una computadora Mac con Apple Chip

Descripción general

A diferencia de las políticas de seguridad de una computadora Mac basadas en Intel, las de una Mac con Apple Chip son para cada sistema operativo instalado. Esto significa que se admiten varias instancias de macOS instaladas con diferentes versiones y políticas de seguridad en una misma Mac. Por este motivo, se agregó un *selector de sistema operativo* en Utilidad de Seguridad de Arranque.

En una computadora Mac con Apple Chip, Utilidad de Seguridad del Sistema indica el estado de seguridad general configurado por el usuario de macOS, tal como la ejecución de un kext o la configuración de la protección de la integridad del sistema (SIP). Si el cambio de una configuración de seguridad reduce significativamente la seguridad o la haría más fácil de transgredir, para hacer el cambio el usuario deberá entrar en el modo recoveryOS manteniendo presionado el botón de encendido (de forma que el malware no pueda activar la señal, sino sólo una persona con acceso físico). Debido a esto, una Mac basada en Apple Chip tampoco requerirá (ni será compatible con) una contraseña de firmware, ya que todos los cambios críticos se acreditan mediante la autorización del usuario. Para obtener más información sobre la SIP, consulta Protección de la integridad del sistema.

Las seguridades máxima y reducida se pueden configurar mediante la app Utilidad de Seguridad de Arranque en recoveryOS. Sin embargo, la seguridad permisiva se puede acceder sólo desde las herramientas de línea de comandos para los usuarios que aceptan el riesgo de hacer que su Mac sea mucho menos segura.

Política de máxima seguridad

La opción predeterminada es Máxima seguridad, y se comporta como iOS y iPadOS. En el momento en que se descarga el software y se prepara para su instalación, en lugar de usar la firma global que viene con el software, macOS se comunica con el mismo servidor de firma de Apple que se utiliza para iOS y iPadOS, y solicita una firma reciente "personalizada". Una firma es personalizada cuando incluye el identificador de chip exclusivo (ECID), un ID único específico para el CPU de Apple en este caso, como parte de la solicitud de firma. La firma devuelta por el servidor de firma es entonces única y sólo la puede usar ese CPU de Apple en particular. Cuando la política de máxima seguridad está en vigor, la ROM de arranque y LLB ayudan a garantizar que una firma específica no esté firmada sólo por Apple, sino por esta Mac específica; lo que en esencia vincula esa versión de macOS a esa Mac.

Usar un servidor de firma en línea también brinda una mejor protección contra los ataques de retroceso que los métodos de firma global típicos. En un sistema de firma global, el epoch de seguridad pudo haberse retrocedido muchas veces, pero un sistema que nunca ha visto el último firmware no lo sabe. Por ejemplo, una computadora que cree actualmente que está en el epoch de seguridad 1, acepta software del epoch de seguridad 2, aunque el epoch actual de seguridad sea el 5. Con el sistema de firma en línea de Apple Chip, el servidor de firmas puede rechazar crear firmas para software que estén en cualquier epoch de seguridad que no sea el más reciente.

Además, si un atacante descubre una vulnerabilidad después de un cambio de epoch de seguridad, no puede simplemente tomar el software vulnerable de un epoch anterior del sistema A y aplicarlo al sistema B para atacarlo. El hecho de que el software vulnerable de un epoch anterior se personalice al sistema A ayuda a evitar que pueda transferirse y usarse para atacar el sistema B. Todos estos mecanismos trabajan juntos para brindar garantías mucho más fuertes de que los atacantes no puedan colocar software vulnerable en una Mac para evadir las protecciones provistas por el último software. Sin embargo, un usuario que tenga un nombre de usuario y contraseña de administrador para la Mac, siempre podrá seleccionar la política de seguridad que funcione mejor para sus casos de uso.

Política de seguridad reducida

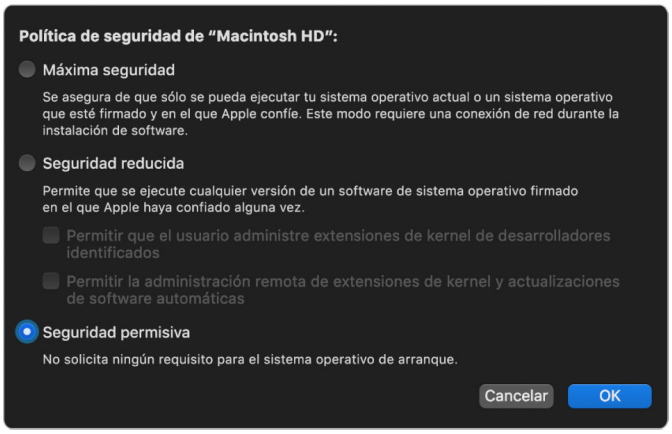
La seguridad reducida es similar al comportamiento de seguridad media en las computadoras Mac basadas en Intel con chip T2, en donde un proveedor (en este caso, Apple) genera una firma digital para el código con la finalidad de asegurar de que provenga del proveedor. Esto está diseñado para ayudar a impedir que los atacantes inserten código sin firmar. Apple hace referencia a esta firma como una firma "global", porque se puede usar en cualquier Mac, por cualquier cantidad de tiempo, para una Mac que actualmente tenga configurada la política Seguridad reducida. La seguridad reducida no proporciona en sí misma protección contra los ataques de retroceso (aunque los cambios no autorizados en el sistema operativo pueden hacer que los datos del usuario queden inaccesibles). Para obtener más información, consulta Extensiones del kernel en una Mac con Apple Chip.

Además de permitir que los usuarios ejecuten versiones anteriores de macOS, la seguridad reducida es necesaria en otras acciones que pueden poner en riesgo la seguridad del sistema del usuario, tales como implementar extensiones del kernel (kexts) de terceros. Las kexts tienen los mismos privilegios que el kernel, por lo que cualquier vulnerabilidad en las kexts de terceros tiene el potencial de vulnerar el sistema operativo completo. Es por esto que se les recomienda a los desarrolladores adoptar extensiones del sistema antes de que se elimine el soporte para kext de macOS en los modelos futuros de computadoras Mac con Apple Chip. Incluso cuando se habilitan las kexts de terceros, estas no se pueden cargar en el kernel por solicitud; en su lugar, se combinan en una colección de kernel auxiliar (AuxKC) cuyo hash se almacena en LocalPolicy y, por lo tanto, requiere que se reinicie. Para obtener más información sobre la generación de AuxKC, consulta Extensiones de kernel en macOS.

Política de seguridad permisiva

La seguridad permisiva es para los usuarios que aceptan el riesgo de poner su Mac en un estado mucho más inseguro, y es diferente del modo Sin seguridad de las computadoras Mac basadas en Intel con un chip T2. Con la seguridad permisiva, la verificación de firma se sigue realizando a lo largo de toda la cadena de arranque seguro, pero al configurar la política permisiva se le indica a iBoot que debe aceptar los objetos de arranque firmados por el Secure Enclave de forma local, tales como una colección de kernel de arranque generada por el usuario y construida a partir de un kernel XNU personalizado. De esta manera, la seguridad permisiva también proporciona una capacidad arquitectónica para ejecutar un kernel de "sistema operativo completamente no confiable" arbitrario. Cuando se carga en el sistema una colección de kernel de arranque personalizada o un sistema operativo que no es de confianza, algunas claves de desencriptado no estarán disponibles. Esto está diseñado para evitar que los sistemas operativos que no son de confianza accedan a los datos de los sistemas operativos que sí lo son.

Importante: Apple no ofrece o soporta kernels XNU personalizados.



Existe otra diferencia entre Seguridad permisiva y Sin seguridad en una Mac basada en Intel con el chip T2: la primera es un requisito previo para realizar algunas reducciones en la configuración de seguridad que en el pasado se podían controlar de forma independiente. Más notablemente, para desactivar la protección de la integridad del sistema (SIP) en una Mac basada en Apple Chip, el usuario debe reconocer que está poniendo el sistema en Seguridad permisiva. Esto es necesario debido a que desactivar la SIP ha puesto siempre el sistema en un estado que hace que el kernel sea mucho más vulnerable. En particular, al desactivar la SIP en una Mac con Apple Chip se desactiva la aplicación de la firma de las kexts durante el tiempo de generación de la AuxKC, lo que permite cargar cualquier kext arbitraria en la memoria del kernel. En las Mac con Apple Chip se ha implementado otra mejora en la SIP, en donde el almacenamiento de la política se pasó de la NVRAM a LocalPolicy. Así que ahora, para desactivar la SIP se requiere la autenticación de un usuario con acceso a la clave de la firma de LocalPolicy de recoveryOS (al que se accede manteniendo presionado el botón de encendido). Esto ocasiona que sea mucho más difícil para un atacante sólo de software, o incluso un atacante físicamente presente, desactivar la SIP.

No es posible cambiar a Seguridad permisiva desde la app Utilidad de Seguridad de Arranque. Los usuarios pueden reducir la seguridad sólo al ejecutar herramientas de línea de comandos desde Terminal en recoveryOS, como `csrutil` (para desactivar la SIP). Una vez que el usuario ha reducido la seguridad, este hecho se refleja en Utilidad de Seguridad de Arranque, por lo que el usuario puede configurar fácilmente la seguridad a una más segura.

Nota: una Mac con Apple Chip no requiere ni admite una política de arranque de soporte específica porque técnicamente todos los arranques se realizan de forma local. Si un usuario elige arrancar desde un soporte externo, esa versión del sistema operativo debe personalizarse primero mediante un reinicio autenticado desde recoveryOS. Al hacer esto se crea un archivo LocalPolicy en la unidad interna que se usa para realizar un arranque de confianza desde el sistema operativo almacenado en el soporte externo. Esto significa que la configuración del arranque desde un soporte externo siempre está activada de forma explícita por sistema operativo y ya requiere la autorización del usuario, por lo que no es necesaria una configuración de seguridad adicional.

Administración y creación de claves de firmas para LocalPolicy

Creación

Cuando se realiza la instalación de fábrica de macOS por primera vez, o al ejecutar un borrado e instalado combinado, la Mac ejecuta código del disco RAM de restauración temporal para inicializar el estado predeterminado. Durante este proceso, el entorno de restauración crea un nuevo par de claves pública y privada que se conservan en el Secure Enclave. La clave privada se denomina *clave de identidad del propietario (OIK)*. Si ya existe una OIK, se destruye como parte de este proceso. El entorno de restauración también inicializa la clave usada para el bloqueo de activación: la *clave de identidad del usuario (UIK)*. Parte de ese proceso que es exclusivo de las Mac con Apple Chip consta de la solicitud de la certificación UIK para el bloqueo de activación, en donde se incluye un conjunto de restricciones solicitadas que se aplicarán en LocalPolicy en el momento de la validación. Si el dispositivo no puede obtener una certificación UIK para el bloqueo de activación (por ejemplo, debido a que el dispositivo está actualmente asociado con una cuenta de Encontrar y se reporta como perdido), no podrá continuar el proceso para crear un archivo LocalPolicy. Si un dispositivo recibe un *certificado de identidad de usuario (ucrt)*, ese ucrt contiene restricciones de política impuestas por el servidor y restricciones de política solicitadas por el usuario en una extensión X.509 v3.

Cuando se obtiene correctamente un de bloqueo de activación/`ucrt`, se almacena en una base de datos en el servidor y también se devuelve al dispositivo. Una vez que el dispositivo tiene un ucrt, se envía una solicitud de certificación para la clave pública que corresponde a la OIK al servidor de la autoridad de afirmación básica (BAA). La BAA verifica la solicitud de certificación de OIK utilizando la clave pública del ucrt almacenado en la base de datos accesible de la BAA. Si la BAA puede verificar la certificación, certifica la clave pública, devolviendo el *certificado de identidad de propietario (OIC)* que está firmado por la BAA y contiene las restricciones almacenadas en el ucrt. El OIC se devuelve al Secure Enclave. A partir de ese momento, cada vez que el Secure Enclave firma un LocalPolicy nuevo, adjunta el OIC a Image4. LLB tiene confianza integrada en el certificado raíz de la BAA, lo que hace que confíe en el OIC y, a su vez, en la firma de LocalPolicy general.

Restricciones de RemotePolicy

Todos los archivos de Image4, no sólo los LocalPolicy, contienen restricciones en la evaluación del manifiesto de Image4. Estas restricciones se codifican mediante identificadores de objetos especiales (OID) en el certificado de entidad final. La biblioteca de verificación de Image4 busca los OID de las restricciones de certificado especial de un certificado durante la evaluación de la firma, y luego evalúa de forma mecánica las restricciones especificadas en este. Las restricciones tienen el formato:

- X debe existir
- X no debe existir
- X debe tener un valor específico

Por ejemplo, para las firmas “personalizadas”, las restricciones del certificado incluirán “ECID debe existir” y, para las firmas “globales”, incluirán “ECID no debe existir”. Estas restricciones están diseñadas para garantizar que todos los archivos Image4 firmados por una clave dada cumplan con ciertos requisitos para evitar errores al generar el manifiesto firmado de Image4.

En el contexto de cada LocalPolicy, se hace referencia a estas restricciones de certificado Image4 como *RemotePolicy*. Puede existir un archivo RemotePolicy distinto para los LocalPolicy de diferentes entornos de arranque. RemotePolicy se usa para restringir el LocalPolicy de recoveryOS de forma tal que cuando arranca recoveryOS, sólo puede comportarse como un arranque en modo de máxima seguridad. Esto incrementa la confianza en la integridad del entorno de arranque de recoveryOS, al ser un lugar desde el cual se puede cambiar la política. RemotePolicy restringe el LocalPolicy para que contenga el ECID de la Mac en la que se generó el LocalPolicy, y el `rpnh` (hash de valor único de la política remota) específico almacenado en el componente de almacenamiento seguro de esa Mac. El `rpnh` y, por lo tanto, RemotePolicy, sólo cambian cuando se realizan acciones de Buscar Mi Mac y el bloqueo de activación, tales como la inscripción, anulación de inscripción, bloqueo remoto y borrado remoto. Las restricciones de la política remota se determinan y especifican en el momento de la certificación de la clave de identidad de usuario (UIK) y se firman en el certificado de identidad de usuario (ucrt) emitido. Algunas restricciones de la política remota, como ECID, ChipID y BoardID, las determina el servidor, lo cual está diseñado para evitar que un dispositivo firme archivos de LocalPolicy para otro dispositivo. El dispositivo puede especificar otras restricciones de política remota para evitar reducir la política local sin proporcionar tanto la autenticación local requerida para acceder a la OIK actual como la autenticación remota de la cuenta en la que el dispositivo tiene bloqueo de activación.

Contenidos del archivo LocalPolicy en computadoras Mac con Apple Chip

LocalPolicy es un archivo Image4 firmado por el Secure Enclave. Image4 es un formato de estructura de datos codificado por DER de notación sintáctica abstracta 1 (ASN.1) que se usa para describir información sobre objetos de cadena de arranque seguro en plataformas Apple. En un modelo de arranque seguro basado en Image4, se solicitan las políticas de seguridad al momento de la instalación de software, iniciado por una solicitud de firma a un servidor de firma central de Apple. Si la política es aceptable, el servidor de firma devuelve un archivo Image4 firmado que contiene una variedad de secuencias de códigos de cuatro caracteres (4CC). Software como la ROM de arranque o LLB evalúan estos archivos Image4 firmados y 4CC.

Transferencia de propiedad entre sistemas operativos

El acceso a la clave de identidad del propietario (OIK) se denomina “Propiedad”. Esta propiedad es necesaria para permitir que los usuarios renuncien a LocalPolicy después de realizar cambios en la política o el software. La OIK está protegida con la misma jerarquía de claves que se describe en Protección de claves selladas (SKP) y por la misma clave de encriptación de claves (KEK) que la clave de encriptación del volumen (VEK). Esto significa que normalmente está protegida tanto por la contraseña del usuario como las medidas del sistema operativo y la política. Sólo hay una OIK para todos los sistemas operativos de la Mac, por lo que, al instalar un segundo sistema operativo, se requiere el consentimiento explícito de los usuarios del primer sistema operativo para transferir la Propiedad a los usuarios del segundo sistema operativo. Sin embargo, los usuarios aún no existen para el segundo sistema operativo cuando el instalador se ejecuta desde el primer sistema operativo. Normalmente, los usuarios de los sistemas operativos no se generan hasta que se inicia el sistema operativo y se ejecuta el asistente de configuración. Por lo tanto, se requieren dos nuevas acciones al instalar un segundo sistema operativo en una Mac con Apple Chip:

- Crear un archivo LocalPolicy para el segundo sistema operativo
- Preparar un “Usuario de instalación” para transferir la Propiedad

Cuando se ejecuta un asistente de instalación y se orienta la instalación para un volumen en blanco secundario, un mensaje le pregunta al usuario si quiere copiar un usuario del volumen actual para que sea el primer usuario del segundo volumen. Si el usuario dice que sí, el “Usuario de instalación” que se crea es, en realidad, una KEK que se deriva de la contraseña y las claves de hardware del usuario seleccionado, que luego se utiliza para encriptar la OIK a medida que se entrega al segundo sistema operativo. Después, desde el asistente de instalación del segundo sistema operativo, se solicita la contraseña de ese usuario para permitir el acceso a la OIK en el Secure Enclave para el nuevo sistema operativo. Si un usuario elige no copiar un usuario, el “Usuario de instalación” se crea de la misma manera, pero se usa una contraseña vacía en lugar de la contraseña de un usuario. Este segundo flujo existe para ciertos escenarios de administración del sistema. Sin embargo, los usuarios que quieran tener varias instalaciones de volúmenes y deseen realizar la transferencia de Propiedad de la manera más segura deben optar siempre por copiar un usuario del primer sistema operativo al segundo sistema operativo.

LocalPolicy en una Mac con Apple Chip

En el caso de las Mac con Apple Chip, el control de la política de seguridad local se ha delegado a una aplicación que se ejecuta en el Secure Enclave. Este software puede usar las credenciales del usuario y el modo de arranque del CPU principal para determinar quién puede cambiar la política de seguridad y desde cuál entorno de arranque. Esto ayuda a evitar que el software malicioso utilice los controles de la política de seguridad contra el usuario al reducir la seguridad para obtener más privilegios.

Propiedades del manifiesto de LocalPolicy

El archivo LocalPolicy contiene algunos 4CC arquitectónicos que se encuentran en la mayoría de los archivos Image4, como el ID de modelo o tarjeta (BORD) que indica un chip de Apple en particular (CHIP), o un identificador de chip exclusivo (ECID). Sin embargo, los siguientes 4CC se centran sólo en las políticas de seguridad que los usuarios pueden configurar.

Nota: Apple usa el término *One True recoveryOS (1TR) vinculado* para indicar un arranque en el recoveryOS vinculado al mantener presionado una sola vez el botón físico de encendido. Este es diferente al de un arranque normal de recoveryOS, el cual ocurre utilizando la NVRAM, o al presionar dos veces y mantener presionado el botón físico de encendido, o el cual podría presentarse cuando ocurre un error al arrancar. Presionar el botón físico de una manera específica aumenta la confianza en que el entorno de arranque no es accesible por un atacante sólo de software que ha obtenido acceso a macOS.

Hash de valor único de LocalPolicy (lpnh)

- *Tipo:* OctetString (48)
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* el `lpnh` se utiliza para evitar la reproducción de LocalPolicy. Es un hash SHA384 del valor único de LocalPolicy (LPN) que está guardado en el componente de almacenamiento seguro y que se puede acceder mediante la ROM de arranque del Secure Enclave o el Secure Enclave. El valor único sin procesar nunca es visible para el procesador de aplicaciones, sólo lo es para el sepOS. Un atacante que intente convencer a LLB de que un LocalPolicy previo que se capturó era válido debería colocar un valor en el componente de almacenamiento seguro que tiene el mismo valor `lpnh` que se encuentra en el LocalPolicy que quiere volver a reproducir. Normalmente, sólo hay un LPN válido en el sistema, excepto durante las actualizaciones de software, donde hay dos válidos de forma simultánea para permitir la posibilidad de tener un respaldo y arrancar el software anterior en caso de un error en la actualización. Cuando cambia un LocalPolicy para cualquier sistema operativo, todas las políticas se vuelven a firmar con el nuevo valor lpnh correspondiente al nuevo LPN que se encuentra en el componente de almacenamiento seguro. Este cambio ocurre cuando el usuario modifica la configuración de seguridad o crea nuevos sistemas operativos con un nuevo LocalPolicy para cada uno.

Hash de valor único de la política remota (rpnh)

- *Tipo:* OctetString (48)
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* el `rpnh` tiene el mismo comportamiento que el `lpnh`, pero sólo se actualiza cuando lo hace la política remota, tal como cuando se cambia el estado de registro de Encontrar. Este cambio ocurre cuando el usuario modifica el estado de Encontrar en su Mac.

Hash de valor único de recoveryOS (ronh)

- *Tipo:* OctetString (48)
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* el `ronh` tiene el mismo comportamiento que el lpnh pero sólo se encuentra en el LocalPolicy de recoveryOS y sólo se actualiza cuando lo hace el volumen recoveryOS del sistema, por ejemplo cuando hay una actualización de software. Se usa un valor único separado de `lpnh` y `rpnh` para que cuando Encontrar ponga un dispositivo en un estado desactivado, los sistemas operativos existentes puedan desactivarse (al eliminar su LPN y RPN del componente de almacenamiento seguro), mientras que se permite el arranque con el recoveryOS del sistema. De esta manera, los sistemas operativos se pueden volver a activar cuando el propietario del sistema demuestra su control sobre el sistema al ingresar su contraseña de iCloud que utiliza para la cuenta de Encontrar. Este cambio ocurre cuando un usuario actualiza el recoveryOS del sistema o crea nuevos sistemas operativos.

Hash del manifiesto Image4 de siguiente etapa (nsih)

- *Tipo:* OctetString (48)
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* el campo *nsih* representa un hash SHA384 de la estructura de datos del manifiesto Image4 que describe el arranque de macOS. El manifiesto de Image4 de macOS contiene mediciones para todos los objetos de arranque tales como iBoot, la caché de confianza estática, el árbol de dispositivos, la colección del kernel de arranque y el hash raíz del volumen de sistema firmado (SSV). Cuando se le instruye a LLB que arranque un macOS específico, se asegura de que el hash del manifiesto de Image4 del macOS adjunto a iBoot coincida con lo capturado en el campo `nsih` de LocalPolicy. De esta forma, el `nsih` captura la intención del usuario sobre cuál es el sistema operativo para el que se creó un LocalPolicy. Los usuarios cambian implícitamente el valor de `nsih` cuando realizan una actualización de software.

Hash de la política (auxp) de la colección del kernel auxiliar (AuxKC)

- *Tipo:* OctetString (48)
- *Entornos mutables:* macOS
- *Descripción:* el `auxp` es un hash SHA384 de la política de la lista de kexts autorizadas por el usuario (UAKL). Esto se utiliza al momento de generar la AuxKC para ayudar a garantizar que sólo se incluyan kexts autorizadas por el usuario en la AuxKC. `smb2` es un requisito previo para configurar este campo. Los usuarios cambian el valor `auxp` de forma implícita cuando cambian la UAKL al aprobar una kext desde el panel Seguridad y privacidad de Preferencias del Sistema.

Hash del manifiesto Image4 (auxi) de la colección del kernel auxiliar (AuxKC)

- *Tipo:* OctetString (48)
- *Entornos mutables:* macOS
- *Descripción:* después de que el sistema verifica que el hash de la UAKL coincide con lo que se encuentra en el campo `auxp` de LocalPolicy, solicita que la AuxKC esté firmada por la aplicación de procesador del Secure Enclave, que es responsable de la firma de LocalPolicy. Posteriormente, se coloca en LocalPolicy un hash SHA384 de la firma del manifiesto Image4 de AuxKC para evitar la posibilidad de mezclar y coincidir una AuxKC previamente firmada con un sistema operativo en el momento del arranque. Si iBoot encuentra el campo `auxi` en LocalPolicy, intenta cargar la AuxKC desde el disco y valida su firma. Después, verifica también que el hash de Image4 adjunto a la AuxKC coincida con el valor encontrado en el campo `auxi`. Si la AuxKC no se puede cargar por cualquier motivo, el sistema continúa con el arranque sin este objeto de arranque y, por lo tanto, sin las kexts de terceros. El campo `auxp` es un requisito previo para configurar el campo auxi en LocalPolicy. Los usuarios cambian el valor `auxi` de forma implícita cuando cambian la UAKL al aprobar una kext desde el panel Seguridad y privacidad de Preferencias del Sistema.

Hash de recepción (auxr) de la colección del kernel auxiliar (AuxKC)

- *Tipo:* OctetString (48)
- *Entornos mutables:* macOS
- *Descripción:* el `auxr` es un hash SHA384 de la recepción de AuxKC que indica el conjunto exacto de kexts incluidas en la AuxKC. La recepción de AuxKC puede ser un subconjunto de la UAKL, debido a que las kexts se pueden excluir de la AuxKC, incluso si están autorizadas por el usuario, si se sabe que se utilizan para ataques. Además, algunas kexts que se pueden usar para romper el límite usuario-kernel podrían causar una disminución en la funcionalidad, tal como la incapacidad de usar Apple Pay o de reproducir contenido 4K y HDR. Los usuarios que desean tener estas funcionalidades deberían elegir una inclusión de AuxKC más restrictiva. El campo `auxp` es un requisito previo para configurar el campo `auxr` en LocalPolicy. Los usuarios cambian el valor `auxr` de forma implícita cuando crean una AuxKC nueva desde el panel Seguridad y privacidad de Preferencias del Sistema.

Hash del manifiesto de Image4 de CustomOS (coih)

- *Tipo:* OctetString (48)
- *Entornos mutables:* 1TR
- *Descripción:* el `coih` es un hash SHA384 del manifiesto de Image4 de CustomOS. iBoot (en lugar del kernel XNU) utiliza la carga útil de ese manifiesto para transferir el control. Los usuarios cambian el valor de `coih` implícitamente cuando usan la herramienta de línea de comandos `kmutil configure-boot` en 1TR.

UUID del grupo de volúmenes APFS (vuid)

- *Tipo:* OctetString (16)
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* el `vuid` indica el grupo de volúmenes que el kernel debe usar como raíz. Este campo es principalmente informativo y no se usa para restricciones de seguridad; y el usuario configura el `vuid` de forma implícita al crear una instalación de sistema operativo nueva.

UUID de grupo (kuid) de la clave de encriptación clave (KEK)

- *Tipo:* OctetString (16)
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* el valor `kuid` indica el volumen que se arrancó. La clave de encriptación clave se ha usado generalmente para la protección de datos. Para cada LocalPolicy, se utiliza para proteger la clave de firma de LocalPolicy, y el usuario configura el `kuid` de forma implícita al crear una instalación de sistema operativo nueva.

Medición de la política de arranque confiable (TBPM) del recoveryOS enlazado

- *Tipo:* OctetString (48)
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* una medición de la política de arranque confiable (TBPM) del recoveryOS enlazado es un cálculo de hash SHA384 iterativo especial sobre el manifiesto Image4 de LocalPolicy, sin incluir los valores únicos, con el fin de proporcionar una medición consistente a través del tiempo (ya que los valores únicos como `lpnh` se actualizan frecuentemente). El campo `prot` se encuentra sólo en cada LocalPolicy de macOS, y proporciona un enlace para indicar el LocalPolicy de recoveryOS que corresponde al de macOS.

Política local de recoveryOS firmada por el Secure Enclave (hrlp)

- *Tipo:* booleano
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* `hrlp` indica si el valor de `prot` (arriba) es o no la medición de un LocalPolicy de recoveryOS firmado por el Secure Enclave. Si no lo es, el LocalPolicy de recoveryOS se firma mediante el servidor de firmas en línea de Apple, que firma cosas como archivos Image4 de macOS.

Versión del sistema operativo local (love)

- *Tipo:* booleano
- *Entornos mutables:* 1TR, recoveryOS, macOS
- *Descripción:* el parámetro `love` indica la versión del sistema operativo para la cual se crea la política local, LocalPolicy. La versión se obtiene del siguiente manifiesto de estado durante la creación de LocalPolicy, y se utiliza para aplicar las restricciones de vinculación de recoveryOS.

Arranque múltiple seguro (smb0)

- *Tipo:* booleano
- *Entornos mutables:* 1TR, recoveryOS
- *Descripción:* si el `smb0` está presente y es verdadero, LLB permite que el manifiesto Image4 de siguiente etapa tenga una firma global en lugar de requerir una firma personalizada. Los usuarios pueden cambiar este campo mediante Utilidad de Seguridad de Arranque o `bputil` para cambiar a Seguridad reducida.

Arranque múltiple seguro (smb1)

- *Tipo:* booleano
- *Entornos mutables:* 1TR
- *Descripción:* si el `smb1` está presente y es verdadero, iBoot permite que objetos tales como la colección del kernel personalizada se firmen mediante el Secure Enclave con la misma clave que LocalPolicy. La presencia de `smb0` es un requisito previo para la presencia de `smb1`. Los usuarios pueden cambiar este campo con las herramientas de línea de comandos tales como `csrutil` o `bputil` para cambiar a Seguridad permisiva.

Arranque múltiple seguro (smb2)

- *Tipo:* booleano
- *Entornos mutables:* 1TR
- *Descripción:* si el `smb2` está presente y es verdadero, iBoot permite que la colección del kernel auxiliar se firme mediante el Secure Enclave con la misma clave que LocalPolicy. La presencia de `smb0` es un requisito previo para la presencia de `smb2`. Los usuarios pueden cambiar este campo mediante Utilidad de Seguridad de Arranque o `bputil` para cambiar a Seguridad reducida y activar las kexts de terceros.

Arranque múltiple seguro (smb3)

- *Tipo:* booleano
- *Entornos mutables:* 1TR
- *Descripción:* si el `smb3` está presente y es verdadero, indica que un usuario en el dispositivo ha activado el control mediante administración de dispositivos móviles (MDM) en su sistema. La presencia de este campo hace que la aplicación del procesador del Secure Enclave que controla el archivo LocalPolicy acepte la autenticación MDM en lugar de requerir una autenticación de usuario local. Los usuarios pueden cambiar este campo con Utilidad de Seguridad de Arranque o `bputil` para activar el control administrado sobre las actualizaciones de software y las kexts de terceros. En macOS 11.2 o versiones posteriores, la solución MDM también puede iniciar una actualización a la versión más reciente de macOS si el modo de seguridad actual es Máxima seguridad.

Arranque múltiple seguro (smb4)

- *Tipo:* booleano
- *Entornos mutables:* macOS
- *Descripción:* si el `smb4` está presente y es verdadero, indica que el dispositivo ha activado el control mediante MDM del sistema operativo usando Apple School Manager, Apple Business Manager o Apple Business Essentials. La presencia de este campo hace que la aplicación del Secure Enclave que controla el archivo LocalPolicy acepte la autenticación MDM en lugar de requerir una autenticación de usuario local. La solución MDM cambia este campo cuando detecta que el número de serie de un dispositivo aparece en cualquiera de esos tres servicios.

Protección de la integridad del sistema (sip0)

- *Tipo:* entero de 64 bits sin firmar
- *Entornos mutables:* 1TR
- *Descripción:* el valor `sip0` contiene los bits de la política de protección de la integridad del sistema (SIP) que anteriormente estaban almacenados en la NVRAM. Los nuevos bits de la política SIP se agregan aquí (en lugar de usar los campos del archivo LocalPolicy como se muestra a continuación) si sólo se usan en macOS y no los utiliza LLB. Los usuarios pueden cambiar este campo con `csrutil` desde 1TR para desactivar la SIP y cambiar a Seguridad permisiva.

Protección de la integridad del sistema (sip1)

- *Tipo:* booleano
- *Entornos mutables:* 1TR
- *Descripción:* si el valor `sip1` está presente y es verdadero, iBoot permitirá fallos para verificar el hash raíz del SSV. Los usuarios pueden cambiar este campo usando `csrutil` o `bputil` desde 1TR.

Protección de la integridad del sistema (sip2)

- *Tipo:* booleano
- *Entornos mutables:* 1TR
- *Descripción:* si el valor sip2 está presente y es verdadero, iBoot no bloqueará el registro de hardware de la *región de sólo lectura de texto configurable (CTRR*) que marca la memoria del kernel como no escribible. Los usuarios pueden cambiar este campo usando `csrutil` o `bputil` desde 1TR.

Protección de la integridad del sistema (sip3)

- *Tipo:* booleano
- *Entornos mutables:* 1TR
- *Descripción:* si el valor `sip3` está presente y es verdadero, iBoot no aplicará su lista autorizada integrada para la variable NVRAM boot-args, que de otra forma filtraría las opciones pasadas al kernel. Los usuarios pueden cambiar este campo usando `csrutil` o `bputil` desde 1TR.

Certificados y RemotePolicy

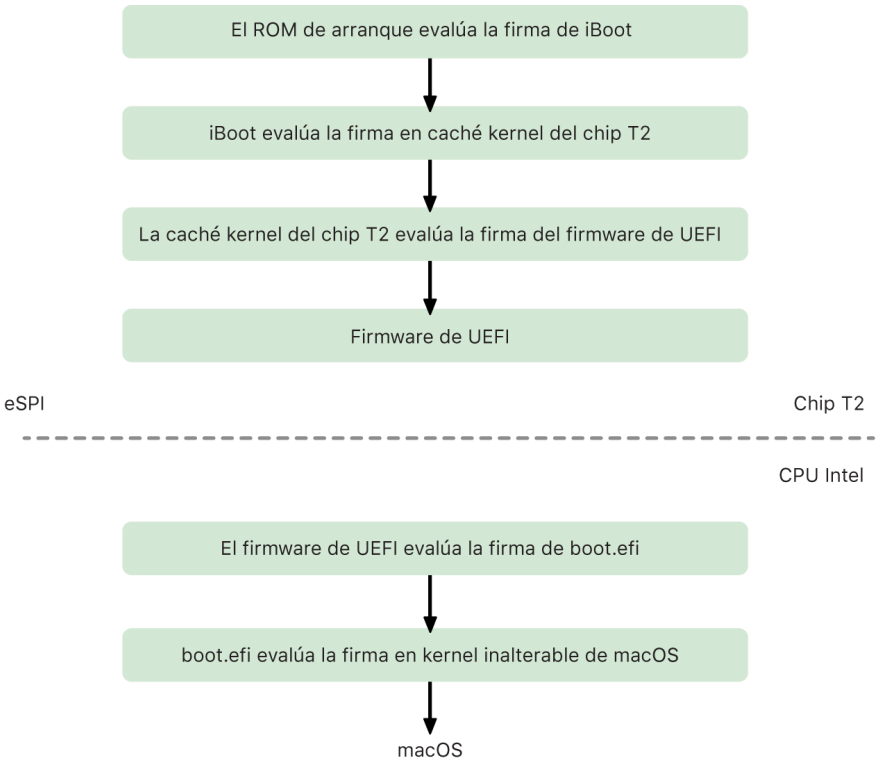
Como se describe en Administración y creación de claves de firmas para LocalPolicy, el Image4 de LocalPolicy también contiene el certificado de identidad de propietario (OIC) y el RemotePolicy incrustado.

Computadoras Mac basadas en Intel

Proceso de arranque de computadoras Mac basadas en Intel

Computadoras Mac basadas en Intel con el chip de seguridad T2 de Apple

Cuando se enciende una computadora Mac basada en Intel con el chip de seguridad T2 de Apple, el chip realiza un arranque seguro desde su ROM de arranque de la misma forma que sucede en los iPhone, iPad y computadoras Mac con Apple Chip. Esto verifica el gestor de arranque de iBoot, y es el primer paso de la cadena de confianza. iBoot verifica el kernel y el código de extensión del kernel del chip T2, lo que verifica el firmware UEFI de Intel. El firmware UEFI y la firma relacionada inicialmente están disponibles únicamente con el chip T2.



Después de la verificación, la imagen del firmware UEFI se asigna en una porción de la memoria del chip T2. Esta memoria se pone a disposición del CPU de Intel a través de la interfaz periférica serial mejorada (eSPI). Cuando el CPU de Intel arranca por primera vez, obtiene el firmware UEFI mediante la eSPI desde la copia asignada en la memoria y con verificación de integridad del firmware ubicado en el chip T2.

La evaluación de la cadena de confianza continúa en el CPU de Intel, mientras el firmware UEFI evalúa la firma de boot.efi, que es el administrador de arranque de macOS. Las firmas de arranque seguro de macOS que residen en Intel se almacenan en el mismo formato Image4 utilizado para iOS, iPadOS y el arranque seguro del chip T2, y el código que analiza los archivos Image4 es el mismo código endurecido de la implementación actual del arranque seguro de iOS y iPadOS. A su vez, boot.efi verifica la firma de un nuevo archivo llamado immutablekernel. Cuando se activa el arranque seguro, el archivo immutablekernel representa el conjunto completo de extensiones kernel de Apple requeridas para arrancar macOS. La política de arranque seguro termina en la entrega del immutablekernel, y después de eso, las políticas de seguridad de macOS (como la protección de la integridad del sistema y las extensiones kernel firmadas) entran en efecto.

Si hay algún error o fallo en este proceso, la Mac entra en el modo de recuperación, el modo de recuperación del chip de seguridad T2 de Apple, o el modo de actualización del firmware del dispositivo (DFU).

Microsoft Windows en una Mac basada en Intel con el chip T2

De manera predeterminada, una computadora Mac basada en Intel que es compatible con el arranque seguro únicamente confía en contenido firmado por Apple. Sin embargo, para mejorar la seguridad de las instalaciones de Boot Camp, Apple también es compatible con el arranque seguro para Windows. El firmware de la interfaz del firmware extensible unificado (UEFi) incluye una copia del certificado Microsoft Windows Production CA 2011 para autenticar los gestores de arranque de Microsoft.

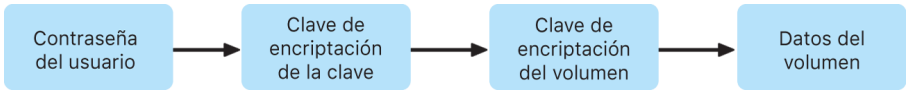
Nota: actualmente no hay confianza para el certificado Microsoft Corporation UEFI CA 2011, que permitiría la verificación del código firmado por los socios de Microsoft. El UEFI CA se utiliza comúnmente para verificar la autenticidad de los gestores de arranque para otros sistemas operativos, como las variantes de Linux.

El soporte para el arranque seguro de Windows no está activado de forma predeterminada; en lugar de ello, se activa usando el asistente de Boot Camp (BCA). Cuando un usuario ejecuta el BCA, se reconfigura macOS para confiar en el código de origen de Microsoft durante el arranque. Después de que el BCA termine, si macOS no puede aprobar la evaluación de confianza de origen de Apple durante el arranque seguro, el firmware UEFI intenta evaluar la confianza del objeto de acuerdo con el formato de arranque seguro de UEFI. Si la evaluación de confianza tiene éxito, la Mac procede e inicia Windows. Si no, la Mac entra en recoveryOS y le informa al usuario sobre el fallo en la evaluación de la confianza.

Computadoras Mac basadas en Intel sin el chip T2

Las computadoras Mac basadas en Intel que no tienen el chip T2 no son compatibles con el arranque seguro. Por lo tanto, el firmware de la interfaz del firmware extensible unificado (UEFi) carga el arrancador de macOS (boot.efi) desde el sistema de archivos sin verificación, y el arrancador carga el kernel (prelinkedkernel) desde el filesystem sin verificación. Para proteger la integridad de la cadena de arranque, los usuarios deberían activar todos los siguientes mecanismos de seguridad:

- *Protección de la integridad del sistema (SIP):* está activada de forma predeterminada y protege al arrancador y al kernel de escrituras maliciosas desde el interior de una macOS en funcionamiento.
- *FileVault:* se puede activar de dos formas, ya sea por parte del usuario o mediante un administrador de administración de dispositivos móviles (MDM). Esto evita que los atacantes físicamente presentes usen el modo de disco objetivo para sobrescribir el arrancador.
- *Contraseña del firmware:* se puede activar de dos formas, ya sea por parte del usuario o mediante un administrador MDM. Esto ayuda a evitar que algún atacante físicamente presente inicie modos alternativos de arranque como recoveryOS, el modo de usuario único o el modo de disco objetivo, desde los cuales se puede sobrescribir el arrancador. Esto también evita que se realice el arranque desde soportes alternativos, desde los cuales los atacantes podrían ejecutar código para sobrescribir el arrancador.



Modos de arranque para computadoras Mac basadas en Intel con el chip de seguridad T2 de Apple

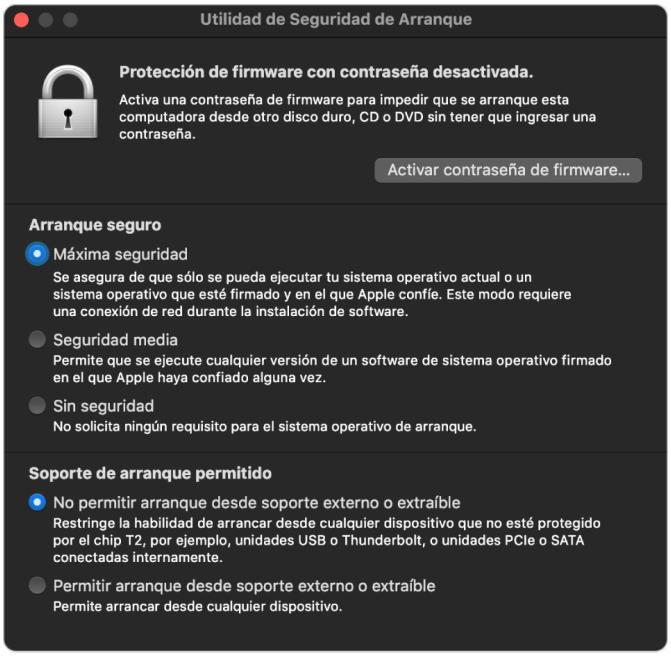
Una computadora Mac basada en Intel que tiene el chip de seguridad T2 de Apple tiene diversos modos de arranque a los que se puede acceder durante el encendido al presionar combinaciones de teclas reconocidas por el arrancador o el firmware UEFI. Algunos modos de arranque, como el modo de usuario único, no funcionarán a menos que se cambie la política de seguridad a Sin seguridad en Utilidad de Seguridad de Arranque.

Modo	Combinación de teclas	Descripción
Arranque de macOS	Ninguno	El firmware UEFI le entrega el proceso al arrancador de macOS (una aplicación UEFI), la cual se lo entrega al kernel de macOS. En el arranque estándar de una Mac con FileVault activado, el arrancador de macOS presenta la interfaz de ventana de inicio de sesión, la cual obtiene la contraseña y desencripta el almacenamiento.
Administrador de arranque	Tecla Opción (⌥)	El firmware UEFI inicia la aplicación UEFI integrada, que le presenta al usuario una interfaz de selección del dispositivo de arranque.
Modo de disco objetivo (TDM)	T	El firmware UEFI inicia la aplicación UEFI integrada que expone el dispositivo de almacenamiento interno sin procesar y basado en bloques mediante FireWire, Thunderbolt, USB o cualquier otra combinación de los tres (dependiendo del modelo de la Mac).
Modo de usuario único	Comando (⌘) + S	El kernel de macOS pasa el indicador –s en el vector del argumento launchd, y luego launchd genera la shell de único usuario en el tty de la app Consola. *Nota:* si el usuario sale del shell, macOS continúa con el arranque hasta llegar a la ventana de inicio de sesión.
recoveryOS	Comando (⌘) + R	El firmware UEFI carga un macOS mínimo desde un archivo de imagen de disco firmada (.dmg) en el dispositivo de almacenamiento interno.
recoveryOS por Internet	Opción (⌥) + Comando (⌘) + R	La imagen de disco firmada se descarga de Internet usando HTTP.
Diagnóstico	D	El firmware UEFI carga un entorno de diagnóstico UEFI mínimo desde un archivo de imagen de disco firmada en el dispositivo de almacenamiento interno.
Diagnóstico por Internet	Opción (⌥) + D	La imagen de disco firmada se descarga de Internet usando HTTP.
Arranque de Windows	Ninguno	Si se ha instalado Windows usando Boot Camp, el firmware UEFI entrega al arrancador de Windows, el cual entrega al kernel de Windows.

Utilidad de Seguridad de Arranque en las computadoras Mac con el chip de seguridad T2 de Apple

Descripción general

En una computadora Mac basada en Intel que tiene el chip de seguridad T2 de Apple, Utilidad de Seguridad de Arranque maneja un conjunto de configuraciones para las políticas de seguridad. Se puede acceder a la utilidad al arrancar en recoveryOS y seleccionar Utilidad de Seguridad de Arranque desde el menú Utilidades, y su función es proteger la configuración de seguridad admitida de una manipulación por parte de un atacante.



Los cambios a las políticas críticas requieren autenticación, aunque se esté en el modo de recuperación. Cuando se abre por primera vez Utilidad de Seguridad de Arranque, se le pide al usuario que ingrese la contraseña de administrador de la instalación primaria de macOS relacionada con el recoveryOS que se está arrancando actualmente. Si no existe ningún administrador, se debe crear uno para poder cambiar la política. El chip T2 requiere que la computadora Mac se haya arrancado en recoveryOS y que se haya producido una autenticación con una credencial respaldada por el Secure Enclave para que se pueda realizar cualquier cambio en la política. Los cambios en las políticas de seguridad tienen dos requerimientos implícitos. recoveryOS debe:

- Arrancarse desde un dispositivo de almacenamiento conectado directamente al chip T2, pues las particiones en otros dispositivos no tienen credenciales respaldadas por el Secure Enclave y enlazadas al dispositivo de almacenamiento interno.
- Estar en un volumen basado en APFS, puesto que sólo hay soporte para almacenar las credenciales de autenticación de recuperación que se enviaron al Secure Enclave en el volumen APFS de “prearranque” de una unidad. Los volúmenes con formato HFS plus no pueden utilizar el arranque seguro.

Esta política únicamente se muestra en Utilidad de Seguridad de Arranque en las computadoras Mac basadas en Intel que tienen el chip T2. Aunque la mayoría de los casos de uso no requieren cambios en la política de arranque seguro, los usuarios tienen el control de la configuración de su dispositivo, y pueden decidir según sus necesidades si desean desactivar o reducir la funcionalidad del arranque seguro de su Mac.

Los cambios a la política de arranque seguro realizados desde esta app únicamente se aplican a la evaluación de la cadena de confianza verificada en el procesador Intel. La opción de arranque seguro siempre está en vigor en el chip T2.

Se puede configurar la política de arranque seguro a una de estas configuraciones: Máxima seguridad, Seguridad media y Sin seguridad. La política Sin seguridad desactiva completamente la evaluación del arranque seguro en el procesador Intel, y le permite al usuario arrancar lo que quiera.

Política de arranque con máxima seguridad

La política de arranque predeterminada es Máxima seguridad, y su comportamiento es similar al de iOS y iPadOS, y al de Máxima seguridad en las Mac con Apple Chip. En el momento en que se descarga el software y se prepara para su instalación, como parte de la solicitud de firma, se personaliza mediante una firma que incluye el identificador de chip exclusivo (ECID), que en este caso es un identificador único específico para el chip T2. La firma que devuelve el servidor de firmas es única, y la puede usar solamente ese chip T2 particular. El firmware de la interfaz del firmware extensible unificado (UEFi) está diseñado para garantizar que cuando la política Máxima seguridad esté en vigor, una firma específica no esté firmada sólo por Apple, sino por esta Mac específica, esencialmente al vincular esa versión de macOS a esa Mac. Esto ayuda a prevenir ataques de retroceso como se describe para Máxima seguridad en una Mac con Apple Chip.

Política de arranque con Seguridad media

La política de arranque Seguridad media es similar a la de arranque seguro UEFI tradicional, en donde un proveedor (en este caso, Apple) genera una firma digital para el código, a fin de asegurar que viene del proveedor. De este modo, se evita que los atacantes inserten código sin firmar. Nos referimos a esta firma como una firma “global”, porque se puede usar en cualquier Mac, por cualquier cantidad de tiempo, para una Mac que actualmente tenga configurada la política Seguridad media. Ni iOS y iPadOS, ni el chip T2 en sí, son compatibles con firmas globales. Esta configuración no intenta evitar los ataques de retroceso.

Política de arranque de medios

La política de arranque de medios existe sólo en las computadoras Mac basadas en Intel con el chip T2, y es independiente de la política de arranque seguro. Así que, incluso si el usuario desactiva el arranque seguro, esto no cambia el comportamiento predeterminado que impide el arranque desde cualquier lugar que no sea el dispositivo de almacenamiento conectado directamente al chip T2 para arrancar la Mac (la política de arranque de medios no es necesaria en una Mac basada en Apple Chip; para obtener más información, consulta Control de la política de seguridad del disco de arranque).

Protección con contraseña del firmware en una Mac basada en Intel

El sistema macOS en computadoras Mac basadas en Intel y que cuentan con el chip de seguridad T2 de Apple es compatible con el uso de una contraseña para el firmware que tiene la finalidad de ayudar a evitar que se realicen modificaciones no intencionadas en la configuración del firmware de una Mac específica. La contraseña del firmware está diseñada para evitar la selección de modos de arranque alternativos, como arrancar en modo recoveryOS o en modo de un solo usuario, arrancar desde un volumen no autorizado, o dentro del modo de disco objetivo.

Nota: la contraseña de firmware no es necesaria en las computadoras Mac con Apple Chip, ya que la funcionalidad del firmware crítica que restringe se pasó a recoveryOS y, cuando FileVault está activado, recoveryOS requiere autenticación del usuario antes de que se pueda alcanzar su funcionalidad crítica.

El modo más básico de contraseña del firmware se puede obtener con Utilidad Contraseña Firmware de recoveryOS en computadoras Mac basadas en Intel que *no* tienen el chip T2; y desde Utilidad de Seguridad de Arranque en computadoras Mac basadas en Intel que *sí* tienen el chip T2. Hay opciones avanzadas (como la capacidad de solicitar la contraseña en cada arranque) disponibles en la herramienta de la línea de comandos `firmwarepasswd` en macOS.

Configurar una contraseña para el firmware es especialmente importante para reducir el riesgo de ataques en computadoras Mac basadas en Intel que no tienen el chip T2 por parte de atacantes físicamente presentes. La contraseña del firmware puede ayudar a evitar que un atacante arranque en recoveryOS, desde donde podría desactivar la protección de la integridad del sistema (SIP). Además, al restringir el arranque desde soportes alternativos, los atacantes no pueden ejecutar código privilegiado desde otro sistema operativo para atacar los firmwares periféricos.

Existe un mecanismo para restablecer la contraseña del firmware que ayuda a los usuarios que olviden la contraseña. Los usuarios presionan una combinación de teclas durante el arranque y se les brinda una cadena específica para el modelo, que deberán proporcionarle a AppleCare. AppleCare firma de forma digital un recurso, y el identificador de recurso uniforme (URI) verifica esta firma. Si la firma se valida, y el contenido es para la Mac específica, el firmware UEFI elimina la contraseña del firmware.

Para los usuarios que no quieran que nadie más que ellos pueda eliminar la contraseña de su firmware mediante software, se agregó la opción `–disable–reset–capability` a la herramienta de línea de comandos `firmwarepasswd` en macOS 10.15. Antes de configurar esta opción, los usuarios deben aceptar que en caso de que olviden la contraseña y se necesite eliminar, el usuario deberá cubrir los costos del reemplazo de la tarjeta madre necesario para lograr esto. Las organizaciones que deseen proteger sus computadoras Mac de atacantes externos y de empleados deben configurar una contraseña del firmware en los sistemas que son propiedad de la organización. Esto se puede lograr en el dispositivo de cualquiera de las siguientes formas:

- Al momento de entregar la computadora, usando manualmente la herramienta de la línea de comandos `firmwarepasswd`.
- Con herramientas de administración de terceros que usen la herramienta de la línea de comandos `firmwarepasswd`.
- Usando la administración de dispositivos móviles (MDM).

recoveryOS y entornos de diagnóstico en computadoras Mac basadas en Intel

recoveryOS

El sistema recoveryOS está completamente separado de sistema macOS principal, y su contenido completo se almacena en un archivo de imagen de disco llamado BaseSystem.dmg. También hay un BaseSystem.chunklist asociado, que se usa para verificar la integridad de BaseSystem.dmg. El chunklist es una serie de hashes de fragmentos de 10 MB de BaseSystem.dmg. El firmware de la interfaz del firmware extensible unificado (UEFi) evalúa primero la firma del archivo chunklist y luego el hash de cada fragmento de BaseSystem.dmg a la vez, lo que ayuda a garantizar que coincida con el contenido firmado presente en el chunklist. Si cualquiera de estos hashes no coincide, se cancela el arranque desde el recoveryOS local, y el firmware UEFI intenta arrancar desde el recoveryOS por Internet en su lugar.

Si el proceso de verificación se completa de forma exitosa, el firmware UEFI monta el BaseSystem.dmg. como disco RAM e inicia el boot.efi que contiene. No hay necesidad de que el firmware UEFI realice una revisión específica del boot.efi, ni de que boot.efi realice una revisión del kernel, pues ya se ha revisado la integridad del contenido completado del sistema operativo (del cual estos elementos son sólo un subconjunto).

Diagnóstico de Apple

El procedimiento para arrancar el entorno de diagnóstico local es principalmente el mismo que se realiza al arrancar recoveryOS. Se utilizan archivos AppleDiagnostics.dmg y AppleDiagnostics.chunklist separados, pero se verifican de la misma forma que los archivos BaseSystem. En lugar de arrancar boot.efi, el firmware UEFI inicia un archivo dentro de la imagen de disco (archivo .dmg) llamado diags.efi, que a su vez es responsable de invocar otros controladores UEFI que pueden interactuar con el hardware y verificar si hay errores.

recoveryOS por Internet y entorno de diagnóstico

Si ocurre un error durante el arranque de la recuperación local o de los entornos de diagnóstico, el firmware UEFI intenta descargar las imágenes de Internet (un usuario también puede solicitar específicamente que las imágenes se obtengan de Internet usando una secuencia especial de teclas que se presiona durante el arranque). La validación de la integridad de las imágenes del disco y chunklists descargadas del servidor de recuperación de OS se realiza de la misma forma que las imágenes obtenidas de un dispositivo de almacenamiento.

Mientras que la conexión al servidor de recuperación de OS se realice mediante HTTP, la integridad del contenido descargado completo se verifica como se describió anteriormente y, por lo tanto, está protegido contra manipulación por parte de algún atacante con control de la red. En caso de que falle la verificación de la integridad de algún fragmento individual, se vuelve a solicitar 11 veces al servidor de recuperación de OS, antes de darse por vencido y mostrar un error.

En 2011, cuando se agregaron los modos de recuperación y diagnóstico por Internet a las computadoras Mac, se decidió que sería mejor usar el transporte HTTP simplificado, y manejar la autenticación de contenido con el mecanismo chunklist, en lugar de implementar una funcionalidad HTTPS más complicada en el firmware UEFI e incrementar así la superficie de ataque del firmware.

Seguridad del volumen del sistema firmado en iOS, iPadOS y macOS

En macOS 10.15, Apple implementó el volumen del sistema de sólo lectura, el cual es un volumen dedicado y separado para el contenido del sistema. macOS 11 o versiones posteriores agregan protección criptográfica fuerte al contenido del sistema con un *volumen de sistema firmado (SSV)*. El SSV cuenta con un mecanismo de kernel que verifica la integridad del contenido del sistema durante la ejecución, y rechaza cualquier dato, ya sea código o no, que no cuente con una firma criptográfica válida de Apple. A partir de iOS 15 y iPadOS 15, el volumen del sistema de un dispositivo iOS y iPadOS también obtiene la protección criptográfica de un volumen del sistema firmado.

El SSV no sólo ayuda a evitar la manipulación de cualquier software de Apple que sea parte del sistema operativo, sino que también hace que la actualización del software macOS sea más confiable y mucho más segura. Además, debido a que el SSV usa instantáneas Apple File System (APFS), si no se puede ejecutar una actualización, se puede restaurar la versión del sistema antiguo sin necesidad de reinstalarlo.

Desde su implementación, APFS ha proporcionado integridad a los metadatos del sistema de archivos usando sumas no criptográficas en el dispositivo de almacenamiento interno. SSV refuerza el mecanismo de integridad al agregar hashes criptográficos, lo que la extiende para incluir todos los bytes de los datos del archivo. Los datos del dispositivo de almacenamiento interno (incluidos los metadatos del sistema de archivos) se generan en un hash de forma criptográfica, y posteriormente el hash se compara con un valor esperado en los metadatos del sistema de archivos. En caso de no coincidir, el sistema asume que los datos han sido alterados y no los devolverá al software que los solicita.

Cada hash SHA256 del SSV se almacena en el árbol de metadatos del sistema de archivos principal, el cual tiene generados hash. Y, debido a que cada nodo del árbol verifica de forma recursiva la integridad de los valores hash de los elementos secundarios (similar a un árbol hash binario (Merkle), el valor hash del nodo raíz, llamado *sello*, abarca cada byte de datos en el SSV, lo que significa que la firma criptográfica cubre todo el volumen del sistema.

Durante la instalación y actualización de macOS, el sello se recalcula desde el sistema de archivos en el dispositivo, y esa medición se verifica respecto a las medidas firmadas por Apple. En las computadoras Mac con Apple Chip, el gestor de arranque verifica el sello antes de transferir el control al kernel. En las computadoras Mac basadas en Intel que cuentan con el chip de seguridad T2 de Apple, el gestor de arranque reenvía la medición y firma al kernel, que posteriormente verifica el sello directamente antes de montar el sistema de archivos raíz. En cualquier caso, si falla la verificación, el proceso de arranque se detendrá, y se le pedirá al usuario que reinstale macOS. Este procedimiento se repite en cada arranque, a menos que el usuario haya elegido entrar en un modo de seguridad más bajo y que haya decidido desactivar el volumen de sistema firmado.

Durante las actualizaciones de software de iOS y iPadOS, el volumen del sistema se prepara y se vuelve a calcular de forma similar. Los cargadores de arranque de iOS y iPadOS verifican que el sello esté intacto y que coincida con un valor firmado por Apple antes de permitir que el dispositivo inicie el kernel. Las inconsistencias en el arranque hacen que el usuario actualice el software del sistema en el dispositivo. Los usuarios no pueden desactivar la protección de un volumen de sistema firmado en iOS y iPadOS.

SSV y firma de código

La firma de código todavía está presente y obligada por el kernel. El volumen del sistema firmado ofrece protección cuando se leen bytes desde el dispositivo de almacenamiento interno. Por el contrario, la firma de código proporciona protección cuando los objetos Mach se asignan en la memoria como ejecutables. Tanto el SSV como la firma de código protegen el código ejecutable en todas las rutas de lectura y ejecución.

SSV y FileVault

En macOS 11, el SSV proporciona una protección en reposo equivalente para el contenido del sistema y, por lo tanto, ya no es necesario encriptar el volumen del sistema. El sistema de archivos detectará cualquier modificación que se realice al sistema de archivos en reposo cuando se realice la lectura. Si el usuario habilitó FileVault, el contenido del usuario en el volumen de datos se mantiene encriptado con un secreto proporcionado por el usuario.

Si el usuario elige desactivar el SSV, el sistema en reposo se vuelve vulnerable a las alteraciones, y estas alteraciones podrían permitir a un atacante extraer datos del usuario encriptados la próxima vez que arranque el sistema. Es por esto que el sistema no permite al usuario desactivar el SSV si FileVault está activado. La protección durante el reposo se debe activar o desactivar para ambos volúmenes de una forma consistente.

En macOS 10.15 o versiones anteriores, FileVault protege el software del sistema operativo en reposo al encriptar el contenido de usuario y sistema con una clave protegida por un secreto proporcionado por el usuario. Esto protege contra un atacante con acceso físico al dispositivo para que no acceda o modifique efectivamente el sistema de archivos que contiene el software del sistema.

SSV y computadoras Mac con el chip de seguridad T2 de Apple

En las computadoras Mac con el chip de seguridad T2 de Apple, sólo macOS está protegido por el SSV. El software que se ejecuta en el chip T2 y verifica macOS está protegido por el arranque seguro.

Actualizaciones seguras del software

La seguridad es un proceso; no basta con arrancar de manera confiable la versión del sistema operativo instalada de forma predeterminada, sino que también debe existir un mecanismo que permita obtener de manera rápida y segura las últimas actualizaciones de seguridad. Apple publica periódicamente actualizaciones de software para solucionar problemas de seguridad emergentes. Los usuarios de dispositivos iOS y iPadOS reciben notificaciones de actualizaciones en el dispositivo, mientras que los usuarios de Mac pueden encontrarlas en Preferencias del Sistema. Las actualizaciones se entregan por vía inalámbrica, para la adopción rápida de las últimas correcciones de seguridad.

El proceso de actualización

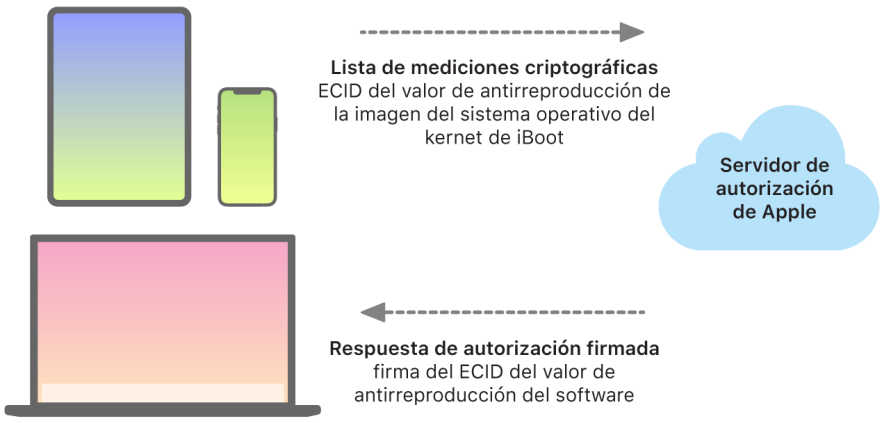
El proceso de actualización utiliza la misma raíz de confianza basada en hardware que el arranque seguro usa y que está diseñada para instalar únicamente código firmado por Apple. El proceso de actualización también utiliza la autorización del software del sistema para revisar que sólo las copias de las versiones del sistema operativo que estén actualmente firmadas por Apple se puedan instalar en los dispositivos iOS y iPadOS, o en las computadoras Mac que tengan Máxima seguridad como la política de seguridad configurada para el arranque seguro en Utilidad de Seguridad de Arranque. Con estos procesos seguros, Apple puede dejar de firmar versiones anteriores del sistema operativo con vulnerabilidades conocidas y, por lo tanto, ayuda a prevenir ataques de retroceso.

Para ofrecer una mayor seguridad al actualizar el software, cuando un dispositivo está conectado físicamente a una Mac, se descarga e instala una copia completa de iOS o de iPadOS. Sin embargo, en el caso de las actualizaciones de software inalámbricas (OTA) *sólo se descargan los componentes necesarios para llevar a cabo la actualización* en lugar de descargar todo el sistema operativo. De este modo, se mejora la eficiencia de la red. Además, las actualizaciones de software se pueden almacenar en la memoria caché de una Mac con macOS 10.13 o versiones posteriores que tenga activada la función de almacenamiento de contenido en caché, de tal forma que los dispositivos iOS y iPadOS no tengan que volver a descargar de Internet la actualización necesaria. Sin embargo, aún será necesario ponerse en contacto con los servidores de Apple para completar el proceso de actualización.

Proceso de actualización personalizado

Durante las actualizaciones, se realiza una conexión al servidor de autorización de instalaciones de Apple, el cual incluye una lista de medidas criptográficas para cada parte del paquete de instalación que se vaya a instalar (por ejemplo, iBoot, el kernel y la imagen del sistema operativo), un valor antirreproducción aleatorio (el valor único) y el identificador de chip exclusivo (ECID) del dispositivo.

El servidor de autorización coteja la lista de medidas presentada con las versiones cuya instalación se permite y, si encuentra una coincidencia, agrega el ECID a la medición y firma el resultado. Como parte del proceso de actualización, el servidor envía un conjunto completo de datos firmados al dispositivo. Agregar ECID "personaliza" la autorización para el dispositivo que realiza la solicitud. El servidor sólo autoriza y firma las medidas conocidas, de modo que ayuda a garantizar que la actualización se lleve a cabo de acuerdo con las especificaciones de Apple.



La evaluación de la cadena de confianza del tiempo de arranque verifica que la firma sea de Apple y que la medición del elemento que se carga desde el dispositivo de almacenamiento, junto con el identificador de chip exclusivo (ECID) del dispositivo, coincidan con lo que cubre la firma. Estos pasos están diseñados para garantizar que, en dispositivos compatibles con la personalización, la autorización se realice para un dispositivo específico y que no se pueda copiar un sistema operativo anterior de la versión del firmware de un dispositivo a otro. El valor único ayuda a impedir que un atacante guarde la respuesta del servidor y la utilice para manipular un dispositivo o que se modifique el software del sistema de algún otro modo.

El proceso de personalización es la razón por la que siempre se requiere una conexión de red a Apple para actualizar cualquier dispositivo que tenga un Apple Chip, incluidas las computadoras Mac basadas en Intel que tienen el chip de seguridad T2 de Apple.

Por último, el volumen de datos del usuario nunca se monta durante una actualización de software, lo que ayuda a impedir que se lea o se escriba algo en él durante las actualizaciones.

En los dispositivos con Secure Enclave, este hardware utiliza de forma similar el proceso de autorización de software del sistema para revisar la integridad de su software, y está diseñado para impedir la instalación de versiones anteriores.

Integridad del sistema operativo

El software del sistema operativo de Apple está diseñado pensando en la seguridad. Este diseño incluye una raíz de confianza de hardware, que se utiliza para permitir un arranque seguro, y un proceso de actualización de software seguro que es rápido y seguro. Los sistemas operativos de Apple también aprovechan las funcionalidades del hardware basado en silicio especialmente diseñadas para ayudar a prevenir la explotación mientras se ejecuta el sistema. Estas funciones de tiempo de ejecución protegen la integridad del código de confianza mientras se ejecuta. En resumen, el software del sistema operativo de Apple ayuda a mitigar las técnicas de ataque y explotación, ya sea que se originen en una app maliciosa, en la web o mediante cualquier otro canal. Las protecciones que se enumeran aquí están disponibles en dispositivos con SoC de Apple compatibles, los cuales incluyen iOS, iPadOS, tvOS, watchOS y ahora macOS (en computadoras Mac con Apple Chips).

Funcionalidad	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Familia M1
Protección de la integridad del kernel	✓	✓	✓	✓	✓	✓
Restricciones rápidas de permisos		✓	✓	✓	✓	✓
Protección de la integridad del coprocesador del sistema			✓	✓	✓	✓
Códigos de autenticación con puntero			✓	✓	✓	✓
Capa de protección de página		✓	✓	✓	✓	Ver nota a continuación.

Nota: la capa de protección de página (PPL) requiere que la plataforma *sólo* ejecute código firmado y de confianza; este es un modelo de seguridad que no es de aplicación en macOS.

Protección de la integridad del kernel

Después de que el kernel del sistema operativo completa la inicialización, se activa la protección de la integridad del kernel (KIP) para ayudar a evitar modificaciones en el código del kernel y del controlador. El controlador de la memoria brinda una región de memoria física protegida que iBoot utiliza para cargar el kernel y sus extensiones. Una vez que se completa el arranque, el controlador de memoria niega la escritura en la región de la memoria física protegida. La unidad de administración de memoria (MMU) del procesador de aplicaciones está configurada para ayudar a evitar que se asigne código privilegiado de la memoria física fuera de la región de memoria protegida y para evitar las asignaciones editables de la memoria física dentro de la región de memoria del kernel.

Para prevenir su reconfiguración, el hardware utilizado para activar la KIP se bloquea después de que se completa el proceso de arranque.

Restricciones rápidas de permisos

A partir de los SoC A11 Bionic y S3 de Apple, se introdujo una nueva primitiva de hardware llamada Restricciones rápidas de permisos, la cual incluye un registrador de CPU que rápidamente restringe los permisos por hilo. Con las restricciones rápidas de permisos (también conocidas como registros APRR), los sistemas operativos compatibles pueden eliminar permisos de ejecución desde la memoria sin tener que realizar una llamada al sistema y un recorrido o barrido de la tabla de la página. Estos registros ofrecen un nivel adicional de mitigación para ataques de la web, particularmente para el código compilado durante la ejecución (compilado en tiempo de ejecución), ya que la memoria no se puede ejecutar eficientemente al mismo tiempo que se lee o que se escribe en ella.

Protección de la integridad del coprocesador del sistema

El firmware del coprocesador maneja muchas tareas críticas del sistema, por ejemplo, el Secure Enclave, el procesador del sensor de imágenes y el coprocesador Motion. Por lo tanto, su seguridad es una parte fundamental de la seguridad de todo el sistema. Para evitar la modificación del firmware del coprocesador, Apple utiliza un mecanismo llamado *protección de la integridad del coprocesador del sistema (SCIP)*.

La SCIP funciona de forma muy similar a la protección de la integridad del kernel (KIP): durante el arranque, iBoot carga el firmware de cada coprocesador en la región de memoria protegida, reservada y separada de la región de la KIP. iBoot configura las unidades de memoria de cada coprocesador para ayudar a evitar lo siguiente:

- Asignaciones ejecutables fuera de la región de memoria protegida
- Asignaciones editables dentro de la región de memoria protegida

También al momento del arranque, para configurar la SCIP para el Secure Enclave, se utiliza el sistema operativo del Secure Enclave. Cuando el proceso de arranque esté completo, el hardware utilizado para activar SCIP se bloquea, lo cual está diseñado para evitar que se vuelva a configurar.

Códigos de autenticación con puntero

Los códigos de autenticación con puntero (PAC) se utilizan para proteger contra la explotación de errores de corrupción de memoria. El software del sistema y las apps integradas usan PAC para prevenir la modificación de punteros de función y direcciones de devolución (punteros de código). PAC utiliza cinco valores secretos de 128 bits para firmar los datos y las instrucciones del kernel, y cada proceso del espacio del usuario tiene sus propias claves B. Los elementos se aleatorizan y firman como se indica a continuación.

Elemento	Clave	Aleatorización
Dirección de retorno de la función	IB	Dirección de almacenamiento
Punteros de función	IA	0
Función de innovación de bloque	IA	Dirección de almacenamiento
Caché del método Objetivo-C	IB	Dirección de almacenamiento + Clase + Selector
Entradas de la tabla virtual de C++	IA	Dirección de almacenamiento + Hash (nombre del método corrupto)
Etiqueta Goto computada	IA	Hash (nombre de la función)
Estado del hilo del kernel	GA	•
Registros del estado del hilo del usuario	IA	Dirección de almacenamiento
Punteros de la tabla virtual de C++	DA	0

El valor de la firma se almacena en los bits de espacio adicional sin utilizar en la parte superior del puntero de 64 bits. La firma se verifica antes del uso, y el espacio adicional se restaura para ayudar a cerciorarse de que la dirección del puntero funcione; si no se verifica, se cancela la operación. Esta verificación aumenta la dificultad de muchos ataques, como el ataque contra la programación orientada a las devoluciones (ROP), que intenta engañar al dispositivo para que ejecute un código malintencionado existente al manipular direcciones de devolución de función almacenadas en la pila.

Capa de protección de página

La capa de protección de página (PPL) en iOS, iPadOS y watchOS está diseñada para impedir que el código de espacio del usuario se modifique después de que se completa la verificación de la firma del código. Encima de la protección de la integridad del kernel y las restricciones rápidas de permisos, la PLL administra las omisiones a los permisos de la tabla de páginas para asegurarse de que sólo la PPL pueda alterar las páginas protegidas que contienen el código del usuario y las tablas de páginas. El sistema brinda una reducción masiva de la superficie de ataque al soportar la aplicación de la integridad del código de todo el sistema, incluso frente a un kernel vulnerado. Esta protección no se ofrece en macOS debido a que la PPL sólo es de aplicación en sistemas donde todo el código ejecutado debe estar firmado.

Funcionalidades adicionales de seguridad del sistema macOS

Funcionalidades adicionales de seguridad del sistema macOS

macOS opera en un conjunto más amplio de hardware (por ejemplo, CPU basados en Intel, CPU basados en Intel en combinación con el chip de seguridad T2 de Apple y SoC basados en Apple Chip) y es compatible con una variedad de casos de uso informático de propósito general. Mientras que algunos usuarios usan sólo las apps básicas preinstaladas o las disponibles en App Store, otros son expertos informáticos del kernel que necesitan deshabilitar esencialmente todas las protecciones de la plataforma para poder ejecutar y probar su código de ejecución con los niveles más altos de confianza. La mayoría se encuentra en algún punto intermedio, y muchos de ellos tienen periféricos y software que requieren distintos niveles de acceso. Apple diseñó la plataforma de macOS con un enfoque integrado hacia el hardware, el software y los servicios; una plataforma que brinda seguridad desde el diseño y que facilita la configuración, implementación y administración a la vez que mantiene la configurabilidad que los usuarios esperan. macOS también incluye tecnologías clave de seguridad que los profesionales de TI necesitan para ayudar a proteger los datos corporativos y que se integran en entornos seguros de redes empresariales.

Las siguientes funcionalidades admiten y ayudan a proteger las diversas necesidades de los usuarios de macOS. Entre ellas se incluyen las siguientes:

- Seguridad del volumen del sistema firmado
- Protección de la integridad del sistema
- Cachés de confianza
- Protección para periféricos
- Seguridad y soporte para Rosetta 2 (traducción automática) en computadoras Mac con Apple Chip
- Protecciones y soporte para DMA
- Seguridad y soporte para las extensiones de kernel (kext)
- Seguridad y soporte para la ROM de opción
- Seguridad del firmware UEFI en computadoras Mac basadas en Intel

Protección de la integridad del sistema

macOS utiliza permisos del kernel para limitar la capacidad de escritura de los archivos críticos del sistema con una función llamada *protección de la integridad del sistema (SIP)*. Esta función es independiente y adicional a la protección de la integridad del kernel (KIP) basada en hardware que está disponible en computadoras Mac basadas en Apple Chip, la cual protege la modificación del kernel en la memoria. Para ofrecer esto, se aprovecha la tecnología de control obligatorio de acceso junto con otras protecciones a nivel de kernel, incluido el aislamiento en zona protegida y la bóveda de datos.

Controles obligatorios de acceso

macOS usa controles obligatorios de acceso, es decir, políticas que establecen restricciones de seguridad creadas por el desarrollador, y que no se pueden omitir. Este método es distinto a los controles de acceso discrecionales, que permiten a los usuarios omitir las políticas de seguridad de acuerdo con sus preferencias.

Los controles obligatorios de acceso no son visibles para los usuarios, pero son la tecnología subyacente que ayuda a activar varias funcionalidades importantes, como la zona protegida, los controles parentales, las preferencias administradas, las extensiones y la protección de la integridad del sistema.

Protección de la integridad del sistema

La *protección de la integridad del sistema* restringe a sólo lectura los componentes que se encuentran en ubicaciones críticas del sistema de archivos para ayudar a impedir que algún código malicioso los modifique. Además, esta protección es una configuración específica de la computadora que se activa de forma predeterminada cuando un usuario actualiza a OS X 10.11 o versiones posteriores. En una computadora Mac basada en Intel, si se desactiva, se elimina la protección para todas las particiones del dispositivo de almacenamiento físico. macOS aplica esta política de seguridad para todos los procesos que se ejecutan en el sistema, independientemente de si se están ejecutando en la zona protegida o con privilegios de administrador.

Cachés de confianza

Uno de los objetos incluidos en la cadena de arranque seguro es la caché de confianza estática, que es un registro de confianza de todos los binarios Mach-O que se controla en el volumen del sistema firmado. Cada Mach-O está representado por un hash de directorio de código. Para una búsqueda eficiente, estos hashes se ordenan antes de insertarse en la caché de confianza. El directorio de códigos es el resultado de la operación de firma realizada por `codesign(1)`. Para hacer cumplir la caché de confianza, la SIP debe permanecer activada. Para desactivar la aplicación de la caché de confianza en una Mac con Apple Chip, el arranque seguro debe configurarse como Seguridad permisiva.

Cuando se ejecuta un binario (ya sea como parte de generar un proceso nuevo o de asignar código ejecutable a un proceso existente), su directorio de códigos se extrae y se genera un hash. Si el hash resultante se encuentra en la caché de confianza, las asignaciones ejecutables creadas para el binario recibirán privilegios de plataforma; es decir que podrán tener cualquier privilegio y podrán ejecutarse sin verificaciones adicionales de la autenticidad de la firma. Esto contrasta con las computadoras Mac basadas en Intel, en donde los privilegios de plataforma se transfieren al contenido del sistema operativo mediante el certificado de Apple que firma los archivos binarios (este certificado no limita qué privilegios puede tener el binario).

Los binarios que no son de plataforma (por ejemplo, código de terceros certificado) deben tener cadenas de certificados válidas para poder ejecutarse, y las autorizaciones que pueden poseer están limitadas por el perfil de firma emitido para el desarrollador por parte del Programa de desarrolladores de Apple.

Todos los binarios enviados dentro de macOS están firmados con un *identificador de plataforma*. En las computadoras Mac con Apple Chip, este identificador se usa para indicar que, aunque el binario está firmado por Apple, el hash de su directorio de códigos debe estar presente en la caché de confianza para poder ejecutarse. En las computadoras Mac basadas en Intel, el identificador de plataforma se usa para realizar la revocación dirigida de binarios de una versión anterior de macOS, la cual ayuda a impedir que se ejecuten los binarios en versiones más recientes.

La caché de confianza estática bloquea por completo un conjunto de binarios en una versión determinada de macOS. Este comportamiento ayuda a impedir que los binarios de sistemas operativos más antiguos que están legítimamente firmados por Apple se introduzcan en sistemas más recientes para que un atacante obtenga algún beneficio.

Código de plataforma enviado fuera del sistema operativo

Apple envía algunos binarios, por ejemplo, Xcode y el conjunto de herramientas de desarrollo, que no están firmados con un identificador de plataforma. Aún así, se les permite ejecutarse con privilegios de plataforma en las Mac con Apple Chip y aquellas que cuentan con un chip T2. Debido a que este software de plataforma se envía de forma separada de macOS, no está sujeto a los comportamientos de revocación impuestos por la caché de confianza estática.

Cachés de confianza cargables

Apple envía algunos paquetes de software con *cachés de confianza cargable*s. Estas cachés tienen la misma estructura de datos que la caché de confianza estática. Sin embargo, aunque sólo hay una caché de confianza estática y se garantiza que sus contenidos siempre se bloquearán en rangos de sólo lectura después de que se haya completado la inicialización del kernel, las cachés de confianza cargables se agregan al sistema durante el tiempo de ejecución.

Estas cachés de confianza se autentican a través del mismo mecanismo que autentica el firmware de arranque (personalización mediante el servicio de firma confiable de Apple) o como objetos firmados globalmente (cuyas firmas no los vinculan a un dispositivo en particular).

Un ejemplo de caché de confianza personalizada es la caché que se envía con la imagen de disco que se utiliza para realizar diagnósticos en campo en computadoras Mac con Apple Chip. Esta caché de confianza se personaliza, junto con la imagen del disco, y se carga en el kernel de la computadora Mac en cuestión mientras se arranca en modo de diagnóstico. La caché de confianza permite que el software que está dentro de la imagen del disco se ejecute con privilegios de plataforma.

Un ejemplo de una caché de confianza firmada globalmente se envía con las actualizaciones de software de macOS. Esta caché de confianza permite que una parte del código dentro de la actualización de software, el *cerebro de la actualización*, se ejecute con privilegios de plataforma. El cerebro de la actualización realiza cualquier proceso necesario para organizar la actualización de software que el sistema host no tenga la capacidad de realizar de manera consistente en todas las versiones.

Seguridad del procesador de periféricos en las computadoras Mac

Todos los sistemas computacionales modernos tienen muchos procesadores de periféricos integrados y dedicados a tareas como redes, gráficos, administración de la energía y más. A menudo, estos procesadores de periféricos tienen un solo propósito y son menos potentes que el CPU principal. Los periféricos integrados que no implementan la seguridad suficiente se convierten en un objetivo más fácil de explotar para los atacantes, a través del cual pueden infectar persistentemente el sistema operativo. Después de infectar el firmware del procesador de un periférico, un atacante podría atacar el software del CPU principal o capturar directamente datos confidenciales (por ejemplo, un dispositivo Ethernet podría ver el contenido de los paquetes que no están encriptados).

Siempre que sea posible, Apple trabaja para reducir el número de procesadores de periféricos necesarios o para evitar diseños que requieran firmware. Sin embargo, cuando se requieren procesadores separados con su propio firmware, se hacen esfuerzos para asegurar que los atacantes no puedan persistir en ese procesador. Esto puede realizarse verificando el procesador de una de estas dos formas:

- Al ejecutar el procesador en modo que descargue firmware verificado del CPU principal durante el arranque.
- Al asegurarse de que el procesador de periféricos implemente su propia cadena de arranque seguro para verificar su propio firmware cada vez que se arranque la Mac.

Apple trabaja con los proveedores para auditar sus implementaciones y mejorar sus diseños para que incluyan propiedades deseadas, como las siguientes:

- Asegurar un mínimo de fortalezas criptográficas.
- Asegurar la revocación fiable de firmware malicioso conocido.
- Desactivar las interfaces de depuración.
- Firmar el firmware con claves criptográficas que se almacenen en los módulos de seguridad de hardware (HSM) controlados por Apple.

En los últimos años, Apple ha trabajado con algunos proveedores externos para adoptar las mismas estructuras de datos “Image4”, código de verificación e infraestructura de firma utilizada por los Apple Chips.

Cuando no sea posible operar sin almacenamiento, ni tener almacenamiento con arranque seguro, el diseño obliga a que las actualizaciones del firmware estén firmadas criptográficamente y verificadas antes de que se pueda actualizar el almacenamiento persistente.

Rosetta 2 en una Mac con Apple Chip

Las computadoras Mac con Apple Chip son capaces de ejecutar código compilado para el conjunto de instrucciones x86_64 mediante un mecanismo de traducción llamado *Rosetta 2*. Se ofrecen dos tipos de traducción: en tiempo de ejecución y anticipada.

Traducción en tiempo de ejecución

En la segmentación de traducción en tiempo de ejecución (JIT), un objeto Mach x86_64 se identifica al principio de la ruta de ejecución de la imagen. Cuando se encuentran estas imágenes, el kernel transfiere el control a un código auxiliar de traducción especial de Rosetta en lugar de al editor de enlace dinámico `dyld(1)`. El código auxiliar de traducción luego traduce las páginas x86_64 durante la ejecución de la imagen. Esta traducción se lleva a cabo completamente dentro del proceso, y el kernel sigue verificando los hashes de código de cada página x86_64 mediante la firma de código adjunta al binario cuando la página tiene fallas. En caso de que el hash no coincida, el kernel aplica la política de corrección correspondiente para ese proceso.

Traducción anticipada

En la ruta de traducción anticipada (AOT), los binarios x86_64 se leen desde almacenamiento en los momentos que el sistema considera óptimos para la capacidad de respuesta de ese código. Los artefactos traducidos se escriben en el almacenamiento como un tipo especial de archivo de objeto Mach. Ese archivo es similar a una imagen ejecutable, pero está marcado para indicar que es el producto traducido de otra imagen.

En este modelo, el artefacto AOT deriva toda su información de identidad de la imagen ejecutable x86_64 original. Para aplicar esta vinculación, una entidad del espacio del usuario con privilegios firma el artefacto de traducción utilizando una clave específica del dispositivo que administra el Secure Enclave. Esta clave se entrega exclusivamente a la entidad del espacio del usuario con privilegios, que se identifica como tal mediante una autorización restringida. El directorio de códigos creado para el artefacto de traducción incluye el hash del directorio de códigos de la imagen ejecutable x86_64 original. La firma del artefacto de traducción en sí se conoce como *firma complementaria*.

La segmentación AOT comienza de manera similar a la de JIT, con la transferencia del control del kernel a la ejecución de Rosetta en lugar de al editor de enlace dinámico `dyld(1)`. Pero la ejecución de Rosetta envía después una consulta de comunicación entre procesos (IPC) al servicio del sistema de Rosetta, que pregunta si hay una traducción AOT disponible para la imagen ejecutable actual. Si se encuentra, el servicio de Rosetta ofrece un manejo para esa traducción, y se asigna al proceso y se ejecuta. Durante la ejecución, el kernel aplica los hash del directorio de códigos del artefacto de traducción que se autentican mediante la firma arraigada en la clave de firma específica del dispositivo. Los hash del directorio de códigos de la imagen x86_64 original no están involucrados en este proceso.

Los artefactos traducidos se almacenan en una bóveda de datos a la que ninguna entidad puede acceder durante la ejecución, excepto el servicio de Rosetta. El servicio de Rosetta administra el acceso a su caché mediante la distribución de descriptores de archivos de sólo lectura a artefactos de traducción individuales; esto limita el acceso a la caché de artefactos AOT. La comunicación entre procesos de este servicio y la huella dependiente se mantienen de manera intencional muy estrechas para limitar su superficie de ataque.

Si el hash del directorio de códigos de la imagen x86_64 original no coincide con el codificado en la firma del artefacto de traducción AOT, este resultado se considera el equivalente a una firma de código no válida y se toman las medidas de aplicación apropiadas.

Si un proceso remoto consulta el kernel para obtener las autorizaciones u otras propiedades de identidad del código de un ejecutable traducido a AOT, se devuelven las propiedades de identidad de la imagen x86_64 original.

Contenido de caché de confianza estática

macOS 11 o versiones posteriores cuentan con archivos binarios “fat” o multiarquitectura de Mach que contienen fragmentos de código de computadora x86_64 y arm64. En las computadoras Mac con Apple Chip, el usuario puede decidir ejecutar el fragmento x86_64 de un binario del sistema a través de la segmentación de Rosetta; por ejemplo, para cargar un módulo que no tiene una variante nativa arm64. Para admitir este enfoque, la caché de confianza estática que se envía con macOS, en términos generales, contiene tres hashes de directorio de códigos por cada archivo de objeto Mach:

- Un hash del directorio de códigos del fragmento arm64
- Un hash del directorio de códigos del fragmento x86_64
- Un hash del directorio de códigos de la traducción AOT del fragmento x86_64

El procedimiento de traducción AOT de Rosetta es determinante en el sentido de que produce una salida idéntica para cualquier entrada proporcionada, independientemente de cuándo se realizó la traducción o en qué dispositivo se realizó.

Durante la compilación de macOS, cada archivo de objeto Mach se ejecuta a través de la segmentación de la traducción AOT de Rosetta asociada con la versión de macOS que se está compilando, y el hash del directorio de códigos resultante se registra en la caché de confianza. Por razones de eficacia, los productos traducidos reales no se envían con el sistema operativo y se reconstituyen por solicitud cuando el usuario los solicita.

Cuando se está ejecutando una imagen x86_64 en una computadora Mac con Apple Chip, si el hash del directorio de códigos de esa imagen está en la caché de confianza estática, se espera que el hash del directorio de códigos del artefacto AOT resultante *también* esté en la caché de confianza estática. Dichos productos no están firmados por la clave específica del dispositivo, ya que la autoridad de firma está arraigada en la cadena de arranque seguro de Apple.

Código x86_64 sin firmar

Una computadora Mac con Apple Chip no permite la ejecución del código arm64 nativo a menos que se adjunte una firma válida. Esta firma puede ser tan simple como una firma de código ad hoc (véase `codesign(1)`) que no tiene ninguna identidad real de la mitad secreta de un par de claves asimétricas (es simplemente una medida no autenticada del binario).

Para la compatibilidad binaria, el código x86_64 traducido puede ejecutarse a través de Rosetta sin ninguna información de firma. No se transmite una identidad específica a este código a través del procedimiento de firma del Secure Enclave específico del dispositivo, y se ejecuta exactamente con las mismas limitaciones que el código nativo sin firmar que se ejecuta en computadoras Mac basadas en Intel.

Protecciones del acceso directo a la memoria en las computadoras Mac

Para lograr un alto rendimiento en interfaces de alta velocidad como PCIe, FireWire, Thunderbolt y USB, las computadoras deben ser compatibles con el acceso directo a la memoria (DMA) por parte de los periféricos. Es decir, que deben ser capaces de leer y escribir en la memoria RAM sin que el CPU tenga que involucrarse continuamente. Desde 2012, las computadoras Mac han implementado diversas tecnologías para proteger el DMA, lo que genera el mejor y más completo conjunto de protecciones al DMA en cualquier PC.

Protecciones del acceso directo a la memoria en computadoras Mac con Apple Chip

Los sistemas en chip de Apple contienen una unidad de administración de memoria de entrada/salida (IOMMU) para cada agente DMA en el sistema, incluidos los puertos PCIe y Thunderbolt. Debido a que cada IOMUU tiene su propio conjunto de tablas de traducción de direcciones para traducir las peticiones de DMA, los periféricos conectados mediante PCIe o Thunderbolt pueden acceder sólo a la memoria que se ha asignado específicamente para su uso. Los periféricos no pueden acceder a la memoria que pertenece a otras partes del sistema, como el kernel o el firmware, o la memoria asignada a otros periféricos. Si una IOMMU detecta que un periférico intenta acceder a una memoria que no está asignada para el uso de tal periférico, activará una señal de pánico del kernel.

Protecciones del acceso directo a la memoria en una Mac basada en Intel

En computadoras Mac basadas en Intel con tecnología de virtualización Intel para E/S dirigida (VT-d) inicializar la IOMMU permite la reasignación del DMA y de interrupciones en las primeras etapas del proceso de arranque para mitigar diversos tipos de vulnerabilidades de seguridad. El hardware IOMMU de Apple comienza su operación con una política de negación predeterminada para que, en el momento en que se enciende el sistema, comienza a bloquear automáticamente las solicitudes DMA de los periféricos. Después de que el software la inicializa, la IOMMU comienza a permitir las solicitudes de DMA de los periféricos a las regiones de la memoria que se han asignado explícitamente para su uso.

Nota: la reasignación de interrupciones para PCIe no es necesaria en computadoras Mac con Apple Chip, ya que cada IOMMU maneja los MSI de sus propios periféricos.

A partir de macOS 11, todas las computadoras Mac con el chip de seguridad T2 de Apple ejecutan controladores UEFI que facilitan el acceso directo a la memoria en un entorno de anillo 3 restringido cuando estos controladores se enlazan con dispositivos externos. Esta propiedad ayuda a mitigar las vulnerabilidades de seguridad que pudieran ocurrir cuando un dispositivo malicioso interactúa con un controlador UEFI de forma inesperada al momento del arranque. En particular, reduce el impacto de las vulnerabilidades en el manejo de controladores de los búfers del DMA.

Extensiones de kernel en macOS

A partir de macOS 11, si se activan las extensiones del kernel (kexts) de terceros, estas no se pueden cargar en el kernel por solicitud. En su lugar, se combinan en una *colección del kernel auxiliar* (AuxKC) que se carga durante el proceso de arranque. Para computadoras Mac con Apple Chip, la medición de la AuxKC se registra en LocalPolicy (mientras que para el hardware anterior, la AuxKC reside en el volumen de datos). La reconstrucción de la AuxKC requiere la aprobación del usuario y el reinicio de macOS para cargar las modificaciones en el kernel, y es necesario que el arranque seguro esté configurado como Seguridad reducida.

Importante: ya no se recomienda el uso de kexts en macOS, ya que ponen en riesgo la integridad y fiabilidad del sistema operativo, y Apple recomienda a los usuarios elegir soluciones que no requieran extender el kernel.

Extensiones del kernel en una Mac con Apple Chip

Las kexts deben activarse explícitamente en computadoras Mac con Apple Chip; para esto, mantén presionado el botón de encendido durante el arranque para ingresar al modo One True Recovery (1TR) y luego cambia a Seguridad reducida y marca la casilla para activar las extensiones del kernel. Esta acción también requiere ingresar una contraseña de administrador para autorizar la reducción de seguridad. La combinación del requisito de 1TR y la contraseña dificulta que los atacantes sólo de software que inician dentro de macOS puedan inyectar kexts en macOS, que luego podrían manipular para obtener privilegios para el kernel.

Después de que un usuario autoriza la carga de kexts, se utiliza el flujo de carga de extensiones de kernel aprobadas por el usuario que se explicó anteriormente para autorizar la instalación de kexts. La autorización que se usa para el flujo anterior también se usa para capturar un hash SHA384 de la lista de kexts autorizadas por el usuario (UAKL) en LocalPolicy. El daemon de administración del kernel (`kmd`) es entonces el responsable de validar sólo aquellas kexts que se encuentran en el UAKL para su inclusión en la AuxKC.

- Si la protección de la integridad del sistema (SIP) está activada, la firma de cada kext se verifica antes de incluirse en la AuxKC.
- Si la SIP se desactiva, la firma de la kext no se aplica.

Este enfoque permite flujos de seguridad permisiva en los que los desarrolladores o usuarios que no forman parte del programa de desarrolladores de Apple prueban las kexts antes de que se firmen.

Después de que se crea la AuxKC, su medición se envía al Secure Enclave para firmarse e incluirse en una estructura de datos Image4 que puede ser evaluada por iBoot durante el arranque. Como parte de la construcción de la AuxKC, también se genera una recepción de kext, la cual contiene la lista de kexts que se incluyeron en la AuxKC, ya que el conjunto podría ser un subconjunto de la UAKL en caso de que se encuentren kexts no permitidas. Un hash SHA384 de la estructura de datos Image4 de la AuxKC y la recepción de la kext se incluyen en LocalPolicy. El hash de Image4 de la AuxKC se utiliza para una verificación adicional por parte de iBoot durante el arranque para garantizar que no sea posible arrancar un archivo Image4 de AuxKC más antiguo firmado por el Secure Enclave con una LocalPolicy más nueva. Los subsistemas, tales como Apple Pay, utilizan la recepción de la kext para determinar si hay alguna kext cargada que pudiera interferir con la confiabilidad de macOS. Si la hay, puede que se desactiven las funcionalidades de Apple Pay.

Alternativas a las kexts (macOS 10.15 o versiones posteriores)

macOS 10.15 permite a los desarrolladores extender las capacidades de macOS al instalar y administrar las extensiones del sistema que se ejecutan en el espacio del usuario, en lugar de hacerlo en el nivel del kernel. Al ejecutarse en el espacio del usuario, las extensiones del sistema aumentan la estabilidad y la seguridad de macOS. Aunque las kexts inherentemente tienen acceso total al sistema operativo completo, las extensiones que se ejecutan en el espacio del usuario sólo reciben los privilegios necesarios para realizar sus funciones específicas.

Los desarrolladores pueden usar infraestructuras, como DriverKit, EndpointSecurity y NetworkExtension para escribir en unidades USB y de interfaz humana, herramientas de seguridad de punto final (como agentes de prevención de pérdida de datos u otros agentes de punto final), y herramientas de VPN y redes; todo sin necesitar escribir kexts. Los agentes de seguridad de terceros sólo se deben usar si aprovechan estas API o si tienen un mapa de ruta sólido para hacer la transición hacia ellas, y fuera de las extensiones de kernel.

Carga de extensiones de kernel aprobadas por el usuario

Para mejorar la seguridad, se necesita el consentimiento del usuario para cargar las extensiones de kernel instaladas durante o después de la instalación de macOS 10.13. A este proceso se le conoce como *carga de extensión de kernel aprobada por el usuario*. Se requiere la autorización del administrador para aprobar una extensión de kernel. Las extensiones de kernel no requieren autorización si ocurre lo siguiente:

- Se instalaron en una Mac con macOS 10.12 o versiones anteriores.
- Están reemplazando extensiones aprobadas previamente.
- Tienen permitido cargarse sin el consentimiento del usuario al usar la herramienta de línea de comandos `spctl` disponible cuando se arranca la Mac en recoveryOS.
- Tienen permitido cargarse usando la configuración de la administración de dispositivos móviles (MDM).

  A partir de macOS 10.13.2, los usuarios pueden usar MDM para especificar una lista de extensiones de kernel que se cargue sin el consentimiento del usuario. Esta opción requiere una Mac con macOS 10.13.2 que esté inscrita en una solución MDM ya sea con Apple School Manager, Apple Business Manager o una inscripción a MDM realizada por el usuario.

Seguridad de la ROM de opción en macOS

Nota: las ROM de opción no son compatibles actualmente en computadoras Mac con Apple Chip.

Seguridad de la ROM de opción en una Mac con el chip de seguridad T2 de Apple

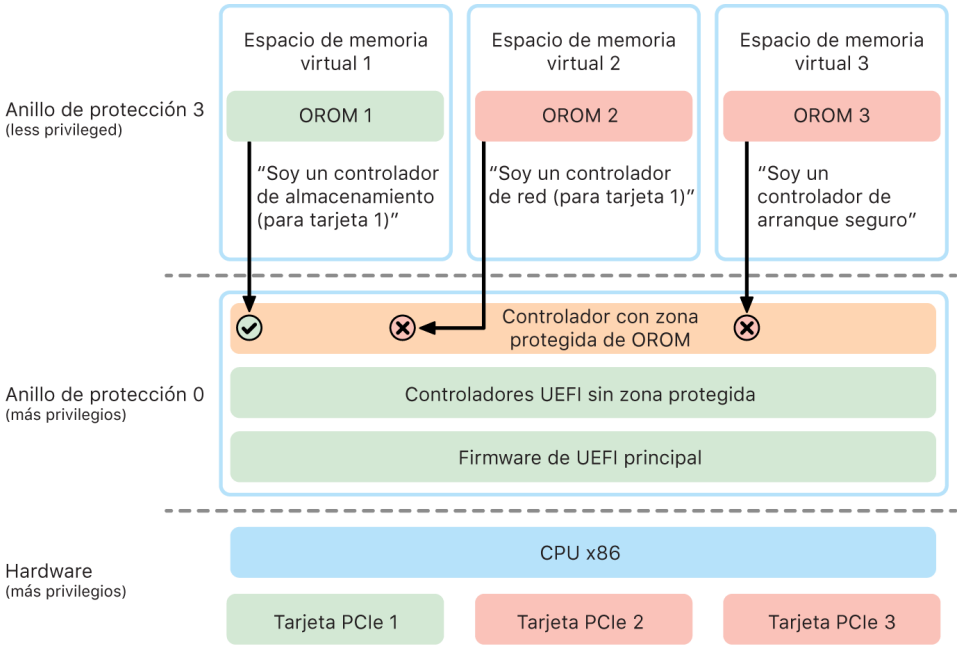
Tanto Thunderbolt como los dispositivos PCIe pueden tener una “ROM de opción” (OROM) conectada físicamente al dispositivo (esta generalmente no es una ROM normal, sino un chip reescribible que almacena firmware). En los sistemas basados en UEFI, el firmware es normalmente un controlador de UEFI, el cual lee y ejecuta el firmware UEFI. El código ejecutado debe inicializar y configurar el hardware desde el que se obtuvo, para que el resto del firmware pueda utilizar el hardware. Esta capacidad es necesaria para que el hardware especializado de terceros pueda cargar y operar durante las fases más tempranas del arranque, por ejemplo, para arrancar desde arreglos de RAID externos.

Sin embargo, como las OROM generalmente son reescribibles, si un atacante sobrescribe la OROM de un periférico legítimo, el código del atacante se ejecutaría temprano en el proceso de arranque y podría alterar el entorno de ejecución y transgredir la integridad del software que se cargue posteriormente. De forma similar, si el atacante introduce su propio dispositivo malicioso al sistema, también podría ejecutar código malicioso.

En macOS 10.12.3, el comportamiento de las computadoras Mac vendidas después de 2011 cambió para que no se ejecuten las OROM de forma predeterminada en el momento en el que la Mac arranca, a menos que se presione una combinación especial de teclas. Esto protege contra las OROM maliciosas que se pudieran introducir inadvertidamente en la secuencia de arranque de macOS. El comportamiento predeterminado de Utilidad Contraseña Firmware también cambió, para que cuando el usuario configure una contraseña para el firmware, las OROM no se puedan ejecutar, incluso si se presiona la combinación de teclas. Esto evita que cualquier atacante físicamente presente introduzca intencionalmente una OROM maliciosa. Para los usuarios que todavía necesitan ejecutar OROM mientras tienen configurada una contraseña de firmware, se puede configurar una opción no predeterminada utilizando la herramienta de línea de comando `firmwarepasswd` en macOS.

Seguridad de zona protegida de OROM

En macOS 10.15, el firmware de UEFI se actualizó para contener un mecanismo para colocar las OROM en la zona protegida y quitarles privilegios. El firmware UEFI normalmente ejecuta todo el código, incluidas las OROM, en el máximo nivel de privilegios de CPU, llamado “anillo 0” y un espacio de memoria virtual única compartida para todos los códigos y datos. Anillo 0 es el nivel de privilegios en el que funciona el kernel de macOS, mientras que el nivel con menores privilegios, anillo 3, es donde se ejecutan las apps. La zona protegida de OROM quita los privilegios a las OROM al usar la separación de la memoria virtual tal como lo hace el kernel, y luego hace que las OROM se ejecuten en el anillo 3.



La zona protegida restringe de forma mucho más significativa las interfaces que las OROM pueden llamar (de forma similar al filtrado de llamadas del sistema en los kernels), y el tipo de dispositivo con el que una OROM se puede registrar (lo que es similar a la aprobación de apps). El beneficio de este diseño es que las OROM maliciosas ya no pueden escribir directamente en ningún lugar dentro de la memoria del anillo 0. En cambio, están limitadas a una interfaz de zona protegida estrecha y bien definida. Esta interfaz limitada reduce significativamente la superficie de ataque, y obliga a los atacantes a tener que salir de la zona protegida y escalar los privilegios.

Seguridad del firmware UEFI en una Mac basada en Intel

Las computadoras Mac basadas en Intel con el chip de seguridad T2 de Apple ofrecen seguridad mediante el firmware UEFI (Intel).

Descripción general

Desde 2006, las computadoras Mac con CPU basado en Intel utilizan un firmware de Intel basado en el kit de desarrollo (EDK) de la interfaz de firmware extensible (EFI) versión 1 o versión 2. El código basado en EDK2 cumple con la especificación de la interfaz de firmware extensible unificada (UEFI). Esta sección se refiere al firmware de Intel como el *Firmware UEFI*. El firmware UEFI fue el primer código que se ejecutó en el chip de Intel.

En las computadoras Mac basadas en Intel que no tienen el chip de seguridad T2 de Apple, la raíz de confianza del firmware UEFI es el chip en donde está almacenado el firmware. Las actualizaciones del firmware UEFI están firmadas digitalmente por Apple, y verificadas por el firmware antes de actualizar el almacenamiento. Para evitar ataques de retroceso, las actualizaciones siempre deben tener una versión más reciente que la existente. Sin embargo, un atacante con acceso físico a la Mac podría potencialmente adjuntar hardware al chip de almacenamiento del firmware y actualizar el chip para integrarle contenido malicioso. De forma similar, si se encuentran vulnerabilidades en el proceso temprano de arranque del firmware UEFI (antes de que el chip de almacenamiento restrinja la escritura), esto también podría ocasionar infecciones persistentes en el firmware UEFI. Esta es una limitación arquitectónica del hardware común en la mayoría de las PC basadas en Intel, y está presente en todas las computadoras Mac basadas en Intel que no tienen el chip T2.

Para ayudar a prevenir ataques físicos que alteran el firmware UEFI, se realizó una reestructuración en las computadoras Mac para arraigar la confianza en el firmware UEFI en el chip T2. En estas computadoras Mac, la raíz de confianza del firmware UEFI es específicamente el firmware T2, como se describe en la sección Proceso de arranque de computadoras Mac basadas en Intel.

Subcomponente Intel Management Engine (ME)

Uno de los subcomponentes que se almacena en el firmware UEFI es el firmware de *Intel Management Engine (ME)*. El ME, un procesador y subsistema separados dentro de los chips Intel, se usa principalmente para la protección de derechos de autor de contenido de audio y video en las Mac que sólo tienen gráficos basados en Intel. Para reducir la superficie de ataque de este subcomponente, las computadoras Mac basadas en Intel ejecutan un firmware ME personalizado del cual se han retirado la mayoría de los componentes. Debido a que el firmware ME de Mac resultante es más pequeño que la versión mínima predeterminada que Intel pone a disposición, muchos componentes que han sido objeto de ataques públicos por parte de investigadores de seguridad en el pasado ya no están presentes.

Modo de administración del sistema (SMM)

Los procesadores Intel tienen un modo especial de ejecución, distinto de la operación normal, llamado *modo de administración del sistema (SMM)*, que originalmente se introdujo para manejar las operaciones en las que el tiempo es muy importante, como la gestión de la energía. Sin embargo, para realizar tales acciones, las computadoras Mac históricamente han utilizado un microcontrolador discreto conocido como el *controlador de administración del sistema (SMC)*. El SMC se ha integrado en el chip T2, por lo que ya no es un microcontrolador separado.

Seguridad del sistema en watchOS

El Apple Watch utiliza muchas de las mismas funcionalidades de seguridad de plataforma basadas en hardware que utilizan iOS y iPadOS. Por ejemplo, el Apple Watch:

- Realiza un arranque seguro y actualizaciones de software seguras.
- Mantiene la integridad del sistema operativo.
- Ayuda a proteger los datos, tanto en el dispositivo como cuando se comunica con un iPhone enlazado o con Internet.

Las tecnologías compatibles incluyen las indicadas en Seguridad del sistema (por ejemplo, KIP, SKP y SCIP), así como las tecnologías de protección de datos, llaveros y redes.

Actualizar watchOS

watchOS puede configurarse para que se actualice durante la noche. Para obtener más información sobre cómo se almacena el código del Apple Watch para su uso durante la actualización, consulta Repositorios de claves.

Detección de la muñeca

Si la detección de muñeca está activada, el dispositivo se bloquea automáticamente poco después de que el usuario se lo quita de la muñeca. Si la detección de muñeca esta desactivada, el centro de control ofrece una opción para bloquear el Apple Watch. Cuando el Apple Watch está bloqueado, se puede usar Apple Pay únicamente si se ingresa el código en el Apple Watch. La detección de la muñeca se desactiva mediante la app Apple Watch del iPhone. Esta configuración también se puede aplicar a través de una solución de administración de dispositivos móviles (MDM).

Bloqueo de activación

Si se activa Encontrar en el iPhone, su Apple Watch enlazado puede utilizar el bloqueo de activación. El bloqueo de activación dificulta el uso o venta del Apple Watch en caso de pérdida o robo. El bloqueo de activación hace que se requiera el Apple ID y la contraseña del usuario para desenlazar, borrar o reactivar el Apple Watch.

Enlazado seguro con iPhone

Un Apple Watch puede estar enlazado con un iPhone a la vez. Cuando un Apple Watch no está enlazado, el iPhone comunica instrucciones para que se borren todos los contenidos y configuraciones del reloj.

El enlace entre el Apple Watch y el iPhone se asegura mediante un proceso fuera de banda para intercambiar claves públicas, seguido del secreto compartido del enlace de Bluetooth de baja energía (BLE). El Apple Watch muestra un patrón animado, que captura la cámara del iPhone. Este patrón contiene un secreto codificado que se utiliza para el enlace fuera de banda de BLE 4.1. En caso necesario, la introducción de la clave de paso de BLE estándar se utiliza como método de enlace de respaldo.

Una vez que se establece y encripta la sesión BLE mediante el protocolo de seguridad más alto disponible en Bluetooth Core Specification, el iPhone y el Apple Watch intercambian las claves mediante lo siguiente:

- Un proceso adaptado del servicio de identidad (IDS) de Apple de la forma que se describe en Descripción general de la seguridad de iMessage.
- Un intercambio de claves mediante IKEv2/IPsec. El intercambio de claves inicial se autentica mediante la clave de sesión de Bluetooth (en casos de enlace) o las claves IDS (en casos de actualización del sistema operativo). Cada dispositivo genera un par de claves Ed25519 de 256 bits públicas y privadas de forma aleatoria, y las claves públicas se intercambian durante el proceso de intercambio de claves inicial.

Nota: El mecanismo utilizado para el encriptado e intercambio de claves varía dependiendo de las versiones del sistema operativo del iPhone y Apple Watch. Los dispositivos iPhone que ejecutan iOS 13 o versiones posteriores que están enlazados con un Apple Watch con watchOS 6 o versiones posteriores usan sólo IKEv2/IPsec para el encriptado e intercambio de claves.

Una vez que se han intercambiado las claves:

- La clave de la sesión Bluetooth se descarta y todas las comunicaciones entre el iPhone y el Apple Watch se encriptan mediante uno de los métodos enumerados antes; y los enlaces encriptados de Bluetooth, Wi-Fi y datos celulares proporcionan una capa de encriptado secundaria.
- En el caso de IKEv2/IPsec, las claves se almacenan en el llavero del sistema y se utilizan para autenticar futuras sesiones IKEv2/IPsec entre los dispositivos. Además, la comunicación entre estos dispositivos está encriptada y protegida en su integridad mediante AES-256-GCM o ChaCha20-Poly1305 (claves de 256 bits) en dispositivos iPhone con iOS 15 o versiones posteriores enlazados con un Apple Watch Series 4 o modelos posteriores con watchOS 8 o versiones posteriores.

La dirección de Bluetooth de baja energía rota en intervalos de 15 minutos para reducir el riesgo del rastreo local del dispositivo si alguien transmite un identificador persistente.

Para admitir las apps que necesitan datos de transmisión en tiempo real, la encriptación se realiza mediante los métodos descritos en Seguridad de FaceTime, que hacen uso del servicio de identidad (IDS) de Apple proporcionado por el iPhone enlazado o una conexión a Internet directa.

El Apple Watch implementa almacenamiento encriptado mediante hardware y protección basada en clases para los archivos y elementos del llavero. Además, también se usan repositorios de claves con control de acceso para los elementos del llavero. Las claves que se utilizan para establecer la comunicación entre el Apple Watch y el iPhone también se aseguran mediante la protección basada en clases. Para obtener más información, consulta Repositorios de claves para la protección de datos.

Desbloqueo automático con Apple Watch

Para mayor comodidad al usar varios dispositivos Apple, algunos dispositivos pueden desbloquear otros automáticamente en determinadas situaciones. El desbloqueo automático admite tres usos:

- Un iPhone puede desbloquear un Apple Watch
- Un Apple Watch puede desbloquear una Mac
- Un Apple Watch puede desbloquear un iPhone cuando se detecta que el usuario utiliza cubrebocas

Los tres casos de uso están basados en el mismo fundamento: un protocolo de estación a estación (STS) autenticado mutuamente, con claves a largo plazo intercambiadas en el momento de la activación de la función y claves de sesión efímeras únicas negociadas para cada solicitud. Independientemente del canal de comunicación subyacente, el túnel STS se negocia directamente entre los Secure Enclave en ambos dispositivos, y todo el material criptográfico se mantiene dentro de ese dominio seguro (con la excepción de las computadoras Mac que no tienen Secure Enclave, que terminan el túnel STS en el kernel).

Desbloqueo

Una secuencia de desbloqueo completa se puede dividir en dos fases: primero, el dispositivo que se desbloquea (el "objetivo") genera un secreto de desbloqueo criptográfico y lo envía al dispositivo que realiza el desbloqueo (el "iniciador"); posteriormente, el iniciador realiza el desbloqueo utilizando el secreto generado previamente.

Para realizar el desbloqueo automático, los dispositivos se conectan entre sí mediante una conexión BLE. Después, mediante el túnel STS, se envía al iniciador un secreto de desbloqueo de 32 bytes generado de forma aleatoria por el dispositivo de destino. Durante el siguiente desbloqueo biométrico o mediante código, el dispositivo de destino envuelve su clave derivada del código (PDK) con el secreto de desbloqueo y descarta el secreto de desbloqueo de su memoria.

Para realizar el desbloqueo, los dispositivos inician una nueva conexión BLE y luego utilizan la red Wi-Fi de punto a punto para aproximar de forma segura la distancia entre ellos. Si los dispositivos están dentro de radio especificado y se cumplen las políticas de seguridad requeridas, el iniciador envía su secreto de desbloqueo al objetivo a través del túnel STS. A continuación, el objetivo genera un nuevo secreto de desbloqueo de 32 bytes y lo devuelve al iniciador. Si el secreto de desbloqueo actual enviado por el iniciador desencripta correctamente el registro de desbloqueo, el dispositivo de destino se desbloquea y la PDK se vuelve a encapsular con un nuevo secreto de desbloqueo. Finalmente, el nuevo secreto de desbloqueo y la PDK se descartan de la memoria del objetivo.

Políticas de seguridad del desbloqueo automático del Apple Watch

Para mayor comodidad, un iPhone puede desbloquear un Apple Watch directamente después del arranque inicial sin necesidad de que el usuario ingrese primero el código en el Apple Watch. Para lograr esto, el secreto de desbloqueo aleatorio (generado durante la primera secuencia de desbloqueo después de la activación de la función) se utiliza para crear un registro de custodia a largo plazo, que se almacena en el repositorio de claves del Apple Watch. El secreto del registro en custodia se almacena en el llavero del iPhone y se usa para iniciar una nueva sesión después de cada reinicio del Apple Watch.

Políticas de seguridad del desbloqueo automático del iPhone

Se aplican políticas de seguridad adicionales para el desbloqueo automático del iPhone con Apple Watch. El Apple Watch no puede usarse en lugar de Face ID en el iPhone para otras operaciones, como para Apple Pay o autorizaciones en apps. Cuando el Apple Watch desbloquea un iPhone enlazado, el reloj muestra una notificación y emite una vibración asociada. Si el usuario toca el botón Bloquear iPhone de la notificación, el reloj envía un comando de bloqueo al iPhone mediante BLE. Cuando el iPhone recibe este comando, se bloquea y desactiva tanto Face ID como el desbloqueo con Apple Watch; y además, el próximo desbloqueo del iPhone deberá realizarse mediante el código de este.

Desbloquear un iPhone enlazado mediante un Apple Watch (cuando está activada la función) requiere que se cumplan los siguientes criterios:

- El iPhone debe haberse desbloqueado con otro método al menos una vez después de que el Apple Watch asociado se haya colocado en la muñeca y se haya desbloqueado.
- Los sensores deben poder detectar que la nariz y la boca están cubiertas.
- La distancia medida debe ser de 2 a 3 metros o menos.
- El Apple Watch no debe estar en la hora de dormir programada.
- El Apple Watch o el iPhone deben haberse desbloqueado recientemente, o bien el Apple Watch debe haber experimentado un movimiento físico que indique que el usuario está activo (por ejemplo, que no está durmiendo).
- El iPhone debe haberse desbloqueado al menos una vez en las últimas 6.5 horas.
- El iPhone debe estar en un estado en el que Face ID tenga permitido realizar un desbloqueo del dispositivo (para obtener más información, consulta Face ID, Touch ID, códigos y contraseñas).

Aprobación con Apple Watch en macOS

Cuando se activa el desbloqueo automático con Apple Watch, el Apple Watch se puede usar en lugar de Touch ID, o junto con él, para aprobar cuadros de diálogos de autenticación o autorización de las siguientes:

- Apps de macOS y de Apple que soliciten autorización
- Apps de terceros que soliciten autenticación
- Contraseñas guardadas de Safari
- Notas seguras

Uso seguro del Wi-Fi, datos celulares, iCloud y Gmail

Cuando el Apple Watch no se encuentre dentro del alcance de Bluetooth, se puede usar Wi-Fi o los datos celulares en su lugar. El Apple Watch se conecta automáticamente a las redes Wi-Fi a las cuales el iPhone enlazado ya había accedido, y a aquellas cuyas credenciales se sincronizaron con el Apple Watch mientras ambos dispositivos estaban dentro del rango. Este comportamiento de conexión automática se puede configurar de manera individual para cada red en la sección Wi-Fi de la app Configuración del Apple Watch. En el caso de las redes Wi-Fi a las que ningún dispositivo se ha conectado, es posible conectarse a ellas en la sección Wi-Fi en la app Configuración del Apple Watch.

Cuando el Apple Watch y el iPhone están fuera del rango, el Apple Watch se conecta directamente a los servidores de iCloud y Gmail para obtener los datos de Mail, en lugar de sincronizar los datos de Mail con el iPhone enlazado mediante el Internet. En el caso de las cuentas de Gmail, el usuario debe ingresar sus credenciales de Google en la sección Mail de la app Reloj en el iPhone. El identificador OAuth proporcionado por Google se enviará al Apple Watch en un formato encriptado mediante el servicio de identidad (IDS) de Apple para usarlo y poder obtener datos de Mail. El identificador OAuth nunca se usa para establecer una conexión con el servidor de Gmail desde el iPhone enlazado.

Generación aleatoria de números

Los generadores de números seudoaleatorios criptográficos (CPRNG) son un elemento importante para construir un software seguro. De este lado, Apple brinda un CPRNG de software de confianza, para ejecutarse en los kernels de iOS, iPadOS, macOS, tvOS y watchOS. Es responsable de agregar entropía sin procesar del sistema y de brindar números aleatorios seguros a los consumidores tanto en el kernel como en el espacio del usuario.

Fuentes de entropía

El CPRNG del kernel se sincroniza a partir de varias fuentes de entropía durante el arranque y el ciclo de vida del dispositivo. Estas incluyen (sujetos a disponibilidad):

- El TRNG del hardware del Secure Enclave
- Fluctuaciones basadas en el tiempo recabadas durante el arranque
- Entropía recolectada de interrupciones en el hardware
- Un archivo semilla utilizado para que la entropía persista a través de los arranques
- Instrucciones aleatorias de Intel (por ejemplo, RDSEED y RDRAND; sólo en Mac basadas en Intel)

El CPRNG del kernel

El CPRNG del kernel es un diseño derivado de Fortuna que se enfoca en un nivel de seguridad de 256 bits. Brinda números aleatorios de alta calidad a los consumidores del espacio del usuario mediante las siguientes API:

- La llamada del sistema de `getentropy`(2)
- El dispositivo aleatorio (/dev/random)

El CPRNG acepta la entropía proporcionada por el usuario mediante escrituras en el dispositivo aleatorio.

Dispositivo de investigación de seguridad de Apple

El dispositivo de investigación de seguridad de Apple es un dispositivo iPhone prototipo específico que permite que los investigadores de seguridad realicen su labor en iOS sin tener que anular o desactivar las funciones de seguridad de la plataforma del iPhone. Con este dispositivo, un investigador puede cargar de forma lateral contenido que se ejecuta con permisos equivalentes a la plataforma y, por lo tanto, permite realizar una investigación en una plataforma que emula más de cerca la de los dispositivos de producción.

Para garantizar que el dispositivo del usuario no resulte afectado por la política de ejecución del dispositivo de investigación de seguridad, los cambios de la política se implementan en una variante de iBoot y en la colección del kernel de arranque. Estos no pueden arrancar en el hardware del usuario. El iBoot de investigación busca un nuevo estado de prototipo y entra en un circuito de pánico si se ejecuta en hardware prototipo que no tenga fines de investigación.

El subsistema criptex permite a los investigadores cargar una caché de confianza personalizada y una imagen de disco con contenido correspondiente. Se han implementado medidas de defensa a fondo diseñadas para asegurar que este subsistema no permita la ejecución en los dispositivos del usuario:

- `launchd` no carga la lista de propiedades de `cryptexd` de launchd si detecta un dispositivo.
- `cryptexd` aborta si detecta un dispositivo de usuario normal.
- `AppleImage4` no proporciona el nonce utilizado para verificar un criptex de investigación si detecta un dispositivo de usuario normal.
- El servidor de firmas rechaza la personalización de imágenes de disco del criptex para un dispositivo que no está explícitamente en la lista autorizada.

Para respetar la privacidad del investigador de seguridad, durante la personalización sólo se envían a Apple las medidas (por ejemplo, los hashes) de los ejecutables o de la caché del kernel y los identificadores del dispositivo de investigación de seguridad. Apple no recibe el contenido del criptex que se carga en el dispositivo.

Para evitar que una parte maliciosa intente enmascarar un dispositivo de investigación como un dispositivo de usuario para engañar a un objetivo para que lo use de forma cotidiana, el dispositivo de investigación de seguridad cuenta con las siguientes diferencias:

- El dispositivo de investigación de seguridad sólo arrancará mientras carga. Para esto se puede usar un cable Lightning o un cargador compatible con Qi. Si el dispositivo no se está cargando durante el arranque, entrará en modo de recuperación. Si el usuario comienza a cargarlo y reinicia el dispositivo, este arrancará en modo normal. En cuanto se inicia XNU, ya no será necesario cargar el dispositivo para que siga funcionando.
- Se muestran las palabras *Dispositivo de investigación de seguridad* debajo del logotipo de Apple durante el arranque de iBoot.
- El kernel XNU arranca en modo detallado.
- El dispositivo se marca en un lado con el mensaje “Propiedad de Apple. Confidencial y privado. Llama al +1 877 595 1125”.

Las siguientes son medidas adicionales que se implementan en el software que aparece después del arranque:

- Se muestran las palabras *Dispositivo de investigación de seguridad* durante la configuración del dispositivo.
- Se muestran las palabras *Dispositivo de investigación de seguridad* en la pantalla bloqueada y en la app Configuración.

El dispositivo de investigación de seguridad permite a los investigadores las siguientes capacidades, las cuales no están disponibles al usuario del dispositivo. Los investigadores pueden:

- Realizar la carga lateral del código ejecutable en el dispositivo con privilegios arbitrarios al mismo nivel que los de los componentes del sistema operativo de Apple.
- Iniciar servicios durante el arranque.
- Cargar contenido persistente entre arranques.
- Usar el derecho `research.com.apple.license-to-operate` para permitir que un proceso depure cualquier otro proceso del sistema, incluidos los procesos del sistema.

  El espacio de nombres `research.` sólo es respetado por la variante RESEARCH de la extensión del kernel AppleMobileFileIntegrity; cualquier proceso con este derecho se termina en el dispositivo del cliente durante la validación de la firma.
- Personalizar y restaurar una caché de kernel personalizada.

Encriptación y protección de datos

Descripción general de la encriptación y protección de datos

La cadena de arranque seguro, la seguridad del sistema y las características de seguridad de las apps ayudan a verificar que sólo las apps y los códigos de confianza se ejecuten en un dispositivo. Los dispositivos Apple tienen funcionalidades adicionales de encriptación que protegen los datos del usuario incluso si otras partes de la infraestructura han sido vulneradas (por ejemplo, si un dispositivo se pierde o si está ejecutando código que no es de confianza). Todas estas funcionalidades ofrecen grandes ventajas tanto a los usuarios como a los administradores de TI, puesto que la información personal y corporativa está protegida y se proporcionan métodos para un borrado remoto, inmediato y completo, en caso de robo o pérdida del dispositivo.

Los dispositivos iOS y iPadOS utilizan una metodología de encriptación de archivos llamada *Protección de datos*, mientras que los datos en las computadoras Mac con procesadores Intel se protegen mediante una tecnología de encriptación de volúmenes llamada *FileVault*. Las computadoras Mac con Apple Chip utilizan un modelo híbrido que es compatible con Protección de datos, pero con dos observaciones: el nivel más bajo de protección Clase D no es compatible; y el nivel predeterminado (Clase C) utiliza una clave de volumen y funciona igual que FileVault en las Mac con procesadores Intel. En todos los casos, las jerarquías de administración de claves tienen su raíz en el silicio dedicado del Secure Enclave; y un motor AES permite la encriptación de velocidad de línea y ayuda a garantizar que las claves de encriptación de vida larga no se expongan al sistema operativo del kernel o al CPU (pues ahí se podrían vulnerar). Una Mac basada en Intel con un T1 o que carece de Secure Enclave no utiliza un silicio dedicado para proteger sus claves de encriptación de FileVault.

Además de utilizar la protección de datos y FileVault para ayudar a impedir el acceso no autorizado a los datos, Apple utiliza *kernels del sistema operativo* para aplicar la protección y seguridad. El kernel utiliza controles de acceso para colocar las apps en un área protegida (que restringe a qué datos puede acceder una app) y un mecanismo llamado *bóveda de datos* (que en lugar de restringir las llamadas que puede realizar una app, restringe el acceso a los datos de una app de todas las otras apps solicitantes).

Códigos y contraseñas

Para proteger los datos de los usuarios de ataques malintencionados, Apple utiliza códigos de acceso en iOS y iPadOS, y contraseñas en macOS. Cuanto más largo sea un código de acceso o una contraseña, más segura será, y más fácil será disuadir los ataques de fuerza bruta. Para desalentar aún más los ataques, Apple aplica tiempos de espera (para iOS y iPadOS) y un número limitado de intentos de contraseña (para Mac).

En iOS y iPadOS, al configurar el código de acceso o la contraseña del dispositivo, el usuario activa automáticamente la protección de datos. La protección de datos también se activa en otros dispositivos que incorporan un sistema en chip (SoC) de Apple, como en las computadoras Mac con Apple Chip, en el Apple TV y en el Apple Watch. En macOS, Apple usa el programa integrado de encriptación de volumen *FileVault*.

Cómo aumentan la seguridad los códigos de acceso y las contraseñas fuertes

iOS y iPadOS admiten códigos de acceso alfanuméricos de seis o cuatro caracteres, y de cualquier longitud. Además de desbloquear el dispositivo, un código o contraseña proporciona entropía para determinadas claves de encriptación. Esto significa que un atacante que haya obtenido un dispositivo no podrá acceder a los datos de clases de protección específicas si no dispone del código.

Este código o contraseña está vinculado al UID del dispositivo, por lo que tendría que realizar ataques de fuerza bruta. Para que cada intento sea más lento, se utiliza un recuento de iteraciones elevado. El recuento de iteraciones se calibra de manera que un intento tarde alrededor de 80 milisegundos. De hecho, se tardaría más de cinco años y medio en intentar todas las combinaciones de un código alfanumérico de seis caracteres con letras en minúscula y números.

Cuanto más seguro sea el código del usuario, más segura será la clave de encriptación. Asimismo, al usar Face ID y Touch ID, el usuario puede establecer un código mucho más seguro en lugar de práctico. Con un código más seguro se consigue aumentar la entropía real que protege las claves de encriptación utilizadas para la protección de datos, sin que se vea perjudicada la experiencia del usuario al desbloquear un dispositivo muchas veces a lo largo del día.

Si se ingresa una contraseña larga compuesta únicamente por números, se mostrará un teclado numérico en la pantalla bloqueada en lugar de un teclado completo. Es posible que sea más fácil ingresar un código numérico largo que un código alfanumérico corto, aunque ambos proporcionen un nivel de seguridad parecido.

Los usuarios pueden especificar un código alfanumérico de mayor longitud seleccionando la opción Código alfanumérico personalizado en Opciones de código desde Configuración > Touch ID y código o Face ID y código.

Cómo el aumento escalado de los tiempos de espera desalienta los ataques de fuerza bruta (iOS y iPadOS)

En iOS y iPadOS, a fin de desalentar aún más los posibles ataques de fuerza bruta, existen tiempos de espera cada vez mayores después de ingresar un código no válido en la pantalla de bloqueo, como se muestra en la siguiente tabla.

Intentos	Demora impuesta
1-4	Ninguno
5	1 minuto
6	5 minutos
7-8	15 minutos
9	1 hora

Si la opción Borrar datos está activada (en Configuración > Touch ID y código), se eliminarán todo el contenido y la configuración del almacenamiento después de 10 intentos fallidos consecutivos de ingresar el código. El límite no toma en cuenta los intentos consecutivos del mismo código incorrecto. Esta configuración, que se puede definir con un umbral inferior, también está disponible como política mediante una solución de administración de dispositivos móviles (MDM) compatible con esta función y a través de Exchange ActiveSync de Microsoft.

En dispositivos con Secure Enclave, las demoras se aplican mediante el Secure Enclave. Si el dispositivo se reinicia durante un tiempo de demora, la demora aún se aplica, con el temporizador empezando de nuevo para el periodo actual.

Cómo el aumento escalado de los tiempos de espera desalienta los ataques de fuerza bruta (macOS)

Para ayudar a impedir los ataques de fuerza bruta, cuando la Mac arranca, no se permiten más de 10 intentos de contraseña en la ventana de inicio de sesión o al usar el modo de disco de destino, y se escala el tiempo de demora de forma obligatoria después de una cantidad dada de intentos incorrectos. Es el Secure Enclave el que impone los tiempos de demora. Si la Mac se reinicia durante un tiempo de demora, la demora aún se aplica, con el temporizador empezando de nuevo para el periodo actual.

La siguiente tabla muestra los tiempos de espera entre intentos de ingreso de contraseña en una computadora Mac con Apple Chip y en una computadora Mac con el chip T2.

Intentos	Demora impuesta
5	1 minuto
6	5 minutos
7	15 minutos
8	15 minutos
9	1 hora
10	Desactivado

Para ayudar a impedir que el malware cause la pérdida permanente de los datos al intentar atacar la contraseña del usuario, estos límites no se imponen una vez que el usuario ha logrado iniciar sesión en la Mac, pero se vuelven a imponer después de un reinicio. Si se terminan los 10 intentos, hay 10 intentos más disponibles después de reiniciar en recoveryOS. Si también se terminan esos intentos, hay disponibles 10 intentos más para cada mecanismo de recuperación de FileVault (recuperación de iCloud, clave de recuperación de FileVault y clave institucional), lo que da un máximo de 30 intentos adicionales. Si se terminan esos intentos adicionales, el Secure Enclave ya no procesará ninguna petición para desencriptar el volumen o verificar la contraseña, y los datos de la unidad ya no se podrán recuperar.

Para ayudar a proteger los datos en un entorno empresarial, el departamento de TI debería definir e imponer políticas de configuración de FileVault utilizando la solución MDM. Las organizaciones tienen varias opciones para administrar los volúmenes encriptados, entre las que se incluyen las claves institucionales, las claves personales de recuperación (que se pueden almacenar de forma opcional en la MDM para su custodia), o una combinación de ambas. La rotación de claves también se puede establecer como política en la MDM.

En una computadora Mac con el chip de seguridad T2 de Apple, la contraseña tiene una función similar, excepto que la clave generada se utiliza para la encriptación de FileVault y no para Protección de datos. macOS también ofrece opciones adicionales de recuperación de contraseñas:

- Recuperación de iCloud
- Recuperación de FileVault
- Clave institucional de FileVault

Protección de datos

Descripción general de la protección de datos

Apple utiliza una tecnología llamada Protección de datos para proteger los datos almacenados en el almacenamiento flash en los dispositivos que cuentan con un SoC de Apple, como el iPhone, iPad, Apple Watch, Apple TV y computadoras Mac con Apple Chip. Con la protección de datos, un dispositivo puede responder ante eventos habituales, como las llamadas de teléfono entrantes, y al mismo tiempo proporcionar un alto nivel de encriptación para los datos del usuario. Algunas apps del sistema (como Mensajes, Mail, Calendario, Contactos, Fotos) y los valores de los datos de Salud usan la protección de datos de forma predeterminada. Las apps de terceros reciben esta protección automáticamente.

Implementación

La protección de datos se implementa mediante la creación y administración de una jerarquía de claves y se basa en las tecnologías de encriptación de hardware integradas en los dispositivos Apple. La protección de datos se controla por archivo, asignando cada archivo a una clase. La accesibilidad se determina dependiendo de si se han desbloqueado o no las claves de la clase. Apple File System (APFS) permite que el sistema de archivos subdivida aún más las claves según la extensión (donde diferentes porciones de un archivo pueden tener diferentes claves).

Cada vez que se crea un archivo en el volumen de datos, la función de protección de datos crea una nueva clave de 256 bits (la *clave por archivo*) y se la proporciona al motor AES de hardware, que utiliza la clave para encriptar el archivo como si se hubiese escrito en la memoria flash. En los dispositivos con chips A14, A15 y la familia M1, la encriptación utiliza AES-256 en modo XTS, donde la clave de archivo de 256 bits pasa por una función de derivación de clave (Publicación especial NIST 800-108) para derivar una modificación de 256 bits y una clave de encriptado de 256 bits. Las generaciones de hardware de A9 a A13, S5, S6 y S7 utilizan AES-128 en modo XTS, donde la clave de archivo de 256 bits se divide para proporcionar una modificación de 128 bits y una clave de encriptado de 128 bits.

En una Mac con Apple Chip, la protección de datos se configura de forma predeterminada como Clase C (véase Clases de protección de datos) pero utiliza una clave de volumen en lugar de una clave por archivo o por extensión, recreando efectivamente el modelo de seguridad de FileVault para los datos del usuario. Los usuarios aún pueden optar por usar FileVault para recibir la protección completa que conlleva entrelazar la jerarquía de claves de encriptado con su contraseña, y los desarrolladores también pueden optar por usar una clase de protección más alta que utilice una clave por archivo o por extensión.

Protección de datos en dispositivos Apple

En dispositivos Apple con Protección de datos, cada archivo está protegido por una clave por archivo (o por extensión) única. La clave, envuelta con el algoritmo de encapsulación de claves NIST AED, se envuelve aún más con una de varias claves de clase, dependiendo de cómo se debe acceder al archivo. La clave por archivo encapsulada se almacena luego en los metadatos del archivo.

Los dispositivos con el formato APFS pueden permitir la clonación de archivos (copias sin costo y que utilizan la tecnología de copia al escribir). Si se clona un archivo, cada mitad del archivo clonado obtiene una clave nueva para aceptar escrituras entrantes, de modo que los datos nuevos se escriben en el contenido con una nueva clave. Con el paso del tiempo, el archivo podría estar compuesto de varias extensiones (o fragmentos), y cada una estaría asignada a una clave diferente. Sin embargo, la misma clave de clase protege todas las extensiones que comprenden un archivo.

Si se abre un archivo, sus metadatos se desencriptan con la clave del sistema de archivos, lo que revela la clave por archivo encapsulada y una anotación sobre la clase que lo protege. La clave por archivo (o por extensión) se desencapsula con la clave de clase y, después, se proporciona al motor AES de hardware, que desencripta el archivo cuando se lee en la memoria flash. La administración de claves de archivos encapsulados se realiza en el Secure Enclave; la clave de archivo nunca se expone directamente al procesador de aplicaciones. Durante el arranque, el Secure Enclave negocia una clave efímera con el motor AES. Cuando el Secure Enclave desencapsula las claves de un archivo, estas vuelven a encapsularse con la clave efímera y se vuelven a enviar al procesador de aplicaciones.

Los metadatos de todos los archivos del sistema de archivos del volumen de datos se encriptan con una clave aleatoria para el volumen, que se crea la primera vez que se instala el sistema operativo o cuando un usuario borra el contenido del dispositivo. La clave se encripta y encapsula mediante una clave de encapsulado de claves que sólo conoce el Secure Enclave para almacenamiento a largo plazo. La clave de encapsulado de claves cambia cada vez que el usuario borra su dispositivo. En los SoC A9 y modelos posteriores, el Secure Enclave se basa en la entropía, respaldada por sistemas antirreproducción, para lograr borrabilidad y proteger su clave de encapsulado de claves, entre otros recursos. Para obtener más información, consulta Almacenamiento no volátil seguro.

Igual que las claves por archivo o por extensión, la clave de metadatos del volumen de datos nunca se expone directamente al procesador de aplicaciones; en su lugar, el Secure Enclave proporciona una versión efímera y única a cada arranque. Cuando se almacena, la clave encriptada del sistema de archivos se encapsula de forma adicional mediante una “clave borrable” almacenada en Effaceable Storage o mediante una clave de encapsulado de claves de contenido protegida por el mecanismo antirreproducción del Secure Enclave. Esta clave no proporciona confidencialidad de datos adicional. En cambio, fue diseñada para permitir su borrado rápido por petición (si el usuario usa la opción Borrar todo el contenido y configuración, o si un usuario o administrador envía un comando de borrado remoto desde una solución de administración de dispositivos móviles (MDM), Microsoft Exchange ActiveSync o iCloud). Al borrar la clave de esta manera, todos los archivos quedan criptográficamente inaccesibles.

El contenido de un archivo puede estar encriptado con una o varias claves por archivo (o por extensión) que se encapsulan con una clave de clase y se almacenan en los metadatos de un archivo, el cual está encriptado con la clave del sistema de archivos. La clave de clase se protege con el UID de hardware y, en el caso de algunas clases, con el código del usuario. Esta jerarquía proporciona flexibilidad y rendimiento. Por ejemplo, para cambiar la clase de un archivo, basta con volver a encapsular su clave por archivo para que luego un cambio de código vuelva a encapsular la clave de clase.

Clases de protección de datos

Cuando se crea un archivo nuevo en un dispositivo compatible con la protección de datos, la app que lo crea le asigna una clase. Cada clase utiliza una política diferente para determinar si se puede acceder a los datos. En las secciones siguientes, se describen las clases y políticas básicas. Las computadoras Mac basadas en Apple Chip no son compatibles con la Clase D: Sin protección, y se establece un límite de seguridad para el inicio y el cierre de sesión (no para el bloqueo o desbloqueo, como en iPhone, iPad y iPod touch).

Clase	Tipo de protección
Clase A: Protección completa	NSFileProtectionComplete
Clase B: Protegido a menos que se abra	NSFileProtectionCompleteUnlessOpen
Clase C: Protegido hasta la primera autenticación del usuario *Nota:* macOS usa una clave de volumen para recrear las funcionalidades de protección de FileVault.	NSFileProtectionCompleteUntilFirstUserAuthentication
Clase D: Sin protección *Nota:* no es compatible con macOS.	NSFileProtectionNone

Protección completa

NSFileProtectionComplete: la clave de clase está protegida con una clave creada a partir del código o contraseña de usuario y el UID del dispositivo. Poco después de que el usuario bloquea un dispositivo (10 segundos, si la opción Solicitar contraseña está configurada como Inmediatamente), se descarta la clave de clase desencriptada y ya no se puede acceder a los datos en esa clase hasta que el usuario vuelva a ingresar el código o desbloquee o inicie sesión en el dispositivo utilizando Face ID o Touch ID.

En macOS, poco después de que se cierra la sesión del último usuario, se descarta la clave de clase desencriptada y ya no se podrá acceder a los datos en esa clase hasta que un usuario vuelva a ingresar el código o inicie sesión en el dispositivo utilizando Touch ID.

Protegido a menos que se abra

NSFileProtectionCompleteUnlessOpen: algunos archivos pueden requerir escritura mientras el dispositivo está bloqueado o el usuario tiene cerrada la sesión. Por ejemplo, al descargar un archivo adjunto de correo en segundo plano. Este proceso se logra utilizando la criptografía de curva elíptica asimétrica (ECDH sobre Curve25519). La clave por archivo usual está protegida por una clave derivada utilizando el acuerdo de clave de Diffie-Hellman de un pase, según se describe en el documento NIST SP 800-56A.

La clave pública efímera del acuerdo se almacena junto a la clave por archivo encapsulada. KDF hace referencia a la función de derivación de claves de concatenación (alternativa aprobada 1), tal como se describe en el apartado 5.8.1 de la publicación SP 800-56A del NIST. AlgorithmID se omite; PartyUInfo y PartyVInfo son las claves públicas efímera y estática, respectivamente; mientras que SHA256 se utiliza como función hash. En cuanto se cierra el archivo, la clave por archivo se borra de la memoria. Para volver a abrir el archivo, se vuelve a crear el secreto compartido mediante la clave privada de la clase Protegido a menos que se abra y la clave pública efímera del archivo; que se usan para desencapsular la clave por archivo que luego se usa para desencriptar el archivo.

En macOS, la parte privada de NSFileProtectionCompleteUnlessOpen se puede acceder siempre y cuando un usuario del sistema esté autenticado o tenga iniciada la sesión.

Protegido hasta la primera autenticación del usuario

NSFileProtectionCompleteUntilFirstUserAuthentication: esta clase se comporta del mismo modo que Protección completa, con la diferencia de que la clave de clase desencriptada no se elimina de la memoria al bloquear el dispositivo o cerrar la sesión del usuario. La protección de esta clase tiene propiedades similares a la encriptación de volumen completo de escritorio y protege los datos frente a ataques que impliquen un reinicio. Esta es la clase predeterminada para todos los datos de apps de terceros que no tengan una clase de protección de datos asignada por otra vía.

En macOS, esta clase utiliza una clave de volumen a la que se puede acceder siempre que el volumen esté montado, y actúa igual que FileVault.

Sin protección

NSFileProtectionNone: esta clave de clase está protegida sólo con el UID y se mantiene en el Effaceable Storage. Dado que todas las claves necesarias para desencriptar los archivos de esta clase se almacenan en el dispositivo, la encriptación sólo agrega la ventaja del borrado remoto rápido. Aunque un archivo no tenga asignada una clase de protección de datos, se almacena en formato encriptado (igual que todos los datos de un dispositivo iOS y iPadOS).

Esto no es compatible con macOS.

Nota: en macOS, para los volúmenes que no corresponden a un sistema operativo arrancado, se puede acceder a todas las clases de protección siempre y cuando el volumen esté montado. La clase de protección de datos predeterminada es NSFileProtectionCompleteUntilFirstUserAuthentication. La funcionalidad de claves por extensión está disponible tanto para Rosetta 2 como para apps nativas.

Repositorios de claves para la protección de datos

Las claves tanto para la clase de protección de datos de llaveros como la de archivos se recopilan y administran en repositorios de claves en iOS, iPadOS, watchOS y tvOS. Estos sistemas operativos utilizan los siguientes repositorios de claves: usuario, dispositivo, respaldo, custodia y respaldo en iCloud.

Repositorio de claves del usuario

En el repositorio de claves del usuario se almacenan las claves de clase encapsuladas que se utilizan durante el funcionamiento normal del dispositivo. Por ejemplo, cuando se ingresa un código, se carga *NSFileProtectionComplete* del repositorio de claves del usuario y se desencapsula. Es un archivo binario de lista de propiedades (.plist) almacenado en la clase Sin protección.

Para dispositivos con SoC anteriores al A9, el contenido del archivo .plist se encripta con una clave contenida en Effaceable Storage. Con el propósito de proporcionar mayor seguridad a los repositorios de claves, esta clave se borra y se vuelve a generar cada vez que un usuario cambia el código.

En los dispositivos con SoC A9 o modelos posteriores, el archivo .plist contiene una clave que indica que el llavero está almacenado en un locker protegido por el valor único de antirreproducción controlado por el Secure Enclave.

El Secure Enclave administra el repositorio de claves del usuario y admite consultas relativas al estado de bloqueo del dispositivo. Indica si el dispositivo está desbloqueado sólo si se puede acceder a todas las claves de clase del repositorio de claves del usuario y si se han desencapsulado correctamente.

Repositorio de claves del dispositivo

El llavero del dispositivo se utiliza para almacenar las claves de clase encapsuladas que se utilizan para operaciones que involucran datos específicos del dispositivo. Los dispositivos iPadOS configurados para el uso compartido a veces necesitan acceso a las credenciales antes de que cualquier usuario haya iniciado sesión y, por lo tanto, se requiere un llavero que no esté protegido por el código del usuario.

iOS y iPadOS no son compatibles con la separación criptográfica del contenido del sistema de archivos por usuario, lo que significa que el sistema utiliza claves de clase del llavero del dispositivo para encapsular las claves por archivo. Sin embargo, el llavero usa las claves de clase del repositorio de claves del usuario para proteger los elementos que se encuentran en el llavero del usuario. En un dispositivo iOS o iPadOS configurado para que lo utilice un único usuario (que es la configuración predeterminada), el repositorio de claves del dispositivo y el repositorio de claves del usuario son el mismo, y están protegidos por el código del usuario.

Repositorio de claves del respaldo

El repositorio de claves de respaldo se crea cuando se realiza un respaldo encriptado desde el Finder (macOS 10.15 o versiones posteriores) o en iTunes (macOS 10.14 o versiones anteriores), y se almacena en la computadora donde se efectúa el respaldo del dispositivo. Se crea un repositorio de claves nuevo con un conjunto de claves nuevo, y los datos del respaldo se vuelven a encriptar en estas claves nuevas. Como se explicó anteriormente, los elementos no migratorios del llavero permanecen encapsulados con la clave derivada del UID, lo que permite su restauración en el dispositivo desde el cual se respaldaron inicialmente, pero se vuelven inaccesibles desde otros dispositivos.

El repositorio de claves, protegido con la contraseña establecida, se ejecuta a través de 10 millones de iteraciones de la función de derivación de claves PBKDF2. A pesar de la gran cantidad de iteraciones, no existen vínculos a un dispositivo específico y, por lo tanto, los ataques de fuerza bruta realizados en paralelo en muchas computadoras tendrían lugar, teóricamente, en el repositorio de claves de respaldo. Esta amenaza se puede mitigar con una contraseña que sea lo suficientemente segura.

Si un usuario opta por no encriptar el respaldo, los archivos del respaldo no se encriptan, sea cual sea su clase de protección de datos, pero el llavero sigue estando protegido con una clave derivada del UID. Por este motivo, los elementos del llavero sólo migran a un dispositivo nuevo cuando se establece una contraseña de respaldo.

Repositorio de claves de custodia

El repositorio de claves de custodia se utiliza para sincronizar con el Finder (macOS 10.15 o versiones posteriores) o con iTunes (macOS 10.14 o versiones anteriores) mediante USB y una administración de dispositivos móviles (MDM). Este repositorio de claves permite que iTunes o el Finder realicen un respaldo y la sincronización sin necesidad de que el usuario ingrese un código, y permite que una solución MDM borre de forma remota el código de un usuario. Se almacena en la computadora usada para la sincronización con iTunes o el Finder, o en la solución MDM que administra el dispositivo de manera remota.

El repositorio de claves de custodia mejora la experiencia del usuario durante la sincronización del dispositivo, que podría requerir el acceso a todas las clases de datos. La primera vez que un dispositivo bloqueado con contraseña se conecta al Finder o a iTunes, el usuario tiene que ingresar un código. A continuación, el dispositivo crea un repositorio de claves de custodia que contiene las mismas claves de clase que se utilizan en el dispositivo, y se protege con una clave recién creada. El repositorio de claves de custodia y la clave que lo protege se dividen entre el dispositivo y el host o servidor, y los datos se almacenan en el dispositivo en la clase Protegido hasta la primera autenticación del usuario. Por eso es necesario ingresar el código del dispositivo antes de que el usuario realice el primer respaldo con el Finder o iTunes después de un reinicio.

En caso de una actualización de software de forma inalámbrica (OTA), el usuario tiene que ingresar su código al inicio del proceso. Este se utiliza para crear de forma segura un identificador de desbloqueo de uso único, que desbloquea el repositorio de claves del usuario después de la actualización. Este identificador no se puede generar si no se ingresa el código de usuario; todos los identificadores generados anteriormente quedan invalidados si se cambia el código de usuario.

Los identificadores de desbloqueo de uso único sirven para instalar con o sin supervisión una actualización de software. Se encriptan con una clave derivada del valor actual de un contador monótono del Secure Enclave, el UUID del repositorio de claves y el UID del Secure Enclave.

En los SoC A9 (y modelos posteriores), el identificador de desbloqueo de uso único ya no depende de conteos o de Effaceable Storage; sino que está protegido por un valor único anti-reproducción controlado por el Secure Enclave.

El identificador de desbloqueo de uso único para actualizaciones de software con supervisión caduca a los 20 minutos. En iOS 13 y iPadOS 13.1, el identificador se almacena en un locker protegido por el Secure Enclave. En sistemas operativos anteriores a iOS 13, este identificador se exportaba desde el Secure Enclave y se escribía en Effaceable Storage o se protegía mediante el mecanismo antirreproducciones del Secure Enclave. Un temporizador de políticas incrementaba el contador si el dispositivo no se había reiniciado en 20 minutos.

Las actualizaciones automáticas se realizan cuando el sistema detecta que hay una actualización disponible y una de las siguientes condiciones es verdadera:

- Las actualizaciones automáticas están activadas en iOS 12 o versiones posteriores.
- El usuario elige Instalar más tarde cuando se le notifica de la actualización.

Después de que el usuario ingresa su código, se genera un identificador de desbloqueo de uso único que puede permanecer válido en el Secure Enclave hasta por 8 horas. Si aún no se realiza la actualización, este identificador de desbloqueo de uso único se destruye en cada bloqueo y se vuelve a crear en cada desbloqueo posterior. Cada desbloqueo restablece el periodo de 8 horas. Después de 8 horas, el temporizador de la política anula el identificador de desbloqueo de uso único.

Repositorio de claves del respaldo en iCloud

El repositorio de claves de respaldo de iCloud es similar al repositorio de claves de respaldo. Todas las claves de clase de este repositorio son asimétricas (utilizan Curve25519, como la clase de protección de datos Protegido a menos que se abra). También se utiliza un repositorio de claves asimétrico para el respaldo en el aspecto de recuperación de llaveros del llavero de iCloud.

Protección de claves en modos de arranque alternos

La protección de datos está diseñada para proporcionar acceso a los datos del usuario sólo después de una autenticación exitosa, y solamente al usuario autorizado. Las clases de protección de datos están diseñadas para admitir una variedad de casos de uso, como la capacidad de leer y escribir algunos datos incluso cuando un dispositivo está bloqueado (pero después del primer desbloqueo). Se toman medidas adicionales para proteger el acceso a los datos del usuario durante los modos de arranque alternativos, como los que se utilizan para el modo de actualización del firmware del dispositivo (DFU), el modo de recuperación, el diagnóstico de Apple o incluso durante la actualización del software. Estas funcionalidades se basan en una combinación de características de hardware y de software, y se han ampliado a medida que evoluciona el silicio diseñado por Apple.

Funcionalidad	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, familia M1
Recuperación: todas las clases de protección de datos están protegidas.	✓	✓	✓	✓	✓
Arranques alternativos del modo DFU, recuperación y actualizaciones de software: las clases A, B y C están protegidas.		✓	✓	✓	✓

El motor AES del Secure Enclave está equipado con bits semilla de software que se pueden bloquear. Cuando las claves se crean desde la UID, estos bits semilla se incluyen en la función de derivación de claves para crear jerarquías de claves adicionales. El uso de los bits semillas varía según el sistema en chip:

- A partir de los SoC A10 y S3 de Apple, se dedica un bit semilla para distinguir las claves protegidas con el código del usuario. El bit semilla se configura para las claves que requieren el código del usuario (incluyendo las claves de clase A, B y C de protección de datos) y se borran las claves que no requieren el código del usuario (incluyendo las claves de metadatos del sistema de archivos y claves de clase D).
- En iOS 13 o versiones posteriores, y iPadOS 13.1 o versiones posteriores en dispositivos con el chip A10 o más reciente, todos los datos del usuario se vuelven criptográficamente inaccesibles cuando los dispositivos se arrancan en el modo de diagnóstico. Esto se logra al introducir un bit semilla adicional, cuya configuración gobierna la capacidad de acceder a la clave de contenidos, la cual es necesaria para acceder a los metadatos (y por lo tanto al contenido de todos los archivos) del volumen de datos encriptado con la protección de datos. Esta protección incluye los archivos protegidos de todas las clases (A, B, C y D), no sólo los que requieren la contraseña del usuario.
- En el SoC A12, la ROM de arranque del Secure Enclave bloquea el bit semilla del código si el procesador de aplicaciones entró al modo de actualización del firmware del dispositivo (DFU) o al Modo de recuperación. Cuando el bit semilla del código está bloqueado, no se permite ninguna operación para cambiarlo, lo que está diseñado para impedir el acceso a los datos protegidos mediante el código del usuario.

Restaurar un dispositivo una vez que entra en modo DFU hace que vuelva a un estado anterior que se sabe que no tiene fallas con la certeza de que contiene sólo el contenido firmado por Apple que no ha sido modificado. Se puede entrar al modo DFU manualmente.

Consulta los siguientes artículos de soporte de Apple sobre cómo poner un dispositivo en modo DFU:

Dispositivo	Artículo
iPhone, iPad, iPod touch	Si olvidaste el código del iPhone
Apple TV	Si ves un símbolo de advertencia en el Apple TV
Una Mac con Apple Chip	Reactivar o restaurar una Mac con Apple Chip

Protección de los datos del usuario ante un ataque

Los atacantes que intentan extraer los datos de usuario a menudo prueban una variedad de técnicas: extraer los datos encriptados a otro soporte para realizar un ataque de fuerza bruta, manipular la versión del sistema operativo o cambiar o debilitar la política de seguridad del dispositivo para facilitar el ataque. Para realizar un ataque en los datos del dispositivo a menudo se requiere comunicarse con el dispositivo mediante interfaces físicas como Lightning o USB, sin embargo, los dispositivos Apple incluyen funciones que ayudan a prevenir estos ataques.

Los dispositivos Apple son compatibles con una tecnología llamada *protección de claves selladas (SKP)* que está diseñada para garantizar que el material criptográfico no esté disponible fuera del dispositivo, y que se utiliza si se realizan manipulaciones en la versión del sistema operativo o en la configuración de seguridad sin la autorización del usuario correspondiente. Esta función *no* la proporciona el Secure Enclave; sino que se basa en registros de hardware que existen en una capa inferior y que proporcionan protección adicional a las claves necesarias para desencriptar los datos de usuario de forma independiente del Secure Enclave.

Nota: la SKP sólo está disponible en dispositivos con SoC diseñados por Apple.

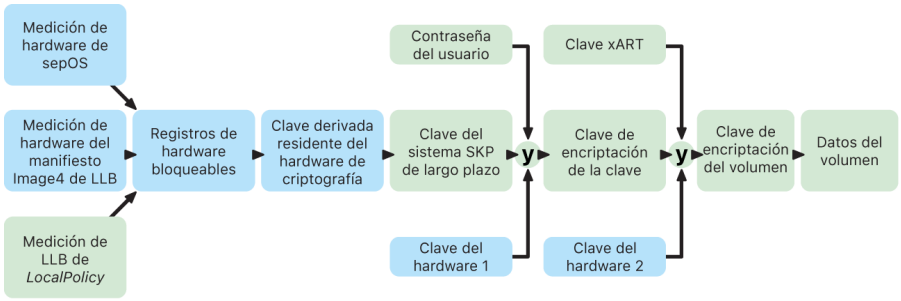
Funcionalidad	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, familia M1
Protección de claves selladas	✓	✓	✓	✓	✓

Los dispositivos iPhone y el iPad también pueden configurarse para activar las conexiones de datos sólo en condiciones que sean más propensas a indicar que el dispositivo aún está bajo el control físico del propietario autorizado.

Protección de claves selladas (SKP)

En dispositivos Apple compatibles con la función de protección de datos, la clave de encriptación de claves (KEK) está protegida (o sellada) con mediciones del software en el sistema y, a su vez, está vinculada al UID que está disponible sólo en el Secure Enclave. En una computadora Mac con Apple Chip, la protección de la KEK se potencia aún más al incorporar información sobre la política de seguridad en el sistema, porque macOS admite cambios críticos en la política de seguridad (por ejemplo, desactivar el arranque seguro o la SIP) que no son compatibles con otras plataformas. En una Mac con Apple Chip, esta protección abarca las claves de FileVault, ya que FileVault se implementa mediante la protección de datos (Clase C).

La clave resultante al combinar la contraseña del usuario, la clave SKP a largo plazo y la clave de hardware 1 (el UID del Secure Enclave) se denomina *clave derivada de la contraseña*. Esta clave se utiliza para proteger el repositorio de claves del usuario (en todas las plataformas compatibles) y la KEK (sólo en macOS), y luego activa el desbloqueo biométrico o el desbloqueo automático con otros dispositivos, como el Apple Watch.



El monitor de arranque del Secure Enclave captura la medición del sistema operativo del Secure Enclave que se carga. Cuando la ROM de arranque del procesador de aplicaciones mide el manifiesto de Image4 adjunto a LLB, ese manifiesto contiene una medición de todo el resto del firmware vinculado con el sistema que también está cargado. LocalPolicy contiene las configuraciones de seguridad básicas para macOS que se cargan, y también contiene el campo `nsih`, que es un hash del manifiesto de Image4 de macOS. El manifiesto de Image4 de macOS contiene mediciones de todo el firmware vinculado con macOS y de los objetos de arranque de macOS centrales, como la colección del kernel de arranque o el hash raíz del volumen del sistema firmado (SSV).

Si un atacante puede cambiar inesperadamente cualquiera de los componentes de configuración de seguridad, software o firmware medidos anteriormente, modifica las medidas almacenadas en los registros del hardware. La modificación de las mediciones ocasiona que la *clave raíz de medición del sistema (SMRK)* derivada del hardware criptográfico obtenga un valor diferente, lo que rompe efectivamente el sello en la jerarquía de claves. Eso causa que la *clave del dispositivo de medición del sistema (SMDK)* sea inaccesible, lo que a su vez hace que la KEK y, por lo tanto, los datos sean inaccesibles.

Sin embargo, cuando el sistema no está bajo ataque, este debe admitir actualizaciones de software legítimas que cambian las medidas de firmware y el campo `nsih` en LocalPolicy para apuntar a nuevas medidas de macOS. En otros sistemas que intentan incorporar medidas de firmware, pero que no cuentan con una fuente de la verdad conocida sólida, el usuario debe desactivar la seguridad, actualizar el firmware y luego volver a activarla para poder capturar una nueva línea de base de medición. Esto aumenta significativamente el riesgo de que el atacante pueda manipular el firmware durante una actualización de software. El hecho de que el manifiesto de Image4 contiene todas las medidas necesarias sirve de ayuda al sistema. El hardware que desencripta la SMDK mediante la SMRK cuando las medidas coinciden durante un arranque normal también puede encriptar la SMDK a una futura SMRK propuesta. Al especificar las medidas que se esperan después de una actualización de software, el hardware puede encriptar una SMDK a la que se puede acceder en el sistema operativo actual, de modo que siga siendo accesible en un sistema operativo futuro. De forma similar, cuando un cliente cambia su configuración de seguridad de forma legítima en LocalPolicy, la SMDK debe encriptarse en la futura SMRK en función de la medición de LocalPolicy, que LLB valoraría en el próximo reinicio.

Activar las conexiones de datos de forma segura en iOS y iPadOS

En dispositivos iOS y iPadOS, si no se ha establecido una conexión de datos recientemente, los usuarios deben usar Face ID, Touch ID o su código para activar las conexiones de datos a través de una interfaz Lightning, USB o Smart Connector. Esto limita la superficie de ataque contra dispositivos conectados físicamente, tales como cargadores malintencionados, y a la vez permite el uso de otros accesorios bajo limitaciones de tiempo razonables. Una hora después del bloqueo del dispositivo iOS o iPadOS, o desde que se desactivó la conexión de datos de un dispositivo, el dispositivo no permitirá que se establezcan nuevas conexiones de datos hasta que se desbloquee el dispositivo. Durante esta hora, sólo se permitirá activar conexiones de datos de accesorios que se hayan conectado previamente al dispositivo cuando este estaba desbloqueado. Estos accesorios se recuerdan por 30 días después de la última conexión. Si se intenta abrir una conexión de datos desde un accesorio desconocido durante este tiempo, se desactivarán todas las conexiones de datos de accesorios mediante el cable Lightning, USB y Smart Connector hasta que el dispositivo se desbloquee de nuevo. Este periodo de una hora:

- Ayuda a garantizar que los usuarios que usan a menudo conexiones con una Mac, PC, accesorios o CarPlay por cable no tengan que ingresar sus códigos cada vez que conecten su dispositivo.
- Esto es necesario porque el ecosistema de accesorios no ofrece una forma criptográficamente segura de identificar los accesorios antes de establecer una conexión de datos.

Además, si transcurren más de tres días desde que se estableció una conexión de datos con un accesorio, el dispositivo no permitirá nuevas conexiones de datos inmediatamente después de bloquearse. Con esta medida se busca aumentar la protección de los usuarios que no usan este tipo de accesorios a menudo. Las conexiones de datos mediante el cable Lightning, USB y Smart Connector también se desactivan cuando el dispositivo está en un estado que requiere un código para reactivar la autenticación biométrica.

El usuario puede optar por volver a activar las conexiones de datos siempre activas en Configuración (configurar algunos dispositivos de asistencia hace esto automáticamente).

El papel de Apple File System

Apple File System (APFS) es un sistema de propiedad exclusiva que se diseñó teniendo en mente la seguridad. Este sistema funciona en todas las plataformas de Apple: iPhone, iPad, iPod touch, Mac, Apple TV y Apple Watch. Optimizado para el almacenamiento Flash/SSD, contiene una encriptación fuerte, metadatos de copia sobre escritura, uso compartido del espacio, clonación de archivos y directorios, instantáneas, dimensionamiento rápido del directorio, primitivos con guardado seguro atómico y fundamentos del sistema de archivos mejorados, así como un diseño copiar al escribir único que utiliza la unión de E/S para brindar un máximo rendimiento a la vez que se asegura la confiabilidad de los datos.

Compartir espacio

APFS asigna el espacio de almacenamiento por solicitud. Cuando un solo contenedor APFS tiene varios volúmenes, se comparte el espacio libre del contenedor y se puede asignar a cualquiera de los volúmenes individuales que se necesite. Cada volumen utiliza únicamente parte del contenedor general, de manera que el espacio disponible es el tamaño total del contenedor menos el espacio utilizado en todos los volúmenes del contenedor.

Volúmenes múltiples

En macOS 10.15 o versiones posteriores, un contenedor APFS utilizado para arrancar la Mac debe contener al menos cinco volúmenes, y los tres primeros están ocultos para el usuario:

- *Volumen de prearranque:* este volumen está desencriptado y contiene los datos necesarios para arrancar cada volumen del sistema en el contenedor.
- *Volumen de máquina virtual:* este volumen está desencriptado, y macOS lo utiliza para almacenar archivos de intercambio encriptados.
- *Volumen de recuperación:* este volumen está desencriptado y debe estar disponible sin desbloquear un volumen del sistema para poder arrancar en recoveryOS.
- *Volumen del sistema:* contiene lo siguiente:
  - Todos los archivos necesarios para encender la Mac
  - Todas las apps instaladas de forma nativa por macOS (las apps que solían estar en la carpeta /Aplicaciones ahora están en /Sistema/Aplicaciones)

  Nota: de forma predeterminada, ningún proceso puede escribir en el volumen del sistema, ni siquiera los procesos de Apple.
- *Volumen de datos:* contiene datos que están sujetos a cambios, como por ejemplo:
  - Cualquier dato dentro de la carpeta del usuario, incluyendo fotos, música, videos y documentos
  - Las apps que el usuario instaló, incluyendo AppleScript, y las aplicaciones de Automator
  - Infraestructuras y daemons personalizados instalados por el usuario, la organización o apps de terceros
  - Otras ubicaciones propiedad del usuario y que permiten escritura, como /Aplicaciones, /Biblioteca, /Usuarios, /Volúmenes, /usr/local, /private, /var y /tmp

Se crea un volumen de datos por cada volumen del sistema adicional. Los volúmenes de recuperación, máquina virtual y prearranque son compartidos y no duplicados.

En macOS 11 o versiones posteriores, el volumen del sistema viene capturado en una instantánea. El sistema operativo se arranca desde una instantánea del volumen del sistema, no sólo desde un montaje de sólo lectura del volumen del sistema mutable.

En iOS y iPadOS, el almacenamiento se divide en al menos dos volúmenes APFS:

- Volumen del sistema
- Volumen de datos

Protección de datos del llavero

Muchas apps necesitan administrar contraseñas y otros datos pequeños pero confidenciales, como las claves o los identificadores de inicio de sesión, y el llavero constituye un sistema seguro para almacenar estos elementos. Los diversos sistemas operativos de Apple utilizan diferentes mecanismos para aplicar las garantías asociadas con las diferentes clases de protección de llaveros. En macOS (incluidas las computadoras Mac con Apple Chip), la protección de datos no se utiliza directamente para aplicar estas garantías.

Descripción general

Los elementos del llavero se encriptan usando dos claves AES-256-GCM diferentes: una clave de tabla (metadatos) y una clave por fila (clave secreta). Los metadatos del llavero (todos los atributos que no sean kSecValue) se encriptan usando la clave de metadatos con el fin de acelerar las búsquedas; mientras que el valor secreto (kSecValueData) se encripta usando la clave secreta. La clave de metadatos está protegida por el Secure Enclave, pero se almacena en la caché del procesador de aplicaciones para permitir solicitudes rápidas del llavero. La clave secreta siempre requiere un ciclo entero a través del Secure Enclave.

El llavero se implementa como una base de datos SQLite almacenada en el sistema de archivos. Sólo hay una base de datos, y el daemon `securityd` determina a qué elementos del llavero puede acceder cada proceso o app. Las API de Acceso a Llaveros generan llamadas al daemon, que envía una consulta a las autorizaciones “keychain-access-groups”, “application-identifier” y “application-group” de la app. En lugar de limitar el acceso a un solo proceso, los grupos de acceso permiten que los elementos del llavero se compartan entre apps.

Los elementos del llavero sólo se pueden compartir entre las apps de un mismo desarrollador. Para compartir elementos del llavero, las apps de terceros usan grupos de acceso con un prefijo asignado a través del programa para desarrolladores de Apple en sus grupos de aplicaciones. El requisito de prefijo y la exclusividad del grupo de aplicaciones se aplican mediante la firma de código, perfiles de datos y el programa para desarrolladores de Apple.

Los datos del llavero se protegen con una estructura de clases similar a la utilizada en la protección de datos de archivo. Estas clases tienen comportamientos equivalentes a las clases de protección de datos de archivo, pero utilizan funciones y claves distintas.

Disponibilidad	Protección de datos de archivo	Protección de datos del llavero
Cuando está desbloqueado	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Cuando está bloqueado	NSFileProtectionCompleteUnlessOpen	N/A
Después del primer desbloqueo	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Siempre	NSFileProtectionNone	kSecAttrAccessibleAlways
Código activado	N/A	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

Las apps que utilizan servicios de actualización en segundo plano pueden usar *kSecAttrAccessibleAfterFirstUnlock* para los elementos del llavero a los que sea necesario acceder durante este tipo de actualizaciones.

La clase *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* muestra el mismo comportamiento que *kSecAttrAccessibleWhenUnlocked*; sin embargo, está disponible sólo cuando el dispositivo está configurado con un código. Esta clase existe únicamente en el repositorio de claves del sistema, el cual:

- No se sincroniza con el llavero de iCloud;
- No se respalda;
- No se incluye en el repositorio de claves de custodia.

Si se elimina o restablece el código, se descartan las claves de clase y los elementos dejan de ser útiles.

Otras clases de llavero tienen un equivalente a Sólo este dispositivo que siempre está protegido con el UID cuando se copia de un dispositivo durante un respaldo, de modo que deja de ser útil si se restaura en otro dispositivo. Apple ha equilibrado la seguridad y la capacidad de uso cuidadosamente mediante la selección de clases de llavero que dependen del tipo de información que se esté protegiendo y de cuándo la necesite iOS y iPadOS. Por ejemplo, un certificado VPN debe estar disponible en todo momento para que el dispositivo esté continuamente conectado, pero se clasifica como “no migratorio” para evitar que se pueda trasladar a otro dispositivo.

Protecciones de las clases de datos del llavero

Las protecciones de clase que se enumeran a continuación se aplican a los elementos del llavero.

Elemento	Accesible
Contraseñas de Wi-Fi	Después del primer desbloqueo
Cuentas de Mail	Después del primer desbloqueo
Cuentas de Exchange ActiveSync de Microsoft	Después del primer desbloqueo
Contraseñas de VPN	Después del primer desbloqueo
LDAP, CalDAV y CardDAV	Después del primer desbloqueo
Identificadores de cuentas de redes sociales	Después del primer desbloqueo
Claves de encriptación de anuncios de Handoff	Después del primer desbloqueo
Identificador de iCloud	Después del primer desbloqueo
Claves de iMessage	Después del primer desbloqueo
Contraseña de Compartir en casa	Cuando está desbloqueado
Contraseñas de Safari	Cuando está desbloqueado
Marcadores de Safari	Cuando está desbloqueado
Respaldo de iTunes/Finder	Cuando está desbloqueado; no migratorio
Claves privadas instaladas por un perfil de configuración	Cuando está desbloqueado; no migratorio
Certificados VPN	Siempre; no migratorio
Claves de Bluetooth®	Siempre; no migratorio
Identificador de servicio de notificaciones push de Apple (APNs)	Siempre; no migratorio
Clave privada y certificados de iCloud	Siempre; no migratorio
PIN de la SIM	Siempre; no migratorio
Certificados instalados por un perfil de configuración	Siempre
Identificador de Encontrar	Siempre
Buzón de voz	Siempre

Control de acceso al llavero

Los llaveros pueden utilizar listas de control de acceso (ACL) para establecer políticas de accesibilidad y requisitos de autenticación. Los elementos pueden establecer condiciones que requieran la presencia del usuario al especificar que no se puede acceder a ellos a menos que se lleve a cabo una autenticación con Face ID, Touch ID o que se ingrese el código o la contraseña del dispositivo. De igual manera, se puede limitar el acceso a los elementos al especificar que el registro de Face ID o Touch ID no puede haber cambiado desde que el elemento se agregó. Esta limitación ayuda a prevenir que un atacante agregue su propia huella digital para acceder al elemento de llavero. Las ACL se evalúan en el Secure Enclave y sólo se desbloquean en el kernel si se cumplen las restricciones especificadas.

Arquitectura del llavero en macOS

macOS también ofrece acceso al llavero para almacenar de forma segura y conveniente nombres de usuario y contraseñas, identidades digitales, claves de encriptación y notas seguras. Se puede acceder al abrir la app Acceso a Llaveros en Aplicaciones/Utilidades/. Al usar el llavero, se elimina la necesidad de ingresar (o incluso recordar) las credenciales de cada recurso. Se crea un llavero inicial predeterminado para cada usuario de la Mac, pero los usuarios pueden crear otros llaveros para fines específicos.

Además de depender de los llaveros del usuario, macOS se basa en diversos llaveros a nivel del sistema que mantienen los recursos de autenticación que no son específicos para el usuario, como las credenciales de la red y las identidades de la infraestructura de la clave pública (PKI). Uno de estos llaveros, System Roots, es inmutable y almacena los certificados de la autoridad certificadora (CA) de la raíz del PKI de Internet para facilitar tareas comunes como usar la banca en línea y el comercio electrónico. El usuario puede implementar internamente de forma similar los certificados de CA provistos para las computadoras Mac administradas, para ayudar a validar sitios y servicios internos.

FileVault

Encriptación del volumen con FileVault en macOS

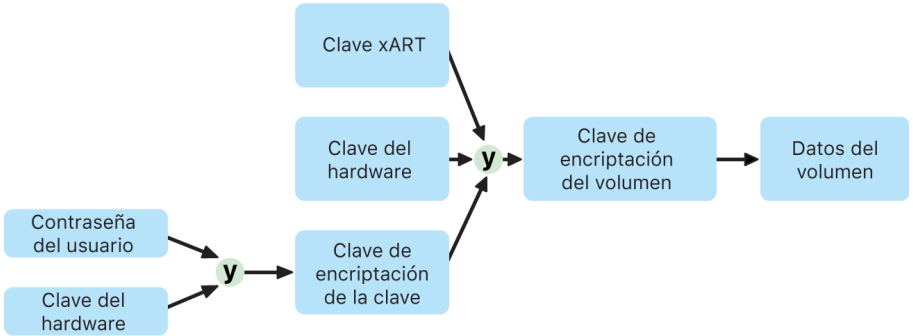
Las computadoras Mac ofrecen FileVault, una funcionalidad de encriptación integrada capaz de dar seguridad a todos los datos que no se estén utilizando. FileVault utiliza el algoritmo de encriptación de datos AES-XTS para proteger volúmenes completos en dispositivos de almacenamiento internos y extraíbles.

FileVault en las computadoras Mac con Apple Chip se implementa en realidad utilizando la clase C de protección de datos con una clave de volumen. En computadoras Mac con el chip de seguridad T2 de Apple, así como computadoras Mac con Apple Chip, los dispositivos de almacenamiento interno encriptados directamente y conectados al Secure Enclave aprovechan las funcionalidades de seguridad del hardware, así como las del motor AES. Cuando un usuario activa FileVault en una Mac, requerirá brindar sus credenciales durante el proceso de arranque.

Almacenamiento interno con FileVault activado

Sin las credenciales de acceso válidas o la clave criptográfica de recuperación, los volúmenes APFS internos permanecen encriptados y protegidos del acceso no autorizado, incluso si el dispositivo de almacenamiento se retira físicamente y se conecta a otra computadora. En macOS 10.15, esto incluye tanto el volumen del sistema como el volumen de datos. A partir de macOS 11, el volumen del sistema está protegido mediante la función de volumen del sistema firmado (SSV), pero el volumen de datos permanece protegido mediante encriptación. La encriptación del volumen interno en computadoras Mac con Apple Chip, así como en las que cuentan con el chip T2, se implementa al construir y administrar una jerarquía de claves, y se crea sobre la base de las tecnologías de encriptación de hardware integradas en el chip. Esta jerarquía de claves está diseñada para lograr cuatro metas de forma simultánea:

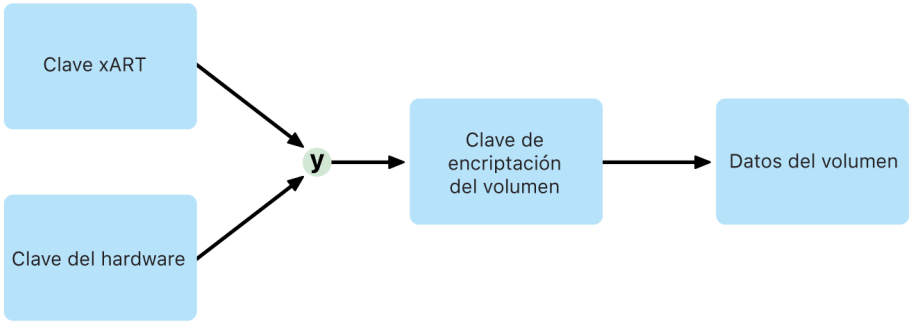
- Requerir la contraseña del usuario para desencriptar.
- Proteger el sistema de un ataque de fuerza bruta hecho directamente contra un medio de almacenamiento retirado de la Mac.
- Brindar un método rápido y seguro de borrar el contenido mediante la eliminación del material criptográfico necesario.
- Permitir a los usuarios cambiar su contraseña (y por lo tanto, las claves criptográficas utilizadas para proteger sus archivos) sin tener que volver a encriptar todo el volumen.



En computadoras Mac con Apple Chip y aquellas que cuentan con el chip T2, el manejo completo de las claves de FileVault se realiza en el Secure Enclave; las claves de encriptación nunca se exponen directamente al CPU de Intel. Todos los volúmenes APFS se crean de forma predeterminada con una clave de encriptación de volumen. El contenido del volumen y de los metadatos se encripta con esta clave de encriptación de volumen, la cual se encapsula con la clave de clase. La clave de clase está protegida por una combinación de la contraseña del usuario y el UID del hardware cuando se activa FileVault.

Almacenamiento interno con FileVault desactivado

Si durante el proceso inicial del asistente de configuración no se activa FileVault en una Mac con Apple Chip o en una que tiene el chip T2, el volumen seguirá estando encriptado, pero la clave de encriptación del volumen sólo estará protegida por el UID del hardware en el Secure Enclave.



Si FileVault se activa después (un proceso que es inmediato, puesto que los datos ya estaban encriptados), un mecanismo antirreproducción ayuda a evitar que la clave anterior (basada únicamente en el UID del hardware) se pueda utilizar para desencriptar el volumen. El volumen quedará protegido por una combinación de la contraseña del usuario y el UID del hardware, como se describió anteriormente.

Eliminar volúmenes de FileVault

Al eliminar un volumen, el Secure Enclave elimina de forma segura su clave de encriptación del volumen, lo que ayuda a evitar el acceso futuro con esta clave, incluso por parte del Secure Enclave. Además, todas las claves de encriptación se encapsulan con una clave de contenidos. Esta clave de contenidos no brinda confidencialidad adicional a los datos; en lugar de ello, está diseñada para permitir la eliminación rápida y segura de los datos, pues sin ella es imposible desencriptar.

En computadoras Mac con Apple Chip y aquellas que cuentan con el chip T2, se garantiza que la clave de contenidos se borrará mediante la tecnología compatible del Secure Enclave, por ejemplo, mediante comandos MDM remotos. Al borrar la clave de contenidos de esta manera, el volumen queda criptográficamente inaccesible.

Dispositivos de almacenamiento extraíbles

La encriptación de dispositivos extraíbles de almacenamiento no utiliza las funcionalidades de seguridad del Secure Enclave y se realiza de la misma forma que en las computadoras Mac basadas en Intel que no tienen el chip T2.

Administración de FileVault en macOS

En macOS, las organizaciones pueden administrar FileVault mediante SecureToken o el identificador Bootstrap.

Utilizar el identificador seguro

Apple File System (APFS), en macOS 10.13 o versiones posteriores, cambia la forma en la que se generan las claves de encriptación de FileVault. En versiones anteriores de macOS en volúmenes CoreStorage, las claves utilizadas en el proceso de encriptación de FileVault se creaban cuando el usuario o la organización activaba FileVault en una Mac. En macOS en volúmenes APFS, las claves se generan ya sea durante la creación del usuario, al configurar la primera contraseña del usuario, o durante el primer inicio de sesión del usuario de la Mac. Esta implementación de las claves de encriptación, cuándo se generan, y la forma en la que se almacenan son parte de una función conocida como *Identificador seguro*. Específicamente, un identificador seguro es una versión encapsulada de una clave de encriptación clave (KEK) protegida por la contraseña del usuario.

Al implementar FileVault en APFS, el usuario puede:

- Utilizar las herramientas y procesos existentes, como almacenar una clave personal de recuperación (PRK) con una solución de administración de dispositivos móviles (MDM) para tenerla en custodia.
- Crear y usar una clave institucional de recuperación (IRK).
- Aplazar la activación de FileVault hasta que un usuario inicie o cierre sesión en la Mac.

En macOS 11, establecer la contraseña inicial para el primer usuario en la Mac genera la concesión de un identificador seguro para el usuario. En algunos flujos de trabajo, puede que ese no sea el comportamiento deseado, como se explicó anteriormente, otorgar el primer identificador seguro habría requerido que la cuenta de usuario inicie sesión. Para evitar que esto suceda, agrega `;DisabledTags;SecureToken` al atributo `AuthenticationAuthority` del usuario creado mediante programación antes de configurar la contraseña del usuario, como se muestra a continuación:

```
sudo dscl . append /Users/<user name> AuthenticationAuthority
";DisabledTags;SecureToken"
```

Utilizar el identificador Bootstrap

macOS 10.15 introduce una funcionalidad nueva, el *identificador Bootstrap*, para ayudar a otorgar un identificador seguro tanto a las cuentas móviles como a la cuenta de administrador opcional creada por la inscripción del dispositivo (“administrador administrado”). En macOS 11, un identificador Bootstrap puede otorgar un identificador seguro a cualquier usuario que inicie sesión en una computadora Mac, incluidas las cuentas de usuario locales. Para utilizar la funcionalidad del identificador Bootstrap de macOS 10.15 se requiere lo siguiente:

- Que la Mac se inscriba en la MDM utilizando Apple School Manager o Apple Business Manager, lo que la convierte en supervisada
- Soporte por parte del proveedor de la MDM

En macOS 10.15.4 o versiones posteriores, cuando inicia sesión un usuario que tiene el identificador seguro activado, se genera un identificador Bootstrap y se pone en custodia de la solución MDM (si la solución MDM admite la función). De ser necesario, también puede generarse un identificador Bootstrap y ponerse en custodia de la solución MDM usando la línea de comandos `profiles`.

En macOS 11, un identificador Bootstrap también se puede utilizar para más que sólo otorgar un identificador seguro a las cuentas de usuario. En computadoras Mac con Apple Chip, un identificador Bootstrap, si está disponible, se puede utilizar para autorizar la instalación de las extensiones del kernel y las actualizaciones de software cuando se administra mediante MDM.

Cómo Apple protege los datos personales de los usuarios

Protección del acceso de las apps a los datos de usuario

Además de encriptar los datos que no están en uso, los dispositivos Apple evitan que las apps accedan sin permiso a la información personal del usuario mediante varias tecnologías, incluidas las bóvedas de datos. En Configuración en iOS y iPadOS, o en Preferencias del Sistema en macOS, los usuarios pueden ver cuáles son las apps a las que han otorgado acceso a determinada información, así como conceder o revocar permisos para cualquier acceso futuro. Este acceso se aplica en lo siguiente:

- *iOS, iPadOS y macOS:* Calendarios, cámara, contactos, micrófono, fotos, recordatorios y reconocimiento de voz.
- *iOS y iPadOS:* Bluetooth, Casa, contenido, apps de contenido, Apple Music, movimiento y condición física.
- *iOS y watchOS:* Salud.
- *macOS:* Monitoreo de entradas (por ejemplo, presiones del teclado), mensajes emergentes, grabaciones de pantalla (por ejemplo, capturas de pantalla estáticas y video) y Preferencias del Sistema.

En iOS 13.4 o versiones posteriores, y iPadOS 13.4 o versiones posteriores, todas las apps de terceros tienen sus datos protegidos de forma automática en una bóveda de datos. Esta ayuda a proteger contra el acceso no autorizado a los datos, incluso de procesos que no están en el área protegida. Las clases adicionales en iOS 15 o versiones posteriores incluyen Red local, Interacciones cercanas, Datos de uso y sensores de Investigación, y Enfoque.

Si el usuario inicia sesión en iCloud, las apps en iOS y iPadOS tendrán permiso de acceso a iCloud Drive de forma predeterminada. Los usuarios pueden controlar el acceso de cada app en Configuración > iCloud. Además, iOS y iPadOS también proporcionan restricciones que están diseñadas para impedir la transferencia de datos entre las apps y las cuentas instaladas mediante una solución de administración de dispositivos móviles (MDM) y aquellas que haya instalado el usuario.

Protección del acceso a los datos de salud del usuario

HealthKit ofrece un repositorio central de datos de salud y condición física en iPhone y Apple Watch. HealthKit también funciona directamente con dispositivos de salud y condición física, tales como monitores de frecuencia cardiaca compatibles con Bluetooth de baja energía (BLE) o el coprocesador de movimiento integrado en muchos de los dispositivos iOS. Todas las interacciones de HealthKit con apps de salud y condición física, instituciones médicas y dispositivos de salud y condición física requieren el permiso del usuario. Estos datos se almacenan en la clase de protección de datos Protegido a menos que se abra. El acceso a los datos se deniega 10 minutos después de que el dispositivo se bloquea. Para volver a acceder a los datos, el usuario debe desbloquear el dispositivo ingresando su código o mediante Face ID o Touch ID.

Recopilar y almacenar datos de salud y condición física

HealthKit también recopila y almacena datos de administración, como permisos de acceso para apps, nombres de dispositivos conectados a HealthKit e información de programación utilizada para abrir apps cuando hay datos nuevos disponibles. Estos datos se almacenan en la clase de protección de datos Protegido hasta la primera autenticación de usuario. Los archivos de registro temporales almacenan los datos de salud que se generan cuando el dispositivo está bloqueado, por ejemplo, cuando el usuario está haciendo ejercicio. Estos datos se almacenan en la clase de protección de datos Protegido a menos que se abra. Cuando el dispositivo está desbloqueado, los archivos de registro temporales se importan a las bases de datos de salud principales y se eliminan una vez que termina la asociación.

Los datos de salud se pueden almacenar en iCloud. La encriptación de extremo a extremo de los datos de Salud requiere iOS 12 o versiones posteriores y la autenticación de dos factores. De lo contrario, los datos del usuario se encriptan en el almacenamiento y la transmisión, pero no se encriptan de extremo a extremo. Después de activar la autenticación de dos factores y actualizar a iOS 12 o versiones posteriores, los datos de salud del usuario migran a la encriptación de extremo a extremo.

Si el usuario respalda su dispositivo usando el Finder (macOS 10.15 o versiones posteriores) o iTunes (macOS 10.14 o versiones anteriores), los datos de salud sólo se almacenan si el respaldo está encriptado.

Registros de salud clínicos

Los usuarios pueden iniciar sesión en sistemas de salud compatibles dentro de la app Salud para obtener una copia de sus expedientes clínicos. Al conectar al usuario a un sistema de salud, el usuario verifica su identidad utilizando credenciales del cliente OAuth 2. Una vez establecida la conexión, los expedientes clínicos se descargan directamente de la institución de salud mediante una conexión protegida con TLS 1.3. Una vez que termina la descarga, los expedientes clínicos se almacenan junto con otros datos de salud.

Integridad de los datos de salud

En la base de datos, también se almacenan metadatos para hacer un seguimiento de la procedencia de cada registro de datos. Estos metadatos incluyen un identificador de app que identifica la app que almacenó el registro. Además, otros metadatos opcionales pueden contener un respaldo con firma digital. El objetivo es proporcionar integridad de datos para los registros generados por un dispositivo de confianza. La firma digital está en el formato de sintaxis de mensajes criptográficos (CMS) que se especifica en la RFC 5652 del IETF.

Acceso a los datos de Salud por parte de apps de terceros

El acceso a la API de HealthKit se controla mediante autorizaciones, y las apps deben respetar las restricciones relativas al uso de los datos. Por ejemplo, las apps no pueden utilizar los datos de salud para fines publicitarios. Además las apps tienen que proporcionar a los usuarios una política de privacidad donde se especifique el uso que hacen de los datos de salud.

El acceso de las apps a los datos de salud se controla mediante la configuración de privacidad del usuario. Los usuarios tienen que otorgar acceso a los datos de salud cuando las apps lo solicitan, igual que en el caso de Contactos, Fotos y otras fuentes de datos de iOS. Sin embargo, en el caso de los datos de salud, el acceso que reciben las apps para lectura de datos es independiente del de escritura y también es independiente por cada tipo de datos de salud. Los usuarios pueden ver y revocar los permisos que se les hayan concedido para el acceso a datos de Salud en Configuración > Salud > Dispositivos y accesos de datos.

Si disponen de permiso para escribir datos, las apps también pueden leer los datos que escriban. Si disponen de permiso para leer datos, las apps pueden leer los datos escritos por todas las fuentes. Sin embargo, las apps no pueden saber el acceso que tienen otras apps. Además, las apps no pueden saber con seguridad si disponen de acceso de lectura a los datos de salud. Cuando una app no tiene acceso de lectura, las consultas no devuelven datos, al igual que sucede cuando una base de datos está vacía. Esto está diseñado para evitar que las apps infieran el estado de salud del usuario al conocer el tipo de datos que este registra.

Ficha médica para los usuarios

La app Salud permite a los usuarios llenar un formulario con sus datos médicos e información que pueda ser importante durante una emergencia médica. La información se ingresa o actualiza manualmente y no se sincroniza con la información de las bases de datos de salud.

Para ver la información de Ficha médica, basta con presionar el botón SOS en la pantalla bloqueada. La información se almacena en el dispositivo con la clase de protección de datos Sin protección, de modo que se pueda acceder a ella sin necesidad de ingresar el código del dispositivo. Ficha médica es una función opcional que permite a los usuarios decidir cómo conseguir un equilibrio entre seguridad y privacidad. Estos datos se respaldan mediante Respaldo en iCloud en iOS 13 o versiones anteriores. En iOS 14, la ficha médica se sincroniza entre dispositivos usando CloudKit y tiene las mismas características de encriptado que el resto de los datos de salud.

Compartir datos de Salud

En iOS 15, la app Salud ofrece a los usuarios la opción de compartir sus datos de Salud con otros usuarios. Los datos de Salud se comparten entre los dos usuarios utilizando el cifrado de extremo a extremo de iCloud, y Apple no puede acceder a los datos que se envían al usar Compartir datos de Salud. Para usar la función, tanto el usuario que envía como el que recibe deben tener instalado iOS 15 o versiones posteriores, y deben tener activada la autenticación de dos factores.

Los usuarios también pueden optar por compartir sus datos de Salud con su proveedor de servicios de cuidado de la salud mediante la función Compartir con proveedor, disponible en la app Salud. Los datos compartidos mediante esta función sólo se ponen a disposición de las instituciones sanitarias seleccionadas por el usuario mediante un cifrado de extremo a extremo, y Apple no mantiene ni tiene acceso a las claves de cifrado para descifrar, ver o acceder de ninguna manera a los datos de Salud compartidos mediante la función Compartir con proveedor. Para obtener más información sobre cómo el diseño de este servicio protege los datos de Salud de los usuarios, consulta la sección Seguridad y privacidad de la Guía de registro para organizaciones de salud de Apple.

Firma digital y encriptación

Listas de control de acceso

Los datos del llavero se dividen en particiones y se protegen con listas de control de acceso (ACL). Como resultado, las credenciales almacenadas por apps de terceros no admiten el acceso por parte de apps con entidades distintas, a menos que el usuario las apruebe explícitamente. Esta protección brinda un mecanismo para asegurar las credenciales de autenticación en los dispositivos Apple a lo largo de una variedad de apps y servicios dentro de la organización.

Mail

En la app Mail, los usuarios pueden enviar mensajes firmados digitalmente y encriptados. Mail descubre automáticamente el asunto de la dirección de correo electrónico con RFC 5322 y distinción de mayúsculas y minúsculas, o los nombres alternativos del asunto, en los certificados de encriptado y firma digital de los identificadores de verificación de identificación personal (PIV) en tarjetas inteligentes. Si una cuenta de correo configurada concuerda con una dirección de correo de un certificado de firma digital o de encriptación en un identificador PIV adjunto, Mail automáticamente muestra el botón de firma en la barra de herramientas de la ventana de nuevo mensaje. Si Mail tiene el certificado de encriptación del correo del receptor, o puede descubrirlo en la lista de direcciones globales de Microsoft Exchange (GAL), aparece un ícono de desbloqueo en la barra de herramientas del mensaje nuevo. Un ícono de candado bloqueado indica que el mensaje se enviará encriptado con la clave pública del receptor.

S/MIME por mensaje

iOS, iPadOS y macOS son compatibles con S/MIME por mensaje. Esto significa que los usuarios de S/MIME pueden elegir siempre firmar y encriptar mensajes de forma predeterminada, o firmar y encriptar mensajes individuales de forma selectiva.

Las identidades utilizadas con S/MIME se pueden entregar a los dispositivos Apple usando un perfil de configuración, una solución de administración de dispositivos móviles (MDM), el protocolo de inscripción de certificados simples (SCEP) o la autoridad de certificación de Active Directory de Microsoft.

Tarjetas inteligentes

macOS 10.12 o versiones posteriores incluyen compatibilidad nativa para las tarjetas PIV. Estas tarjetas se utilizan mucho en organizaciones comerciales y gubernamentales para la autenticación de dos factores, firmas digitales y encriptación.

Las tarjetas inteligentes incluyen una o más identidades digitales que tienen un par de claves públicas y privadas y un certificado asociado. Desbloquear una tarjeta inteligente con el número de identificación personal (PIN) brinda acceso a las claves privadas utilizadas para las operaciones de autenticación, encriptación y firma. El certificado determina para qué se puede utilizar una clave, qué atributos se relacionan con ella y si está validada (firmada) por una autoridad certificadora (CA).

Las tarjetas inteligentes se pueden usar para la autenticación de dos factores. Los dos factores necesarios para desbloquear una tarjeta son "algo que el usuario tiene" (la tarjeta) y "algo que el usuario conoce" (el PIN). macOS 10.12 o versiones posteriores también tienen compatibilidad nativa para la autenticación de la ventana de inicio de sesión de tarjetas inteligentes y para la autenticación de certificados de cliente de sitios web en Safari. También es compatible con la autenticación de Kerberos usando pares de claves (PKINIT) para el único inicio de sesión de los servicios compatibles con Kerberos. Para obtener más información sobre las tarjetas inteligentes y macOS, consulta Introducción a la integración de tarjetas inteligentes en la guía *Implementación de las plataformas de Apple*.

Imágenes de disco encriptadas

En macOS, las imágenes de disco encriptadas sirven como contenedores seguros en los que los usuarios pueden almacenar o transferir documentos confidenciales u otros archivos. Las imágenes de disco encriptadas se crean usando Utilidad de Discos, ubicada en /Aplicaciones/Utilidades/. Las imágenes de disco se pueden encriptar usando la encriptación AES ya sea de 128 bits o de 256 bits. Como una imagen de disco montada se trata como un volumen local conectado a la Mac, los usuarios pueden copiar, mover y abrir archivos y carpetas almacenados en ella. Al igual que con FileVault, el contenido de una imagen de disco se encripta y desencripta en tiempo real. Con las imágenes de disco encriptadas, los usuarios pueden intercambiar de forma segura documentos, archivos y carpetas al guardar la imagen de disco encriptada en algún soporte extraíble, enviarla como archivo adjunto en un correo, o almacenarla en un servidor remoto. Para obtener más información sobre las imágenes de disco encriptadas, consulta el Manual del usuario Utilidad de Discos.

Seguridad de las apps

Descripción general de la seguridad de las apps

Hoy en día, las apps son uno de los elementos más importantes de una arquitectura de seguridad. Aunque sus ventajas en cuanto a productividad son increíbles, si no se administran bien, también pueden repercutir negativamente en la seguridad y estabilidad del sistema, o en los datos de usuario.

Debido a esto, Apple brinda capas de protección para ayudar a asegurar que las apps no contengan ningún malware conocido y que no las hayan alterado. Las protecciones adicionales obligan a que haya una cuidadosa mediación en el acceso de las apps a los datos del usuario. Estos controles de seguridad proporcionan una plataforma estable y segura para las apps, donde miles de desarrolladores pueden ofrecer sus apps en iOS, iPadOS y macOS sin que se vea afectada la integridad del sistema. Además, los usuarios pueden acceder a estas apps en sus dispositivos Apple sin temor a virus, software malicioso o ataques no autorizados.

En los iPhone, iPad y iPod touch, todas las apps se obtienen de App Store (y todas se colocan en la zona protegida) para brindar los controles más estrictos.

En la Mac, muchas apps se obtienen de App Store, pero los usuarios de Mac también pueden descargar y usar apps de Internet. Para dar soporte de forma segura a las descargas por Internet, macOS brinda capas de control adicional. Primero, de forma predeterminada en macOS 10.15 o versiones posteriores, todas las apps para Mac deben estar certificadas por Apple para poderse abrir. Este requisito ayuda a asegurarse de que estas apps no tengan ningún malware conocido, sin que sea necesario que las apps se proporcionen mediante App Store. Además, macOS incluye protección antivirus de vanguardia para bloquear (y si es necesario, eliminar) el malware.

Como control adicional a través de las plataformas, la zona segura ayuda a proteger los datos de usuario del acceso no autorizado por parte de las apps. En macOS, los datos de áreas críticas están en sí protegidos, lo que ayuda a asegurarse de que los usuarios tengan el control del acceso por parte de todas las apps a los archivos ubicados en Escritorio, Documentos, Descargas y otras áreas, sin importar si las apps que intentan acceder están en la zona protegida o no.

Capacidad nativa	Equivalente de terceros
Lista de módulos no aprobados, lista de extensiones de Safari no aprobadas	Definiciones de virus/malware
Cuarentena de archivos	Definiciones de virus/malware

Capacidad nativa	Equivalente de terceros
Firmas XProtect/YARA	Definiciones de virus/malware; protección de punto final
Gatekeeper	Protección de punto final; impone la firma de código en las apps para ayudar a garantizar que sólo se ejecute software de confianza
eficheck (necesario para las computadoras Mac que no tienen el chip de seguridad T2 de Apple)	Protección de punto final; detección de rootkit
Firewall de la aplicación	Protección de punto final; firewall
Filtro de paquetes (pf)	Soluciones de firewall
Protección de la integridad del sistema	Integrada en macOS
Controles obligatorios de acceso	Integrada en macOS
Lista de exclusión KEXT	Integrada en macOS
Firma de código de app obligatoria	Integrada en macOS
Certificación de apps	Integrada en macOS

Seguridad de las apps en iOS y iPadOS

Introducción a la seguridad de las apps en iOS y iPadOS

A diferencia de otras plataformas móviles, iOS y iPadOS no permiten a los usuarios instalar apps procedentes de sitios web que no estén firmadas y puedan ser maliciosas, ni ejecutar apps que no sean de confianza. Durante la ejecución, la firma de código verifica que todas las páginas de la memoria ejecutable se creen a medida que se cargan para ayudar a garantizar que una app no se haya modificado desde la última vez que se instaló o actualizó.

Después de que se ha comprobado que una app procede de una fuente aprobada, iOS y iPadOS ponen en marcha medidas de seguridad diseñadas para impedir que ponga en peligro otras apps o el resto del sistema.

Proceso para firmar el código de apps en iOS y iPadOS

En iOS y iPadOS, Apple ofrece seguridad para las apps a través de elementos como la firma de código obligatoria, el inicio de sesión del desarrollador requerido y más.

Firma de código obligatoria

Después de que se ha iniciado, el kernel de iOS o iPadOS controla los procesos y apps del usuario que se pueden ejecutar. Para ayudar a garantizar que todas las apps procedan de una fuente conocida y aprobada, y que no se han manipulado, iOS y iPadOS requieren que todo el código ejecutable se firme con un certificado emitido por Apple. Las apps proporcionadas con el dispositivo, como Mail y Safari, están firmadas por Apple. Las apps de terceros también deben estar validadas y firmadas mediante un certificado emitido por Apple. La firma de código obligatoria extiende el concepto de cadena de confianza del sistema operativo a las apps y ayuda a impedir que apps de terceros carguen código sin firmar o utilicen código que se modifique automáticamente.

Cómo firman sus apps los desarrolladores

Los desarrolladores pueden firmar sus apps mediante la validación del certificado (a través del programa para desarrolladores de Apple). También pueden incrustar infraestructuras dentro de sus apps y validar ese código mediante un certificado emitido por Apple (a través de una cadena de identificador de equipo).

- *Validación del certificado:* para poder desarrollar e instalar apps en dispositivos iOS o iPadOS, los desarrolladores deben registrarse en Apple y unirse al programa para desarrolladores de Apple. Apple verifica la identidad real de cada desarrollador, ya sea una persona individual o una empresa, antes de emitir su certificado. Este certificado permite a los desarrolladores firmar apps y enviarlas a App Store para su distribución. Así que todas las apps que están en App Store han sido enviadas por personas u organizaciones identificables, lo cual funciona como elemento disuasorio para la creación de apps maliciosas. Además, Apple las ha revisado para ayudar a garantizar que funcionen generalmente según lo esperado y que no contienen errores ni otros problemas evidentes y notorios. Este proceso de revisión, organización y distribución, que se suma a la tecnología ya comentada, da confianza a los usuarios en cuanto a la calidad de las apps que compran.
- *Validación de la firma del código:* los sistemas operativos iOS y iPadOS permiten a los desarrolladores incorporar en sus apps infraestructuras que pueden ser utilizadas por las propias apps o las extensiones incrustadas en ellas. Para proteger el sistema y otras apps frente a la carga de código de terceros en su espacio de direcciones, el sistema valida la firma de código en todas las bibliotecas dinámicas vinculadas a un proceso al iniciarse. Esta verificación se consigue mediante el identificador de equipo (Team ID), que se extrae de un certificado emitido por Apple. Un identificador de equipo es una cadena de 10 caracteres alfanuméricos, como 1A2B3C4D5F. Un programa puede tener un enlace a cualquier biblioteca de plataformas proporcionada con el sistema o a cualquier biblioteca que tenga el mismo identificador de equipo en su firma de código que el ejecutable principal. Los ejecutables que se envían con el sistema no cuentan con un identificador de equipo, por lo que sólo pueden contener enlaces a bibliotecas que se envíen con el propio sistema.

Verificar apps internas y propietarias

Las empresas elegibles también pueden crear apps internas y propietarias para utilizarlas dentro de su organización y distribuirlas a sus empleados. Las empresas y organizaciones pueden solicitar el registro en el Apple Developer Enterprise Program (ADEP). Para obtener más información y consultar los requisitos de elegibilidad, consulta el sitio web del Apple Developer Enterprise Program. Después de que una organización se convierte en miembro de ADEP, puede registrarse para obtener un perfil de datos que permita ejecutar apps internas y propietarias en los dispositivos autorizados.

Los usuarios deben tener instalado el perfil de datos para ejecutar estas apps. De este modo se ayuda a garantiza que sólo los usuarios que elija la organización puedan cargar las apps en sus dispositivos iOS y iPadOS. Se confía implícitamente en las apps instaladas mediante la administración de dispositivos móviles (MDM), dado que la relación entre la organización y el dispositivo ya está establecida. De lo contrario, los usuarios tienen que aprobar el perfil de datos de la app en Configuración. Las organizaciones también pueden aplicar restricciones a los usuarios para que no puedan aprobar apps de desarrolladores desconocidos. En el primer lanzamiento de cualquier app interna y propietaria, el dispositivo debe recibir la confirmación positiva de que Apple permite ejecutar la app.

Seguridad del proceso de ejecución en iOS y iPadOS

iOS y iPadOS ayudan a garantizar la seguridad de la ejecución mediante el uso de una zona protegida, autorizaciones declaradas y la aleatorización del espacio de direcciones (ASLR).

Zona protegida

Todas las apps de terceros se "aíslan" para impedir que accedan a los archivos almacenados por otras apps o que realicen cambios en el dispositivo. El aislamiento en zona protegida ayuda a evitar que las apps recopilen o modifiquen la información almacenada por otras apps. Cada una tiene un directorio de inicio único para sus archivos, que se asigna de forma aleatoria al instalarla. Si una app de terceros necesita acceder a información ajena, lo hace únicamente mediante los servicios que iOS y iPadOS proporcionan de forma explícita.

Los archivos y recursos del sistema también están blindados contra las apps del usuario. La mayoría de los archivos y recursos del sistema de iOS y iPadOS se ejecuta como "plataformas móviles" de un usuario sin privilegios, igual que todas las apps de terceros. Toda la partición del sistema operativo se instala como de sólo lectura. Las herramientas que no son necesarias, como los servicios de inicio de sesión remoto, no se incluyen en el software del sistema y las API no permiten que las apps transfieran sus privilegios para modificar otras apps o iOS y iPadOS.

Uso de las autorizaciones

El acceso de apps de terceros a información del usuario y funciones como iCloud, así como su extensibilidad, se controla mediante autorizaciones declaradas. Las autorizaciones son pares de clave-valor que se utilizan para acceder a una app y permiten la autenticación más allá de los factores en tiempo de ejecución, como un ID de usuario UNIX. Las autorizaciones llevan una firma digital, por lo que no se pueden modificar. Los daemons y las apps del sistema las utilizan mucho para realizar operaciones con privilegios específicos que, de otro modo, requerirían la ejecución del proceso como root. Esto reduce considerablemente la posibilidad de que un daemon o una app del sistema en peligro transfiera privilegios.

Además, las apps sólo pueden realizar procesos en segundo plano a través de las API proporcionadas por el sistema. Esto permite que las apps sigan funcionando sin que su rendimiento o la duración de la batería se vean afectados.

Aleatorización del espacio de direcciones

La aleatorización del espacio de direcciones (ASLR) ayuda a proteger el sistema frente a los ataques que aprovechan la vulnerabilidad de una memoria dañada. Al abrirse, las apps integradas utilizan la ASLR para ayudar a aleatorizar todas las regiones de la memoria. Además de funcionar después del lanzamiento, la ASLR ordena de forma aleatoria las direcciones de memoria de código ejecutable, las bibliotecas del sistema y las estructuras de programación relacionadas para reducir aún más la probabilidad de que haya muchas vulnerabilidades. Por ejemplo, en un ataque "return-to-libc" se intenta engañar a un dispositivo para que ejecute código malicioso mediante la manipulación de las direcciones de memoria de la pila y las bibliotecas del sistema, pero la aleatorización en su colocación dificulta la ejecución del ataque, especialmente en varios dispositivos. Xcode y los entornos de desarrollo de iOS y iPadOS compilan automáticamente programas de terceros que tengan activada la compatibilidad con la ASLR.

Función Execute Never

iOS y iPadOS aumentan el nivel de protección con la función Execute Never (XN) de ARM, que marca las páginas de memoria como no ejecutables. Sólo las apps en condiciones muy controladas pueden utilizar las páginas de memoria marcadas como grabables y ejecutables: el kernel comprueba la presencia de la autorización de firma de código dinámica exclusiva de Apple. Incluso entonces, sólo se puede realizar una llamada `mmap` para solicitar una página ejecutable y grabable, a la que se le proporciona una dirección aleatorizada. Safari utiliza esta funcionalidad para su compilador JavaScript Just-in-Time (JIT).

Compatibilidad con extensiones en iOS, iPadOS y macOS

iOS, iPadOS y macOS permiten a las apps proporcionar funcionalidad a otras apps mediante la distribución de extensiones. Las extensiones son binarios ejecutables firmados para fines específicos y empaquetados en una app. Durante la instalación, el sistema detecta automáticamente las extensiones y las pone disponibles para otras apps usando un sistema de concordancia.

Puntos de extensión

Las áreas del sistema que admiten extensiones se conocen como *puntos de extensión*. Cada punto de extensión proporciona API y aplica políticas para el área correspondiente. El sistema determina qué extensiones están disponibles en función de las reglas de coincidencia específicas de cada punto de extensión. El sistema inicia los procesos de extensión automáticamente cuando es necesario y administra su duración. Las autorizaciones se pueden utilizar para restringir la disponibilidad de las extensiones a apps específicas del sistema. Por ejemplo, un widget de la vista Hoy sólo aparece en el centro de notificaciones, y la extensión para compartir sólo está disponible en el panel Compartir. Algunos ejemplos de puntos de extensión son los widgets Hoy, Compartir, Acciones, Edición de fotos, Proveedor de archivos y Teclado personalizado.

Cómo se comunican las extensiones

Las extensiones se ejecutan en su propio espacio de direcciones. La comunicación entre la extensión y la app desde la que se ha activado dicha extensión usa una comunicación entre procesadores mediada por la infraestructura del sistema. Las extensiones no tienen acceso a los archivos o espacios de memoria de las otras extensiones. Se han diseñado de forma que estén aisladas entre sí, al igual que de las apps contenedoras y de las apps que las utilizan. Se aíslan igual que cualquier otra app de terceros y tienen un contenedor diferente al de la app que las contiene. Sin embargo, comparten el mismo acceso a los controles de privacidad que la app contenedora. De este modo, si un usuario autoriza el acceso de una app a Contactos, las extensiones incorporadas en la app también gozarán del acceso, pero no así las extensiones activadas por ella.

Cómo se utilizan los teclados personalizados

Los teclados personalizados son un tipo de extensión especial que el usuario activa para todo el sistema. Una vez que se haya activado, la extensión de teclado se utiliza para cualquier campo de texto, excepto para ingresar el código y cualquier vista de texto seguro. Para restringir la transferencia de datos del usuario, los teclados personalizados se ejecutan de forma predeterminada en una zona protegida muy restrictiva que bloquea el acceso a la red, los servicios que realizan operaciones de red en nombre de un proceso y las API que permiten que la extensión sustraiga los datos ingresados. Los desarrolladores de teclados personalizados pueden solicitar que su extensión tenga acceso abierto, lo cual permitiría que el sistema ejecutase la extensión en la zona protegida normal después de obtener el consentimiento del usuario.

MDM y las extensiones

En el caso de los dispositivos inscritos en una solución de administración de dispositivos móviles (MDM), las extensiones de teclado y documentos obedecen las reglas “Managed Open In”. Por ejemplo, la solución MDM puede ayudar a impedir que un usuario exporte un documento de una app administrada a un proveedor de documentos sin administrar, o que utilice un teclado sin administrar con una app administrada. Además, los desarrolladores de apps pueden impedir el uso de extensiones de teclado de terceros en su app.

Protección de apps y grupos de apps en iOS y iPadOS

En iOS y iPadOS, las organizaciones pueden proteger las apps mediante el SDK de IOS y al acceder a un grupo de apps desde el portal de desarrolladores de Apple.

Adopción de la protección de datos en apps

El kit de desarrollo de software (SDK) para iOS y iPadOS ofrece un conjunto completo de API que facilita a los desarrolladores internos y de terceros la adopción de la protección de datos y contribuye a garantizar el máximo nivel de protección en sus apps. La protección de datos está disponible para las API de archivo y de base de datos, como NSFileManager, CoreData, NSData y SQLite.

La base de datos de la app Mail (archivos adjuntos incluidos), los libros administrados, los marcadores de Safari, las imágenes de apertura de apps y los datos de ubicación también se almacenan mediante encriptación con claves protegidas por el código del usuario en su dispositivo. Las apps Calendario (salvo los archivos adjuntos), Contactos, Recordatorios, Notas, Mensajes y Fotos implementan la autorización de protección de datos Protegido hasta la primera autenticación del usuario.

Las apps instaladas por el usuario que no activan una clase de protección de datos específica reciben de forma predeterminada la clase Protegido hasta la primera autenticación de usuario.

Unirse a un grupo de apps

Las apps y extensiones que forman parte de una cuenta de un desarrollador determinado pueden compartir contenido cuando se configuran como parte de un grupo de apps. El desarrollador puede optar por crear los grupos correspondientes en el Portal de desarrolladores de Apple e incluir el conjunto de apps y extensiones que desee. Una vez que se han configurado como parte de un grupo de apps, las apps tienen acceso a lo siguiente:

- Un contenedor en volumen compartido para el almacenamiento, que permanece en el dispositivo mientras al menos una de las apps del grupo esté instalada.
- Preferencias para compartir.
- Elementos del llavero compartidos.

El portal de desarrolladores de Apple ayuda a garantizar que los identificadores de grupos (GID) de apps sean únicos en todo el ecosistema de apps.

Verificación de los accesorios en iOS y iPadOS

El programa de licencias Made for iPhone, iPad y iPod touch (MFi) proporciona a los fabricantes de accesorios aprobados acceso al Protocolo de accesorios para iPod (iAP) y los componentes de hardware necesarios.

Cuando un accesorio MFi se comunica con un dispositivo iOS o iPadOS mediante un conector de Lightning a USB-C o vía Bluetooth, el dispositivo pide al accesorio que responda con un certificado proporcionado por Apple, el cual verifica el dispositivo con la finalidad de demostrar que cuenta con la autorización de Apple. Entonces, el dispositivo envía un reto, que el accesorio debe contestar con una respuesta firmada. Este proceso está totalmente administrado por un circuito integrado (IC) personalizado que Apple proporciona a los fabricantes de accesorios aprobados y es transparente para el accesorio.

Los accesorios pueden solicitar acceso a distintas funcionalidades y métodos de transporte; por ejemplo, acceso a transmisiones de audio digital a través del cable de Lightning a USB-C, o a información de ubicación proporcionada por Bluetooth. Un circuito integrado de autenticación está diseñado para garantizar que sólo los accesorios aprobados tengan acceso total al dispositivo. Si un accesorio no es compatible con la autenticación, su acceso queda limitado al audio analógico y a un pequeño subconjunto de controles de reproducción de audio en serie (UART).

AirPlay también utiliza el circuito integrado de autenticación para verificar si los receptores cuentan con la aprobación de Apple. Las secuencias de audio de AirPlay y de video de CarPlay utilizan el Protocolo de asociación segura (SAP) MFi, que encripta la comunicación entre el accesorio y el dispositivo con AES128 en modo CTR. Las claves efímeras se intercambian mediante el intercambio de claves de ECDH (Curve25519) y se firman con la clave RSA de 1024 bits del circuito integrado de autenticación como parte del protocolo de estación a estación (STS).

Seguridad de las apps en macOS

Introducción a la seguridad de las apps en macOS

La seguridad de las apps en macOS consta de diversas capas superpuestas, y la primera es la opción de ejecutar únicamente las apps firmadas y de confianza provenientes de App Store. Además, las capas de protecciones de macOS ayudan a garantizar que las apps descargadas de Internet estén libres de malware conocido. macOS ofrece tecnologías para detectar y eliminar malware, y ofrece protecciones adicionales diseñadas para evitar que apps que no son de confianza accedan a los datos del usuario. Los servicios de Apple, como las actualizaciones de certificación de apps y XProtect, están diseñados para ayudar a evitar la instalación de malware. Cuando es necesario, estos servicios localizan el malware que pudo haber evitado la detección previamente, y lo elimina de manera rápida y eficaz. Al final, los usuarios de macOS son libres de operar dentro del modelo de seguridad que tenga sentido para ellos (incluso si eso significa ejecutar código sin firmar y que no sea de confianza).

Proceso para firmar el código de apps en macOS

Todas las apps de App Store están firmadas por Apple para ayudar a garantizar que nadie las haya alterado o modificado. Apple firma todas las apps proporcionadas con los dispositivos Apple.

En macOS 10.15, todas las apps distribuidas fuera de App Store deben estar firmadas por el desarrollador mediante un certificado de ID de desarrollador emitido por Apple (combinado con una clave privada) y certificadas por Apple para poder ejecutarse bajo la configuración predeterminada de Gatekeeper. Las apps desarrolladas internamente también deben estar firmadas con un ID de desarrollador emitido por Apple para que los usuarios puedan validar su integridad.

En macOS, la firma y la certificación del código funcionan de forma independiente, y pueden realizarlas distintos actores con distintos objetivos. El desarrollador realiza la firma del código utilizando el certificado de ID de desarrollador (emitido por Apple); y la verificación de esta firma le demuestra al usuario que el software del desarrollador no se ha alterado desde que el desarrollador lo creó y firmó. Cualquier persona dentro de la cadena de distribución del software puede realizar la certificación, y demuestra que Apple ha recibido una copia del código para verificar que no se haya encontrado ningún malware conocido. El resultado de la certificación es un ticket, que se almacena en los servidores de Apple y puede engraparse de forma opcional a la app (cualquiera puede hacerlo) sin que esto invalide la firma del desarrollador.

Los controles obligatorios de acceso (MAC) requieren que se firme el código para permitir las autorizaciones protegidas por el sistema. Por ejemplo, las apps que requieren acceso a través del firewall deben tener su código firmado con las autorizaciones MAC adecuadas.

Gatekeeper y la protección del tiempo de ejecución en macOS

macOS ofrece la tecnología Gatekeeper y protección durante la ejecución para ayudar a garantizar que sólo se ejecute software de confianza en la Mac de un usuario.

Gatekeeper

macOS incluye una tecnología de seguridad llamada *Gatekeeper* que está diseñada para ayudar a garantizar que sólo se ejecute software de confianza en la Mac del usuario. Cuando un usuario descarga y abre una app, un módulo o un paquete de instalación desde una ubicación que no es App Store, Gatekeeper verifica que el software provenga de un desarrollador identificado, esté certificada por Apple para verificar que no tenga contenido malicioso conocido, y que no haya sido alterada. Gatekeeper también solicita la aprobación del usuario antes de abrir software descargado por primera vez para asegurar que el usuario no haya sido engañado para abrir código ejecutable pensando que era simplemente un archivo de datos.

De manera predeterminada, Gatekeeper ayuda a garantizar que todo el software descargado esté firmado por App Store o por un desarrollador registrado y certificado por Apple. Tanto el proceso de revisión de App Store como la línea de certificación están diseñadas para garantizar que las apps no contengan ningún malware conocido. Por lo tanto, de forma predeterminada, *todo el software en macOS se revisa para verificar que no contenga contenido malicioso la primera vez que se abre, independientemente de cómo llegó a la Mac*.

Los usuarios y las organizaciones tienen la opción de permitir únicamente el software instalado desde App Store. De forma alternativa, los usuarios pueden omitir las políticas de Gatekeeper para abrir cualquier software, a menos que lo restrinja la solución de administración de dispositivos móviles (MDM). Las organizaciones pueden utilizar la MDM para realizar la configuración de Gatekeeper, lo que incluye permitir software firmado con identidades alternativas. Gatekeeper también puede desactivarse por completo, de ser necesario.

Gatekeeper también protege contra la distribución de módulos maliciosos en apps benignas, en donde, al usar la app se activa la carga de un módulo malicioso sin el conocimiento del usuario. Cuando se requiere, Gatekeeper puede abrir apps desde ubicaciones aleatorias de sólo lectura, lo cual está diseñado para impedir la carga automática de módulos distribuidos junto con la app.

Protección del tiempo de ejecución

Los archivos del sistema, los recursos y el kernel están resguardados del espacio de las apps del usuario. Todas las apps de App Store están en la zona protegida para restringir el acceso a los datos almacenados por otras apps. Si una app de App Store necesita acceder a datos de otra app, sólo lo puede hacer usando las API y servicios proporcionados por macOS.

Protección contra el malware en macOS

Apple opera un proceso de inteligencia de amenazas para identificar y bloquear rápidamente el malware.

Tres capas de defensa

Las defensas contra malware se estructuran en tres capas:

1. *Evitar el arranque o ejecución de malware:* App Store o Gatekeeper combinado con la certificación de apps.

2. *Bloquear la ejecución de malware en sistemas de usuarios:* Gatekeeper, la certificación de apps y XProtect.

3. *Solucionar malware que se haya ejecutado:* XProtect.

La primera capa de defensa está diseñada para inhibir la distribución de malware y evitar que se ejecute incluso una sola vez; y este es el objetivo de App Store, y de Gatekeeper en conjunto con la certificación de apps.

La siguiente capa de defensa ayuda a garantizar que si se detecta malware en cualquier Mac, este se identifica y bloquea rápidamente, tanto para detener la propagación así como corregir los sistemas de la Mac en donde ya se haya afianzado. XProtect agrega esta defensa, junto con Gatekeeper y la certificación de apps.

Por último, XProtect se ejecuta para gestionar el malware que haya logrado ejecutarse.

Estas protecciones, las cuales se explican con mayor detalle a continuación, trabajan en conjunto para ofrecer la mejor protección posible contra virus y malware. Existen protecciones adicionales, especialmente en computadoras Mac con Apple Chip, que limitan el daño potencial del malware que sí se ejecute. Consulta Protección del acceso de las apps a los datos de usuario para obtener información sobre las formas en que macOS puede ayudarte a proteger los datos de usuario del malware, así como la sección Integridad del sistema operativo para ver las formas en que macOS puede limitar las acciones que el malware puede realizar en el sistema.

Certificación

La *certificación* es un servicio de escaneo de malware proporcionado por Apple. Los desarrolladores que quieran distribuir apps para macOS fuera de App Store deberán enviar sus apps para escanearlas como parte del proceso de distribución. Apple escanea este software en busca de malware conocido y, si no se encuentra ninguno, emite un ticket de certificación. Normalmente, los desarrolladores anexan este ticket a su app para que Gatekeeper pueda verificar y ejecutarla, incluso cuando no se cuenta con conexión.

Apple también puede emitir un ticket de revocación para apps que se sabe que son maliciosas, incluso si se han certificado anteriormente. macOS comprueba periódicamente si hay tickets de revocación nuevos para que Gatekeeper tenga la información más reciente y pueda bloquear la ejecución de estos archivos. Este proceso puede bloquear rápidamente las apps maliciosas, ya que las actualizaciones ocurren en segundo plano con mucha más frecuencia que las actualizaciones en segundo plano que impulsan las firmas XProtect nuevas. Además, esta protección se puede aplicar tanto a las apps que se hayan certificado previamente, como a las que no.

XProtect

macOS incluye una tecnología antivirus incorporada llamada *XProtect* que utiliza firmas para la detección y eliminación de malware. El sistema utiliza firmas YARA, una herramienta que se utiliza para realizar una detección de malware basada en firmas que Apple actualiza periódicamente. Apple monitorea las nuevas infecciones y cepas de malware, y actualiza las firmas automáticamente (independientemente de las actualizaciones del sistema) para defender una computadora Mac de las infecciones de malware. XProtect detecta y bloquea automáticamente la ejecución de malware conocido. En macOS 10.15 o versiones posteriores, XProtect verifica las apps para detectar contenido malicioso cada vez que ocurra lo siguiente:

- Se ejecuta una app por primera vez.
- Se modifica una app (en el sistema de archivos).
- Se actualizan las firmas XProtect.

Cuando XProtect detecta malware conocido, el software se bloquea y se le notifica al usuario, quien recibe la opción de mover el software al Basurero.

Nota: la certificación es eficaz contra archivos conocidos (o hash de archivos) y se puede utilizar en apps que ya se han abierto anteriormente. Las reglas basadas en firmas de XProtect son más genéricas que un hash de archivo específico, por lo que puede encontrar variantes que Apple no ha detectado. XProtect sólo escanea apps que han cambiado o las apps que se abren por primera vez.

En caso de que algún malware llegue a la Mac, XProtect también incluye tecnología para corregir las infecciones. Por ejemplo, XProtect incluye un motor que corrige las infecciones mediante las actualizaciones entregadas automáticamente por Apple (como parte de las actualizaciones automáticas de los archivos de datos del sistema y las actualizaciones de seguridad). También elimina el malware al recibir información actualizada, y sigue comprobando periódicamente si hay infecciones. XProtect no reinicia automáticamente la Mac.

Actualizaciones de seguridad automáticas para XProtect

Apple distribuye actualizaciones para XProtect de forma automática según la información más reciente sobre amenazas. De manera predeterminada, macOS verifica estas actualizaciones diariamente. Las actualizaciones de certificación de apps, las cuales se distribuyen a través de la sincronización de CloudKit, son mucho más frecuentes.

Cómo Apple responde cuando se descubre un nuevo malware

Cuando se detecta un malware nuevo, se pueden realizar varios pasos:

- Se revocan todos los certificados de ID de desarrollador asociados.
- Se emiten tickets de revocación de certificación para todos los archivos (apps y archivos asociados).
- Se desarrollan y publican firmas XProtect.

  Estas firmas también se aplican retroactivamente al software previamente certificado, y cualquier nueva detección puede ocasionar una o más de las acciones anteriores.

En última instancia, una detección de malware lanza una serie de pasos durante los próximos segundos, horas y días para propagar las mejores protecciones posibles a los usuarios de Mac.

Controlar el acceso de las app a los archivos en macOS

Apple considera que los usuarios deberían tener completa transparencia, consentimiento y control sobre lo que las apps hacen con sus datos. En macOS 10.15, este modelo se aplica de forma obligatoria en el sistema para ayudar a garantizar que todas las apps deban obtener el consentimiento del usuario antes de acceder a archivos de Documentos, Descargas, Escritorio, iCloud Drive y volúmenes de red. Las apps que requieran acceso al dispositivo de almacenamiento completo deben agregarse explícitamente en Preferencias del Sistema en macOS 10.13 o versiones posteriores. Además, la accesibilidad y las capacidades de automatización requieren que el usuario dé su permiso para ayudar a garantizar que no se pasen por alto otras protecciones. Según la política de acceso, se podría solicitar, o incluso podría ser obligatorio, que los usuarios cambien la configuración desde Preferencias del Sistema > Seguridad y privacidad > Privacidad:

Elemento	La app solicita una acción por parte del usuario	El usuario debe editar la configuración de privacidad del sistema
Accesibilidad		✓
Acceso completo al almacenamiento interno		✓
Archivos y carpetas *Nota:* incluye Escritorio, Documentos, Descargas, volúmenes de red y volúmenes extraíbles	✓	
Automatización (eventos de Apple)	✓	

Los elementos que estén en el Basurero del usuario están protegidos de cualquier app que esté usando el acceso completo al disco; no se le pedirá al usuario que le dé acceso a la app. Si el usuario desea que las apps accedan a los archivos, deben moverse del Basurero a otro lugar.

Los usuarios que activen FileVault en la Mac deben brindar credenciales válidas antes de continuar con el proceso de arranque y obtener acceso a los modos de inicio especializados. Sin las credenciales de acceso válidas o la clave de recuperación, el volumen entero permanece encriptado y protegido del acceso no autorizado, aunque el dispositivo de almacenamiento se retire físicamente y se conecte a otra computadora.

Para proteger los datos en un entorno empresarial, el departamento de TI debería definir e imponer políticas de configuración de FileVault utilizando la administración de dispositivos móviles (MDM). Las organizaciones tienen varias opciones para administrar los volúmenes encriptados, entre las que se incluyen las claves institucionales, las claves personales de recuperación (que se pueden almacenar de forma opcional en la MDM para su custodia), o una combinación de ambas. La rotación de claves también se puede establecer como política en la MDM.

Funcionalidades de seguridad en la app Notas

La app Notas incluye la función de notas seguras (en iPhone, iPad, Mac y el sitio web de iCloud) que permite al usuario proteger el contenido de notas específicas. Los usuarios también pueden compartir notas de forma segura.

Notas seguras

Las notas seguras se encriptan de extremo a extremo usando una contraseña proporcionada por el usuario que se solicita para ver las notas en dispositivos iOS, iPadOS y macOS, así como en el sitio web de iCloud. Cada cuenta de iCloud (incluidas las cuentas En mi [dispositivo]) puede tener una contraseña separada.

Cuando un usuario protege una nota, se deriva una clave de 16 bytes a partir de la contraseña usando PBKDF2 y SHA256. La nota y todos sus archivos adjuntos se encriptan utilizando AES con el modo Galois/Counter (AES-GCM). Se crean nuevos registros en Core Data y CloudKit para almacenar la nota encriptada, los archivos adjuntos, la etiqueta y el vector de inicialización. Después de que se hayan creado los registros nuevos, se eliminan los datos originales sin encriptar. Los archivos adjuntos compatibles con la encriptación incluyen imágenes, dibujos, tablas, mapas y sitios web. Las notas que contienen otros tipos de archivos adjuntos no se pueden encriptar, y no se pueden agregar archivos adjuntos que no sean compatibles a las notas que ya están protegidas.

Para ver una nota segura, el usuario debe ingresar su contraseña o autenticarse usando Face ID o Touch ID. Después de que el usuario se haya autenticado correctamente, ya sea para ver o crear una nota protegida, Notas abre una sesión segura. Mientras la sesión segura está abierta, el usuario puede ver o asegurar otras notas sin tener que autenticarse nuevamente. Sin embargo, la sesión segura se aplica sólo a las notas protegidas con la contraseña proporcionada. El usuario aún deberá autenticarse para abrir notas protegidas con una contraseña distinta. La sesión segura se cierra cuando ocurre lo siguiente:

- El usuario toca el botón Bloquear ahora en Notas.
- Notas permanece en segundo plano durante más de 3 minutos (8 minutos en macOS).
- El sistema iOS o iPadOS se bloquea.

Para cambiar la contraseña de una nota segura, el usuario debe ingresar la contraseña actual, ya que Face ID o Touch ID no están disponibles al cambiar la contraseña. Después de seleccionar una nueva contraseña, la app Notas vuelve a encapsular, en la misma cuenta, las claves de todas las notas existentes que están encriptadas con la contraseña anterior.

Si un usuario escribe mal la contraseña tres veces seguidas, Notas muestra una pista establecida por el usuario (si el usuario la proporcionó durante la configuración). Si el usuario sigue sin poder recordar la contraseña, puede restablecerla en la configuración de Notas. Esta función permite que los usuarios creen nuevas notas seguras protegidas usando la nueva contraseña, pero no les permitirá ver las notas protegidas anteriormente. Si el usuario recuerda la contraseña anterior, podrá ver las notas protegidas anteriormente. Para restablecer la contraseña, se requiere la contraseña de la cuenta de iCloud del usuario.

Notas compartidas

Las notas que no están encriptadas de extremo a extremo con contraseña se pueden compartir con otras personas. Las notas compartidas aún utilizan el tipo de datos encriptados de CloudKit para todo el texto y los archivos adjuntos que el usuario ingrese en una nota. Los componentes siempre se encriptan con una clave que está encriptada en el CKRecord. No se encriptan los metadatos, tales como las fechas de creación y modificación. CloudKit administra el proceso mediante el cual los participantes pueden encriptar y desencriptar los datos de los otros.

Funcionalidades de seguridad en la app Atajos

En la app Atajos, los atajos se sincronizan de forma opcional en todos los dispositivos Apple del usuario utilizando iCloud. Los atajos se pueden compartir con otros usuarios mediante iCloud. Los atajos se almacenan localmente en un formato encriptado.

Los atajos personalizados son versátiles, algo parecidos a los scripts o programas. Cuando se descargan atajos de Internet, se le advierte al usuario que Apple no ha verificado el atajo y se le da la oportunidad de inspeccionarlo. Para proteger contra atajos maliciosos, se descargan definiciones actualizadas de malware para identificar atajos maliciosos durante el tiempo de ejecución.

Los atajos personalizados también pueden ejecutar scripts de JavaScript personalizados por el usuario en sitios web en Safari cuando se activan desde la hoja de compartir. Para proteger contra scripts de JavaScript malintencionados que, por ejemplo, intentan engañar al usuario para que ejecute un script en un sitio web de redes sociales que recopila sus datos, se valida el JavaScript con respecto a las definiciones de malware mencionadas anteriormente. La primera vez que un usuario ejecuta un script de JavaScript en un dominio, se solicita al usuario que permita la ejecución de atajos con JavaScript en la página web actual en ese dominio.

Servicios de seguridad

Descripción general de los servicios de seguridad

Apple ha desarrollado un robusto grupo de servicios para ayudar a los usuarios a obtener más utilidad y productividad de sus dispositivos. Estos servicios brindan capacidades poderosas para el almacenamiento en la nube, sincronización, autenticación, pagos, mensajes, comunicaciones y más, todo mientras se protege la privacidad del usuario, y la seguridad de sus datos.

Este capítulo abarca las tecnologías de seguridad utilizadas en iCloud, Iniciar sesión con Apple, Apple Pay, iMessage, Apple Messages for Business, FaceTime, Encontrar y Continuidad.

Nota: no todos los servicios y contenidos de Apple están disponibles en todos los países o regiones.

Apple ID y Apple ID administrado

Descripción general de la seguridad del Apple ID

Un Apple ID es la cuenta que se usa para iniciar sesión en los servicios de Apple. Es importante que los usuarios protejan su Apple ID para ayudar a evitar que se produzca un acceso no autorizado a sus cuentas. Para ayudar con esto, los Apple ID requieren contraseñas seguras que cumplan con lo siguiente:

- Tener al menos ocho caracteres de longitud.
- Contener tanto letras como números.
- No contener tres o más caracteres idénticos consecutivos.
- No ser una contraseña usada comúnmente.

Se recomienda a los usuarios que aumenten el grado de protección indicado agregando más caracteres o signos de puntuación para que sus contraseñas resulten aún más seguras.

Apple también avisa mediante mensajes de correo electrónico o notificaciones push, o ambos, a los usuarios cuando se producen cambios importantes en sus cuentas. Por ejemplo, si se modifica una contraseña o la información de facturación, o bien si el Apple ID se usa para iniciar sesión en un dispositivo nuevo. Si los usuarios detectan algo que no les resulte familiar, deben cambiar la contraseña de su Apple ID inmediatamente.

Además, Apple usa una variedad de políticas y procedimientos diseñados para proteger las cuentas de los usuarios. Estos incluyen limitar las veces que se pueden reingresar los datos de inicio de sesión o restablecer la contraseña, el monitoreo activo de fraude para identificar ataques en el momento en el que ocurran, y revisiones periódicas de las políticas que permiten a Apple adaptarse a cualquier información nueva que pueda afectar la seguridad del usuario.

Nota: la política de contraseñas para el Apple ID administrado la configura un administrador en Apple School Manager o Apple Business Manager.

Autenticación de dos factores

Para ayudar a los usuarios a proteger sus cuentas, Apple ofrece de forma predeterminada la *autenticación de dos factores*, una capa de seguridad adicional para los Apple ID. Está diseñada para asegurar que sólo el propietario de la cuenta pueda acceder a esta, incluso si alguien más conoce la contraseña. Con la autenticación de dos factores, se puede acceder a la cuenta del usuario solamente en dispositivos de confianza, como el iPhone, iPad, iPod touch o Mac del usuario, o en otros dispositivos después de haber realizado una verificación desde uno de estos dispositivos de confianza o desde un número telefónico de confianza. Para iniciar sesión por primera vez en cualquier dispositivo nuevo, se necesitan dos datos: la contraseña del Apple ID y un código de verificación de seis dígitos que se muestra automáticamente en los dispositivos de confianza del usuario o que se envía a un número telefónico de confianza. Al ingresar este código, el usuario confirma que confía en el nuevo dispositivo y que es seguro iniciar sesión. Dado que una contraseña por sí misma no es suficiente para acceder a la cuenta del usuario, la autenticación de dos factores mejora la seguridad del Apple ID del usuario y de toda la información personal que almacene con Apple. Esta autenticación viene integrada directamente en iOS, iPadOS, macOS, tvOS, watchOS y los sistemas de autenticación usados en los sitios web de Apple.

Cuando un usuario inicia sesión en un sitio web de Apple mediante un navegador web, se envía una petición de segundo factor a todos los dispositivos de confianza asociados con la cuenta de iCloud del usuario solicitando aprobación para la sesión web. Si el usuario inicia sesión en un sitio web de Apple desde un navegador en un dispositivo de confianza, verá que el código de verificación se mostrará localmente en el dispositivo que está usando. Cuando el usuario ingresa el código en ese dispositivo, la sesión web se aprueba.

Restablecimiento de la contraseña y recuperación de la cuenta

Si un usuario olvida la contraseña de una cuenta de Apple ID, puede restablecerla en un dispositivo de confianza. Si no hay un dispositivo de confianza disponible y se conoce la contraseña, el usuario puede usar un número telefónico de confianza para autenticar mediante verificación vía SMS. Además, para ofrecer recuperación inmediata del Apple ID, se puede utilizar un código usado anteriormente para restablecerlo en conjunto con el mensaje SMS. Si estas opciones no son posibles, se debe seguir el proceso de recuperación de cuentas. Para obtener más información, consulta el artículo de soporte de Apple Cómo usar la recuperación de la cuenta cuando no puedes restablecer la contraseña del Apple ID.

Seguridad del Apple ID administrado

Los Apple ID administrados funcionan de manera muy similar a un Apple ID, pero se trata de cuentas que son propiedad de una empresa u organización educativa, que es la que los controla. Estas organizaciones pueden restablecer contraseñas, limitar las compras y las comunicaciones (tales como FaceTime y Mensajes), y configurar permisos basados en roles para empleados, profesores, estudiantes y el resto del personal.

Para los Apple ID administrados, algunos servicios están desactivados (por ejemplo, Apple Pay, llavero de iCloud, HomeKit y Encontrar).

Inspeccionar Apple ID administrados

Los Apple ID administrados se pueden *inspeccionar*, lo que permite a las instituciones cumplir con las regulaciones legales y de privacidad. Un profesor, gestor o administrador de Apple School Manager puede inspeccionar cuentas de Apple ID administrados específicas.

Los inspectores sólo pueden monitorear las cuentas que estén por debajo de su posición jerárquica en la organización. Por ejemplo, los profesores pueden monitorear las cuentas de los estudiantes; los directivos pueden inspeccionar las de los profesores y estudiantes; y los administradores pueden inspeccionar las de los directivos, profesores y estudiantes.

Cuando se solicitan credenciales de inspección mediante Apple School Manager, se crea una cuenta especial que tiene acceso sólo a los Apple ID administrados para los cuales se solicitó inspección. El inspector puede leer y modificar el contenido del usuario almacenado en iCloud o en apps compatibles con CloudKit. Cada solicitud de acceso de auditoría se registra en Apple School Manager. El registro muestra quién fue el inspector, el Apple ID administrado al que se solicitó acceso, la hora de la solicitud y si se realizó la inspección.

Apple ID administrados y dispositivos personales

Los Apple ID administrados también pueden usarse en dispositivos iOS, iPadOS y Mac personales. Los estudiantes pueden iniciar sesión en iCloud usando un Apple ID administrado proporcionado por la institución y una contraseña adicional de uso particular que funge como segundo factor en el proceso de autenticación de dos factores del Apple ID. Cuando los estudiantes usan un Apple ID administrado en un dispositivo personal, el llavero de iCloud no está disponible y la institución podría restringir otras funciones, tales como FaceTime o Mensajes. Todos los documentos de iCloud creados por estudiantes mientras tengan iniciada la sesión están sujetos a auditoría de la manera previamente descrita en esta sección.

iCloud

Descripción general de la seguridad de iCloud

iCloud almacena los contactos, calendarios, fotos, documentos y otra información del usuario y la mantiene actualizada automáticamente en todos sus dispositivos. Además, las apps de terceros también pueden usar iCloud para almacenar y sincronizar documentos, así como datos clave-valor para datos de apps según las indicaciones del desarrollador. Los usuarios pueden configurar iCloud al iniciar sesión con un Apple ID y elegir los servicios que quieren usar. Los administradores de TI pueden desactivar ciertas funciones de iCloud, como iCloud Drive y el respaldo en iCloud usando los perfiles de configuración de la administración de dispositivos móviles (MDM).

iCloud utiliza métodos de seguridad avanzados y emplea políticas estrictas para proteger los datos de los usuarios. La mayor parte de los datos de iCloud se encriptan primero en el dispositivo del usuario utilizando claves de iCloud generadas por el dispositivo antes de cargarse a los servidores de iCloud. En el caso de los datos que no están encriptados de extremo a extremo, el dispositivo del usuario carga de forma segura estas claves de iCloud a los módulos de seguridad de hardware de iCloud en los centros de datos de Apple, lo que permite que Apple ayude al usuario con la recuperación de los datos y que los desencripte en su nombre siempre que sea necesario (por ejemplo, cuando se inicia sesión en un nuevo dispositivo, se restaura desde un respaldo o se accede a los datos de iCloud en Internet). Los datos que se pasan entre los dispositivos del usuario y los servidores de iCloud se encriptan de forma separada durante el tránsito mediante TLS, y los datos del usuario se mantienen almacenados en los servidores de iCloud con una capa adicional de encriptación.

Las claves de encriptación, en caso de que estén disponibles para Apple, se protegen en los centros de datos de Apple. Cuando se procesan datos almacenados en un centro de datos de terceros, solamente se puede acceder a estas claves de encriptación mediante el software de Apple que se ejecuta en servidores seguros, y sólo mientras se realiza el procesamiento necesario. Para mayor privacidad y seguridad, muchos servicios de Apple utilizan encriptación de extremo a extremo, lo que significa que sólo el usuario puede acceder a su información, y sólo en dispositivos de confianza en los que haya iniciado sesión con su Apple ID.

Apple ofrece a los usuarios dos opciones para encriptar y proteger los datos que almacenan en iCloud:

- **Protección de datos estándar (configuración predeterminada):** los datos en iCloud del usuaario se encriptan, las claves de encriptación se protegen en los centros de datos de Apple y Apple puede ayudar con la recuperación de los datos y de la cuenta. Solamente algunos datos de iCloud (14 categorías de datos entre las que se incluyen los datos de Salud y las contraseñas del llavero de iCloud) se encriptan de extremo a extremo.
- **Protección de datos avanzada para iCloud:** configuración opcional que ofrece el nivel más alto de Apple en relación con la seguridad de los datos en la nube. Si un usuario elige activar la protección de datos avanzada, sus dispositivos de confianza conservan el acceso exclusivo a las claves de encriptación para la mayoría de sus datos en iCloud, protegiéndolos así mediante encriptación de extremo a extremo. Si activas la protección de datos avanzada, la cantidad de categorías de datos que usan la encriptación de extremo a extremo aumenta a 23 e incluye tu respaldo en iCloud, fotos, notas y más.

En el siguiente artículo de soporte de Apple se enumeran las categorías específicas de datos en iCloud que se protegen mediante encriptación de extremo a extremo: Descripción general de la seguridad de datos de iCloud.

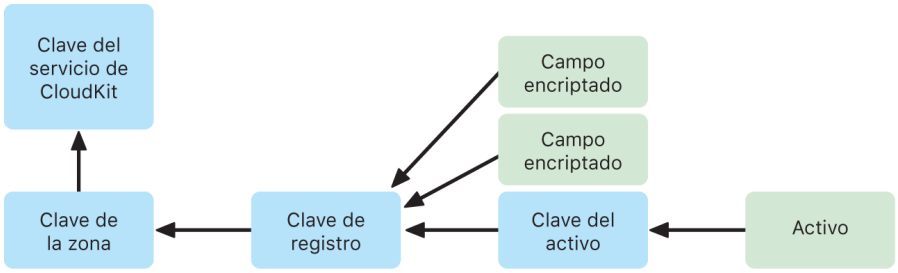
Encriptación en iCloud

La encriptación de datos en iCloud está relacionada directamente con el modelo de almacenamiento de datos, comenzando con las infraestructuras y las API de CloudKit que permiten que las apps y el software del sistema almacenen datos en iCloud en nombre del usuario y que mantengan todo actualizado en todos los dispositivos y en Internet.

Encriptación de CloudKit

CloudKit es una infraestructura que permite a los desarrolladores de apps almacenar en iCloud datos de clave-valor, datos estructurados y recursos (datos de gran tamaño almacenados de forma separada de la base de datos, tales como imágenes o videos). CloudKit es compatible con bases de datos tanto públicas como privadas, agrupadas en contenedores. Las bases de datos públicas se comparten globalmente, se usan por lo general para recursos genéricos y no están encriptadas. Mientras que las bases de datos privadas almacenan los datos en iCloud de cada usuario.

CloudKit utiliza una jerarquía de claves que coincide con la estructura de los datos. La base de datos privada de cada contenedor está protegida por una jerarquía de claves, arraigada en una clave asimétrica denominada *clave de servicio de CloudKit*. Estas claves son únicas para cada usuario de iCloud y se generan en su dispositivo de confianza. Al escribir datos en CloudKit, todas las claves de registro se generan en el dispositivo de confianza del usuario y se ajustan a la jerarquía de claves adecuada antes de que se carguen los datos.



Muchos servicios de Apple, enumerados en el artículo de soporte de Apple Descripción general de la seguridad de datos de iCloud, usan encriptación de extremo a extremo con una clave de servicio de CloudKit protegida mediante la sincronización del llavero de iCloud. En el caso de estos contenedores de CloudKit, las claves de servicio se almacenan en el llavero de iCloud del usuario y comparten las características de seguridad de llavero. Las claves de servicio están disponibles sólo en los dispositivos de confianza del usuario, y ni Apple ni terceras partes pueden acceder a ellas. En caso de perder el dispositivo, los usuarios pueden recuperar sus datos del llavero de iCloud mediante el uso de la recuperación segura del llavero de iCloud, los contactos de recuperación de la cuenta o una clave de recuperación de la cuenta.

Administración de las claves de encriptación

La seguridad de los datos encriptados en CloudKit está basada en la seguridad de las claves de encriptación correspondientes. Las claves de servicio de CloudKit se dividen en dos categorías: las encriptadas de extremo a extremo y las disponibles después de la autenticación.

- **Claves de servicio encriptadas de extremo a extremo:** en el caso de los servicios de iCloud encriptados de extremo a extremo, las claves privadas del servicio CloudKit nunca están disponibles para los servidores de Apple. Los pares de claves de servicio, incluyendo las claves privadas, se crean de forma local en el dispositivo de confianza del usuario y se transfieren a sus otros dispositivos mediante la seguridad del llavero de iCloud. Aunque los flujos de sincronización y recuperación del llavero de iCloud están mediados por los servidores de Apple, se impide criptográficamente que estos servidores accedan a los datos del llavero del usuario. En el peor de los casos, si se pierde el acceso al llavero de iCloud y a todos sus mecanismos de recuperación, los datos encriptados de extremo a extremo en CloudKit se pierden. Apple no puede ayudar a recuperar estos datos.
- **Claves de servicio disponibles después de la autenticación:** en el caso de otros servicios, como Fotos y iCloud Drive, las claves de servicio se almacenan en los módulos de seguridad del hardware de iCloud en los centros de datos de Apple, y es posible que algunos servicios de Apple puedan acceder a ellas. Cuando un usuario inicia sesión en iCloud en un nuevo dispositivo y autentica su Apple ID, los servidores de Apple pueden acceder a estas claves sin necesidad de otra interacción o entrada del usuario. Por ejemplo, después de iniciar sesión en iCloud.com, el usuario puede ver inmediatamente sus fotos en línea. Estas claves de servicio son claves que están *disponibles después de la autenticación*.

Protección de datos avazada para iCloud

La protección de datos avanzada para iCloud es una configuración opcional que ofrece el nivel más alto de Apple en relación con la seguridad de los datos en la nube. Cuando un usuario activa la protección de datos avanzada, sus dispositivos de confianza conservan el acceso exclusivo a las claves de encriptación para la mayoría de sus datos en iCloud, protegiéndolos así mediante *encriptación de extremo a extremo*. Para los usuarios que activan la protección de datos avanzada, la cantidad total de categorías de datos que se protegen mediante encriptación de extremo a extremo aumenta de 14 a 23 e incluye el respaldo en iCloud, las fotos, las notas y más.

La protección de datos avanzada para iCloud estará disponible para los usuarios de EE.UU. a fines de 2022 y comenzará a implementarse en el resto del mundo a principios de 2023.

En concepto, la protección de datos avanzada en sencilla: Todas las claves de servicio de CloudKit que se generaron en el dispositivo y luego se cargaron en los módulos de seguridad de hardware (HSM) de iCloud *disponibles después de la autenticación* en los centros de datos de Apple se eliminan de esos HSM y, en su lugar, se mantienen completamente dentro del dominio de protección del llavero de iCloud de la cuenta. Se tratan como las claves de servicio *encriptadas de extremo a extremo* existentes, lo que significa que Apple ya no puede leer ni acceder a ellas.

La protección avanzada de datos también protege automáticamente los campos de CloudKit que los desarrolladores de terceros eligen marcar como encriptados, así como todos los componentes de CloudKit.

Activar la protección de datos avanzada

Cuando un usuario activa la protección de datos avanzada, su dispositivo de confianza realiza dos acciones: Primero, comunica la intención del usuario de activar la protección de datos avanzada a sus otros dispositivos que participan en la encriptación de extremo a extremo. Esto se lleva a cabo escribiendo un nuevo valor, firmado por claves locales del dispositivo, en los metadatos del dispositivo del llavero de iCloud. Los servidores de Apple no pueden eliminar ni modificar esta afirmación mientras se sincroniza con los otros dispositivos del usuario.

En segundo lugar, el dispositivo inicia la eliminación de las claves de servicio *disponibles después de la autenticación* de los centros de datos de Apple. Como estas claves están protegidas por los HSM de iCloud, esta eliminación es inmediata, permanente e irrevocable. Una vez que se eliminan las claves, Apple ya no puede acceder a *ninguno* de los datos protegidos por las claves de servicio del usuario. En este momento, el dispositivo inicia una operación de rotación de claves asíncrona, que crea una nueva clave de servicio para cada servicio cuya clave estaba disponible anteriormente para los servidores de Apple. Si la rotación de claves falla debido a una interrupción de la red o a cualquier otro error, el dispositivo vuelve a intentar la rotación de claves hasta que se realice correctamente.

Una vez que la rotación de la clave de servicio se realiza correctamente, los nuevos datos escritos en el servicio no se pueden desencriptar con la clave anterior. Estos datos se protegen con la nueva clave que está controlada únicamente por los dispositivos de confianza del usuario y que nunca ha estado disponible para Apple.

Protección de datos avanzada y acceso web a iCloud.com

Cuando un usuario activa por primera vez la protección de datos avanzada, se desactiva automáticamente el acceso web a sus datos en iCloud.com. Esto sucede debido a que los servidores web de iCloud ya no tienen acceso a las claves necesarias para desencriptar y mostrar los datos del usuario. El usuario puede optar por volver a activar el acceso web y utilizar la participación de su dispositivo de confianza para acceder a sus datos encriptados de iCloud desde Internet.

Después de activar el acceso web, el usuario tendrá que autorizar el inicio de sesión web en uno de sus dispositivos de confianza cada vez que visite iCloud.com. La autorización “habilita” el dispositivo para el acceso web. Durante la próxima hora, este dispositivo acepta solicitudes de servidores de Apple específicos para cargar claves de servicio individuales, pero solamente aquellas que corresponden a una lista de servicios permitidos normalmente accesibles en iCloud.com. En otras palabras, incluso después de que el usuario autorice un inicio de sesión web, una solicitud del servidor no podrá ocasionar que el dispositivo del usuario cargue las claves de servicio para los datos que no deben poder visualizarse en iCloud.com (como los datos de salud o las contraseñas del llavero de iCloud). Los servidores de Apple solicitan solamente las claves de servicio necesarias para desencriptar los datos específicos a los que el usuario solicita acceder en la web. Cada vez que se carga una clave de servicio, se encripta mediante una clave efímera vinculada a la sesión web que autorizó el usuario, y aparece una notificación en el dispositivo del usuario que muestra el servicio de iCloud cuyos datos están temporalmente disponibles para los servidores de Apple.

Preservar las elecciones del usuario

Solamente el usuario puede modificar la configuración de la protección avanzada de datos y el acceso web a iCloud.com. Estos valores se almacenan en los metadatos del dispositivo del llavero iCloud del usuario y sólo se pueden cambiar desde uno de los dispositivos de confianza del usuario. Los servidores de Apple no pueden modificar esta configuración en nombre del usuario, ni pueden revertirla a una configuración anterior.

Implicaciones de seguridad de las funciones de compartir y la colaboración

En la mayoría de los casos, cuando los usuarios comparten contenido para colaborar entre sí (por ejemplo, con notas compartidas, recordatorios compartidos, carpetas compartidas en iCloud Drive o la fototeca compartida en iCloud) y todos los usuarios tienen activada la protección de datos avanzada, los servidores de Apple se utilizan exclusivamente para establecer el uso compartido, pero no tienen acceso a las claves de encriptación de los datos compartidos. El contenido permanece encriptado de extremo a extremo y sólo se puede acceder a él en los dispositivos de confianza de los participantes. Para cada acción de compartir, Apple puede almacenar un título y una miniatura representativa con protección de datos estándar para mostrar una vista previa a los usuarios destinatarios.

Si se selecciona la opción Cualquier persona con el enlace al activar la colaboración, el contenido estará disponible para los servidores de Apple bajo la protección de datos estándar, ya que los servidores deben poder proporcionar acceso a cualquier persona que abra la URL.

La colaboración en iWork y la función Álbumes compartidos de Fotos no son compatibles con la protección de datos avanzada. Cuando los usuarios colaboran en un documento de iWork o abren un documento de iWork desde una carpeta compartida en iCloud Drive, las claves de encriptación del documento se cargan de forma segura en los servidores de iWork en los centros de datos de Apple. Esto se debe a que la colaboración en tiempo real en iWork requiere la mediación del lado del servidor para coordinar los cambios de los documentos entre los participantes. Las fotos agregadas a Álbumes compartidos se almacenan con protección de datos estándar, ya que la función permite que los álbumes se compartan públicamente en Internet.

Desactivar la protección de datos avanzada

El usuario puede desactivar la protección de datos avanzada en cualquier momento. Si decide hacerlo, sucede lo siguiente:

1. El dispositivo del usuario primero registra su nueva elección en los metadatos de participación del llavero de iCloud, y esta configuración se sincroniza de forma segura con todos sus dispositivos.

2. El dispositivo del usuario carga de forma segura las claves de servicio de todos los servicios *disponibles después de la autenticación* en los HSM de iCloud en los centros de datos de Apple. Esto nunca incluye las claves de servicios que están encriptadas de extremo a extremo bajo la protección de datos estándar, como los datos de Salud y del llavero de iCloud.

El dispositivo carga tanto las claves de servicio originales (generadas antes de que se activara la protección de datos avanzada) como las nuevas claves de servicio que se generaron después de que el usuario activara la función. Esto ocasiona que se pueda acceder a todos los datos de estos servicios después de autenticarse y devuelve la cuenta a la protección de datos estándar, con lo cual Apple puede ayudar nuevamente al usuario a recuperar la mayoría de sus datos en caso de que pierda el acceso a su cuenta.

Datos de iCloud no cubiertos por la protección de datos avanzada

Debido a la necesidad de interoperar con los sistemas globales de correo electrónico, contactos y calendario, los datos de Contactos, Calendario y Mail en iCloud no se encriptan de extremo a extremo.

iCloud almacena algunos datos sin la protección de las claves de servicio de CloudKit específicas del usuario, incluso cuando la protección de datos avanzada está activada. Los campos de registro de CloudKit deben declararse explícitamente como "encriptados" en el esquema del contenedor para que cuenten con la protección; y la lectura y escritura de los campos encriptados requiere el uso de API dedicadas. Las fechas y horas en que se modificó un archivo u objeto se usan para ordenar la información del usuario, y las sumas de verificación de los datos de archivos y fotos se utilizan para ayudar a Apple a deduplicar y optimizar iCloud y el almacenamiento del dispositivo del usuario; todo sin tener acceso a los archivos y a las fotos en sí. En el artículo de soporte de Apple Descripción general de la seguridad de datos de iCloud puedes encontrar detalles sobre cómo se utiliza la encriptación en categorías de datos específicas.

El diseño original de los servicios de iCloud al momento de su lanzamiento incluía una técnica habitual llamada *encriptación convergente*, en donde se tomaban decisiones como el uso de sumas de verificación para la deduplicación de datos. Estos metadatos siempre están encriptados, pero Apple almacena las claves de encriptación con protección de datos estándar. Para seguir fortaleciendo las protecciones de seguridad para todos los usuarios, Apple se compromete a garantizar que más datos, incluido este tipo de metadatos, se encripten de extremo a extremo al activar la protección de datos avanzada.

Requisitos para la protección de datos avanzada

Los requisitos para activar la protección de datos avanzada para iCloud incluyen lo siguiente:

- La cuenta del usuario debe ser compatible con la encriptación de extremo a extremo, y esta a su vez requiere que el Apple ID cuente con autenticación de dos factores y que los dispositivos de confianza tengan establecido un código de acceso o una contraseña. Para obtener más información, consulta el artículo de soporte de Apple Autenticación de dos factores para Apple ID.
- Los dispositivos en los que el usuario haya iniciado sesión con su Apple ID deben contar con iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 o la versión más reciente de iCloud para Windows. Este requisito impide que una versión anterior de iOS, iPadOS, macOS, tvOS o watchOS manipule incorrectamente las claves de servicio recién creadas al volver a cargarlas en los HSM *disponibles después de la autenticación* en un intento erróneo de reparar el estado de la cuenta.
- El usuario debe configurar al menos un método de recuperación alternativo (uno o más contactos de recuperación o una clave de recuperación) que pueda usar para recuperar sus datos de iCloud en caso de que pierda el acceso a su cuenta.

Si los métodos de recuperación fallan (por ejemplo, si la información del contacto de recuperación no está actualizada o si el usuario olvida la información necesaria), Apple no puede ayudar a recuperar los datos de iCloud encriptados de extremo a extremo del usuario.

La protección de datos avanzada para iCloud solamente puede activarse para los Apple ID. Los Apple ID administrados y las cuentas de menores de edad (varía según el país o la región) no son compatibles.

Seguridad del respaldo en iCloud

iCloud realiza un respaldo de la información, incluida la configuración del dispositivo, los datos de las apps, las fotos y los videos del rollo fotográfico, y las conversaciones de la app Mensajes, todos los días a través de la red Wi-Fi. El respaldo en iCloud se lleva a cabo solamente cuando el dispositivo está bloqueado, conectado a una fuente de alimentación y tiene acceso a Internet mediante una red Wi-Fi. El respaldo en iCloud toma en cuenta la encriptación del almacenamiento que se usa en iOS y en iPadOS, por lo que está diseñado para mantener protegidos los datos al mismo tiempo que permitir que se realicen respaldos y restauraciones progresivas y sin supervisión. De forma predeterminada, la clave de servicio del respaldo en iCloud se respalda de manera segura en los módulos de seguridad de hardware de iCloud en los centros de datos de Apple y forma parte de la categoría de datos disponibles después de la autenticación. En el caso de los usuarios que activan la protección de datos avanzada para iCloud, la clave de servicio del respaldo en iCloud está protegida con encriptación de extremo a extremo y sólo está disponible para los usuarios en sus dispositivos de confianza.

Cuando se crean archivos en las clases de protección de datos a las que no se puede acceder cuando el dispositivo está bloqueado, las claves por archivo correspondientes se encriptan usando las claves de clase del repositorio de claves del respaldo en iCloud, respaldando los archivos en iCloud en su estado encriptado original. Todos los archivos se encriptan cuando se transfieren y además, durante su almacenamiento, se encriptan usando claves basadas en la cuenta, tal como se describe en Encriptación de CloudKit.

El repositorio de claves del respaldo en iCloud contiene claves asimétricas (Curve25519) para las clases de protección de datos que no son accesibles cuando el dispositivo está bloqueado. El conjunto de respaldos se almacena en la cuenta de iCloud del usuario y consiste en una copia de los archivos del usuario y el repositorio de claves del respaldo en iCloud. Este repositorio está protegido mediante una clave aleatoria, que también está almacenada en el conjunto de respaldos La contraseña de iCloud del usuario no se usa para la encriptación; de este modo, cambiar la contraseña de iCloud no invalida los respaldos existentes.

Durante la restauración, se obtienen de la cuenta de iCloud del usuario los archivos de los que se ha realizado un respaldo, el repositorio de claves del respaldo en iCloud y la clave para el repositorio. El repositorio de claves del respaldo en iCloud se desencripta usando su clave, luego las claves por archivo del repositorio de claves se usan para desencriptar los archivos del conjunto de respaldos, que se escriben como archivos nuevos en el sistema de archivos y, de este modo, se vuelven a encriptar según la clase de protección de datos correspondiente.

Los siguientes elementos se respaldan usando el respaldo en iCloud:

- Registros de música, películas, programas de TV, apps y libros comprados. El respaldo en iCloud de un usuario incluye información sobre el contenido comprado presente en el dispositivo, pero no contiene el contenido comprado en sí. Cuando el usuario realiza una restauración a partir de un respaldo en iCloud, su contenido comprado se descarga automáticamente desde iTunes Store, App Store, la app Apple TV o Apple Books. Algunos tipos de contenidos no se descargan automáticamente en todos los países o regiones, y las compras previas podrían no estar disponibles si se han reembolsado o si ya no están disponibles en la tienda correspondiente. El historial de compras completo está asociado al Apple ID del usuario.
- Fotos y videos en un dispositivo del usuario. Toma en cuenta que si un usuario activa Fotos en iCloud en iOS 8.1, iPadOS 13.1 u OS X 10.10.3 o versiones posteriores, sus fotos y videos ya se encuentran almacenados en iCloud, por lo que no se incluyen en el respaldo en iCloud.
- Contactos, eventos de calendario, recordatorios y notas.
- Configuración del dispositivo.
- Datos de apps.
- Organización de apps y la pantalla de inicio.
- Configuración de HomeKit.
- Datos de la ficha médica.
- Contraseña de Notas de Voz (de ser necesario, requiere la tarjeta SIM física que se usó durante el respaldo).
- Mensajes de la app Mensajes, Apple Messages for Business, mensajes de texto (SMS) y mensajes MMS (de ser necesario, se requiere la tarjeta SIM física que se usó durante el respaldo).

El respaldo en iCloud se usa también para hacer un respaldo del llavero del dispositivo local, encriptado con una clave derivada de la clave criptográfica raíz (UID) del Secure Enclave del dispositivo. Esta clave es exclusiva del dispositivo y Apple no la conoce. Esto permite que la base de datos sólo se pueda restaurar en el mismo dispositivo en el que se originó; es decir que nadie más (incluido Apple) puede leerla. Para obtener más información, consulta Secure Enclave.

Mensajes en iCloud

La función Mensajes en iCloud mantiene todo el historial de mensajes de un usuario actualizado y disponible en todos sus dispositivos.

Gracias a la protección de datos estándar, los mensajes en iCloud se encriptan de extremo a extremo si el respaldo en iCloud está desactivado. Si se activa el respaldo en iCloud, el respaldo incluye una copia de la clave de encriptación de Mensajes en iCloud, de forma que Apple puede ayudar al usuario a recuperar sus mensajes incluso si perdieron el acceso al llavero de iCloud y a sus dispositivos de confianza. Si el usuario desactiva el respaldo en iCloud, se genera una nueva clave en su dispositivo para proteger los futuros mensajes en iCloud. Esta nueva clave se almacena únicamente en el llavero de iCloud y sólo el usuario puede acceder a ella en sus dispositivos de confianza; además, los nuevos datos escritos en el contenedor no se pueden desencriptar con la clave del contenedor anterior.

Con la protección de datos avanzada, los mensajes en iCloud siempre están encriptados de extremo a extremo. Si se activa el respaldo en iCloud, todo lo que contiene se encripta de extremo a extremo, incluidos los mensajes en la clave de encriptación de iCloud. Tanto la clave de servicio del respaldo en iCloud como la clave del contenedor de Mensajes en iCloud se implementan cuando el usuario activa la protección de datos avanzada. Para obtener más información, consulta el artículo de soporte de Apple Descripción general de la seguridad de datos de iCloud.

Seguridad de Contactos de recuperación de cuenta

Los usuarios pueden agregar un máximo de cinco personas de confianza como contactos de recuperación de cuenta para que les ayuden a recuperar sus datos y su cuenta de iCloud, incluidos los datos encriptados de extremo a extremo (independientemente de si han activado o no la protección de datos avanzada). Ni Apple ni el contacto de recuperación tienen la información necesaria individualmente para recuperar los datos de iCloud encriptados de extremo a extremo del usuario.

La función de contactos de recuperación se diseñó tomando en cuenta la privacidad del usuario. Apple no sabe a quién elige un usuario como contacto de recuperación. Los servidores de Apple sólo obtienen información sobre un contacto de recuperación al final de un intento de recuperación después de que el usuario le pide ayuda al contacto y este comienza a ayudar con la recuperación. Una vez que se completa la recuperación, esa información no se retiene.

Proceso de seguridad de los contactos de recuperación

Cuando un usuario configura un contacto de recuperación de cuenta, la clave necesaria para acceder a los datos de iCloud del usuario, incluidos los datos de CloudKit encriptados de extremo a extremo, se encripta con una clave aleatoria segura. Esta clave aleatoria se divide después entre el contacto de recuperación y Apple. La clave original puede obtenerse durante el proceso de recuperación solamente cuando se vuelven a combinar estas dos claves, permitiendo así el acceso a los datos en iCloud del usuario.

Para configurar un contacto de recuperación, el dispositivo del usuario se comunica con los servidores de Apple para cargar la porción de la clave que Apple conservará. A continuación, establece un contenedor de CloudKit encriptado de extremo a extremo con el contacto de recuperación para compartir la porción que este requiere. Tanto Apple como el contacto de recuperación reciben el mismo secreto de autorización del usuario, el cual se requiere más tarde para la recuperación. La comunicación para invitar y aceptar contactos de recuperación se lleva a cabo a través de un canal IDS autentificado mutuamente. El contacto de recuperación almacena automáticamente la información recibida en su llavero de iCloud. Apple no puede acceder ni a los contenidos del contenedor de CloudKit ni al llavero de iCloud que almacena esta información. Al momento de compartir, los servidores de Apple visualizan solamente un ID anónimo del contacto de recuperación.

Más tarde, cuando un usuario necesite recuperar su cuenta y sus datos en iCloud, puede solicitar ayuda a su contacto de recuperación. En ese momento, el dispositivo del contacto de recuperación genera un código de recuperación, que debe proporcionar al usuario por un medio separado (por ejemplo, en persona o mediante una llamada telefónica). A continuación, el usuario ingresa este código en su dispositivo para establecer una conexión segura entre dispositivos utilizando el protocolo SPAKE2+, cuyos contenidos no son accesibles para Apple. Esta interacción la organizan los servidores de Apple, pero Apple no puede iniciar el proceso de recuperación.

Una vez que se establece la conexión segura y se completan todas las comprobaciones de seguridad necesarias, el dispositivo del contacto de recuperación devuelve su porción de la información de la clave y el secreto de autorización establecido anteriormente al usuario que solicitó la recuperación. El usuario presenta este secreto de autorización a un servidor de Apple, lo que autoriza el acceso a la información de la clave que Apple tiene. Al presentar el secreto de autorización, también se permite el restablecimiento de la contraseña de la cuenta para poder restaurar el acceso a la misma.

Por último, el dispositivo del usuario vuelve a combinar la información de la clave recibida de Apple y del contacto de recuperación de cuenta, y luego la usa para desencriptar y recuperar sus datos de iCloud.

Estas son protecciones que sirven para impedir que un contacto de recuperación inicie el proceso sin el consentimiento del usuario, lo cual incluye una revisión de actividad o inactividad de la cuenta del usuario. Si la cuenta se usa de forma activa, la recuperación mediante un contacto de recuperación también requerirá que se conozca un código reciente del dispositivo o el código de seguridad de iCloud.

Seguridad de Contactos para legado

Si un usuario quiere que sus datos de iCloud sean accesibles para los beneficiarios designados después de su muerte, puede configurar los contactos para legado en su cuenta. Un beneficiario designado como contacto para legado obtiene acceso a todos los datos en iCloud de la persona difunta, incluidos casi todos los datos encriptados de extremo a extremo excepto los datos del llavero de iCloud, tales como las contraseñas de las cuentas. La tecnología subyacente de la función de contacto para legado es similar a la de contactos de recuperación: una clave aleatoria segura que se divide entre Apple y el contacto para legado, de modo que ninguno pueda desencriptar los datos por su cuenta. Una persona beneficiaria recibe las mismas clases de datos, independientemente de si el usuario activó o no la protección de datos avanzada.

La información de clave que recibe un beneficiario se denomina clave de acceso en la documentación dirigida al usuario final, y se guarda automáticamente en los dispositivos compatibles, aunque también puede imprimirse y almacenarse físicamente para su uso. Para obtener más información, consulta el artículo de soporte de Apple Cómo agregar un contacto para legado para tu Apple ID.

Tras el fallecimiento del usuario, los contactos para legado inician sesión en el sitio web de reclamaciones de Apple para iniciar el acceso. Esto requiere un certificado de defunción y se autoriza en parte mediante el secreto de autorización mencionado en la sección anterior. Una vez completadas todas las comprobaciones de seguridad, Apple emite un nombre de usuario y una contraseña para la nueva cuenta y libera la información de clave necesaria al contacto para legado.

Para facilitar el ingreso de la clave de acceso cuando sea necesario, esta se presenta como un código alfanumérico con un código QR asociado. Una vez ingresada, se restablece el acceso a los datos en iCloud de la persona difunta. Esto puede hacerse en un dispositivo, o el acceso puede establecerse en línea. Para obtener más información, consulta el artículo de soporte de Apple Solicitar acceso a una cuenta de Apple como contacto para legado.

Seguridad de la retransmisión privada de iCloud

La retransmisión privada de iCloud ayuda a proteger a los usuarios principalmente cuando navegan por Internet con Safari, pero también incluye todas las solicitudes de resolución de nombres DNS. Esto ayuda a garantizar que ninguna parte, ni siquiera Apple, pueda correlacionar la dirección IP de un usuario y su actividad de navegación. Para ello, se utilizan diferentes proxies: un proxy de entrada, administrado por Apple, y un proxy de salida, administrado por un proveedor de contenidos. Para usar la retransmisión privada de iCloud, el usuario debe tener instalado iOS 15, iPadOS 15 o macOS 12.0.1 o versiones posteriores, y debe haber iniciado sesión en su cuenta de iCloud+ con su Apple ID. La retransmisión privada de iCloud puede activarse en Configuración > iCloud, o en Configuración del Sistema > iCloud.

Para obtener más información, consulta Resumen de la retransmisión privada de iCloud.

Administración de códigos y contraseñas

Descripción general de la seguridad de las contraseñas

iOS, iPadOS y macOS le facilitan al usuario autenticarse en apps y sitios web de terceros que utilizan contraseñas. La mejor manera de administrar las contraseñas es no tener que usar contraseñas. La función Iniciar sesión con Apple les permite a los usuarios iniciar sesión en apps y sitios web de terceros sin tener que crear ni administrar una cuenta o contraseña adicional al mismo tiempo que protege el inicio de sesión mediante la autenticación de dos factores para el Apple ID. En el caso de los sitios que no son compatibles con Iniciar sesión con Apple, la funcionalidad de contraseña segura automática permite a los dispositivos del usuario crear, sincronizar e ingresar automáticamente contraseñas seguras en sitios y apps. En iOS y iPadOS, las contraseñas se guardan en un llavero especial para el autorrelleno de contraseñas que el usuario puede controlar y administrar desde Configuración > Contraseñas.

En macOS, las contraseñas guardadas se pueden administrar en las preferencias de contraseñas de Safari. Este sistema de sincronización también se puede usar para sincronizar las contraseñas que el usuario crea manualmente.

Seguridad de Iniciar sesión con Apple

La función Iniciar sesión con Apple protege la privacidad a la vez que ofrece una alternativa a otros sistemas con inicio de sesión único. Brinda la conveniencia y la eficiencia de iniciar sesión con un solo toque, a la vez que le da al usuario más transparencia y control sobre su información personal.

La función Iniciar sesión con Apple les permite a los usuarios configurar una cuenta e iniciar sesión en apps y sitios web usando el Apple ID que ya tienen, y les da más control sobre su información personal. Las apps sólo pueden pedir el nombre y la dirección de correo electrónico del usuario cuando se está configurando una cuenta, y el usuario siempre tiene la elección: puede compartir su dirección de correo electrónico personal con una app, o bien puede elegir mantener esa dirección en privado y usar el nuevo servicio de retransmisión privada de correo electrónico de Apple. Este servicio de retransmisión de correo comparte una dirección de correo electrónico única y anónima que se reenvía a la dirección personal del usuario para que pueda seguir recibiendo comunicación útil de parte del desarrollador, a la vez que mantiene un nivel de privacidad y control sobre su información personal.

La función Iniciar sesión con Apple se desarrolló pensando en la seguridad. Todos los usuarios de Iniciar sesión con Apple deben tener activada la autenticación de dos factores para su Apple ID. La autenticación de dos factores no sólo ayuda a que el Apple ID del usuario esté seguro, sino también las cuentas que configure con sus apps. Además, Apple desarrolló e integró una señal antifraude que respeta la privacidad en la función Iniciar sesión con Apple. Esta señal les brinda a los desarrolladores la confianza de que los nuevos usuarios que adquieren son personas reales y no bots o cuentas falsas.

Contraseñas seguras automáticas

Cuando el llavero de iCloud está activado, iOS, iPadOS y macOS crean contraseñas seguras, aleatorias y únicas cuando los usuarios se registran o cambian sus contraseñas en un sitio web en Safari. En iOS y iPadOS, la generación de contraseñas seguras automáticas también está disponible para las apps. Si así lo desean, los usuarios pueden rechazar la opción para usar contraseñas seguras. Las contraseñas generadas se guardan en el llavero y se actualizan en los demás dispositivos que usan el llavero de iCloud, cuando está activado.

De forma predeterminada, las contraseñas generadas por iOS y iPadOS tienen 20 caracteres de extensión; contienen un dígito, una letra mayúscula, dos guiones y 16 letras en minúscula. Estas contraseñas son seguras y contienen 71 bits de entropía.

Las contraseñas se generan siguiendo un método heurístico que determina que la experiencia de un campo de contraseñas es para la creación de contraseñas. Si el método heurístico no logra reconocer una contraseña específica del contexto que se utiliza durante la creación de la contraseña, los desarrolladores de apps pueden establecer `UITextContentType.newPassword` en su campo de texto, y los desarrolladores web pueden establecer `autocomplete= “new–password”` en sus elementos <input>.

Para ayudar a garantizar que las contraseñas generadas sean compatibles con los servicios correspondientes, las apps y los sitios web pueden brindar reglas. Los desarrolladores proporcionan estas reglas utilizando `UITextInputPasswordRules` o el atributo `passwordrules` en sus elementos “input”. Los dispositivos entonces generan la contraseña más segura que puedan que cumpla con estas reglas.

Seguridad del relleno automático de contraseñas

El relleno automático de contraseñas ingresa automáticamente los datos de inicio de sesión almacenados en el llavero. El administrador de contraseñas del llavero de iCloud y la función Autorrellenar contraseñas ofrecen las siguientes funciones:

- Rellenar credenciales en apps y sitios web.
- Generar contraseñas seguras.
- Guardar contraseñas de apps y sitios web de Safari.
- Compartir contraseñas de manera segura con los contactos del usuario.
- Proporcionar contraseñas a un Apple TV cercano que las solicita.

La funciones para generar y almacenar contraseñas dentro de apps, así como proporcionar contraseñas para un Apple TV, sólo están disponibles en iOS y iPadOS.

Autorrellenar contraseñas en apps

iOS y iPadOS les permiten a los usuarios ingresar nombres de usuario y contraseñas guardados en los campos relacionados con el inicio de sesión en apps, de forma similar a como funciona en Safari. En iOS y iPadOS, los usuarios pueden tocar una posibilidad de clave en la barra QuickType del teclado virtual. En las apps desarrolladas con Mac Catalyst para macOS, aparece un menú desplegable Contraseñas debajo de los campos relacionados con el inicio de sesión.

Cuando una app está fuertemente asociada con un sitio web que usa el mismo mecanismo de asociación app-sitio web y que está habilitado por el mismo archivo de asociación apple-app-sitio, el menú desplegable de macOS y la barra QuickType de iOS y iPadOS sugieren directamente los datos de inicio de sesión para la app, si cualquiera de ellos se guardó en el llavero de autorrelleno de contraseñas. Esto permite que el usuario elija si se revelan las credenciales guardadas en Safari a las apps que tienen las mismas propiedades de seguridad, sin necesidad de que las apps tengan que adoptar una API.

El relleno automático de contraseñas no revela información de credenciales a la app hasta que el usuario haya aceptado compartir una credencial con la app. Las listas de datos de inicio de sesión se presentan u obtienen desde fuera del proceso de la app.

Cuando una app y un sitio web tienen una relación de confianza y el usuario envía credenciales dentro de la app, iOS y iPadOS pueden preguntarle al usuario si desea guardar esas credenciales en el llavero de autorrelleno de contraseñas para usarlas posteriormente.

Acceso de las apps a las contraseñas guardadas

Las apps de iOS, iPadOS y macOS pueden solicitar la asistencia del llavero de autorrelleno de contraseñas para iniciar la sesión de un usuario con `ASAuthorizationPasswordProvider` y `SecAddSharedWebCredential`. El proveedor de la contraseña y su solicitud se pueden usar junto con Iniciar sesión con Apple, de forma que se llame a la misma API para que ayude a los usuarios a iniciar sesión en una app independientemente de si la cuenta del usuario está basada en contraseña o si se generó usando Iniciar sesión con Apple.

Se puede conceder a las apps acceso a las contraseñas guardadas sólo si tanto el desarrollador de la app como el administrador del sitio web han dado su aprobación; y el usuario, su consentimiento. Los desarrolladores de apps incluyen una autorización en su app para expresar su intención de acceder a las contraseñas guardadas de Safari. La autorización enumera los nombres de dominios cualificados de sitios web asociados y los sitios web deben colocar un archivo en su servidor indicando los identificadores de app únicos de las apps que Apple ha aprobado.

Cuando se instala una app con la autorización com.apple.developer.associated-domains, iOS y iPadOS envían una solicitud de TLS a cada sitio web de la lista para solicitar uno de los siguientes archivos:

- apple-app-site-association
- .well-known/apple-app-site-association

Si el archivo incluye el identificador de apps de la app que se está instalando, iOS y iPadOS marcarán que el sitio web y la app tienen una relación de confianza. Las llamadas a estas dos API sólo generan una solicitud para el usuario cuando existe una relación de confianza; se requiere la aceptación del usuario para que se lleve a cabo la entrega de contraseñas a la app o para que se actualicen o eliminen.

Recomendaciones de seguridad para las contraseñas

La lista de contraseñas del autorrelleno de contraseñas en iOS, iPadOS y macOS indica cuál de las contraseñas guardadas del usuario se *reutiliza* también en otros sitios web, cuáles se consideran *no seguras*, y cuáles se han transgredido en una *filtración de datos*.

Descripción general

Usar la misma contraseña para más de un servicio puede dejar a esas cuentas vulnerables a un ataque de relleno de datos de inicio de sesión. Si un servicio se ve vulnerado y se filtran las contraseñas, los atacantes pueden intentar usar los mismos datos de inicio de sesión de otros servicios para intentar entrar a otras cuentas.

- Las contraseñas se marcan como *reutilizadas* si una misma contraseña se ha usado en más de una ocasión en diferentes dominios.
- Las contraseñas se marcan como *no seguras* si algún atacante las podría adivinar fácilmente. iOS, iPadOS y macOS detectan patrones comunes para crear contraseñas que se pueden recordar, como las palabras del diccionario, sustituciones comunes de caracteres (como “c0ntr4s3n4” en lugar de “contraseña”), patrones del teclado (como “q12we34r” en un teclado QWERTY), o secuencias repetidas (como “123123”). Estos patrones a menudo se utilizan para crear contraseñas que cumplan con los requisitos mínimos de los servicios, pero también las usan comúnmente los atacantes para intentar obtener una contraseña mediante un ataque forzado.

  Debido a que muchos servicios requieren específicamente un código NIP de cuatro o seis dígitos, estas contraseñas cortas se evalúan con reglas distintas. Los códigos NIP se consideran no seguros si son algunos de los más utilizados, si son números consecutivos en aumento o disminución, como “1234” o “8765,” o si siguen un patrón de repetición, como “123123” o “123321”.
- Las contraseñas se marcan como *filtradas* si la función de monitoreo de contraseñas descubre que fue expuesta mediante una filtración de datos. Para obtener más información, consulta Monitoreo de contraseñas.

Las contraseñas no seguras, reutilizadas y filtradas se indican en la lista de contraseñas (macOS) o están presentes en la interfaz de recomendaciones de seguridad (iOS y iPadOS). Si el usuario inicia sesión en un sitio web en Safari usando una contraseña previamente guardada y no segura, o que ha sido transgredida por una filtración de datos, se muestra una alerta que aconseja fuertemente actualizarla a una contraseña segura automática.

Actualizar la seguridad de la autenticación de cuentas en iOS y iPadOS

Las apps que implementan la extensión de modificación de autenticación de la cuenta (en la estructura de servicios de autenticación) pueden brindar actualizaciones fáciles y con sólo tocar un botón para las cuentas basadas en contraseñas; esto significa que pueden usar Iniciar sesión con Apple o una contraseña segura automática. Este punto de extensión está disponible en iOS y iPadOS.

Si la app implementó el punto de extensión y está instalado en el dispositivo, los usuarios ven las opciones de actualización de extensión en las recomendaciones de seguridad para las credenciales asociadas con la app en el administrador de contraseñas del llavero de iCloud que se encuentra en Configuración. También se ofrecen actualizaciones cuando los usuarios inician sesión en la app con la credencial en riesgo. Las apps pueden solicitar al sistema que no muestre a los usuarios las opciones de actualización después de iniciar sesión. Con la nueva API de AuthenticationServices, las apps también pueden invocar sus extensiones y realizar actualizaciones por sí mismas, idealmente desde la configuración de una cuenta o la pantalla de administración de cuentas en la app.

Las apps pueden permitir actualizar a una contraseña más segura, actualizar a Iniciar sesión con Apple, o ambas. Cuando se actualiza a una contraseña más segura, el sistema generará una de forma automática para el usuario. De ser necesario, la app puede brindar reglas personalizadas para la contraseña que deberán seguirse al generar la nueva contraseña. Cuando un usuario deja de usar una contraseña y cambia a Iniciar sesión con Apple en una cuenta, el sistema le proporciona una credencial nueva de Iniciar sesión con Apple a la extensión para asociarla con la cuenta. El correo electrónico del Apple ID del usuario no se incluye en la credencial. Después de actualizar correctamente a Iniciar sesión con Apple, el sistema borra la credencial de la contraseña anterior del llavero (si estaba guardada ahí).

Las extensiones de modificación de autenticación de la cuenta pueden realizar una autenticación adicional del usuario antes de realizar una actualización. En el caso de las actualizaciones iniciadas desde el administrador de contraseñas o después de iniciar sesión en la app, la extensión proporciona el nombre de usuario y la contraseña para actualizar la cuenta. Para las actualizaciones dentro de la app, sólo se proporciona el nombre de usuario. Si la extensión requiere una autenticación de usuario adicional, se puede solicitar que se muestre una interfaz de usuario personalizada antes de proceder con la actualización. La intención del caso de uso al mostrar esta interfaz es que el usuario ingrese un segundo factor de autenticación para autorizar la actualización.

Monitoreo de contraseñas

El monitoreo de contraseñas es una función que verifica si las contraseñas del usuario almacenadas en el llavero de autorrelleno de contraseñas coinciden con una lista de contraseñas que se sabe que han sido expuestas en filtraciones de varias fuentes en línea. Si la función está activada, el protocolo de monitoreo verifica continuamente si hay coincidencias entre las contraseñas del llavero de autorrelleno de contraseñas y la lista revisada.

Cómo funciona el monitoreo

El dispositivo del usuario realiza continuamente comprobaciones en las contraseñas del usuario, realizando consultas en un intervalo que es independiente de las contraseñas del usuario o de los patrones de uso de su administrador de contraseñas. Esto ayuda a garantizar que los estados de verificación se mantengan actualizados con la lista actual de contraseñas filtradas. Para ayudar a evitar la filtración de información relacionada con el número de contraseñas únicas del usuario, las solicitudes se agrupan y se ejecutan de forma paralela. Con cada comprobación, se verifica en paralelo un número fijo de contraseñas y, si el número tiene menos contraseñas que esta cantidad, se generan contraseñas aleatorias y se añaden a las consultas para compensar la diferencia.

Coincidencia de contraseñas

Las coincidencias de contraseñas se realizan en un proceso que consta de dos partes. Las contraseñas más comúnmente filtradas se encuentran dentro de una lista local en el dispositivo del usuario. Si una de las contraseñas del usuario coincide con una de la lista, se notifica de inmediato al usuario sin interacción externa alguna. Esto está diseñado para garantizar que no se filtre información sobre las contraseñas que tiene un usuario y que tienen mayor riesgo de ser transgredidas.

Si la contraseña no está en la lista de las más frecuentes, entonces se verifica en la lista de contraseñas menos filtradas.

Comparación de las contraseñas del usuario con la lista revisada

Para verificar si una contraseña coincide o no con alguna de las que están en la lista local, es necesario establecer una interacción con los servidores de Apple. Para ayudar a garantizar que no se envíen a Apple contraseñas legítimas de los usuarios, se implementa un tipo de *intersección de conjunto criptográfico privado*, el cual compara las contraseñas del usuario respecto a un conjunto extenso de contraseñas filtradas. Esto está diseñado para garantizar que se comparta menos información con Apple sobre las contraseñas que tienen menos riesgo de filtrarse. Para la contraseña de un usuario, esta información está limitada a un prefijo de 15 bits de un hash criptográfico. Eliminar de este proceso interactivo las contraseñas filtradas con mayor frecuencia (utilizando la lista local de contraseñas filtradas comúnmente) reduce el delta en la frecuencia relativa de contraseñas en los depósitos de servicios web, lo que hace que no sea práctico inferir las contraseñas de los usuarios a partir de estas consultas.

El protocolo subyacente divide la lista revisada de contraseñas, que contiene aproximadamente 1,500 millones de contraseñas al momento de esta publicación, en 2^{15} buckets diferentes. El bucket al que pertenece una contraseña se basa en los primeros 15 bits del valor hash SHA256 de la contraseña. Además, cada contraseña filtrada, pw, se asocia con un punto curvo elíptico en la curva NIST P256: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, donde α es una clave aleatoria secreta que sólo Apple conoce, y H_{SWU} es una función aleatoria de Oracle que asigna las contraseñas en los puntos de la curva basada en el método Shallue-van de Woestijne-Ulas. Esta transformación está diseñada para ocultar de forma computacional los valores de las contraseñas y ayuda a evitar revelar contraseñas recientemente filtradas mediante el monitoreo de contraseñas.

Para computar la intersección de conjunto privado, el dispositivo del usuario determina a cuál bucket pertenece la contraseña del usuario mediante λ, el prefijo de 15 bits de SHA256(upw), donde upw es una de las contraseñas del usuario. El dispositivo genera su propia constante aleatoria, β, y envía el punto $P_c = \beta \cdot H_{SWU}(upw)$ al servidor, junto con una solicitud para el bucket que corresponde a λ. Aquí, β oculta información sobre la contraseña del usuario y limita a λ la información expuesta de la contraseña a Apple. Por último, el servidor toma el punto enviado por el dispositivo del usuario, realiza el cómputo $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$ y lo devuelve junto con el bucket correspondiente de puntos ($B\lambda = \{ P_{pw} \mid$ SHA256(pw) comienza con el prefijo λ}) al dispositivo.

La información que se devuelve permite al dispositivo realizar el cómputo $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$, y confirma que la contraseña del usuario ha estado en una filtración si $\alpha P_c \in B'_\lambda$.

Envío de contraseñas a otros usuarios o dispositivos Apple

Apple envía contraseñas de forma segura a otros usuarios o dispositivos Apple mediante AirDrop o en Apple TV.

Guardar credenciales en otro dispositivo mediante AirDrop

Cuando iCloud está activado, los usuarios pueden usar AirDrop para enviar una credencial guardada a otro dispositivo. La credencial incluye el nombre y la contraseña del usuario y los sitios web para los que está guardada. El envío de credenciales mediante AirDrop únicamente funciona en el modo Sólo contactos, independientemente de la configuración que haya seleccionado el usuario. En el dispositivo receptor, después de que el usuario dé su consentimiento, las credenciales se almacenan en el llavero de autorrelleno de contraseñas.

Rellenar credenciales en apps en el Apple TV

Autorrellenar contraseñas también puede ingresar contraseñas en las apps de Apple TV. Cuando el usuario elige un campo de texto de nombre de usuario o contraseña en tvOS, el Apple TV inicia una solicitud a Autorrellenar contraseñas mediante Bluetooth de baja energía (BLE).

Cualquier iPhone, iPad o iPod touch cercano pregunta al usuario si desea compartir una credencial con el Apple TV. El método de encriptación se establece de la siguiente manera:

- Si el dispositivo y el Apple TV utilizan la misma cuenta de iCloud, la encriptación entre los dispositivos sucede automáticamente.
- Si el dispositivo tiene iniciada sesión en una cuenta de iCloud distinta a la que utiliza el Apple TV, se le pide al usuario que establezca una conexión encriptada mediante el uso de un código NIP. Para recibir la solicitud, el iPhone debe estar desbloqueado y cerca del Siri Remote enlazado al Apple TV.

Una vez que se estableció la conexión encriptada mediante BLE, la credencial se envía al Apple TV y se ingresa automáticamente en los campos de texto correspondientes en la app.

Extensiones que proporcionan credenciales

En iOS, iPadOS y macOS, los usuarios pueden designar a una app de terceros participante como el proveedor de credenciales para el autorrelleno de contraseñas desde Configuración > Contraseñas (iOS y iPadOS) o en Preferencias del Sistema > Configuración de extensiones (macOS). Este mecanismo funciona mediante extensiones de app. La extensión del proveedor de credenciales debe ofrecer una visualización para elegir credenciales. Opcionalmente, puede proporcionar metadatos sobre las credenciales guardadas para poder ofrecerlas directamente en la barra de sugerencias QuickType (iOS y iPadOS) o en una sugerencia de autocompletar (macOS). Los metadatos incluyen el sitio web de la credencial y el nombre de usuario asociado, pero no la contraseña. iOS, iPadOS y macOS se comunicarán con la extensión para obtener la contraseña cuando el usuario decida rellenar una credencial en una app o sitio web en Safari. Los metadatos de las credenciales se almacenan dentro del contenedor de app del proveedor de credenciales y se eliminan automáticamente después de desinstalar la app.

Llavero de iCloud

Descripción general de la seguridad del llavero de iCloud

iCloud permite a los usuarios sincronizar de manera segura sus contraseñas entre sus dispositivos iOS y iPadOS y computadoras Mac sin revelar su información a Apple. Además de un alto grado de privacidad y seguridad, existen otros objetivos que han influido notablemente en el diseño y la arquitectura del llavero de iCloud como, por ejemplo, su facilidad de uso y la posibilidad de recuperarlo. El llavero de iCloud consta de dos servicios: sincronización y recuperación.

Apple diseñó el llavero de iCloud y su recuperación para que las contraseñas del usuario se mantuvieran protegidas en las siguientes circunstancias:

- Si se puso en riesgo la seguridad de la cuenta de iCloud de un usuario.
- Si se puso en riesgo la seguridad de iCloud a causa de un ataque externo o de un empleado.
- Si un tercero accedió a las cuentas del usuario.

Integración del administrador de contraseñas en el llavero de iCloud

iOS, iPadOS y macOS pueden generar automáticamente cadenas aleatorias criptográficamente seguras para usarlas como contraseñas para las cuentas en Safari. Además, iOS y iPadOS pueden generar contraseñas seguras para las apps. Las contraseñas generadas se almacenan en el llavero y se sincronizan con otros dispositivos. Los elementos del llavero se transfieren de un dispositivo a otro a través de los servidores de Apple. Sin embargo, están encriptados de manera que ni Apple ni otros dispositivos pueden leer su contenido.

Sincronización segura del llavero

Cuando un usuario activa el llavero de iCloud por primera vez, el dispositivo establece un círculo de confianza y crea una identidad de sincronización para sí mismo. La identidad de sincronización consta de una clave privada y una clave pública, las cuales se almacenan en el llavero del dispositivo. La clave pública de la identidad de sincronización se coloca en el círculo y el círculo se firma dos veces: primero, lo firma la clave privada de la identidad de sincronización y, después, una clave de curva elíptica asimétrica (con P-256) derivada de la contraseña de la cuenta de iCloud del usuario. Junto con el círculo también se almacenan los parámetros (valor de sal aleatorio e iteraciones) usados para crear la clave que se basa en la contraseña de iCloud del usuario.

Para las cuentas con autenticación de dos factores, se crea un círculo de sincronización similar adicional, el cual se almacena en CloudKit. Las identidades de los dispositivos en este sistema consisten en dos pares de claves elípticas asimétricas (utilizando el protocolo P-384), las cuales también se almacenan en el llavero. Cada dispositivo mantiene su propia lista de identidades en las que confía, y firma esta lista usando una de sus claves de identidad.

Almacenamiento en iCloud del círculo de sincronización

El círculo de sincronización firmado se almacena en el área de almacenamiento de datos clave-valor de iCloud del usuario. No se puede leer sin conocer la contraseña de iCloud del usuario y no se puede modificar de forma válida sin disponer de la clave privada de la identidad de sincronización de su miembro.

En el caso de las cuentas con la autenticación de dos factores, la lista de sincronización de cada dispositivo se almacena en CloudKit. No se pueden leer las listas sin conocer la contraseña de iCloud del usuario, y no se pueden modificar sin disponer de las claves privadas del dispositivo que las contiene.

Cómo se agregan los otros dispositivos de un usuario al círculo de sincronización

Los dispositivos nuevos, al iniciar sesión en iCloud, se unen al círculo de sincronización del llavero de iCloud de una de las siguientes dos maneras: enlazándose y siendo patrocinados por un dispositivo existente en el llavero de iCloud, o utilizando la recuperación del llavero de iCloud.

Durante los flujos de enlace, el dispositivo solicitante crea nuevas identidades de sincronización tanto para el círculo de sincronización como para las listas de sincronización (para las cuentas con autenticación de dos factores) y las presenta al dispositivo patrocinador. El dispositivo patrocinador agrega la clave pública del nuevo miembro al círculo de sincronización y vuelve a firmarlo con la identidad de sincronización correspondiente y la clave derivada de la contraseña de iCloud del usuario. El nuevo círculo de sincronización se ubica en iCloud, donde el nuevo miembro lo firma de manera similar. En las cuentas con autenticación de dos factores, el dispositivo patrocinador también proporciona al dispositivo que se está uniendo un *comprobante* firmado por sus claves de identidad, que indica que el dispositivo solicitante debería ser de confianza. Después, actualiza su lista individual de identidades de sincronización de confianza para incluir al solicitante.

Así, el círculo de sincronización tiene dos miembros y cada uno de ellos dispone de la clave pública del otro. Estos empiezan a intercambiar elementos individuales del llavero mediante el almacenamiento de datos clave-valor de iCloud, o se almacenan en CloudKit, lo que sea más adecuado para la situación. Si los dos miembros del círculo tienen actualizaciones del mismo elemento, se elige uno u otro, lo que da lugar a una eventual coherencia. Cada elemento sincronizado se encripta a fin de que sólo pueda ser desencriptado en un dispositivo perteneciente al círculo de confianza del usuario; ningún otro dispositivo ni Apple podrán desencriptarlo.

A medida que se unen nuevos dispositivos al círculo de sincronización, este “proceso de enlace” se repite. Por ejemplo, cuando se une un tercer dispositivo, este puede enlazarse utilizando cualquiera de los dispositivos existentes. A medida que se agregan nuevos miembros, cada uno se sincroniza con este, lo que está diseñado para garantizar que todos tengan los mismos elementos de llavero.

Sólo se sincronizan algunos elementos

Algunos elementos del llavero son específicos del dispositivo, como las claves de iMessage, de modo que deben permanecer en el dispositivo. Como resultado, cada elemento que se sincronizará deberá estar marcado explícitamente con el atributo`kSecAttrSynchronizable`.

Apple configura este atributo para los datos de usuario de Safari (que incluyen los nombres de usuario, contraseñas y números de tarjetas de crédito), así como para las contraseñas de redes Wi-Fi, las claves de encriptación de HomeKit, y otros elementos del llavero compatibles con la encriptación de punto a punto de iCloud.

Además, de forma predeterminada, los elementos del llavero que hayan agregado apps de terceros no se sincronizan. Los desarrolladores deben definir el atributo `kSecAttrSynchronizable` al momento de agregar elementos al llavero.

Seguridad de la recuperación del llavero de iCloud

El llavero de iCloud pone en custodia los datos del llavero del usuario con Apple *sin* permitir que Apple lea las contraseñas u otros datos que contenga. Incluso si el usuario solamente dispone de un dispositivo, la recuperación del llavero le proporciona una red de seguridad frente a la pérdida de datos. Esto es especialmente importante cuando Safari se usa para generar contraseñas seguras y aleatorias para cuentas web, ya que el único registro de esas contraseñas está en el llavero.

Dos de los conceptos básicos de la recuperación del llavero son la autenticación secundaria y el servicio de custodia segura, ambos creados por Apple específicamente para admitir esta función. El llavero del usuario se encripta mediante un código seguro, y el servicio de custodia proporciona una copia del llavero únicamente si se cumple una serie de condiciones estrictas.

Usar una autenticación secundaria

Hay varias formas de establecer un código seguro:

- Si la autenticación de dos factores está activada en la cuenta del usuario, se usa el código del dispositivo para recuperar un llavero en custodia.
- Si no está activada la autenticación de dos factores, se le pide al usuario que cree un código de seguridad de iCloud utilizando un código de seis dígitos. De forma opcional, sin la autenticación de dos factores, los usuarios pueden especificar su propio código, que puede ser más largo, o bien permitir que sus dispositivos generen un código aleatorio criptográfico, que pueden registrar y guardar.

Proceso de custodia del llavero

Después de que se establece el código, el llavero se pone en custodia de Apple. El dispositivo iOS, iPadOS o macOS primero exporta una copia del llavero del usuario y luego la encripta encapsulándola con claves en un repositorio de claves asimétrico y la coloca en el área de almacenamiento de datos clave-valor de iCloud del usuario. El repositorio de claves se encapsula con el código de seguridad de iCloud del usuario y la clave pública del clúster del módulo de seguridad de hardware (HSM), que almacenará el registro de la custodia, convirtiéndose así en el *registro de la custodia de iCloud* del usuario. En el caso de las cuentas con autenticación de dos factores, el llavero se guarda también en CloudKit y se encapsula con claves intermedias que sólo se pueden recuperar con los contenidos del registro de custodia de iCloud, lo que brinda el mismo nivel de protección.

El contenido del registro de custodia también permite que el dispositivo recuperado vuelva a unirse al llavero de iCloud, lo que demuestra a cualquier dispositivo existente que el dispositivo recuperado completó satisfactoriamente el proceso de custodia y, por lo tanto, cuenta con la autorización del propietario de la cuenta.

Nota: si el usuario decide aceptar un código de seguridad criptográficamente aleatorio en lugar de especificar el propio o utilizar un valor de cuatro dígitos, el registro de la custodia no será necesario, puesto que el código de seguridad de iCloud se utilizará para encapsular directamente la clave aleatoria.

Además de establecer un código de seguridad, los usuarios deben registrar un número de teléfono. Esto ofrece un nivel secundario de autenticación durante la recuperación del llavero. El usuario recibirá un mensaje SMS al que se debe responder para continuar con la recuperación.

Seguridad de la custodia para el llavero de iCloud

iCloud proporciona una infraestructura segura para custodias de llaveros, para ayudar a garantizar que sólo los usuarios y los dispositivos autorizados puedan realizar una recuperación. Hay clústeres de módulos de seguridad de hardware (HSM) posicionados topográficamente detrás de iCloud que guardan los registros de la custodia. Cada uno tiene una clave que sirve para encriptar los registros de la custodia bajo su supervisión, tal como se describió anteriormente en este documento.

Para recuperar el llavero, los usuarios deben autenticarse con su cuenta de iCloud y su contraseña, y deben responder a un SMS que se envía al teléfono que hayan registrado. Una vez hecho esto, los usuarios deben ingresar su código de seguridad de iCloud. El clúster HSM utiliza el protocolo de contraseña remota segura (SRP) para verificar que un usuario conoce el código de seguridad de iCloud; el código en sí no se envía a Apple. Cada miembro del clúster verifica de manera independiente que el usuario no haya superado el número máximo de intentos permitidos para recuperar el registro, como se indica a continuación. Si la mayoría está de acuerdo, el clúster desencapsula el registro de la custodia y lo envía al dispositivo del usuario.

A continuación, el dispositivo usa el código de seguridad de iCloud para desencapsular la clave aleatoria que se ha usado para encriptar el llavero del usuario. Con esta clave, el llavero (recuperado del almacén de valores de claves de iCloud y de CloudKit) se desencripta y restaura en el dispositivo. iOS, iPadOS y macOS sólo permiten 10 intentos para autenticar y recuperar un registro en custodia. Después de varios intentos fallidos, el registro se bloquea y el usuario debe ponerse en contacto con el servicio de soporte de Apple para que se le concedan más intentos. Después del décimo intento fallido, el clúster del HSM destruye el registro de la custodia y el llavero se pierde para siempre. Este sistema ofrece protección frente a un intento de ataque de fuerza bruta para recuperar el registro aunque conlleve el sacrificio de los datos del llavero.

Estas políticas se codifican en el firmware del HSM. Las tarjetas de acceso administrativo que permiten que el firmware se modifique se han destruido. Cualquier intento de alterar el firmware o de acceder a la clave privada provoca que el clúster del HSM elimine dicha clave. Si esto sucede, el propietario de cada llavero que protege el clúster recibirá un mensaje en el que se indica que se perdió el registro de la custodia. A continuación, podrán decidir si desean volver a inscribirse.

Apple Pay

Descripción general de la seguridad de Apple Pay

Con Apple Pay, los usuarios pueden utilizar dispositivos iPhone, iPad, Mac y Apple Watch para pagar de forma sencilla, segura y privada en tiendas, en apps y en la web mediante Safari. Los usuarios también pueden agregar a Apple Wallet sus tarjetas de transporte público, tarjetas de identificación de estudiante y tarjetas de acceso compatibles con Apple Pay. Es un sistema fácil para los usuarios que incluye seguridad integrada tanto en el hardware como en el software.

Además Apple Pay está diseñado para proteger la información personal del usuario. Apple Pay no recopila información de las transacciones que se pueda vincular al usuario. Las transacciones de pago quedan entre el usuario, el beneficiario y la entidad emisora de la tarjeta.

Seguridad del componente de Apple Pay

Apple Pay usa diversas funciones de hardware y software para poder realizar compras seguras y confiables.

Secure Element

Secure Element es un chip estándar certificado en el que se ejecuta la plataforma Java Card, que cumple con los requisitos del sector financiero en cuanto a pagos electrónicos. El IC del Secure Element y la plataforma para tarjetas de Java están certificados de acuerdo con el proceso de evaluación de seguridad de EMVCo. Después de completar de forma exitosa la evaluación de seguridad, EMVCo emite certificados únicos de IC y de la plataforma.

El IC de Secure Element está certificado según el estándar de Criterios Comunes. Para obtener más información, consulta Certificaciones de seguridad del procesador Secure Enclave en la guía Certificaciones de las plataformas de Apple.

Controlador NFC

El controlador de comunicación de corto alcance (NFC) administra los protocolos NFC y dirige la comunicación entre el procesador de aplicaciones y el Secure Element, y entre el Secure Element y la terminal del punto de venta.

Apple Wallet

La app Wallet se utiliza para agregar y administrar tarjetas de crédito, de débito o de tiendas para hacer pagos con Apple Pay. En Apple Wallet, los usuarios pueden ver sus tarjetas así como información adicional proporcionada por la entidad emisora, tal como la política de privacidad de la entidad emisora de la tarjeta, las transacciones recientes y otros datos. También pueden agregar tarjetas a Apple Pay en los siguientes lugares:

- El Asistente de Configuración y en Configuración de iOS y iPadOS.
- La app Reloj del Apple Watch.
- Wallet y Apple Pay en Preferencias del Sistema de computadoras Mac con Touch ID.

Además, Apple Wallet permite a los usuarios agregar y administrar tarjetas de transporte público, tarjetas de recompensas, pases de abordar, boletos, tarjetas de regalo, tarjetas de identificación de estudiante, tarjetas de acceso y más.

Secure Enclave

En dispositivos iPhone, iPad y Apple Watch y en computadoras Mac con Touch ID y computadoras Mac con Apple Chip que usan el Magic Keyboard con Touch ID, Secure Enclave administra el proceso de autenticación y permite que se realice la transacción de pago.

En el caso del Apple Watch, el dispositivo debe estar desbloqueado y el usuario debe presionar dos veces el botón lateral. Al detectar que se presiona el botón dos veces, la acción se transfiere directamente al Secure Element, o Secure Enclave si está disponible, sin pasar por el procesador de aplicaciones.

Servidores de Apple Pay

Los servidores de Apple Pay administran la configuración y aprovisionamiento de las tarjetas de crédito, débito, transporte público, identificación de estudiante y de acceso en Apple Wallet. Los servidores también administran los números de cuenta del dispositivo almacenados en el Secure Element. Se comunican tanto con el dispositivo como con los servidores de la red de pagos o del emisor de la tarjeta. Los servidores de Apple Pay también son los responsables de volver a encriptar las credenciales de pago para los pagos realizados desde las apps o en la web.

Cómo Apple Pay protege las compras de los usuarios

Secure Element

Secure Element aloja un applet diseñado específicamente para administrar Apple Pay. También incluye applets certificados por redes de pagos o emisores de tarjetas. Los datos de las tarjetas de crédito, débito o prepago se envían a estos applets desde la red de pagos o la entidad emisora de la tarjeta, encriptados con claves que sólo conocen la red de pago o el emisor de la tarjeta y el dominio de seguridad de los applets. Estos datos se almacenan en los applets y se protegen con las funciones de seguridad del Secure Element. Durante una transacción, la terminal se comunica directamente con el Secure Element a través del controlador NFC mediante un bus de hardware dedicado.

Controlador NFC

Como puerta de enlace al Secure Element, el controlador NFC ayuda a garantizar que todas las transacciones de pago sin contacto se realicen a través de una terminal de punto de venta que esté cerca del dispositivo. El controlador NFC sólo marca como transacciones sin contacto aquellas solicitudes de pago procedentes de una terminal cercana.

Una vez almacenada la tarjeta de crédito, débito o prepago (incluyendo las tarjetas de tiendas) el titular de la tarjeta autoriza el pago mediante Face ID, Touch ID o su código, o bien al presionar dos veces el botón lateral de un Apple Watch desbloqueado, el controlador dirige únicamente al campo de NFC las respuestas sin contacto preparadas por los applets de pago del Secure Element. En consecuencia, los datos de autorización de pagos para las transacciones de pago sin contacto se incluyen en el campo local de NFC y nunca se exponen al procesador de aplicaciones. En comparación, los datos de autorización de pagos realizados en las apps y en la web se dirigen al procesador de aplicaciones, pero siempre después de que el Secure Element los encripta en el servidor de Apple Pay.

Tarjetas de crédito, débito y prepago

Descripción general de la seguridad del aprovisionamiento de tarjetas

Cuando un usuario agrega una tarjeta de crédito, débito o prepago (incluidas las tarjetas de tiendas) a Apple Wallet, Apple envía la información de la tarjeta, junto con otra información sobre la cuenta y el dispositivo del usuario, a la entidad emisora o al proveedor de servicios autorizado de la entidad emisora de la tarjeta de forma segura. La entidad emisora de la tarjeta utiliza esta información para decidir si aprueba agregar la tarjeta a Apple Wallet. Como parte del proceso de aprovisionamiento de tarjetas, Apple Pay utiliza tres llamadas del servidor para la comunicación con la entidad emisora de la tarjeta o la red:

- Campos obligatorios
- Verificación de la tarjeta
- Enlace y aprovisionamiento

La entidad emisora de la tarjeta o la red utilizan estas llamadas para verificar, aprobar y agregar tarjetas a Apple Wallet. Estas sesiones entre cliente y servidor usan encriptación TLS 1.2 para transferir los datos.

En el dispositivo y los servidores de Apple Pay, no se almacenan los números de tarjeta completos, sino que se crea un número de cuenta de dispositivo encriptado que después se almacena en el Secure Element. Este número único se encripta de forma que Apple no pueda acceder a él. El número de cuenta de dispositivo es único y diferente de la mayoría de los números de tarjeta de crédito o débito; la entidad emisora de la tarjeta o red de pagos puede impedir su uso en tarjetas de banda magnética, por teléfono o en sitios web. El número de cuenta del dispositivo en Secure Element nunca se guarda en los servidores de Apple Pay ni se respalda en iCloud, y está aislado de los dispositivos iOS, iPadOS y watchOS, y de las computadoras Mac con Touch ID.

Las tarjetas que se utilizan con el Apple Watch se transmiten a Apple Pay mediante la app Apple Watch del iPhone o una app para iPhone proporcionada por el emisor de la tarjeta. Para agregar una tarjeta al Apple Watch es necesario que el reloj esté dentro del radio de alcance de Bluetooth. Las tarjetas están registradas específicamente para su uso con el Apple Watch y disponen de sus propios números de cuenta de dispositivo, los cuales están almacenados en el Secure Element del Apple Watch.

Al agregar tarjetas de crédito, débito o prepago (incluyendo las tarjetas de tiendas), estas aparecen en una lista de tarjetas durante el Asistente de Configuración en los dispositivos que están conectados a la misma cuenta de iCloud. Estas tarjetas permanecen en la lista siempre y cuando estén activas en al menos un dispositivo. Las tarjetas se eliminan de esta lista después de su eliminación en todos los dispositivos durante un periodo de siete días. Esta función requiere que la autenticación de dos factores esté activada en la cuenta de iCloud correspondiente.

Agregar tarjetas de crédito o débito a Apple Pay

Se pueden agregar tarjetas de crédito manualmente a Apple Pay en los dispositivos Apple.

Agregar tarjetas de crédito o débito manualmente

Para agregar una tarjeta manualmente, se utilizan el nombre, el número de la tarjeta, la fecha de vencimiento y el código CVV con el fin de facilitar el proceso de aprovisionamiento. Desde Configuración, la app Wallet o la app Apple Watch, los usuarios pueden ingresar dicha información ya sea mediante el teclado o utilizando la cámara del dispositivo. Cuando la cámara captura la información de la tarjeta, Apple intenta rellenar los campos de nombre, número de tarjeta y fecha de vencimiento. La foto no se guarda nunca en el dispositivo ni se almacena en la fototeca. Una vez que todos los campos estén completos, en el proceso Comprobar tarjeta se verifican todos los campos excepto el código CVV. Luego, esta información se encripta y envía al servidor de Apple Pay.

Si se devuelve un identificador de condiciones de uso con el proceso Comprobar tarjeta, Apple descarga las condiciones de la entidad emisora de la tarjeta y se las muestra al usuario. Si el usuario las acepta, Apple envía el identificador de las condiciones aceptadas y el código CVV al proceso Enlazar y enviar datos. Además, como parte del proceso de enlace y aprovisionamiento, Apple comparte la información del dispositivo con el emisor de la tarjeta o la red. Esto incluye información sobre (a) la actividad de la cuenta del usuario en las tiendas iTunes Store y App Store (por ejemplo, si dispone de un amplio historial de transacciones dentro de iTunes), (b) el dispositivo del usuario (por ejemplo, el número de teléfono, el nombre y el modelo del dispositivo, así como de cualquier dispositivo iOS con el que está enlazado y que es necesario para configurar Apple Pay) y (c) la ubicación aproximada del usuario al momento de agregar su tarjeta (si tiene activada la función Localización). La entidad emisora de la tarjeta utiliza esta información para decidir si aprueba agregar la tarjeta a Apple Pay.

El proceso de enlace y envío de datos tiene dos consecuencias:

- El dispositivo empieza a descargar el archivo de Apple Wallet correspondiente a la tarjeta de crédito o débito.
- El dispositivo empieza a vincular la tarjeta al Secure Element.

El archivo de la tarjeta contiene varias direcciones URL para descargar imágenes y metadatos de la tarjeta (p. ej., la información de contacto), la app de la entidad emisora de la tarjeta correspondiente y otras funciones compatibles. También contiene su estado, que incluye información como, por ejemplo, si se ha completado la personalización del Secure Element, si la entidad emisora de la tarjeta ha suspendido su uso, o bien si es necesario realizar otra verificación antes de poder pagar con la tarjeta mediante Apple Pay.

Agregar tarjetas de crédito o débito registradas en una cuenta de iTunes Store

En el caso de una tarjeta de crédito o débito que ya esté registrada en iTunes, el usuario tendrá que volver a ingresar la contraseña de su Apple ID. El número de la tarjeta se obtiene desde iTunes y se inicia el proceso Comprobar tarjeta. Si la tarjeta es compatible con Apple Pay, el dispositivo descarga y muestra las condiciones de uso y luego enviará la información sobre el ID y el código de seguridad de la tarjeta para pasar al proceso Enlazar y enviar datos. Puede que se realice una verificación adicional en el caso de las tarjetas de las cuentas de iTunes registradas.

Agregar tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta

Cuando una app está registrada para su uso con Apple Pay, se establecen claves para el servidor del emisor de la tarjeta y la app. Estas claves se utilizan para encriptar la información de la tarjeta que se envía al emisor de esta. Esto está diseñado para evitar que el dispositivo Apple lea la información. El flujo de aprovisionamiento es similar al que se utiliza para tarjetas agregadas de forma manual, descrito anteriormente, exceptuando que se utilizan contraseñas de un solo uso en lugar del código CVV.

Agregar tarjetas de crédito o débito desde el sitio web de la entidad emisora de la tarjeta

Algunos emisores de tarjetas ofrecen la posibilidad de iniciar el proceso de aprovisionamiento de la tarjeta para Apple Wallet directamente desde sus sitios web. En este caso, el usuario inicia la tarea seleccionando la tarjeta a aprovisionar desde el sitio web del emisor. A continuación, se dirige al usuario a una experiencia independiente de inicio de sesión de Apple (contenida en el dominio de Apple) y se le pide que inicie sesión con su Apple ID. Una vez iniciada la sesión, el usuario elige uno o más dispositivos para enviar la tarjeta y se le pide que confirme el resultado del proceso de aprovisionamiento en cada dispositivo de destino.

Agregar una verificación adicional

La entidad emisora de la tarjeta puede decidir si una tarjeta de crédito o débito requiere una verificación adicional. Dependiendo de la oferta de la entidad emisora de la tarjeta, es posible que el usuario pueda elegir entre diferentes opciones para realizar la verificación adicional. Tales opciones pueden ser, entre otras, un mensaje de texto, un mensaje de correo electrónico, una llamada del servicio de atención al cliente o un método para finalizar la verificación en la app aprobada de un tercero. Para los mensajes de texto o de correo electrónico, el usuario selecciona la información de contacto entre los datos que la entidad emisora de la tarjeta tiene registrados. A continuación, se envía un código que debe ingresarse en Apple Wallet, en Configuración o la app Apple Watch. En el caso de servicio al cliente y verificación mediante una app, el emisor realiza su propio proceso de comunicación.

Autorización de pagos con Apple Pay

En los dispositivos que tienen un Secure Enclave, sólo se puede realizar un pago después de recibir la autorización del Secure Enclave. En iPhone o iPad, esto implica confirmar que el usuario se ha autenticado con Face ID, Touch ID o el código del dispositivo. Si está disponible, Face ID o Touch ID es el método predeterminado, pero siempre se puede usar el código. Después de tres intentos erróneos de reconocimiento de la huella digital, o dos intentos fallidos de reconocimiento facial, se ofrece la posibilidad de ingresar el código. Después de cinco intentos erróneos, es obligatorio ingresar el código. Además, el código también es necesario si las funciones Face ID o Touch ID no están configuradas o activadas para Apple Pay. Para realizar un pago en Apple Watch, el dispositivo debe haberse desbloqueado con el código y se debe presionar dos veces el botón lateral.

Usar una clave de enlace

La comunicación entre el Secure Enclave y el Secure Element se realiza mediante una interfaz serial, con el Secure Element conectado al controlador NFC que, a su vez, se conecta al procesador de aplicaciones. Aunque no estén directamente conectados, el Secure Enclave y el Secure Element se pueden comunicar de forma segura gracias a una clave de enlace suministrada durante el proceso de fabricación. La encriptación y la autenticación de la comunicación se basan en el estándar AES, con valores únicos criptográficos que usan ambas partes para protegerse de los ataques de reproducción. La clave de enlace se genera dentro del Secure Enclave a partir de la clave UID y el identificador único del Secure Element. Después, se transfiere del Secure Enclave a un módulo de seguridad de hardware (HSM) en la fábrica, que dispone del material necesario para ingresar la clave de enlace en el Secure Element.

Autorización de una transacción segura

Cuando el usuario autoriza una transacción (lo cual incluye un gesto físico comunicado directamente al Secure Enclave), el Secure Enclave envía datos firmados acerca del tipo de autenticación e información detallada sobre el tipo de transacción (sin contacto o dentro de apps) al Secure Element, que está vinculado a un valor de autorización aleatorio (AR). Este valor se genera en el Secure Enclave cuando un usuario facilita por primera vez una tarjeta de crédito, y no cambia mientras Apple Pay esté activado. La encriptación del Secure Enclave y el mecanismo antirretroceso protegen este valor, que se envía de forma segura al Secure Element al aprovechar la clave de enlace. Al recibir un valor AR nuevo, el Secure Element marca como eliminada cualquier tarjeta agregada previamente.

Uso de un criptograma de pago para seguridad dinámica

Las transacciones de pago que se originan en los applets de pago incluyen un criptograma de pago junto con un número de cuenta del dispositivo. Este criptograma, un código de una sola vez, se calcula usando un contador de transacción y una clave. El contador de transacción se incrementa para cada nueva transacción. La clave se proporciona en el applet del pago durante la personalización y es conocida por la red del pago o el emisor de la tarjeta, o ambos. Dependiendo del sistema de pago, puede que también se usen otros datos en el cálculo, entre los que se incluyen:

- Un número de terminal impredecible, para transacciones NFC
- Un valor único del servidor de Apple Pay, en el caso de transacciones dentro de las apps

Estos códigos de seguridad se proporcionan tanto a la red de pago como a la entidad emisora de la tarjeta y le sirven a la emisora como herramienta para la verificación de cada transacción. La longitud de esos códigos de seguridad puede variar en función del tipo de transacción.

Pagos con tarjeta mediante Apple Pay

Apple Pay se puede usar para pagar las compras hechas en tiendas, dentro de apps y en sitios web.

Pagar con tarjetas en tiendas

Si el iPhone o el Apple Watch está encendido y detecta un campo NFC, mostrará al usuario la tarjeta solicitada (si la selección automática de esa tarjeta está activada) o bien la tarjeta predeterminada (que se administra desde Configuración). El usuario también puede ir a Apple Wallet y seleccionar una tarjeta; o cuando el dispositivo esté bloqueado, puede realizar lo siguiente:

- Presionar dos veces el botón lateral, en los dispositivos con Face ID.
- Presionar dos veces el botón de inicio, en los dispositivos con Touch ID.
- Usar las funciones de accesibilidad que permiten el uso de Apple Pay desde la pantalla bloqueada.

A continuación, antes de que se transmita información, el usuario deberá autenticarse mediante Face ID, Touch ID o el código del dispositivo. Si el Apple Watch está desbloqueado, presionar dos veces el botón lateral hace que se active la tarjeta predeterminada para realizar el pago. No se envía ninguna información de pago sin la autenticación del usuario.

Una vez que el usuario se ha autenticado, se utiliza el número de cuenta del dispositivo y un código de seguridad dinámico específico para cada transacción. Ni Apple ni ningún dispositivo del usuario enviarán los números completos de la tarjeta de crédito o débito a los beneficiarios. Puede que Apple reciba información anónima relacionada con la transacción como, por ejemplo, la ubicación y la hora aproximada en la que se realizó. Esta información sirve de ayuda para mejorar Apple Pay, así como otros productos y servicios de Apple.

Pagar con tarjetas en las apps

También se puede usar Apple Pay para realizar pagos dentro de las apps en iPhone, iPad, Mac y Apple Watch. Cuando los usuarios pagan dentro de apps usando Apple Pay, Apple recibe la información de la transacción encriptada. Antes de que se envíe información al desarrollador o al comerciante, Apple vuelve a encriptar la transacción con una clave específica del desarrollador. Apple Pay guarda información sobre la transacción de forma anónima como, por ejemplo, el importe aproximado de la compra. Esta información no permite identificar al usuario y nunca incluye lo que se compró.

Cuando una app inicia una transacción de pago de Apple Pay, los servidores de Apple Pay reciben la transacción encriptada desde el dispositivo antes de que el beneficiario la reciba. A continuación, los servidores de Apple Pay vuelven a encriptar la transacción con la clave específica del beneficiario antes de transmitirla.

Cuando una app solicita un pago, llama a una API para determinar si el dispositivo es compatible con Apple Pay y si la tarjeta de crédito o débito del usuario puede utilizarse para realizar pagos en una red de pago que acepte el beneficiario. La app solicita todos los datos que necesita para procesar y completar la transacción tal como las direcciones de envío y facturación, o la información de contacto. A continuación, la app pide a iOS, iPadOS o watchOS que presente la hoja de Apple Pay, que solicita información para la app, así como otra información necesaria, como la tarjeta que se va a utilizar.

Es entonces cuando la app muestra la información relacionada con la ciudad, el país y el código postal para calcular los gastos de envío finales. Sin embargo, no recibe toda la información solicitada hasta que el usuario autoriza el pago mediante Face ID, Touch ID o el código del dispositivo. Una vez autorizado el pago, la información que se muestra en la hoja de Apple Pay se envía al beneficiario.

Autorización de pagos en apps

Cuando el usuario autoriza el pago, se envía un aviso a los servidores de Apple Pay para obtener un valor único criptográfico, que se parece al valor que devuelve la terminal NFC y que se utiliza para realizar transacciones en las tiendas. El valor único, junto con otros datos de la transacción, se transfieren al Secure Element para calcular una credencial de pago que se encripta mediante una clave de Apple. La credencial de pago encriptada se devuelve a los servidores de Apple Pay, que la desencriptan, cotejan su valor único enviado inicialmente por los servidores de Apple Pay y la encriptan de nuevo con la clave del beneficiario asociada a su ID. Después, el pago se regresa al dispositivo, que se encarga de devolverlo a la app mediante la API. A continuación, la app se la facilita al sistema del beneficiario para que la procese. En ese momento, el beneficiario podrá desencriptar la credencial de pago con la ayuda de su clave privada para procesarla. Esto, en combinación con la firma de los servidores de Apple, permite que el beneficiario verifique que él es el destinatario de la transacción.

Las API requieren una autorización en la que se indiquen los ID compatibles del beneficiario. Las apps también pueden incluir datos adicionales (como número de pedido o identidad del cliente) para enviarlos a Secure Element para su firma, a fin de asegurar que la transacción no se envíe a un cliente distinto. Esto lo lleva a cabo el desarrollador de la app, quien puede especificar applicationData en PKPaymentRequest. En los datos de pago encriptados, se incluye un hash de estos datos. A continuación, el beneficiario será responsable de verificar que su hash de applicationData coincida con el de los datos de pago.

Pagar con tarjetas en sitios web

Apple Pay se puede usar para realizar pagos en sitios web en dispositivos iPhone, iPad, Apple Watch y computadoras Mac con Touch ID. Las transacciones de Apple Pay también se pueden iniciar en una Mac y completarse en un iPhone compatible con Apple Pay, o un Apple Watch que utilice la misma cuenta de iCloud.

Apple Pay en la web requiere que todos los sitios web participantes se registren con Apple. Después del registro del dominio, la validación del nombre de dominio se realiza sólo después de que Apple emite un certificado de cliente TLS. Los sitios web que soportan Apple Pay deben publicar su contenido a través de HTTPS. Para cada transacción de pago, los sitios web necesitan obtener una sesión de comerciante única y segura con un servidor de Apple utilizando el certificado de cliente TLS emitido por Apple. Los datos de la sesión del comerciante están firmados por Apple. Una vez que se verifica la firma de una sesión de comerciante, un sitio web podría revisar si el usuario tiene un dispositivo compatible con Apple Pay y si tiene una tarjeta de crédito, débito o prepago activa en el dispositivo. No se comparte ninguna otra información. Si el usuario no desea compartir esta información, puede desactivar las consultas de Apple Pay en la configuración de privacidad de Safari en dispositivos iPhone, iPad y Mac.

Una vez que se valida una sesión de comerciante, todas las medidas de privacidad y seguridad son las mismas que cuando un usuario paga en una app.

Si el usuario transmite información relacionada con el pago desde una Mac a un iPhone o Apple Watch, Handoff de Apple Pay utiliza el protocolo del servicio de identidad (IDS) de Apple con encriptado de extremo a extremo para transmitir la información relacionada con el pago entre la Mac del usuario y el dispositivo de autorización. El cliente del IDS en la Mac utiliza las claves de dispositivo del usuario para realizar el encriptado, por lo que ningún otro dispositivo puede desencriptar esta información y las claves no están disponibles para Apple. La detección de dispositivos para la función Handoff de Apple Pay contiene el tipo e identificador único de las tarjetas de crédito del usuario junto con algunos metadatos. El número de cuenta específico del dispositivo de la tarjeta del usuario no se comparte y se conserva almacenado de forma segura en el iPhone o Apple Watch del usuario. Apple también transfiere de forma segura las direcciones de contacto, envío y facturación usadas recientemente por el usuario a través del llavero de iCloud.

Una vez que el usuario autoriza el pago con Face ID, Touch ID o el código del dispositivo, o presiona dos veces el botón lateral del Apple Watch, se envía de forma segura un identificador de pago encriptado único al certificado de comerciante de cada sitio web desde el iPhone o Apple Watch del usuario a la Mac y luego se envía al sitio web del comerciante.

Sólo los dispositivos cercanos pueden solicitar y completar el pago. La proximidad se determina a través de los anuncios de Bluetooth de baja energía (BLE).

Pases sin contacto en Apple Pay

Para transmitir datos de pases compatibles a terminales NFC compatibles, Apple utiliza el protocolo de servicio de valor agregado (VAS) de Apple. El protocolo VAS puede implementarse en las terminales sin contacto o en apps de iPhone, y utiliza NFC para establecer la comunicación con dispositivos Apple compatibles. El protocolo VAS funciona dentro de una distancia reducida y se puede usar para presentar pases sin contacto de manera independiente o como parte de una transacción de Apple Pay.

Cuando se mantiene el dispositivo cerca de la terminal NFC, esta inicia la recepción de la información del pase mediante una solicitud del pase. Si el usuario dispone de un pase con el identificador del proveedor del pase, se le solicitará que autorice su uso mediante Face ID, Touch ID o el código del dispositivo. Se utiliza la información del pase, una fecha y una clave P-256 de ECDH aleatoria de un solo uso junto con la clave pública del proveedor del pase para derivar una clave de encriptación para los datos del pase, que se envían a la terminal.

Desde iOS 12.0.1 hasta iOS 13, los usuarios pueden seleccionar manualmente un pase antes de presentarlo a la terminal NFC del comerciante. En iOS 13.1 o versiones posteriores, los proveedores de pases pueden configurar los pases seleccionados manualmente para que requieran la autenticación del usuario o para que se puedan usar sin autenticación.

Inhabilitar las tarjetas con Apple Pay

Las tarjetas de crédito, débito o prepago que se hayan agregado al Secure Element se pueden usar solamente si se le presenta a este una autorización con la misma clave de enlace y el mismo valor de autorización aleatoria (AR) que cuando se agregó la tarjeta. Al recibir un valor AR nuevo, el Secure Element marca como eliminada cualquier tarjeta agregada previamente. Esto permite que el sistema operativo dé instrucciones al Secure Enclave para que inhabilite las tarjetas marcando su copia del valor AR como no válida en las siguientes circunstancias:

Método	Dispositivo
Se desactiva el código.	iPhone, iPad, Apple Watch
Se desactiva la contraseña.	Mac
El usuario cierra su sesión en iCloud.	iPhone, iPad, Mac, Apple Watch
El usuario selecciona Borrar contenido y configuración.	iPhone, iPad, Mac, Apple Watch
El dispositivo se restaura desde el modo de recuperación.	iPhone, iPad, Mac, Apple Watch
Desenlazar	Apple Watch

Suspensión, eliminación y borrado de tarjetas

Los usuarios pueden suspender el servicio de Apple Pay en el iPhone, iPad y Apple Watch al activar el modo perdido en sus dispositivos mediante Encontrar. Los usuarios también tienen la posibilidad de eliminar y borrar sus tarjetas de Apple Pay utilizando Encontrar, iCloud.com, o bien directamente en sus dispositivos mediante Apple Wallet. En el Apple Watch, las tarjetas se pueden eliminar mediante la configuración de iCloud, la app Apple Watch del iPhone, o bien directamente en el reloj. La entidad emisora de la tarjeta o la red de pago correspondiente suspende o elimina la posibilidad de realizar pagos mediante las tarjetas del dispositivo con Apple Pay, aunque el dispositivo no esté en línea ni conectado a una red de datos celular o Wi-Fi. Los usuarios también pueden llamar a la entidad emisora de la tarjeta para suspender o eliminar tarjetas de Apple Pay.

Cuando un usuario borra todo el dispositivo utilizando la opción Borrar todo el contenido y configuración, mediante Encontrar o restaurándolo, los dispositivos iPhone, iPad, iPod touch, Mac y Apple Watch le indican al Secure Element que marque todas las tarjetas como eliminadas. El resultado inmediato es que las tarjetas dejan de poder utilizarse hasta que se pueda establecer contacto con los servidores de Apple Pay para solicitarles que eliminen las tarjetas del Secure Element por completo. Independientemente, el Secure Enclave marca el valor AR como no válido para impedir cualquier autorización de pago con las tarjetas registradas previamente. Cuando el dispositivo está en línea, intenta ponerse en contacto con los servidores de Apple Pay para ayudar a cerciorarse de que todas las tarjetas se hayan borrado del Secure Element.

Seguridad de Apple Card

En los modelos compatibles de iPhone y Mac, el usuario puede solicitar una Apple Card de forma segura.

Solicitud de Apple Card

En iOS 12.4 o versiones posteriores, macOS 10.14.6 o versiones posteriores, y watchOS 5.3 o versiones posteriores, se puede utilizar Apple Card con Apple Pay para hacer pagos en tiendas, apps y sitios web.

Para solicitar una Apple Card, el usuario debe haber iniciado sesión en su cuenta de iCloud en un dispositivo iOS o iPadOS compatible con Apple Pay, y debe tener la autenticación de dos factores configurada en la cuenta de iCloud. Cuando la solicitud se aprueba, la Apple Card queda disponible en Apple Wallet o desde Configuración > Wallet y Apple Pay en cualquiera de los dispositivos elegibles en los que el usuario haya iniciado sesión con su Apple ID.

Cuando un usuario solicita una Apple Card, la identidad de este se verifica de forma segura mediante los socios proveedores de revisión de identidad de Apple y luego se comparten con Goldman Sachs Bank USA con fines de verificación de identidad y evaluación de crédito.

La información, como el número de seguridad social o la imagen del documento de identificación provisto durante la solicitud, se transmite de forma segura a los socios de revisión de identidad de Apple o a Goldman Sachs Bank USA de forma encriptada con sus respectivas claves. Apple no puede desencriptar estos datos.

La información sobre los ingresos, provista durante la solicitud, y la información bancaria utilizada para el pago de facturas se transmite de forma segura y encriptada a Goldman Sachs Bank USA, con sus claves. La información de la cuenta bancaria se guarda en el llavero. Apple no puede desencriptar estos datos.

Al agregar la Apple Card a Apple Wallet, se puede compartir con el banco asociado de Apple (Goldman Sachs Bank USA) y con Apple Payments Inc. la misma información que se utiliza cuando un usuario agrega una tarjeta de crédito o débito. Esta información se usa únicamente con fines regulatorios, de resolución de problemas y de prevención de fraudes.

En iOS 14.6 o versiones posteriores, iPadOS 14.6 o versiones posteriores y watchOS 7.5 o versiones posteriores, el organizador de una familia de iCloud con una Apple Card puede compartir su tarjeta con los miembros de su familia de iCloud mayores de 13 años. Se requiere la autentificación del usuario para confirmar la invitación. Apple Wallet usa una clave en el Secure Enclave para calcular una firma que vincula a la persona propietaria y a la persona invitada. Esa firma se valida en los servidores de Apple.

Opcionalmente, el organizador puede establecer un límite de transacciones para los participantes. También es posible bloquear las tarjetas de los participantes para detener su gasto en cualquier momento desde Apple Wallet. Cuando un copropietario o participante mayor de 18 años acepta la invitación y la solicita, pasa por el mismo proceso de solicitud definido en la sección de solicitud de Apple Card en Apple Wallet.

Uso de Apple Card

Apple Wallet permite solicitar una tarjeta Apple Card física. Una vez que el usuario recibe la tarjeta física, esta se activa usando la etiqueta NFC disponible en el sobre doblado de la tarjeta física. La etiqueta es única para cada tarjeta y no se puede usar para activar la tarjeta de otro usuario. De forma alternativa, la tarjeta se puede activar manualmente en la configuración de Apple Wallet. Además, el usuario puede elegir bloquear o desbloquear la tarjeta física en cualquier momento desde Apple Wallet.

Pagos con Apple Card y detalles de pases de Apple Wallet

Los pagos que se deban realizar a la cuenta de Apple Card se pueden realizar desde Apple Wallet en iOS con Apple Cash y una cuenta bancaria. Se pueden programar los pagos de facturas como recurrentes o como pagos de una sola exhibición en una fecha específica con Apple Cash y una cuenta bancaria. Cuando un usuario realiza un pago, se hace una llamada a los servidores de Apple Pay para obtener un valor único criptográfico, similar a Apple Cash. El valor único, junto con otros datos de configuración del pago, se transfiere al Secure Element para calcular una firma de pago. La firma se devuelve a los servidores de Apple Pay. La autenticación, integridad y exactitud del pago se verifican mediante la firma y el valor único de los servidores de Apple Pay y la orden se pasa a Goldman Sachs Bank USA para su procesamiento.

El número de la Apple Card se obtiene de Apple Wallet presentando un certificado. El servidor de Apple Pay valida el certificado para confirmar que la clave se ha generado en Secure Enclave. A continuación se utiliza esta clave para cifrar el número de la Apple Card antes de devolverlo a Apple Wallet, de modo que sólo el iPhone que solicitó el número de la Apple Card pueda descifrarlo. Una vez desencriptado, el número de la Apple Card se guarda en el llavero de iCloud.

Para mostrar los detalles del número de la Apple Card en el pase que usa Apple Wallet se requiere autenticación por parte del usuario mediante Face ID, Touch ID o un código. El usuario lo puede reemplazar en la sección de información de la tarjeta y puede desactivar el anterior.

Protección avanzada contra el fraude

En iOS 15 o versiones posteriores y en iPadOS 15 o versiones posteriores, el usuario de la Apple Card puede activar la protección avanzada contra el fraude en Apple Wallet, y cuando se activa, el código de seguridad de la tarjeta se actualiza después de unos cuantos días.

Seguridad de Apple Cash

En iOS 11.2 o versiones posteriores, iPadOS 13.1 o versiones posteriores, y watchOS 4.2 o versiones posteriores, se puede usar Apple Pay en un iPhone, iPad, o Apple Watch para enviar, recibir o solicitar dinero a otros usuarios. Cuando un usuario recibe dinero, este se agrega a una cuenta de Apple Cash a la cual se puede acceder desde Apple Wallet o desde Configuración > Wallet y Apple Pay en cualquiera de los dispositivos elegibles en los que el usuario haya iniciado sesión con su Apple ID.

En iOS 14, iPadOS 14 y watchOS 7, el organizador de una familia iCloud que ha verificado su identidad con Apple Cash puede activar Apple Cash para los miembros de su familia menores de 18 años. Opcionalmente, el organizador puede establecer restricciones en la capacidad de envío de dinero de esos usuarios para realizar envíos sólo a miembros de la familia o contactos. Si un miembro de la familia menor de 18 años realiza una recuperación de su cuenta de Apple ID, el organizador de la familia debe reactivar manualmente la tarjeta Apple Cash de ese usuario. Si un miembro de la familia menor de 18 años deja de formar parte de una familia iCloud, su saldo de Apple Cash se transfiere automáticamente a la cuenta del organizador.

Cuando el usuario configura Apple Cash, se podría compartir con nuestro socio bancario Green Dot Bank y con Apple Payments Inc. la misma información que se proporciona cuando se agrega una tarjeta de crédito o débito. Apple Payments Inc. es una filial de propiedad exclusiva creada para proteger la privacidad del usuario al almacenar y procesar información de manera independiente del resto de Apple, y de una forma que el resto de Apple no conoce. Esta información se utiliza sólo para la solución de problemas, prevención del fraude y fines regulatorios.

Usar Apple Cash en iMessage

Para realizar pagos de usuario a usuario y Apple Cash, el usuario debe haber iniciado sesión en su cuenta de iCloud en un dispositivo compatible con Apple Cash, y debe tener la autenticación de dos factores configurada en la cuenta de iCloud. Las solicitudes y transferencias de dinero entre los usuarios se inician desde la app Mensajes o mediante una solicitud a Siri. Cuando un usuario intenta enviar dinero, iMessage muestra la hoja de Apple Pay. En todos los casos, primero se usa el saldo disponible en Apple Cash. Si es necesario, se retiran fondos adicionales de una segunda tarjeta de crédito o débito que el usuario haya agregado a Apple Wallet.

Usar Apple Cash en tiendas, apps y en la web

La tarjeta de Apple Cash en Apple Wallet se puede usar con Apple Pay para realizar pagos en las tiendas, apps y en Internet. El dinero disponible en Apple Cash también se puede transferir a una cuenta bancaria. Además de recibir dinero de otro usuario, se puede agregar dinero a la cuenta Apple Cash desde una tarjeta de débito o crédito en Apple Wallet.

Apple Payments Inc. almacena y puede usar los datos de las transacciones del usuario para solucionar problemas, prevenir fraudes y para fines regulatorios una vez que se complete la transacción. El resto de Apple no sabe a quién le envió dinero el usuario, quién le envió dinero, o dónde realizó una compra con su tarjeta Apple Cash.

Cuando el usuario envía dinero con Apple Pay, agrega dinero a una cuenta de Apple Cash, o transfiere dinero a una cuenta bancaria, se realiza una llamada a los servidores de Apple Pay para obtener un valor único criptográfico similar al valor obtenido para Apple Pay desde las apps. El valor único junto con otros datos de la transacción se transfiere al Secure Element para calcular una firma de pago. La firma se devuelve a los servidores de Apple Pay. Los servidores de Apple Pay verifican la autenticación, integridad y exactitud de la transacción mediante la firma de pago y el valor único. A continuación se inicia la transferencia de dinero y posteriormente el usuario recibirá una notificación cuando se complete la transacción.

Si la transacción implica lo siguiente:

- Una tarjeta de débito para agregar fondos a Apple Cash
- La adición de dinero complementario si el saldo de Apple Cash es insuficiente

Entonces también se genera una credencial de pago encriptada y se envía a los servidores de Apple Pay, similar a la forma en que Apple Pay funciona dentro de apps y sitios web.

Cuando el saldo en la cuenta Apple Cash supera un monto específico, o si se detecta alguna actividad inusual, se pide al usuario que verifique su identidad. La información que se proporciona para verificar la identidad de un usuario, tal como el número de seguro social o las respuestas a preguntas (por ejemplo, confirmar el nombre de la calle en la que solía vivir el usuario) se transmite de forma segura al socio de Apple y se encripta utilizando su clave. Apple no puede desencriptar estos datos. Se pedirá al usuario que verifique otra vez su identidad si solicita la recuperación de su cuenta Apple ID, antes de volver a obtener acceso a su saldo de Apple Cash.

Seguridad de Tap to Pay on iPhone

Tap to Pay on iPhone, disponible en iOS 15.4, permite a los comerciantes en EE. UU. aceptar Apple Pay y otros pagos sin contacto utilizando el iPhone y una app de iOS de los socios. Con este servicio, los usuarios con dispositivos iPhone compatibles pueden aceptar de forma segura pagos sin contacto y pases NFC de *Apple Pay*. Con Tap to Pay on iPhone, los comerciantes no necesitan hardware adicional para aceptar pagos sin contacto.

Tap to Pay on iPhone está diseñada para proteger la información personal del pagador. Este servicio no recopila información sobre las transacciones que pueda vincular al pagador. La información de la tarjeta de pago, como el número de la tarjeta de crédito/débito (PAN), está protegida por Secure Element, y no está disponible para el comerciante. La información de la tarjeta de pago permanece entre el proveedor de servicios de pago del comerciante, el pagador y el emisor de la tarjeta. Además, el servicio Tap to Pay no recopila los nombres, direcciones o números de teléfono del pagador.

Tap to Pay on iPhone ha sido evaluada externamente por un laboratorio de seguridad acreditado y aprobado por American Express, Discover, Mastercard y Visa.

Seguridad del componente de pago sin contacto

- *Secure Element:* el Secure Element ([Link to Apple Pay Secure Element section]) aloja los kernels de pago que leen y protegen los datos de la tarjeta de pago sin contacto.
- *Controlador NFC:* el controlador de comunicación de corto alcance (NFC) administra los protocolos NFC y dirige la comunicación entre el procesador de aplicaciones y el Secure Element, y entre el Secure Element y la tarjeta de pago sin contacto.
- *Servidores de Tap to Pay on iPhone:* los servidores de Tap to Pay on iPhone administran la configuración y el aprovisionamiento de los kernels de pago en el dispositivo. Los servidores también supervisan la seguridad de los dispositivos con Tap to Pay on iPhone de una forma que es compatible con los estándares de pagos sin contacto en COTS (CPoC) del Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC), y también cumplen con la norma PCI DSS.

Cómo Tap to Pay on iPhone lee las tarjetas de crédito, débito y prepago

Descripción general de la seguridad del proceso de aprovisionamiento

Tras el primer uso de Tap to Pay on iPhone utilizando una app con suficientes permisos, el servidor de la función determina si el dispositivo cumple con los criterios de elegibilidad, como el modelo de dispositivo, la versión de iOS y si se ha establecido un código de acceso. Una vez completada esta verificación, el applet de aceptación de pagos se descarga desde el servidor de Tap to Pay on iPhone y se instala en el Secure Element, junto con la configuración del kernel de pago asociado. Esta operación se realiza de forma segura entre los servidores de Tap to Pay on iPhone y el Secure Element. El Secure Element valida la integridad y la autenticidad de estos datos antes de su instalación.

Descripción general de la seguridad de la lectura de tarjetas

Cuando una app compatible con Tap to Pay on iPhone solicita una lectura de tarjeta a la estructura ProximityReader, se muestra una hoja, controlada por iOS, que pide al usuario que toque una tarjeta de pago. iOS inicializa el lector de tarjetas de pago y luego solicita a los kernels de pago del Secure Element que inicien una lectura de tarjeta.

En este momento, el Secure Element asume el control del controlador NFC en modo Lector. Este modo sólo permite el intercambio de datos de la tarjeta entre la tarjeta de pago y el Secure Element a través del controlador de NFC. Las tarjetas de pago sólo se pueden leer en este modo.

Después de que el applet de aceptación de pagos en el Secure Element ha completado la lectura de la tarjeta, este encripta y firma los datos de la tarjeta. Los datos de la tarjeta permanecen encriptados y autentificados hasta que llegan al proveedor de servicios de pago. Sólo el proveedor de servicios de pago utilizado por la app para solicitar la lectura de la tarjeta puede desencriptar los datos de la tarjeta. El proveedor de servicios de pago debe solicitar la clave de desencriptado de los datos de la tarjeta al servidor de Tap to Pay on iPhone. El servidor de Tap to Pay on iPhone emite las claves de desencriptado al proveedor de servicios de pago después de validar la integridad y autenticidad de los datos, y después de verificar que la lectura de la tarjeta se produjo en un plazo de 60 segundos desde la lectura de la tarjeta en el dispositivo.

Este modelo ayuda a garantizar que los datos de la tarjeta no puedan ser desencriptados por nadie más que el proveedor de servicios de pago, el cual procesa esta transacción por el comerciante.

Usar Apple Wallet

Acceder mediante Apple Wallet

En Apple Wallet en dispositivos iPhone y Apple Watch compatibles, los usuarios pueden almacenar sus llaves de casa, llaves de auto y llaves de habitación de hotel. Incluso pueden almacenar gafetes de empresas y tarjetas de identificación de estudiante. Cuando un usuario llega a una puerta, se le presenta automáticamente la llave adecuada, permitiéndole entrar con sólo un toque mediante el protocolo de comunicación de campo cercano (NFC).

Comodidad para el usuario

Cuando se agrega una llave, pase, tarjeta de identificación de estudiante o gafete de empresa a Apple Wallet, se activa el modo express de forma predeterminada. Las tarjetas en modo express interactúan con las terminales que las aceptan sin necesidad de autenticarse mediante Face ID, Touch ID, un código, o presionar dos veces el botón lateral del Apple Watch. Para deshabilitar esta función, los usuarios pueden desactivar el modo express tocando el botón Más en el lado frontal de la tarjeta en Apple Wallet. Para volver a activar el modo express, se requiere Face ID, Touch ID o un código de acceso.

Privacidad y seguridad

Las llaves en Apple Wallet aprovechan al máximo la privacidad y la seguridad integradas en el iPhone y el Apple Watch. Nunca se comparte con Apple ni se almacena en los servidores de Apple cuándo o dónde una persona usa las llaves que tiene en Apple Wallet. Además, las credenciales se almacenan de forma segura dentro del Secure Element (SE) de los dispositivos compatibles. El SE alberga applets especialmente diseñados para gestionar y almacenar de forma segura las claves de acceso, garantizando que estas no puedan ser extraídas.

Antes de aprovisionar una clave de acceso, un usuario debe haber iniciado sesión en su cuenta de iCloud en un iPhone compatible y debe tener activada la autenticación de dos factores para su cuenta de iCloud, salvo si se trata de las claves de una identificación de estudiante, la cual no requiere que la autenticación de dos factores esté activada.

Cuando un usuario inicia el proceso de aprovisionamiento, se siguen pasos similares a los del aprovisionamiento de tarjetas de crédito y débito, como el enlace y aprovisionamiento. Durante una transacción, el lector se comunica con el Secure Element a través del controlador NFC utilizando un canal seguro establecido.

El número de dispositivos, incluidos el iPhone y el Apple Watch, que se pueden aprovisionar con una clave de acceso está definido y controlado por cada socio, y puede variar de un socio a otro. Este enfoque permite a cada socio tener el control sobre el número máximo de claves de acceso aprovisionadas por tipo de dispositivo para adaptarse a sus necesidades específicas. Con este fin, Apple proporciona a los socios el tipo de dispositivo y los identificadores anónimos del mismo. Los identificadores son diferentes para cada socio por motivos de privacidad y seguridad.

Las llaves se pueden desactivar o eliminar de las siguientes maneras:

- Al borrar el dispositivo de forma remota con Encontrar
- Al activar el modo perdido con Encontrar
- Al recibir el comando de borrado remoto de una solución de administración de dispositivos móviles (MDM)
- Al eliminar todas las tarjetas de la página de las cuentas de sus Apple ID
- Al eliminar todas las tarjetas de iCloud.com
- Al eliminar todas las tarjetas de Apple Wallet
- Al eliminar la tarjeta en la app de la entidad emisora

En iOS 15.4 o versiones posteriores, cuando un usuario presiona dos veces el botón lateral en un iPhone con Face ID, o cuando presiona dos veces el botón de inicio en un iPhone con Touch ID, los detalles de sus pases y llaves de acceso no se muestran hasta que se autentifica en el dispositivo. Se requiere la autenticación mediante Face ID, Touch ID o el código para que la información específica del pase, incluidos los detalles de la reservación del hotel, se muestren en Apple Wallet.

Tipos de credenciales de acceso

Apple Wallet permite diferentes tipos de acceso, como el acceso en hoteles, gafetes de empresas, identificaciones de estudiante, llaves de casa y llaves de auto.

Hospitalidad turística

Las llaves de habitación de hotel en Apple Wallet ayudan a ofrecer una experiencia sencilla y sin contacto desde la llegada hasta la salida, y a la vez proporcionan ventajas adicionales de privacidad y seguridad para los huéspedes, adicionales a las tradicionales llaves en tarjeta de plástico de los hoteles. Los huéspedes de hoteles socios pueden tocar para desbloquear con su llave de habitación en Apple Wallet en su iPhone y Apple Watch compatible.

Las funciones de Apple Wallet están diseñadas específicamente para optimizar la experiencia del cliente:

- Aprovisionamiento previo a la llegada desde la app del hotel, al agregar un pase a Apple Wallet antes de la estancia.
- Pases de registro para iniciar el registro y la asignación de habitaciones desde Apple Wallet.
- Actualización de llaves después del aprovisionamiento, para permitir la extensión o modificación de las estancias en curso.
- Compatibilidad con llaves de varias habitaciones para un solo pase en Apple Wallet.
- Archivo automático de llaves caducadas en Apple Wallet.

Gafetes de empresas

Los empleados de socios compatibles pueden agregar su gafete a Apple Wallet en su iPhone y Apple Watch para acceder sin contacto a sus lugares de trabajo. Para agregar su gafete, el empleado debe tener activada la autenticación multifactorial en la cuenta que usa para iniciar sesión en la app proporcionada por su empleador.

El gafete del empleado aprovecha las capacidades de acceso de Apple para permitir al usuario:

- Agregar automáticamente un gafete de empleado al Apple Watch enlazado a través de un aprovisionamiento push que no requiere la instalación de la app del socio.
- Acceder fácilmente a los servicios de la oficina utilizando el modo exprés.
- Acceder al lugar de trabajo incluso cuando el iPhone se queda sin batería.

Tarjetas de identificación de estudiantes

En iOS 12 o versiones posteriores, los estudiantes, el cuerpo docente y el personal de los campus pueden agregar sus tarjetas de identificación a Apple Wallet en modelos compatibles de iPhone y Apple Watch para acceder a ubicaciones y realizar pagos en cualquier lugar donde acepten su tarjeta.

El usuario agrega su tarjeta de identificación de estudiante a Apple Wallet mediante una app proporcionada por el emisor de la tarjeta o escuela participante. El proceso técnico en este caso es el mismo que el que se describe en Agregar tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta. Asimismo, las apps emisoras deben ser compatibles con la autenticación de dos factores en las cuentas que protegen el acceso a sus identificaciones de estudiantes. Es posible configurar simultáneamente hasta dos dispositivos Apple compatibles donde se haya iniciado sesión con el mismo Apple ID.

Viviendas multifamiliares

Los residentes y el personal de los establecimientos socios compatibles pueden usar su llave de casa en Apple Wallet para acceder a su edificio, a su unidad y a las zonas comunes. La llave de casa se puede aprovisionar desde la app proporcionada por el socio. Para los socios que admiten el aprovisionamiento remoto, los administradores de los establecimientos pueden enviar a los residentes un enlace para iniciar el aprovisionamiento mediante su canal de mensajería preferido (por ejemplo, correo electrónico o SMS), de modo que el residente sólo tenga que tocar el enlace para obtener la llave. Los App Clips también proporcionan una experiencia segura y sencilla al permitir el aprovisionamiento de una llave sin necesidad de instalar la app de un socio. Para obtener más información, consulta el artículo de soporte de Apple Usar App Clips en el iPhone.

Llave de casa

Una llave de casa en Apple Wallet puede utilizarse con cerraduras de puertas compatibles con NFC con un simple toque de un iPhone o Apple Watch. Para obtener más información sobre cómo un usuario puede configurar y usar una llave de casa, consulta el artículo del soporte de Apple Abrir puertas con una llave de casa en el iPhone.

Cuando un usuario configura una llave de casa, todos los residentes de su hogar también reciben automáticamente una llave de casa. Para compartir la llave de casa con más personas o para eliminar a un miembro de una casa compartida, el propietario de la casa puede usar la app Casa para administrar las invitaciones y los miembros. Cuando un usuario decide aceptar una invitación para unirse a una casa que tiene una llave de casa, se inicia el aprovisionamiento de la llave de casa en Apple Wallet en sus dispositivos. Si un usuario decide abandonar una casa o si el propietario de la casa retira el acceso a miembro específicos, se elimina la llave de casa correspondiente de Apple Wallet.

Llave de auto

El almacenamiento digital de llaves de auto en Apple Wallet es compatible de forma nativa con dispositivos iPhone y dispositivos Apple Watch enlazados. Las llaves de auto se muestran como pases (creados por Apple en nombre del fabricante del automóvil) en Apple Wallet y son compatibles con el ciclo de vida completo de las tarjetas de Apple Pay (modo perdido de iCloud, borrado remoto, eliminación de pases local y la función Borrar todo el contenido y configuración). Además de la administración estándar de tarjeta de Apple Pay, las llaves de auto compartidas se pueden eliminar desde el iPhone del propietario, el Apple Watch y la interfaz persona-computadora (HMI) del vehículo.

Las llaves de auto se pueden utilizar para poner y quitar el cerrojo del vehículo, así como para arrancar el motor o poner el vehículo en modo de conducción. La “transacción estándar” ofrece autenticación mutua y es obligatoria para arrancar el motor. Las transacciones de apertura y cerrado pueden utilizar la “transacción rápida” cuando sea necesario por motivos de rendimiento.

Las llaves se crean a través del enlace de un iPhone con un vehículo propio y compatible. Todas las llaves se crean en el Secure Element integrado en función de la generación de llaves a bordo (ECC-OBKG) de curva elíptica (NIST P-256), y las llaves privadas nunca salen del Secure Element. La comunicación entre los dispositivos y el vehículo usa el estándar NFC, o una combinación de Bluetooth LE y UWB, mientras que la administración de llaves usa una API que conecta los servidores de Apple con los del fabricante de automóviles con TLS autenticados mutuamente. Después de enlazar una llave con un iPhone, cualquier Apple Watch enlazado con ese iPhone también recibe una llave. Cuando se borra una llave en el vehículo o en el dispositivo, no se puede restaurar. Las claves de los dispositivos perdidos o robados se pueden suspender y reanudar, pero aprovisionarlas nuevamente en un dispositivo nuevo requiere volver a enlazar o compartir.

Seguridad de la función Llave de auto en iOS

Los desarrolladores pueden ofrecer formas seguras y sin llave para acceder a un vehículo en un iPhone compatible y un Apple Watch enlazado.

Enlace del propietario

El propietario debe demostrar que el vehículo es de su propiedad (el método depende del fabricante del automóvil) y puede iniciar el proceso de enlace en la app del fabricante del automóvil utilizando un enlace de correo electrónico recibido del fabricante o del menú del vehículo. En todos los casos, el propietario debe presentar una contraseña de enlace confidencial de uso único en el iPhone, que se utiliza para generar un canal de enlace seguro con el protocolo SPAKE2+ y la curva NIST P-256. Cuando se utiliza la app o el enlace de correo electrónico, la contraseña se transfiere automáticamente al iPhone, mientras que, si se inicia el enlace desde el vehículo, esta se debe ingresar manualmente.

Compartir llaves

El iPhone enlazado del propietario puede compartir llaves con los dispositivos iPhone de amigos y familiares elegibles (y con los dispositivos Apple Watch enlazados) al enviar una invitación específica del dispositivo mediante iMessage y el servicio de identidad (IDS) de Apple. Todos los comandos del proceso de compartir se intercambian mediante la función de IDS encriptada de extremo a extremo. El iPhone enlazado del propietario impide que el canal IDS cambie durante el proceso de compartir con el fin de impedir el reenvío de la invitación.

Después de aceptar la invitación, el iPhone del familiar o amigo crea una clave digital y regresa la cadena del certificado de creación de esta al iPhone enlazado del propietario para verificar que la clave se haya creado en un dispositivo Apple auténtico. El iPhone enlazado del propietario firma la clave ECC pública del iPhone del otro familiar o amigo, y envía la firma al iPhone del familiar o amigo. La operación de firma en el dispositivo del propietario requiere la autenticación del usuario (mediante Face ID, Touch ID o el código) y una intención del usuario segura descrita en la sección Usos de Face ID y Touch ID. La autorización se solicita al enviar la invitación y se almacena en el Secure Element para su uso cuando el dispositivo del amigo devuelva la solicitud de firma. Los derechos de la llave se proporcionan al vehículo ya sea en línea mediante el servidor del fabricante del vehículo o durante el primer uso de la llave compartida en el vehículo.

Eliminación de llaves

Las llaves se pueden eliminar del dispositivo del titular de la llave desde el dispositivo del propietario y el vehículo. Eliminar desde el iPhone del titular surte efecto de inmediato, incluso si el titular está usando la llave; es por esto que se muestra una advertencia antes de completar la eliminación. La eliminación de las llaves en el vehículo puede realizarse en cualquier momento, o sólo cuando el vehículo está en línea.

En ambos casos, al eliminar desde el dispositivo o vehículo del titular de la llave se emite un reporte a un servidor de inventario de llaves (KIS) del fabricante de automóviles, que registra las llaves emitidas para un vehículo con fines de seguro.

El propietario puede solicitar una eliminación desde la parte posterior del pase del propietario. La solicitud se envía primero al fabricante del automóvil para la eliminación de la llave en el vehículo. Las condiciones para eliminar la llave del vehículo las estipula el fabricante de automóviles. Cuando se elimina la llave desde el vehículo, el servidor del fabricante del automóvil envía una solicitud de terminación remota al dispositivo del titular de la llave.

Cuando se finaliza una llave en un dispositivo, el applet que administra las llaves de auto digitales crea una afirmación de finalización firmada criptográficamente, que el fabricante del automóvil utiliza como prueba de eliminación para eliminar la llave del KIS.

Transacciones estándar mediante NFC

Para los vehículos con llave NFC, se puede iniciar un canal seguro entre el lector y un iPhone al generar pares de claves efímeros en el lector y en el iPhone. A través de un método de acuerdo de clave, se puede derivar un secreto compartido en ambos lados y usarse para la generación de una clave simétrica compartida mediante Diffie-Hellman, una función de derivación de clave y firmas de la clave de largo plazo establecida durante el enlace.

La clave pública efímera generada en el lado del vehículo se firma con la clave privada de largo plazo del lector, lo que genera una autenticación del lector por parte del iPhone. Desde la perspectiva del iPhone, este protocolo está diseñado para evitar que se revelen datos delicados a un adversario que intercepta la comunicación.

Por último, el iPhone utiliza el canal seguro establecido para encriptar su identificador de clave pública junto con la firma calculada en el reto derivado de los datos del lector y algunos datos adicionales específicos de la app. Esta verificación de la firma del iPhone por parte del lector permite a este autenticar el dispositivo.

Transacciones rápidas

El iPhone genera un criptograma basado en un secreto previamente compartido durante una transacción estándar. Este criptograma permite que el vehículo auntentique rápidamente el dispositivo en escenarios donde el rendimiento es muy importante. De forma opcional, se establece un canal seguro entre el vehículo y el dispositivo al derivar las claves de sesión de un secreto previamente compartido durante una transacción estándar y un nuevo par de claves efímeras. La capacidad del vehículo para establecer el canal seguro autentica el vehículo en el iPhone.

Transacciones estándar mediante BLE/UWB

Para los vehículos que utilizan una llave UWB, se establece una sesión Bluetooth LE entre el vehículo y el iPhone. De forma similar a la transacción mediante NFC, se obtiene un secreto compartido por ambas partes que se utiliza para establecer una sesión segura. Esta sesión se utiliza para derivar y acordar posteriormente una clave secreta de alcance UWB (URSK). La URSK se proporciona a los radios UWB del dispositivo del usuario y del vehículo para permitir la localización precisa del dispositivo del usuario en una posición específica cerca o dentro del vehículo. A continuación, el vehículo utiliza la posición del dispositivo para tomar decisiones sobre la autorización del desbloqueo o el arranque del vehículo. Las URSK tienen un periodo de validez (TTL) predefinido. Para evitar la interrupción de un alcance cuando un TTL expira, las URSK pueden obtenerse de forma anticipada del SE del dispositivo y del HSM/SE del vehículo mientras el alcance seguro no está activo y BLE está conectado. Esto evita la necesidad de realizar una transacción estándar para obtenerse una nueva URSK en una situación donde el tiempo es esencial. La URSK obtenida con anticipación puede transferirse muy rápidamente a los radios UWB del vehículo y del dispositivo para evitar la interrupción del alcance UWB.

Privacidad

El servidor de inventario de llaves (KIS) del fabricante del automóvil no almacena el ID del dispositivo, el SEID ni el Apple ID; sólo almacena un identificador mutable y el identificador de la CA de instancia. Este identificador no está vinculado con ningún dato privado en el dispositivo o por el servidor, y se elimina cuando el usuario borra su dispositivo por completo (usando la opción Borrar todo el contenido y la configuración).

Agregar tarjetas de transporte público y de monedero electrónico a Apple Wallet

En muchos mercados globales, los usuarios pueden agregar tarjetas de transporte y monederos electrónicos compatibles a Apple Wallet en los modelos de iPhone y Apple Watch compatibles. Dependiendo del operador, esto se puede realizar mediante la transferencia del valor o el pase de transporte (o ambos) de una tarjeta física a su representación digital en Apple Wallet, o agregando una nueva tarjeta de transporte público o monedero electrónico desde Apple Wallet o la app del emisor de dicha tarjeta. Después de agregar tarjetas de transporte público a Apple Wallet, los usuarios pueden pagar su viaje en transporte público con sólo colocar su iPhone o Apple Watch cerca del lector del servicio público. Algunas tarjetas de transporte público también se pueden usar para realizar pagos.

Cómo funcionan las tarjetas de transporte público y monederos electrónicos

Las tarjetas de transporte público y monederos electrónicos se asocian con la cuenta de iCloud del usuario. Si el usuario agrega más de una tarjeta a Apple Wallet, Apple o el emisor de la tarjeta podría enlazar la información personal del usuario y la información de la cuenta asociada entre las tarjetas. Las tarjetas de transporte público y monederos electrónicos, y las transacciones están protegidas por un conjunto de claves criptográficas jerárquicas.

Los usuarios deberán ingresar la información específica de la tarjeta durante el proceso de transferencia de saldo de una tarjeta física a Apple Wallet. Es probable que los usuarios deban proporcionar información personal como prueba de propiedad de la tarjeta. Al transferir pases desde un iPhone a un Apple Watch, ambos dispositivos deben estar conectados a Internet.

Se puede recargar saldo utilizando tarjetas de crédito, débito y prepago mediante Apple Wallet o desde la app del emisor de la tarjeta de transporte público o monedero electrónico. Para conocer más sobre la seguridad de recargar el saldo al usar Apple Pay, consulta Pagar con tarjetas en las apps. Para obtener información sobre cómo se proporciona la tarjeta desde dentro de la app del emisor de la tarjeta, consulta Agregar tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta.

Si se permite agregar mediante una tarjeta física, el emisor de la tarjeta de transporte o monedero electrónico cuenta con las claves criptográficas necesarias para autenticar la tarjeta física y verificar los datos ingresados por el usuario. Después de completar la verificación de los datos, el sistema puede crear un número de cuenta del dispositivo para el Secure Element y activar el pase recién agregado en Apple Wallet con el saldo transferido. Con algunas tarjetas, después de ingresar los datos de una tarjeta física, esta se desactiva.

Al completar el proceso con cualquiera de estos métodos, si el saldo de la tarjeta se guarda en el dispositivo, se encripta y almacena en un applet designado en el Secure Element. El operador tiene las claves para realizar operaciones criptográficas en los datos de la tarjeta para las transacciones de saldo.

De forma predeterminada, los usuarios de tarjetas de transporte público se benefician de la experiencia intuitiva del abordaje express que les permite pagar y viajar sin requerir Face ID, Touch ID o un código. Es posible acceder a información, como estaciones visitadas recientemente, el historial de transacciones y la compra de boletos adicionales, en cualquier lector de tarjetas sin contacto cercano con el modo express activado. Para activar la solicitud de autorización mediante Face ID, Touch ID o código, se debe desactivar el abordaje express en Configuración > Wallet y Apple Pay. El modo Express no es compatible con las tarjetas de monedero electrónico.

Igual que con las tarjetas Apple Pay, los usuarios pueden suspender o eliminar tarjetas de monedero electrónico de las siguientes formas:

- Al borrar el dispositivo de forma remota con Encontrar
- Al activar el modo perdido con Encontrar
- Al ingresar el comando de borrado remoto de una solución de administración de dispositivos móviles (MDM)
- Al eliminar todas las tarjetas de la página de las cuentas de sus Apple ID
- Al eliminar todas las tarjetas de iCloud.com
- Al eliminar todas las tarjetas de Apple Wallet
- Al eliminar la tarjeta en la app de la entidad emisora

Los servidores de Apple Pay solicitarán al operador de la tarjeta que suspenda o desactive esas tarjetas. Si un usuario elimina una tarjeta de transporte público o monedero electrónico de un dispositivo en línea, puede recuperar su saldo al volver a agregarlas a un dispositivo donde haya iniciado sesión con el mismo Apple ID. Si un dispositivo está sin conexión, apagado o no se puede usar, es posible que no se logre la recuperación.

Agregar tarjetas de transporte público y de monedero electrónico al Apple Watch de un miembro de la familia

En iOS 15 y watchOS 8, el organizador de una familia de iCloud puede agregar tarjetas de transporte púbico y de monedero electrónico a los dispositivos Apple Watch de los miembros de su familia a través de la app Watch de su iPhone. Cuando se aprovisiona una de estas tarjetas al Apple Watch de un miembro de la familia, se requiere que el reloj esté cerca y conectado al iPhone del organizador mediante Wi-Fi o Bluetooth. Además, los miembros de la familia deben tener activada la autenticación de dos factores en su Apple ID.

Los miembros de la familia pueden usar iMessage en su Apple Watch para enviar una solicitud para agregar dinero a una tarjeta de transporte público o de monedero electrónico. El contenido del mensaje está protegido por la encriptación de extremo a extremo, como se describe en la sección Descripción general de la seguridad de iMessage. La adición de dinero a una tarjeta en el Apple Watch de un miembro de la familia puede hacerse de forma remota utilizando una conexión Wi-Fi o de red celular. No es necesario que los dispositivos estén cerca.

Nota: esta función podría no estar disponible en todos los países o regiones.

Tarjetas de crédito y débito

En algunas ciudades, los lectores de transporte aceptan tarjetas EMV (inteligentes) para pagar los viajes en transporte público. Cuando un usuario presenta una tarjeta de crédito o débito EMV en esos lectores, se requerirá la autenticación del usuario, al igual que con Pagar con tarjetas de crédito y débito en las tiendas.

En iOS 12.3 o versiones posteriores, puede activarse el abordaje express para algunas tarjetas de crédito/débito EMV existentes en Apple Wallet. El abordaje express permite a los usuarios pagar el pasaje en los operadores de tránsito compatibles sin necesidad de usar Face ID, Touch ID o un código. Cuando un usuario envíe los datos de una tarjeta de débito o crédito EMV, se activa el abordaje express para la primera tarjeta provista a Apple Wallet. El usuario puede tocar el botón Más en la parte frontal de la tarjeta en Apple Wallet y desactivar el modo express para esa tarjeta al especificar la opción Ninguna para Config. para abordar express. El usuario también puede seleccionar otra tarjeta de crédito o débito distinta para usarla con el abordaje express, mediante Apple Wallet. Se requerirá Face ID, Touch ID o el código para volver a activar el modo express o seleccionar una tarjeta distinta.

Apple Card y Apple Cash se pueden usar para abordaje express.

Identificaciones en Apple Wallet

En el iPhone 8 o modelos posteriores con iOS 15.4 o versiones posteriores, y en el Apple Watch Series 4 o modelos posteriores con watchOS 8.4 o versiones posteriores, los usuarios pueden agregar su identificación estatal o su permiso de conducir a Apple Wallet y tocar su iPhone o Apple Watch para presentarlo de forma segura y sencilla en los establecimientos participantes.

Nota: esta función sólo está disponible en los estados participantes de EE. UU.

Las identificaciones en Apple Wallet utilizan funciones de seguridad integradas en el hardware y el software del dispositivo del usuario para ayudar a proteger su identidad y ayudar a mantener segura su información personal.

Agregar un permiso de conducir o una identificación estatal a Apple Wallet

En el iPhone, los usuarios pueden simplemente tocar el botón Agregar (+) en la parte superior de la pantalla de Apple Wallet para empezar a agregar su licencia o identificación. Si los usuarios tienen un Apple Watch enlazado durante la configuración, se les pide que también agreguen su permiso de conducir o su identificación a Apple Wallet en el Apple Watch.

Primero se pide a los usuarios que usen su iPhone para escanear ambas caras de su tarjeta física de permiso de conducir o identificación estatal. El iPhone evalúa la calidad y el tipo de imágenes para ayudar a garantizar que las imágenes proporcionadas son aceptables para la autoridad emisora estatal. Estas imágenes de la tarjeta de identificación se encriptan con la clave de la autoridad emisora estatal en el dispositivo y luego se envían a la autoridad emisora estatal.

A continuación, se pide al usuario que realice una serie de movimientos faciales y de la cabeza. Estos movimientos son evaluados por el dispositivo del usuario y por Apple para ayudar a reducir el riesgo de que alguien utilice una fotografía, un video o una máscara para intentar agregar la identificación de otra persona a Apple Wallet. Los resultados del análisis de estos movimientos se envían a la autoridad emisora estatal, pero no el video de los movimientos.

Para ayudar a garantizar que la persona que agrega la tarjeta de identificación a Apple Wallet es la misma persona de la identificación, se pide a los usuarios que se tomen un selfie. Antes de enviar la foto del usuario a la autoridad emisora estatal, los servidores de Apple y el dispositivo del usuario comparan la foto con el aspecto de la persona que realizó la serie de movimientos faciales y de la cabeza, y ayuda a garantizar que la foto que se envía es de una persona viva con el mismo aspecto que el de la identificación. Una vez realizada la comparación, la foto se encripta en el dispositivo y se envía a la autoridad emisora estatal para que se compare con la imagen que se tiene archivada para su identificación.

Por último, se pide a los usuarios que realicen una autenticación con Face ID o Touch ID. El dispositivo del usuario vincula esta coincidencia biométrica única de Face ID o Touch ID con la identificación estatal para ayudar a garantizar que sólo la persona que agregó la identificación a este iPhone pueda presentarla; y que no se pueda usar otra información biométrica inscrita para autorizar la presentación de la identificación. La autenticación se hace estrictamente en el dispositivo, y no se envía a la autoridad emisora estatal.

La autoridad emisora estatal recibirá la información necesaria para crear la identificación digital. Esto incluye las imágenes de la cara y el reverso de la identificación del usuario, los datos leídos del código de barras PDF417, así como el selfie que el usuario se tomó como parte del proceso de verificación de la identificación. El estado emisor también recibe un valor de un solo dígito, utilizado para ayudar a prevenir el fraude, que se basa en los patrones de uso del dispositivo del usuario, los datos de configuración, e información sobre su Apple ID personal. En última instancia, el estado emisor decide si se aprueba o rechaza la identificación que se agrega a Apple Wallet.

Después de que la autoridad emisora estatal autoriza la adición de la identificación o el permiso de conducir estatal a Apple Wallet, se genera un par de claves en el Secure Element del iPhone que vincula la identificación del usuario a ese dispositivo. Si se agrega al Apple Watch, el Apple Watch genera un par de claves en el Secure Element.

Una vez que la identificación está en el iPhone, la información reflejada en la identificación del usuario en Apple Wallet se almacena en un formato encriptado y protegido por el Secure Enclave.

Usar un permiso de conducir o identificación estatal almacenado en Apple Wallet

Para usar su identificación en Apple Wallet, el usuario debe autenticarse utilizando el dispositivo con Face ID o Touch ID asociado a la identificación en Apple Wallet antes de que el iPhone presente la información al lector de identidad.

Para usar su identificación en Apple Wallet en el Apple Watch, el usuario necesita desbloquear su iPhone utilizando el aspecto de Face ID asociado o la huella dactilar Touch ID asociada cada vez que se ponga el Apple Watch. Posteriormente, el usuario puede usar su identificación en Apple Wallet sin autenticarse hasta que se quite el Apple Watch. Esta capacidad aprovecha las funciones fundamentales del desbloqueo automático detalladas en la sección Seguridad del sistema para watchOS.

Cuando el usuario sostiene su iPhone o Apple Watch cerca del lector de identidad, el dispositivo muestra al usuario qué información específica se está solicitando, quién la solicita, y si se tiene la intención de almacenarla. Después de autorizar con Face ID o Touch ID, la información de identidad solicitada se envía del dispositivo.

Importante: los usuarios no necesitan desbloquear, mostrar o entregar su dispositivo para presentar su identificación.

Si el usuario tiene una función de accesibilidad activada, como Control por voz, Control por botón, o Assistive Touch, en lugar de activar Face ID o Touch ID, puede usar su código para acceder y presentar su información.

La transmisión de datos de identidad al lector de identidad cumple con el estándar ISO/IEC 18013-5, el cual proporciona varios mecanismos de seguridad capaces de detectar, disuadir y mitigar riesgos de seguridad. Estos consisten en la integridad de los datos de identidad y la antifalsificación, la vinculación del dispositivo, el consentimiento informado y la confidencialidad de los datos del usuario a través de enlaces de radio.

Integridad de datos de identidad y antifalsificación

Las identificaciones en Apple Wallet utilizan una firma proporcionada por el emisor para permitir que cualquier lector compatible con el estándar ISO/IEC 18013-5 verifique la identificación de un usuario en Apple Wallet. Además, cada elemento de datos de la identificación en Apple Wallet está protegido individualmente contra la falsificación. Esto permite que el lector de identidad solicite un subconjunto específico de elementos de datos disponibles en la identificación en Apple Wallet y que la identificación en Apple Wallet responda sólo con el subconjunto solicitado, compartiendo así sólo los datos solicitados y maximizando la privacidad del usuario.

Vinculación del dispositivo

Las identificaciones en la autenticación de Apple Wallet utilizan una firma de dispositivo para protegerse contra la clonación de identificaciones y la repetición de una transacción de identidad. Al almacenar la clave privada para la autenticación de la identificación en el Secure Element del iPhone, la identificación queda vinculada al mismo dispositivo para el cual la autoridad emisora estatal creó la identificación.

Consentimiento informado

Las identificaciones en la autenticación de lectores de Apple Wallet autentican el lector de identidad utilizando el protocolo definido en el estándar ISO/IEC 18013-5. Durante la presentación, se muestra un ícono derivado del certificado del lector para dar al usuario la seguridad de que está interactuando con la parte prevista.

Confidencialidad de los datos del usuario durante los enlaces de radio

La encriptación de la sesión ayuda a garantizar que toda la información personal identificable (PII) que se intercambia entre la identificación en Apple Wallet y el lector de identidad está encriptada. La encriptación la realiza la capa de la aplicación. Esto significa que la seguridad de la encriptación de la sesión no depende de la seguridad proporcionada por la capa de transmisión (por ejemplo, NFC, Bluetooth y Wi-Fi).

Las identificaciones en Apple Wallet ayudan a salvaguardar la privacidad de la información de los usuarios

Las identificaciones en Apple Wallet se adhieren al proceso de “obtención en el dispositivo” descrito en el estándar ISO/IEC 18013-5. La obtención en el dispositivo evita la necesidad de hacer llamadas al servidor durante la presentación, lo cual protege a los usuarios de ser rastreados por Apple y el emisor.

iMessage

Descripción general de la seguridad de iMessage

iMessage de Apple es un servicio de mensajería para dispositivos iOS y iPadOS, Apple Watch y computadoras Mac. iMessage admite texto y archivos adjuntos tales como fotos, contactos, ubicaciones y elementos adjuntos directamente en un mensaje, como un ícono de pulgar hacia arriba. Puesto que los mensajes se muestran en todos los dispositivos registrados de un usuario, una conversación se puede continuar desde cualquiera de sus dispositivos. iMessage utiliza el servicio de notificaciones push de Apple (APNs) ampliamente. Apple no registra el contenido de los mensajes o archivos adjuntos, los cuales están protegidos mediante una encriptación de extremo a extremo, de modo que únicamente el emisor y el receptor pueden acceder a ellos. Apple no puede desencriptar los datos.

Cuando un usuario activa iMessage en un dispositivo, genera pares de encriptación y firmas de claves para usarlos con el dispositivo. Para la encriptación, hay una clave de encriptación RSA de 1280 bits, así como una clave de encriptación EC de 256 bits en la curva NIST P-256. Para las firmas, se utilizan claves de firma de 256 bits del algoritmo de firma digital de curva elíptica (ECDSA). Las claves privadas se guardan en el llavero del dispositivo y sólo están disponibles después del primer desbloqueo. Las claves públicas se envían al servicio de identidad (IDS) de Apple, donde se asocian al número de teléfono o la dirección de correo electrónico del usuario, junto con la dirección del servicio de APN del dispositivo.

A medida que los usuarios activan otros dispositivos para usarlos con iMessage, las claves públicas de encriptación y firma, las direcciones del APNs y los números de teléfono asociados se agregan al servicio de directorio. Los usuarios también pueden agregar más direcciones de correo electrónico, que se verifican mediante el envío de un enlace de confirmación. La SIM y la red del operador verifican los números de teléfono. En algunas redes, esto requiere el uso de SMS (aparece un cuadro de diálogo de confirmación en el caso de que el SMS no sea gratuito). Además de iMessage, varios servicios del sistema, como FaceTime y iCloud, podrían requerir la verificación del número telefónico. Todos los dispositivos registrados del usuario muestran un mensaje de aviso al agregar un dispositivo, número de teléfono o dirección de correo electrónico nuevo.

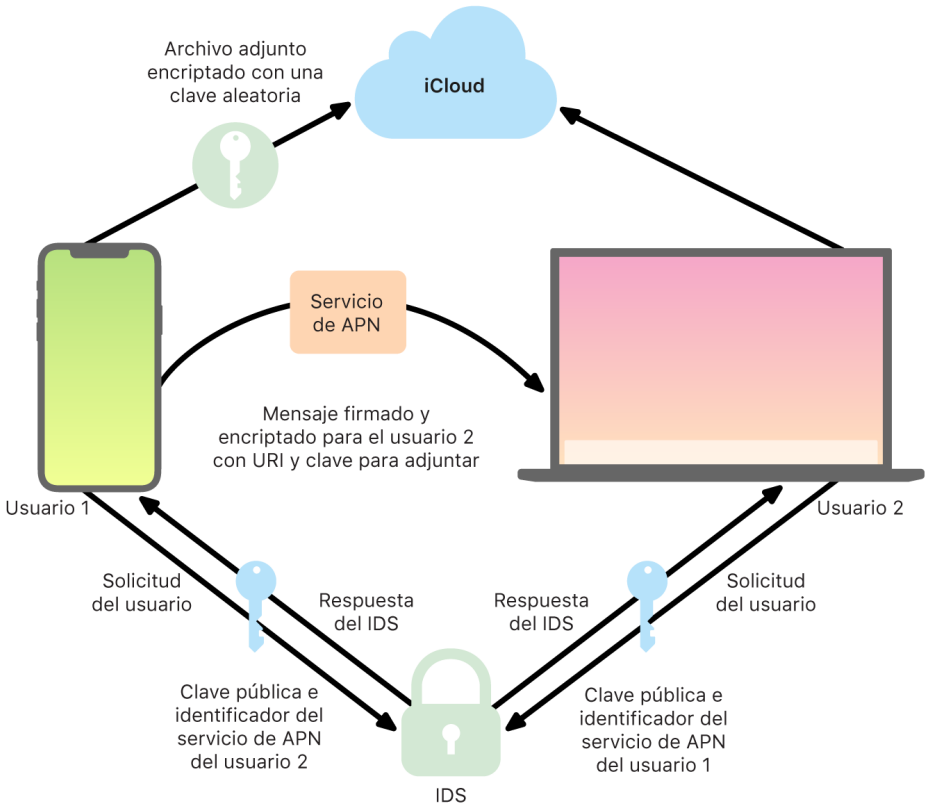
Cómo iMessage envía y recibe mensajes de forma segura

Los usuarios inician una nueva conversación de iMessage al ingresar una dirección o un nombre. Si ingresan un número de teléfono o una dirección de correo electrónico, el dispositivo se pone en contacto con el Servicio de identidad (IDS) de Apple para recuperar las claves públicas y las direcciones del APNs de todos los dispositivos asociados al destinatario. Si el usuario ingresa un nombre, el dispositivo utiliza primero la app Contactos del usuario para recopilar los números de teléfono y las direcciones de correo electrónico asociadas a ese nombre, y luego obtiene las claves públicas y las direcciones del APNs del IDS.

El mensaje que envía el usuario está encriptado de forma individual para cada uno de los dispositivos del destinatario. Las claves de encriptación públicas y las claves de firma de los dispositivos receptores se obtienen del IDS. Para cada dispositivo receptor, el dispositivo emisor genera un valor aleatorio de 88 bits y lo utiliza como una clave HMAC-SHA256 para construir un valor de 40 bits derivado de la clave pública del emisor y del receptor y del texto sin formato. La concatenación de los valores de 88 y 40 bits crea una clave de 128 bits, que encripta el mensaje usando AES en el modo contador CTR. El receptor usa el valor de 40 bits para verificar la integridad del texto sin formato desencriptado. Esta clave AES por mensaje se encripta con RSA-OAEP para la clave pública del dispositivo receptor. Con el texto del mensaje encriptado y la clave del mensaje encriptada se genera un hash SHA-1, que se firma con el algoritmo de firma digital de curva elíptica (ECDSA) utilizando la clave de firma privada del dispositivo emisor. En iOS 13 o versiones posteriores, y iPadOS 13.1 o versiones posteriores, los dispositivos podrían usan un esquema de encriptado integrado de curva elíptica (ECIES) en lugar del encriptado RSA.

Los mensajes que se obtienen, uno para cada dispositivo receptor, están constituidos por el texto del mensaje encriptado, la clave del mensaje encriptada y la firma digital del emisor. A continuación, se mandan al APNs para que los envíe. Los metadatos, como la fecha y la información sobre el enrutamiento del APNs, no se encriptan. La comunicación con el APNs se encripta utilizando un canal TLS de secreto-hacia-adelante.

El APNs sólo puede transmitir mensajes de 4 KB o 16 KB como máximo en función de la versión de iOS o de iPadOS. Si el texto del mensaje es demasiado largo o si se incluye un archivo adjunto (por ejemplo, una foto), el archivo adjunto se encripta con AES en modo CTR utilizando una clave de 256 bits generada aleatoriamente, y se carga a iCloud. Después, la clave AES para el archivo adjunto, su identificador de recursos uniforme (URI) y un hash SHA-1 de su forma encriptada se envían al destinatario como el contenido de un mensaje de iMessage, cuya confidencialidad e integridad están protegidas mediante la encriptación normal de iMessage, como se muestra en el siguiente diagrama.



En el caso de las conversaciones de grupo, este proceso se repite para cada destinatario y sus dispositivos.

En cuanto a la recepción, cada dispositivo recibe una copia del mensaje desde el APNs y, en caso de ser necesario, obtiene el archivo adjunto de iCloud. El número de teléfono o la dirección de correo electrónico del emisor del mensaje se cotejan con los contactos del receptor para que, cuando sea posible, se muestre el nombre.

Como sucede con todas las notificaciones push, el mensaje se elimina del APNs una vez enviado. Sin embargo, a diferencia de lo que sucede con otras notificaciones del APNs, los mensajes de iMessage se ponen en cola para enviarlos a los dispositivos sin conexión. Los mensajes se almacenan en los servidores de Apple durante un plazo máximo de 30 días.

Compartir nombre y foto de forma segura en iMessage

Con la opción Comparte tu nombre y foto en iMessage, los usuarios pueden compartir nombres y fotos al utilizar iMessage. El usuario puede seleccionar la información de su tarjeta de contacto, o puede personalizar el nombre e incluir la imagen que quiera. Esta función de iMessage utiliza un sistema de dos etapas para distribuir el nombre y la foto.

Los datos se subdividen en campos, cada uno encriptado y autenticado por separado, así como autenticados juntos mediante el siguiente proceso. Hay tres campos:

- Nombre
- Foto
- Nombre del archivo de la foto

Uno de los primeros pasos de la creación de datos es generar de forma aleatoria una clave de 128 bits para el registro en el dispositivo. Esta clave de registro luego se deriva con HKDF-HMAC-SHA256 para crear las siguientes subclaves: Clave 1:Clave 2:Clave 3 = HKDF(clave del registro, “apodos”). Para cada campo, se genera un vector de inicialización (IV) aleatorio de 96 bits y los datos se encriptan usando AES-CTR y Clave 1. Luego se computa un código de autenticación de mensaje (MAC) con HMAC-SHA256 usando Clave 2 y que abarca el nombre del campo, el IV del campo y el texto encriptado del campo. Finalmente, el conjunto de valores individuales MAC del campo se concatenan y su MAC se computa con HMAC-SHA256 usando Clave 3. El MAC de 256 bits se almacena junto con los datos encriptados. Los primeros 128 bits de este MAC se usan como recordID.

El registro encriptado luego se almacena en la base de datos pública de CloudKit bajo el recordID. El registro nunca muta, y cuando el usuario decide cambiar su nombre y foto, se genera un nuevo registro encriptado. Cuando el usuario 1 decide compartir su nombre y foto con el usuario 2, se envían la clave del registro junto con el recordID dentro de su carga útil de iMessage, que está encriptada.

Cuando el dispositivo del usuario 2 recibe esta carga útil de iMessage, nota que contiene un recordID con el apodo y la foto, y una clave. El dispositivo del usuario 2 entonces va a la base de datos pública de CloudKit para obtener el nombre y la foto encriptados en el recordID y lo envía mediante iMessage.

Una vez que se obtiene el mensaje, el dispositivo del usuario 2 desencripta la carga útil y verifica la firma usando el recordID mismo. Si se pasa la verificación, al usuario 2 se le muestra el nombre y la foto, y puede elegir agregarlos a sus contactos o usarlo para Mensajes.

Seguridad de Apple Messages for Business

Apple Messages for Business es un servicio de mensajes que permite a los usuarios comunicarse con empresas utilizando la app Mensajes. Con Apple Messages for Business, el usuario tiene siempre el control de la conversación; e incluso puede eliminar la conversación y bloquear la empresa para no recibir mensajes en el futuro. Por razones de privacidad, la empresa no recibe datos del número telefónico, dirección de correo o cuenta de iCloud del usuario, sino que el servicio de identidad (IDS) de Apple genera y comparte con la empresa un identificador único personalizado llamado *identificador opaco*. Este identificador opaco es exclusivo para la relación entre el Apple ID del usuario y el identificador de la empresa. Un usuario tiene un identificador opaco único para cada empresa con la que se comunique mediante Apple Messages for Business. El usuario decide si comparte (o no) y cuándo comparte información que le identifique personalmente con la empresa. El servicio Apple Messages for Business nunca almacena el historial de las conversaciones.

El servicio Apple Messages for Business es compatible con los Apple ID administrados de Apple Business Manager y determina si están habilitados para usar iMessage y FaceTime en Apple School Manager.

Los mensajes que se envían a las empresas se encriptan entre el dispositivo del usuario y los servidores de mensajería de Apple, y utilizan la misma seguridad y servidores que iMessage. Los servidores de mensajería de Apple desencriptan esos mensajes en RAM y los retransmiten a la empresa mediante un enlace encriptado mediante TLS 1.2. Los mensajes nunca se guardan en formato sin encriptar mientras se transmiten mediante el servicio Apple Messages for Business. Las respuestas de las empresas también se envían mediante TLS 1.2 a los servidores de mensajería de Apple, donde se encriptan con las claves públicas únicas de cada dispositivo destinatario.

Si el dispositivo del usuario está en línea, el mensaje se entrega de inmediato y no se almacena en la caché de los servidores de mensajería de Apple; de lo contrario, el mensaje encriptado se almacena en la caché hasta por 30 días para permitir que el usuario lo reciba cuando el dispositivo vuelva a estar en línea. Tan pronto como el dispositivo vuelve a tener conexión, el mensaje se entrega y se elimina de la caché. Después de 30 días, un mensaje en caché que no se haya podido entregar expirará y se borrará permanentemente.

Seguridad de FaceTime

FaceTime es el servicio de llamadas de audio y video de Apple. De forma parecida a iMessage, las llamadas de FaceTime utilizan el servicio de notificaciones push de Apple (APNs) para establecer una conexión inicial con los dispositivos registrados del usuario. El contenido de audio/video de las llamadas FaceTime se protege mediante la encriptación de extremo a extremo, así que únicamente el emisor y el receptor pueden acceder a él, Apple no puede desencriptar los datos.

La conexión inicial de FaceTime se realiza a través de una estructura de servidores de Apple que retransmite los paquetes de datos entre los dispositivos registrados del usuario. Al usar notificaciones APNs y mensajes con Utilidades Transversales de Sesión para NAT (STUN) a través de la conexión retransmitida, los dispositivos verifican sus certificados de identidad y establecen un secreto compartido para cada sesión. El secreto compartido se usa para derivar las claves por sesión para canales de contenido que se transmiten usando el Protocolo de transporte en tiempo real seguro (SRTP). Los paquetes del SRTP se encriptan utilizando el protocolo AES256 en el modo Counter, y se autentican utilizando el protocolo HMAC-SHA1. Después de la conexión inicial y la configuración de seguridad, FaceTime utiliza STUN y el Establecimiento de la conexión a Internet (ICE) para establecer una conexión P2P entre los dispositivos, si es posible.

Las llamadas FaceTime grupales permiten que FaceTime admita hasta 33 participantes simultáneos. Al igual que con las llamadas individuales de FaceTime, las llamadas grupales están encriptadas de extremo a extremo en los dispositivos de los participantes invitados. A pesar de que las llamadas de FaceTime grupales reutilizan gran parte de la infraestructura y diseño de las llamadas individuales de FaceTime, las llamadas grupales cuentan con un nuevo mecanismo de establecimiento de claves creado con base en la autenticidad proporcionada por el Servicio de identidad (IDS) de Apple. Este protocolo tiene la característica conocida como secreto perfecto hacia adelante, lo cual significa que aunque el dispositivo de un usuario se vea comprometido, no filtrará el contenido de las llamadas anteriores. Las claves de sesión se encapsulan usando AES-SIV y se distribuyen entre los participantes utilizando una construcción ECIES con claves efímeras P-256 de ECDH.

Cuando se agrega un nuevo número telefónico o dirección de correo electrónico a una llamada grupal de FaceTime activa, los dispositivos activos establecen nuevas claves de contenido y no comparten las claves utilizadas previamente con los nuevos dispositivos invitados.

Encontrar

Seguridad de Encontrar

La app Encontrar está desarrollada sobre la base de criptografía avanzada de llaves públicas.

Descripción general

La app Encontrar combina Buscar Mi iPhone y Buscar a Mis Amigos en una sola app para iOS, iPadOS y macOS. Encontrar puede ayudar a los usuarios a localizar un dispositivo perdido, incluso una Mac sin conexión. Un dispositivo con conexión puede simplemente reportar su ubicación al usuario mediante iCloud. Encontrar funciona sin conexión al enviar señales Bluetooth de corto alcance desde el dispositivo perdido que otros dispositivos Apple que estén cerca pueden detectar. Esos dispositivos cercanos pueden retransmitir la ubicación detectada del dispositivo perdido a iCloud para que los usuarios puedan localizarlo en la app Encontrar; todo mientras se protege la privacidad y seguridad de todos los usuarios involucrados. Encontrar incluso funciona con una Mac sin conexión y en reposo.

Con el uso de Bluetooth y los cientos de millones de dispositivos iOS, iPadOS y macOS activos alrededor del mundo, un usuario puede localizar su dispositivo perdido, incluso si este no puede conectarse a la red Wi-Fi o celular. Cualquier dispositivo iOS, iPadOS o macOS con “Buscar sin conexión” activado en la configuración de Encontrar puede actuar como “dispositivo localizador”. Esto significa que el dispositivo puede detectar la presencia de otro dispositivo sin conexión perdido usando Bluetooth, y luego usa su conexión en red para reportar la ubicación aproximada de vuelta al propietario. Cuando un dispositivo tiene activada la búsqueda sin conexión, también significa que otros participantes lo pueden localizar de la misma forma. Toda esta interacción está encriptada de extremo a extremo, es anónima y está diseñada para que la batería y los datos sean eficientes. Hay un impacto mínimo en la duración de la batería y el uso del plan de datos celulares, y la privacidad del usuario se protege mejor.

Nota: Encontrar podría no estar disponible en todos los países o regiones.

Encriptación de extremo a extremo

Encontrar está desarrollada sobre la base de criptografía avanzada de llaves públicas. Cuando se activa la búsqueda sin conexión en la configuración de Encontrar, se genera un par de claves de encriptación privada P-224 de curva elíptica (EC) con notación {d,P} directamente en el dispositivo, donde *d* es la llave privada y *P* es la llave pública. Además, un SK_0 de 256 bits secreto y un contador $_i$ se inicializan a cero. Este par de llaves privadas y el secreto nunca se envían a Apple, y se sincronizan únicamente entre los otros dispositivos del usuario de una forma encriptada de extremo a extremo, usando el llavero de iCloud. El secreto y el contador se utilizan para derivar la llave simétrica actual SK_i con la siguiente construcción recursiva: $SK_i = KDF(SK_{i-1}, \text{“actualización”})$.

Basados en la llave SK_i, se computan dos enteros u_i y v_i con $(u_i,v_i) = KDF(SK_i, \text{“diversificar”})$. Tanto la *d* de la clave privada P-224 como la clave pública correspondiente denominada *P* derivan luego utilizando una relación afín que involucra los dos enteros para calcular un par de claves de corta duración: la clave privada derivada es d_i, donde $d_i = u_i * d + v_i$ (realizando una operación módulo en el orden de la curva P-224) y la parte pública correspondiente es P_i y verifica que $P_i = u_i*P + v_i*G$.

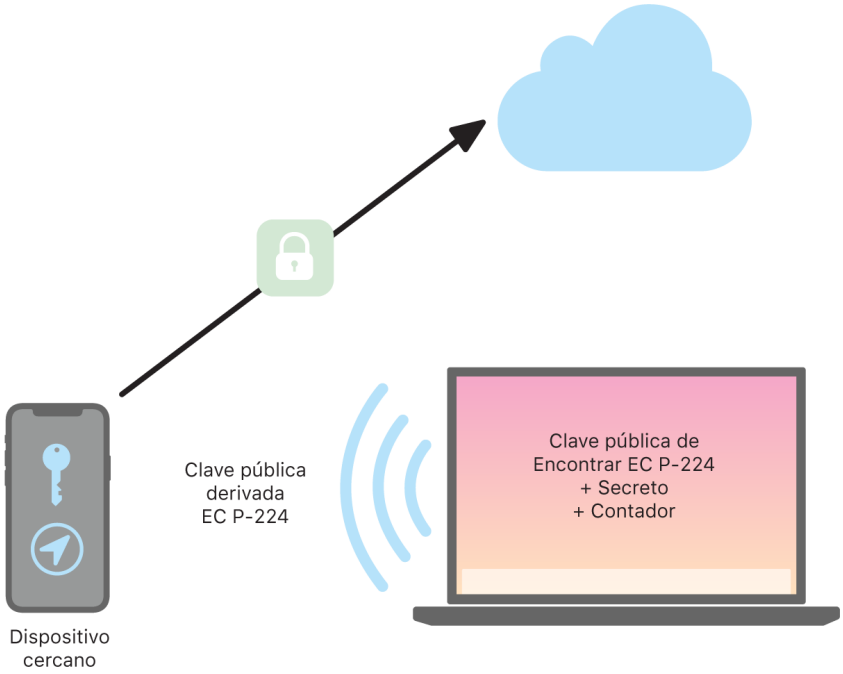
Cuando un dispositivo se pierde y no se puede conectar a la red Wi-Fi o celular, por ejemplo, una MacBook Pro que alguien olvidó en la banca de un parque, comienza a transmitir periódicamente la llave pública derivada P_i por un periodo limitado de tiempo en una carga útil de Bluetooth. Al usar P-224, la representación de la llave pública puede incluirse en una sola carga útil de Bluetooth. Los dispositivos cercanos pueden ayudar a encontrar el dispositivo sin conexión, al encriptar su ubicación en la llave pública. Aproximadamente cada 15 minutos, la llave pública se reemplaza con una nueva usando un valor en incremento del contador y el proceso descrito anteriormente para que no sea posible que un identificador persistente rastree al usuario. El mecanismo de derivación está diseñado para evitar que las varias llaves públicas P_i se enlacen al mismo dispositivo.

Mantener el anonimato de los usuarios y dispositivos

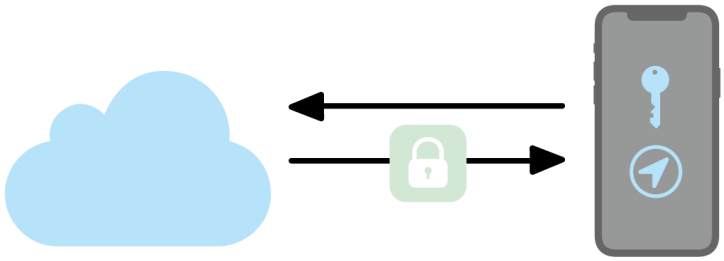
Además de asegurarse de que la información sobre la ubicación y otros datos estén completamente encriptados, las identidades de los participantes se mantienen privadas entre sí y ante Apple. El tráfico enviado a Apple por parte de los dispositivos localizadores no contiene información de autenticación en el contenido ni en los encabezados. Como resultado, Apple no sabe quién es el localizador ni el dispositivo de quién se encontró. Además, Apple no registra información que pudiera revelar la identidad del localizador, ni conserva información que pudiera permitirle a cualquiera relacionar al localizador y al propietario. El propietario del dispositivo recibe únicamente la información sobre la ubicación encriptada que se desencripta y muestra en la app Encontrar, sin indicar quién encontró el dispositivo.

Usar Encontrar para localizar dispositivos Apple perdidos

Cualquier dispositivo Apple que esté dentro del rango de Bluetooth y tenga activada la búsqueda sin conexión puede detectar la señal de otro dispositivo Apple configurado para permitir Encontrar y leer la clave de transmisión P_i actual. Mediante una construcción ECIES y la llave pública P_i de la transmisión, los dispositivos localizadores encriptan la información sobre su ubicación actual y la retransmiten a Apple. La ubicación encriptada se asocia con un índice de servidor, que se computa como el hash SHA256 de la llave pública P-224 P_i obtenida a partir de la carga útil de Bluetooth. Apple nunca tiene la llave de desencriptado, de modo que Apple no puede leer la ubicación encriptada por el localizador. El propietario del dispositivo perdido puede reconstruir el índice y desencriptar la ubicación encriptada.



Al tratar de localizar un dispositivo perdido, se estima un rango esperado de valores del contador para el periodo de búsqueda de localización. Al conocer la llave privada original P-224 *d* y los valores secretos SK_i en el rango de los valores del contador del periodo de búsqueda, el propietario puede reconstruir el conjunto de valores $\{d_i, SHA256(P_i)\}$ de todo el periodo de búsqueda. El dispositivo del propietario que se usó para localizar el dispositivo perdido puede entonces realizar consultas al servidor usando el conjunto de valores índice $SHA256(P_i)$ y descargar las ubicaciones encriptadas del servidor. La app Encontrar entonces desencripta localmente las ubicaciones encriptadas con las llaves privadas d_i que concuerdan, y muestra la ubicación aproximada del dispositivo perdido en la app. Los reportes de localización de varios dispositivos localizadores se combinan en la app del propietario para generar una ubicación más precisa.



Localizar dispositivos sin conexión

Si un usuario tiene Buscar Mi iPhone activado en su dispositivo, la función de búsqueda sin conexión se activa de forma predeterminada cuando actualiza su dispositivo a iOS 13 o versiones posteriores, iPadOS 13.1 o versiones posteriores, y macOS 10.15 o versiones posteriores. Esto está diseñado para cerciorarse de que todos los usuarios tengan la mejor oportunidad posible para localizar sus dispositivos si se pierden. Sin embargo, si en algún momento el usuario prefiere no participar, pueden desactivar la función de búsqueda sin conexión en la configuración de Encontrar de su dispositivo. Cuando se desactiva la búsqueda sin conexión, el dispositivo ya no actuará como localizador ni tampoco lo podrán detectar otros dispositivos. Sin embargo, el usuario puede seguir localizando el dispositivo, siempre y cuando esté conectado a una red Wi-Fi o celular.

Cuando se localiza un dispositivo sin conexión, el usuario recibe una notificación y un mensaje de correo electrónico para informarle que se localizó el dispositivo. Para ver la ubicación del dispositivo perdido, el usuario abre la app Encontrar y selecciona la pestaña Dispositivos. En lugar de mostrar el dispositivo en un mapa en blanco, como se mostraría antes de que se localice, Encontrar muestra una ubicación en el mapa con una dirección aproximada e información sobre hace cuánto se detectó el dispositivo. Si llegan más reportes con la ubicación, la ubicación actual y la hora se actualizan automáticamente. Aunque los usuarios no pueden reproducir un sonido en un dispositivo sin Internet, ni borrar su contenido de forma remota, pueden usar la información sobre la ubicación para rastrear sus pasos o realizar otras acciones para recuperarlo.

Continuidad

Descripción general de la seguridad de Continuidad

Continuidad saca provecho de tecnologías como iCloud, Bluetooth y Wi-Fi para permitir a los usuarios continuar con una actividad en otro dispositivo, hacer y recibir llamadas telefónicas, enviar y recibir mensajes de texto, y compartir la conexión a Internet de un dispositivo celular.

Seguridad de Handoff

Apple maneja las transferencias de Handoff de forma segura, ya sea de un dispositivo a otro, entre una app nativa y un sitio web, e incluso cuando hay una gran cantidad de datos involucrada.

Cómo Handoff funciona de manera segura

Con Handoff, cuando los dispositivos iOS, iPadOS y macOS de un usuario están cerca, el usuario puede transferir automáticamente aquello en lo que esté trabajando de un dispositivo al otro. Handoff permite al usuario cambiar de dispositivo y continuar trabajando de forma instantánea.

Cuando un usuario inicia sesión en iCloud en un segundo dispositivo compatible con Handoff, los dos dispositivos establecen un enlace mediante una conexión Bluetooth de baja energía (BLE) 4.2 fuera de banda a través del servicio de notificaciones push de Apple (APNs). Los mensajes individuales se encriptan de forma muy similar a los mensajes de iMessage. Una vez que los dispositivos están enlazados, cada uno genera una clave simétrica AES de 256 bits que se almacena en el llavero del dispositivo. Esta clave puede encriptar y autenticar los avisos de la conexión BLE que comunican la actividad actual del dispositivo con otros dispositivos enlazados de iCloud utilizando AES256 en modo GCM con medidas de protección de reproducción.

La primera vez que un dispositivo recibe un aviso de una clave nueva, establece una conexión BLE con el dispositivo que origina la clave y genera un intercambio de claves de encriptación del aviso. Esta conexión se protege mediante la encriptación estándar BLE 4.2 y la encriptación de los mensajes individuales, que es parecida a la encriptación de iMessage. En algunas situaciones, estos mensajes se envían usando APNs en lugar de BLE. La carga útil de la actividad se protege y se transfiere del mismo modo que con un iMessage.

Handoff entre apps nativas y sitios web

Handoff permite que una app nativa de iOS, iPadOS o macOS pueda reanudar la actividad del usuario en páginas web en dominios controlados legítimamente por el desarrollador de la app. También permite reanudar la actividad del usuario de la app nativa en un navegador web.

Con el fin de ayudar a evitar que las apps nativas soliciten reanudaciones de sitios web no controlados por el desarrollador, las apps deben demostrar que disponen del control legítimo de los dominios web que desean reanudar. El control de un sitio web se establece usando el mecanismo para credenciales web compartidas. Para ver más detalles, consulta Acceso de las apps a las contraseñas guardadas. El sistema debe validar el control del nombre del dominio de una app antes de que esta tenga permiso para aceptar la continuidad de la actividad del usuario con Handoff.

El origen de Handoff de una página web puede ser cualquier navegador que haya aceptado las API de Handoff. Cuando el usuario visualiza una página web, el sistema anuncia el nombre del dominio de la página web en los bytes de aviso de Handoff encriptados. Únicamente los demás dispositivos del usuario pueden desencriptar los bytes de aviso.

En un dispositivo receptor, el sistema detecta que una app nativa instalada acepta Handoff desde el nombre de dominio anunciado y muestra el ícono de la app nativa como la opción de Handoff. Una vez abierta, la app nativa recibe la dirección URL completa y el título de la página web. No se transfiere ninguna otra información del navegador a la app nativa.

En el sentido inverso, una app nativa puede especificar una URL de respaldo cuando el dispositivo que recibe Handoff no tiene instalada la misma app nativa. En este caso, el sistema muestra el navegador predeterminado del usuario como opción de aplicación de Handoff (si ese navegador ha adoptado las API de Handoff). Cuando se solicite el uso de Handoff, el navegador se abre y se le facilita la URL de respaldo que haya proporcionado la app nativa. No es necesario que la URL de respaldo se limite a los nombres de dominio que controle el desarrollador de la app nativa.

Handoff de datos de mayor tamaño

Como complemento a la función básica de Handoff, es posible que algunas apps elijan usar API que sean compatibles con el envío de un mayor número de datos mediante la tecnología de red Wi-Fi P2P creada por Apple (de forma parecida a AirDrop). Por ejemplo, la app Mail utiliza esas API para poder utilizar Handoff con borradores de mensajes de correo, que podrían incluir archivos adjuntos de gran tamaño.

Cuando una app utiliza estas API, el intercambio entre los dos dispositivos se inicia como en Handoff. Pero, después de recibir la carga útil inicial mediante BLE, el dispositivo receptor inicia una conexión nueva a través de la red Wi-Fi. Esta conexión está encriptada (con TLS), y obtiene la confianza mediante una identidad compartida a través del llavero de iCloud. La identidad de los certificados se coteja con la identidad del usuario. El resto de los datos de carga útil se envía mediante esta conexión encriptada hasta que se completa la transferencia.

Portapapeles universal

El portapapeles universal aprovecha Handoff para transferir de forma segura el contenido del portapapeles del usuario a través de dispositivos para poder copiar contenido en un dispositivo y pegarlo en otro. El contenido se protege de la misma forma que los demás datos de Handoff y se comparte de forma predeterminada mediante el portapapeles universal, a menos que el desarrollador de la app decida desactivar la opción de compartir.

Las apps tienen acceso a los datos del portapapeles incluso si el usuario ha pegado el portapapeles en una app. Con el portapapeles universal, el acceso a estos datos se extiende a las apps que se están ejecutando en otros dispositivos del usuario (establecidos mediante sus sesiones abiertas de iCloud).

Seguridad de la retransmisión de llamadas telefónicas del iPhone

Cuando la Mac, el iPad, el iPod touch o el HomePod de un usuario se encuentren en la misma red Wi-Fi que su iPhone, podrán realizar y recibir llamadas telefónicas utilizando la red celular del iPhone. La configuración requiere que los dispositivos hayan iniciado sesión tanto en iCloud como en FaceTime con la misma cuenta de Apple ID.

Al recibir una llamada entrante, todos los dispositivos configurados reciben una notificación usando el servicio de notificaciones push de Apple (APNs). Con cada notificación se usará la misma encriptación de extremo a extremo de iMessage. Los dispositivos que estén en la misma red presentan la misma interfaz de usuario de notificación de llamada entrante. Cuando el usuario contesta la llamada, el audio se transmite sin interrupciones desde el iPhone del usuario utilizando una conexión P2P segura entre los dos dispositivos.

Cuando se responde una llamada en un dispositivo, se detiene el tono de llamada en los dispositivos enlazados con iCloud que estén cerca con un aviso mediante Bluetooth de baja energía (BLE). Los bytes de aviso se encriptan usando el mismo método que los avisos de Handoff.

Las llamadas salientes también se transmiten al iPhone usando APNs y el audio se transmite de forma parecida mediante el enlace P2P seguro entre dispositivos. Los usuarios pueden desactivar la retransmisión de llamadas telefónicas en un dispositivo desactivando Llamadas telefónicas del iPhone en la configuración de FaceTime.

Seguridad del reenvío de mensajes de texto del iPhone

La opción Reenvío de mensajes de texto permite enviar automáticamente los mensajes de texto SMS recibidos en un iPhone al iPad, iPod touch o Mac inscrito del usuario. Cada dispositivo debe haber iniciado sesión en el servicio iMessage con la misma cuenta de Apple ID. Cuando las funciones de reenvío de mensajes y de autenticación de dos factores están activadas, la inscripción de los dispositivos que están dentro del círculo de confianza del usuario se realiza de forma automática. De lo contrario, el iPhone genera un código numérico de seis dígitos aleatorio que se ingresa en cada dispositivo para verificar su inscripción.

Una vez que los dispositivos están enlazados, el iPhone encripta y reenvía los mensajes de texto SMS entrantes a cada dispositivo mediante los métodos descritos en Descripción general de la seguridad de iMessage. Las respuestas se envían de vuelta al iPhone utilizando el mismo método, y el iPhone las envía como mensajes de texto con ayuda del mecanismo de transmisión de SMS del operador. La opción para el reenvío de mensajes de texto se puede desactivar en la configuración de Mensajes.

Seguridad de Instant Hotspot

Instant Hotspot conecta otros dispositivos Apple a un punto de acceso personal de iOS o iPadOS. Los dispositivos iOS y iPadOS compatibles con Instant Hotspot usan la tecnología Bluetooth de baja energía (BLE) para descubrir y comunicarse con todos los dispositivos que hayan iniciado sesión en la misma cuenta de iCloud o en las cuentas usadas con Compartir en familia (en iOS 13 y iPadOS). Las computadoras Mac compatibles que tienen el sistema operativo OS X 10.10 o versiones posteriores utilizan la misma tecnología para detectar dispositivos iOS y iPadOS y comunicarse con ellos mediante Instant Hotspot.

Inicialmente, cuando un usuario ingresa la configuración de Wi-Fi en un dispositivo, este emite un aviso de BLE que contiene un identificador común para todos los dispositivos que han iniciado sesión en la misma cuenta de iCloud. El identificador se genera desde un identificador DSID (Destination Signaling Identifier) que está vinculado a la cuenta de iCloud y va rotando periódicamente. Si hay otros dispositivos que hayan iniciado sesión en la misma cuenta de iCloud cerca y son compatibles con la función Compartir Internet, estos detectarán la señal y responderán, indicando su disponibilidad para usar Instant Hotspot.

Cuando un usuario que no es parte de Compartir en familia selecciona un iPhone o iPad para compartir Internet, se envía una solicitud de activación de Compartir Internet a dicho dispositivo. La solicitud se envía mediante un enlace que se encripta con la encriptación BLE, y la solicitud se encripta mediante un proceso parecido al de la encriptación de iMessage. A continuación, el dispositivo responde a través del mismo enlace de BLE con la misma encriptación por mensaje con información de la conexión de Compartir Internet.

Para los usuarios que forman parte de Compartir en familia, la información del punto de acceso a Internet compartido se comparte de forma segura mediante un mecanismo similar al utilizado por los dispositivos HomeKit para sincronizar la información. Específicamente, la conexión que comparte la información del punto de acceso entre usuarios está asegurada con una clave efímera ECDH (Curve25519) que se autentica con las respectivas claves públicas Ed25519 específicas de los dispositivos de los usuarios. Las claves públicas que se usan son las que se habían sincronizado anteriormente entre los miembros de Compartir en familia utilizando IDS cuando se configuró la función Compartir en familia.

Seguridad de la red

Descripción general de la seguridad de la red

Además de los métodos de protección integrados que Apple utiliza para proteger los datos almacenados en dispositivos Apple, existen muchas medidas que las organizaciones pueden poner en marcha para proteger la información durante su transferencia a un dispositivo o desde él. Todas estas medidas y protecciones están dentro de la seguridad de la red.

Debido a que los usuarios deben tener la posibilidad de acceder a redes corporativas desde cualquier parte del mundo, es importante ayudar a que tengan autorización y que sus datos estén protegidos durante su transmisión. Para alcanzar estos objetivos de seguridad, iOS, iPadOS y macOS integran tecnologías probadas y los estándares más recientes para conexiones de red de datos celulares y Wi-Fi. Por esto, nuestros sistemas operativos usan protocolos estándar de redes para comunicaciones autenticadas, autorizadas y encriptadas, y también les brindan acceso a los desarrolladores a estos.

Seguridad de TLS

iOS, iPadOS y macOS son compatibles con los protocolos de seguridad de la capa de transporte (TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3) y con los protocolos de seguridad de la capa de transporte de datagramas (DTLS). El protocolo TLS admite tanto AES128 como AES256, y prefiere conjuntos de encriptado con secreto-hacia-adelante. Las apps de Internet como Safari, Calendario y Mail utilizan automáticamente este protocolo para activar un canal de comunicación encriptado entre el dispositivo y los servicios de red. Las API de alto nivel (como CFNetwork) facilitan a los desarrolladores la adopción de TLS en sus apps, mientras que las API de bajo nivel (como Network.framework) proporcionan un control muy preciso. CFNetwork no permite SSL 3 y las apps que utilizan WebKit (como Safari) tienen prohibido realizar una conexión SSL 3.

En macOS 10.13 o versiones posteriores y iOS 11 o versiones posteriores, no se permiten los certificados de SHA-1 para las conexiones TLS a menos que el usuario confíe en ellos. No se permiten en absoluto los certificados con claves RSA de menos de 2048 bits. El conjunto de encriptación simétrico RC4 está obsoleto en iOS 10 y macOS 10.12. De forma predeterminada, los servidores y clientes TLS con API de SecureTransport no permiten conjuntos de encriptación RC4, y no podrán conectarse cuando RC4 sea el único conjunto de encriptación disponible. Para mayor seguridad, las apps y servicios que requieran RC4 deberían actualizarse para usar conjuntos de encriptación seguros. En iOS 12.1, los certificados emitidos después del 15 de octubre de 2018 desde un certificado raíz en el que confía el sistema deben agregarse a un registro de confianza de transparencia de certificados para permitir conexiones TLS. En iOS 12.2, TLS 1.3 se activa de forma predeterminada para las API Network.framework y NSURLSession. Los clientes TLS que usen las API SecureTransport no pueden usar TLS 1.3.

Seguridad de transporte de las apps

La seguridad de transporte de las apps proporciona requisitos de conexión de forma predeterminada, de manera que las apps cumplan las buenas prácticas para conexiones seguras al utilizar las API NSURLConnection, CFURL o NSURLSession. De forma predeterminada, la seguridad de transporte de las apps limita la selección de encriptación para que incluya sólo conjuntos que proporcionen secreto-hacia-adelante, específicamente:

- ECDHE_ECDSA_AES y ECDHE_RSA_AES en el modo Galois/Counter (GCM)
- Modo de encadenamiento de bloques de encriptado (CBC)

Las apps pueden desactivar el requisito de secreto-hacia-adelante por dominio, en cuyo caso se agrega RSA_AES al conjunto de encriptación disponible.

Los servidores deben ser compatibles con TLS 1.2 y secreto-hacia-adelante, y los certificados deben ser válidos y estar firmados mediante SHA256 o más fuerte, con una clave RSA de al menos 2048 bits o una clave de curva elíptica de 256 bits como mínimo.

Las conexiones de red que no cumplan estos requisitos darán error a menos que la app omita la seguridad de transporte de las apps. Los certificados no válidos siempre dan como resultado un fallo grave e imposibilidad de conexión. La seguridad de transporte de las apps se aplica automáticamente a las apps compiladas para iOS 9 o versiones posteriores, o macOS 10.11 o versiones posteriores.

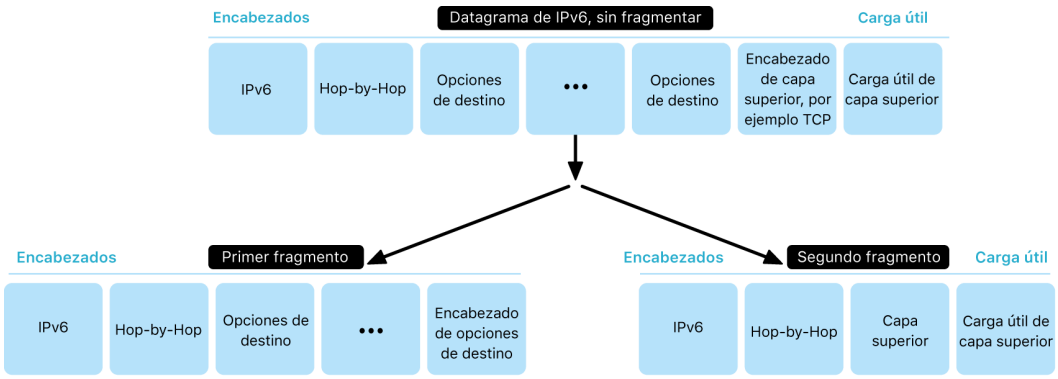
Verificación de la validez del certificado

La evaluación del estado de confianza de un certificado TLS se realiza de acuerdo con los estándares establecidos de la industria, como se indica en RFC 5280, e incorpora estándares tales como RFC 6962 (transparencia de los certificados). En iOS 11 o versiones posteriores y en macOS 10.13 o versiones posteriores, los dispositivos Apple se actualizan periódicamente con una lista actualizada de los certificados revocados y restringidos. La lista se agrega a partir de las listas de revocación de certificados (CRL) que publica cada una de las autoridades de certificados raíz integrados en quienes Apple confía, así como sus emisores de CA subordinados. La lista también puede incluir otras restricciones, a discreción de Apple. Esta información se consulta siempre que la API de una red tenga una función que se utilice para realizar una conexión segura. Si hay demasiados certificados revocados de una CA para enumerarlos de forma individual, una evaluación de confianza podría requerir una respuesta sobre el estado del certificado en línea (OCSP); si la respuesta no está disponible, la evaluación de confianza fallará.

Seguridad de iPv6

Todos los sistemas operativos de Apple admiten IPv6, lo que implementa varios mecanismos para proteger la privacidad de los usuarios y la estabilidad de la pila de redes. Cuando se usa la autoconfiguración de direcciones sin estado (SLAAC), las direcciones IPv6 de todas las interfaces se generan de una manera que ayuda a evitar el rastreo de dispositivos a través de las redes y, al mismo tiempo, permite una buena experiencia de usuario al garantizar la estabilidad de la dirección cuando no se producen cambios en la red. El algoritmo de generación de direcciones se basa en direcciones generadas criptográficamente a partir de RFC 3972, mejoradas por un modificador específico de interfaz para garantizar que incluso diferentes interfaces en la misma red eventualmente tengan diferentes direcciones. Además, las direcciones temporales se crean con una vida útil preferida de 24 horas y se utilizan de forma predeterminada para cualquier conexión nueva. En consonancia con la funcionalidad de dirección Wi-Fi privada introducida en iOS 14, iPadOS 14 y watchOS 7, se genera una dirección de enlace-local única para cada red Wi-Fi a la que accede un dispositivo. El SSID de la red se incorpora como un elemento adicional para la generación de direcciones, similar al parámetro Network_ID a partir de RFC 7217. Este enfoque se utiliza en iOS 14, iPadOS 14 y watchOS 7.

Para protegerse contra ataques basados en fragmentación y encabezados de extensión de IPv6, los dispositivos Apple implementan las medidas de protección especificadas en RFC 6980, RFC 7112 y RFC 8021. Entre otras medidas, estas inhiben los ataques en los que el encabezado de capa superior se puede encontrar sólo en el segundo fragmento (como se muestra a continuación), lo que a su vez podría generar ambigüedades en los controles de seguridad, como los filtros de paquetes sin estado.



Además, para ayudar a garantizar la confiabilidad de la pila IPv6 de los sistemas operativos de Apple, los dispositivos Apple imponen varios límites en las estructuras de datos relacionadas con IPv6, como el número de prefijos por interfaz.

Seguridad de la red privada virtual (VPN)

Los servicios de redes seguras como las redes privadas virtuales normalmente requieren muy poca configuración para funcionar con los dispositivos iOS, iPadOS y macOS.

Protocolos compatibles

Estos dispositivos funcionan con los servidores VPN que son compatibles con los siguientes protocolos y métodos de autenticación:

- IKEv2/IPsec con autenticación por secreto compartido, certificados RSA, algoritmo de firma digital de curva elíptica (ECDSA), EAP-MSCHAPv2 o EAP-TLS.
- SSL-VPN usando la app cliente adecuada de App Store.
- L2TP/IPsec con autenticación de usuarios por contraseña MS-CHAPV2 y autenticación automática por secreto compartido (iOS, iPadOS y macOS), y RSA SecurID o CRYPTOCard (sólo macOS).
- Cisco IPsec con autenticación de usuario mediante contraseña, RSA SecurID o CRYPTOCard y autenticación automática mediante secreto compartido y certificados (sólo macOS).

Implementaciones VPN compatibles

iOS, iPadOS y macOS son compatibles con lo siguiente:

- *VPN por petición:* para las redes que utilizan la autenticación basada en certificados. Las políticas de TI utilizan un perfil de configuración de VPN para especificar los dominios que requieren una conexión VPN.
- *VPN por app:* para facilitar las conexiones VPN de forma mucho más granular. Las soluciones de administración de dispositivos móviles (MDM) pueden especificar una conexión para cada app administrada y para dominios específicos en Safari. Esto ayuda a garantizar que los datos seguros siempre entran y salen de la red corporativa, pero no así los datos personales del usuario.

iOS y iPadOS son compatibles con lo siguiente:

- *VPN siempre activada:* para dispositivos administrados mediante una solución para la administración de dispositivos móviles (MDM) y que se supervisan con Apple Configurator para Mac, Apple School Manager o Apple Business Manager. La VPN siempre activada elimina la necesidad de que los usuarios activen la red VPN para obtener protección al conectarse a redes Wi-Fi y celulares. Esta funcionalidad también proporciona a la organización control absoluto sobre el tráfico del dispositivo al dirigir todo el tráfico IP de vuelta a la organización. Durante el intercambio predeterminado de parámetros y claves para el encriptado posterior, IKEv2, asegura la transmisión del tráfico con encriptado de datos. La organización puede supervisar y filtrar el tráfico de estos dispositivos en ambas direcciones, proteger los datos en la red y restringir el acceso del dispositivo a Internet.

Seguridad de Wi-Fi

Acceso seguro a redes inalámbricas

Todas las plataformas de Apple son compatibles con los protocolos estándar de la industria para autenticación y encriptación de Wi-Fi a fin de brindar acceso autenticado y confidencialidad al usar las siguientes redes inalámbricas seguras:

- WPA2 Personal
- WPA2 Enterprise
- WPA2/WPA3 Transitional
- WPA3 Personal
- WPA3 Enterprise
- WPA3 Enterprise con seguridad de 192 bits

WPA2 y WPA3 autentican cada conexión y brindan encriptación AES de 128 bits para ayudar a garantizar la confidencialidad de los datos enviados de forma inalámbrica. Esto les da a los usuarios la mayor garantía de que sus datos estarán protegidos durante las comunicaciones a través de una conexión de red Wi-Fi.

Compatibilidad con WPA3

WPA3 es compatible con los siguientes dispositivos Apple:

- iPhone 7 o modelos posteriores
- iPad quinta generación o modelos posteriores
- Apple TV 4K o modelos posteriores
- Apple Watch Series 3 o modelos posteriores
- Computadoras Mac (finales de 2013 o modelos posteriores, con 802.11ac o una versión posterior)

Los dispositivos más recientes son compatibles con la autenticación mediante WPA3 Enterprise con seguridad de 192 bits, lo que incluye la compatibilidad con la encriptación AES de 256 bits al conectarse con los puntos de acceso inalámbricos compatibles. Esto brinda protecciones incluso más fuertes a la confidencialidad del tráfico enviado de forma inalámbrica. WPA3 Enterprise con seguridad de 192 bits es compatible con iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max y dispositivos iOS y iPadOS posteriores.

Compatibilidad con PMF

Además de la protección de los datos enviados de forma inalámbrica, las plataformas de Apple extienden las protecciones de nivel WPA2 y WPA3 a las estructuras de administración unicast y multicast mediante el servicio de estructura de administración protegida (PMF) definido en 802.11w. La compatibilidad con PMF está disponible en los siguientes dispositivos Apple:

- iPhone 6 o modelos posteriores
- iPad Air 2 o modelos posteriores
- Apple TV HD o modelos posteriores
- Apple Watch Series 3 o modelos posteriores
- Computadoras Mac (finales de 2013 o modelos posteriores, con 802.11ac o una versión posterior)

Los dispositivos Apple compatibles con 802.1X, se pueden integrar en un amplio abanico de entornos de autenticación RADIUS. Los dispositivos son compatibles con los siguientes métodos de autenticación inalámbrica 802.1X: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 y PEAPv1.

Protecciones de las plataformas

Los sistemas operativos de Apple protegen el dispositivo de vulnerabilidades en el firmware del procesador de red. Esto significa que los controladores de red con Wi-Fi tienen acceso limitado a la memoria del procesador de aplicaciones.

- Cuando se usa USB o SDIO (Secure Digital Input Output) para interactuar con el procesador de la red, este no puede iniciar transacciones de acceso directo a memoria (DMA) hacia el procesador de apps.
- Cuando se usa PCIe, cada procesador de red funciona como su propio bus PCIe aislado. Una IOMMU (unidad de gestión de memoria de entrada/salida) en cada bus PCIe limita aún más el acceso directo a memoria (DMA) del procesador de red a los recursos de la memoria que contienen sus paquetes de red o estructuras de control.

Protocolos obsoletos

Los productos Apple son compatibles con los siguientes protocolos de autenticación y encriptación de Wi-Fi obsoletos:

- WEP abierta, con claves de 40 bits y 104 bits
- WEP con clave compartida, con claves de 40 bits y 104 bits
- WEP con clave dinámica
- Temporal Key Integrity Protocol (TKIP)
- WPA
- WPA/WPA2 transicional

A estos protocolos ya no se les considera seguros, y se desaconseja su uso por motivos de compatibilidad, confiabilidad, rendimiento y seguridad. Son compatibles únicamente con fines de compatibilidad regresiva, y podrían eliminarse en futuras versiones del software.

Se recomienda que todas las implementaciones de Wi-Fi se migren a WPA3 Personal o WPA3 Enterprise para brindar las conexiones Wi-Fi más seguras, robustas y compatibles posibles.

Privacidad de Wi-Fi

Aleatorización de la dirección MAC

Las plataformas de Apple usan una dirección del control de acceso al medio (MAC) aleatoria al realizar exploraciones de redes Wi-Fi cuando no están asociadas con una red Wi-Fi. Estas exploraciones pueden realizarse para encontrar y conectarse a una red Wi-Fi conocida, o para ayudar a la función Localización en apps que usan geocercas, tales como los recordatorios basados en la ubicación o para establecer una ubicación en Mapas de Apple. Toma en cuenta que la exploración Wi-Fi que sucede mientras se intenta conectar a la red Wi-Fi preferida no es aleatoria. El iPhone 5 y los modelos posteriores cuentan con soporte para las direcciones MAC aleatorias para Wi-Fi.

Las plataformas de Apple también utilizan una dirección MAC aleatoria al realizar exploraciones de preferencia de descarga de red mejorada (ePNO) cuando un dispositivo no está asociado a una red Wi-Fi o su procesador está en reposo. Las exploraciones ePNO se ejecutan cuando un dispositivo utiliza Localización para apps con geocercas, como los recordatorios basados en la ubicación que determinan si el dispositivo se encuentra cerca de una ubicación específica.

La dirección MAC de un dispositivo cambia cuando no está conectado a una red Wi-Fi, por lo que no se puede utilizar para realizar un seguimiento continuo de un dispositivo con observadores pasivos del tráfico de la red Wi-Fi, incluso cuando el dispositivo está conectado a una red celular. Apple ha informado a los fabricantes de Wi-Fi que las exploraciones Wi-Fi de iOS y iPadOS utilizan una dirección MAC aleatoria, y que ni Apple ni los fabricantes pueden predecir estas direcciones MAC aleatorias.

En iOS 14 o versiones posteriores, iPadOS 14 o versiones posteriores, y watchOS 7 o versiones posteriores, cuando un iPhone, iPad, iPod touch, o Apple Watch se conecta a una red Wi-Fi, se identifica mediante una dirección MAC única (aleatoria) por red. El usuario puede desactivar esta función, o bien se puede desactivar mediante una opción nueva en la carga útil para Wi-Fi. En determinadas circunstancias, el dispositivo recurrirá a la dirección MAC real.

Para obtener más información, consulta el artículo de soporte de Apple Usar direcciones privadas Wi-Fi en el iPhone, iPad, iPod touch, y Apple Watch.

Aleatorización de los números de secuencia de las estructuras de Wi-Fi

Las estructuras Wi-Fi incluyen un número de secuencia que utiliza el protocolo 802.11 de alto nivel para activar las comunicaciones Wi-Fi eficientes y confiables. Como estos números de secuencia aumentan con cada estructura transmitida, pueden usarse para correlacionar la información transmitida durante la exploración de redes Wi-Fi con otras estructuras transmitidas por el mismo dispositivo.

Para evitar esto, los dispositivos Apple aleatorizan los números de secuencia siempre que se cambia una dirección MAC a una nueva dirección aleatorizada. Esto incluye la aleatorización de los números de secuencia de cada nueva exploración que se inicia mientras el dispositivo no está asociado. Esta aleatorización es compatible con los siguientes dispositivos:

- iPhone 7 o modelos posteriores
- iPad quinta generación o modelos posteriores
- Apple TV 4K o modelos posteriores
- Apple Watch Series 3 o modelos posteriores
- iMac Pro (Retina 5K, 27 pulgadas, 2017) o modelos posteriores
- MacBook Pro (13 pulgadas, 2018) o modelos posteriores
- MacBook Pro (15 pulgadas, 2018) o modelos posteriores
- MacBook Air (Retina, 13 pulgadas, 2018) o modelos posteriores
- Mac mini (2018) o modelos posteriores
- iMac (Retina 4K, 21.5 pulgadas, 2019) o modelos posteriores
- iMac (Retina 5K, 27 pulgadas, 2019) o modelos posteriores
- Mac Pro (2019) o modelos posteriores

Conexiones Wi-Fi

Apple genera direcciones MAC aleatorizadas para las conexiones Wi-Fi P2P que se utilizan para AirDrop y AirPlay. Las direcciones aleatorizadas también se utilizan para la función Compartir Internet de iOS y iPadOS (con una tarjeta SIM) y de macOS.

Se generan direcciones nuevas y aleatorias siempre que se inician estas interfaces, y se generan direcciones únicas para cada interfaz de manera independiente, según sea necesario.

Redes ocultas

Las redes Wi-Fi se identifican por su nombre de red, conocido como el *identificador del conjunto de servicios (SSID)*. Algunas redes Wi-Fi están configuradas para ocultar su SSID, lo que hace que el punto de acceso inalámbrico no transmita el nombre de la red. A estas se les conocen como *redes ocultas*. Los dispositivos iPhone 6s y modelos posteriores detectan automáticamente si una red está oculta. Si una red está oculta, el dispositivo iOS o iPadOS enviará una exploración con el SSID incluido en la petición, no al contrario. Esto ayuda a evitar que el dispositivo transmita los nombres de las redes ocultas a las que el usuario se conectó anteriormente, para asegurar aún más la privacidad.

Seguridad de Bluetooth

Hay dos tipos de Bluetooth en los dispositivos Apple: Bluetooth clásico y Bluetooth de baja energía (BLE). El modelo de seguridad de Bluetooth para ambas versiones incluye las siguientes funciones de seguridad distintivas:

- *Enlace:* el proceso de crear una o más claves secretas
- *Vinculación:* el acto de almacenar las claves creadas durante el enlace para usarlas en las conexiones siguientes, a fin de formar un par de dispositivos de confianza
- *Autenticación:* verificar que los dos dispositivos tengan las mismas claves
- *Encriptación:* confidencialidad de los mensajes
- *Integridad de los mensajes:* protección contra la falsificación de mensajes
- *Enlace simple seguro:* protección contra los ataques de interceptación pasiva y de intermediario

La versión 4.1 de Bluetooth agregó la función de conexiones seguras al transporte físico del Bluetooth clásico (BR/EDR).

Las funciones de seguridad para cada tipo de Bluetooth se mencionan a continuación.

Soporte	Bluetooth clásico	Bluetooth de baja energía
Enlace	Curva elíptica P-256	Algoritmos aprobados por FIPS (AES-CMAC y curva elíptica P-256)
Vinculación	La información del enlace se almacena en un lugar seguro en los dispositivos iOS, iPadOS, macOS, tvOS y watchOS	La información del enlace se almacena en un lugar seguro en los dispositivos iOS, iPadOS, macOS, tvOS y watchOS
Autenticación	Algoritmos aprobados por FIPS (HMAC-SHA-256 y AES-CTR)	Algoritmos aprobados por FIPS
Encriptación	Criptografía AES-CCM (realizada en el controlador)	Criptografía AES-CCM (realizada en el controlador)
Integridad de los mensajes	Se utiliza AES-CCM para la integridad de los mensajes	Se utiliza AES-CCM para la integridad de los mensajes
Enlace simple seguro: protección contra la interceptación pasiva	Intercambio de claves efímeras con Diffie-Hellman de curva elíptica (ECDHE)	Intercambio Diffie-Hellman de curva elíptica (ECDHE)
Enlace simple seguro: protección contra los ataques de intermediario (MITM)	Dos métodos numéricos asistidos por el usuario: comparación numérica o ingreso de la clave	Dos métodos numéricos asistidos por el usuario: comparación numérica o ingreso de la clave Los enlaces requieren la respuesta del usuario, incluidos todos los modos de enlace que no sean MITM
Bluetooth 4.1 o versiones posteriores	iMac (finales de 2015) o modelos posteriores MacBook Pro (principios de 2015) o modelos posteriores	iOS 9 o versiones posteriores iPadOS 13.1 o versiones posteriores macOS 10.12 o versiones posteriores tvOS 9 o versiones posteriores watchOS 2.0 o versiones posteriores

Soporte	Bluetooth clásico	Bluetooth de baja energía
Bluetooth 4.2 o versiones posteriores	iPhone 6 o modelos posteriores	iOS 9 o versiones posteriores iPadOS 13.1 o versiones posteriores macOS 10.12 o versiones posteriores tvOS 9 o versiones posteriores watchOS 2.0 o versiones posteriores

Privacidad de Bluetooth Low Energy

Para ayudar a asegurar la privacidad de los usuarios, BLE incluye las siguientes dos funciones: la aleatorización de direcciones y la derivación de claves a través de transportes.

La función de *aleatorización* reduce la capacidad para rastrear un dispositivo BLE durante un cierto periodo al cambiar frecuentemente la dirección del dispositivo Bluetooth. Para que un dispositivo que usa la función de privacidad se vuelva a conectar con los dispositivos conocidos, la dirección del dispositivo, llamada la *dirección privada*, debe poderse resolver en el otro dispositivo. La dirección privada se genera usando la clave de identidad de resolución del dispositivo que se intercambia durante el proceso de enlace.

Los sistemas iOS 13 o versiones posteriores y iPadOS 13.1 o versiones posteriores tienen la capacidad de derivar claves de enlace entre transportes, una función conocida como *derivación de claves de transporte cruzado*. Por ejemplo, una clave de enlace generada con BLE se puede usar para derivar una clave de enlace para Bluetooth clásico. Además, Apple agregó Bluetooth clásico a la compatibilidad con BLE para los dispositivos que son compatibles con la función de conexiones seguras introducida en Bluetooth Core Specification 4.1 (consulta Bluetooth Core Specification 5.1).

Seguridad de la banda ultraancha en iOS

El nuevo chip U1 diseñado por Apple utiliza la tecnología de banda ultraancha para el reconocimiento del espacio, lo que le permite a los iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max y modelos posteriores de iPhone localizar con precisión otros dispositivos de Apple equipados con U1. La tecnología de banda ultraancha utiliza la misma tecnología para aleatorizar los datos encontrados en otros dispositivos de Apple compatibles:

- Aleatorización de la dirección MAC
- Aleatorización de los números de secuencia de las estructuras de Wi-Fi

Inicio de sesión único

Seguridad del inicio de sesión único

Inicio de sesión único

iOS y iPadOS admiten la autenticación en redes empresariales mediante el inicio de sesión único (SSO). El SSO funciona con redes basadas en Kerberos para autenticar a usuarios en los servicios a los que tienen permitido el acceso. El SSO se puede utilizar para diferentes operaciones de red, desde la navegación segura en Safari hasta el uso de apps de terceros. También admite la autenticación basada en certificados, como PKINIT.

macOS admite la autenticación en las redes empresariales usando Kerberos. Las apps pueden usar Kerberos para autenticar usuarios en los servicios a los que tienen permitido el acceso. Kerberos también se puede usar para diferentes operaciones de red, desde la navegación segura en Safari y la autenticación en sistemas de archivos en red, hasta el uso de apps de terceros. Se admite la autenticación basada en certificados, aunque se requiere que la app adopte una API de desarrollador.

El SSO de iOS, iPadOS y macOS utiliza identificadores SPNEGO y el protocolo HTTP Negotiate para trabajar con puertas de enlace de autenticación basadas en Kerberos y sistemas de autenticación integrada de Windows que admitan vales de Kerberos. La compatibilidad con el SSO se basa en el proyecto de código abierto Heimdal.

Los siguientes tipos de encriptación son compatibles con iOS, iPadOS y macOS:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari admite el SSO, y también se pueden configurar las apps de terceros que utilizan API de conexión a redes de iOS y iPadOS estándar para que lo hagan. Para configurar el SSO, iOS y iPadOS admiten una carga de perfil de configuración que permite a las soluciones de administración de dispositivos móviles (MDM) obtener la configuración necesaria. Aquí se incluye el nombre del principal usuario (es decir, la cuenta de usuario de Active Directory) y la configuración del reino Kerberos, así como la configuración de las apps y direcciones URL web de Safari a las que se debe permitir el uso del SSO.

Para configurar Kerberos en macOS, adquiere tickets con Visor de Tickets, inicia sesión en un dominio de Active Directory de Windows, o usa la herramienta de la línea de comandos `kinit`.

Inicio de sesión extensible

Los desarrolladores de apps pueden brindar sus propias implementaciones de inicio de sesión único usando las extensiones de SSO. Las extensiones de SSO se invocan cuando una app nativa o de Internet necesita usar algún proveedor de identidad para autenticar al usuario. Los desarrolladores pueden brindar dos tipos de extensiones: las que redirigen a HTTPS y las que utilizan un mecanismo de pregunta/respuesta como Kerberos. Esto permite que los esquemas de autenticación de OpenID, OAuth, SAML2 y Kerberos sean compatibles con el inicio de sesión único extensible.

Para usar una extensión de inicio de sesión único, una app puede usar la API AuthenticationServices o puede basarse en el mecanismo de interceptación de URL que ofrece el sistema operativo. WebKit y CFNetwork brindan una capa de interceptación que permite una compatibilidad fluida con el inicio de sesión único para cualquier app nativa o de WebKit. Para invocar una extensión de inicio de sesión único, se debe instalar una configuración proporcionada por un administrador mediante un perfil de administración de dispositivos móviles (MDM). Además de esto, las extensiones de tipo de redirección deben usar la carga útil de los dominios asociados para probar que el servidor de identidad que soportan está al tanto de su existencia.

La única extensión proporcionada con el sistema operativo es la extensión Kerberos SSO.

Seguridad de AirDrop

Los dispositivos Apple compatibles con AirDrop utilizan Bluetooth de baja energía (BLE) y la tecnología Wi-Fi P2P creada por Apple para enviar archivos e información a dispositivos cercanos, incluidos los dispositivos iOS compatibles con AirDrop y dispositivos iPad con iOS 7 o versiones posteriores, y las computadoras Mac con OS X 10.11 o versiones posteriores. El radio de alcance Wi-Fi sirve para la comunicación directa entre dispositivos sin utilizar ningún tipo de conexión a Internet ni punto de acceso (AP) inalámbrico. Esta conexión se encripta con TLS.

La configuración predeterminada de AirDrop para compartir es Sólo contactos. Los usuarios también pueden optar por utilizar AirDrop con la opción de compartir con todos o desactivar la función por completo. Las organizaciones pueden restringir el uso de AirDrop para los dispositivos o apps administradas mediante una solución de administración de dispositivos móviles (MDM).

Operación de AirDrop

AirDrop utiliza servicios de iCloud para ayudar a los usuarios a autenticarse. Cuando un usuario inicia sesión en iCloud, se almacena una identidad RSA de 2048 bits en el dispositivo, y cuando el usuario activa AirDrop, se crea un hash de identidad corta de AirDrop basada en las direcciones de correo electrónico y los números telefónicos asociados con el Apple ID del usuario.

Cuando un usuario elige AirDrop como método para compartir un elemento, el dispositivo emisor emite una señal de AirDrop a través de BLE que incluye el hash de identidad corto de AirDrop del usuario. Otros dispositivos Apple que estén activados, cerca y que tengan activado AirDrop detectan la señal y responden con Wi-Fi P2P para que el dispositivo emisor pueda descubrir la identidad de cualquier dispositivo que responda.

En el modo Sólo contactos, el hash de identidad corto de AirDrop recibido se compara con los hashes de las personas incluidas en la app Contactos del dispositivo receptor. Si se encuentra una coincidencia, el dispositivo receptor responde a través de Wi-Fi P2P con su información de identidad. Si no hay ninguna coincidencia, el dispositivo no responde.

En el modo Todos, se utiliza el mismo proceso general. Sin embargo, el dispositivo receptor responde incluso si no hay concordancia en la app Contactos del dispositivo.

El dispositivo emisor inicia entonces una conexión mediante AirDrop con Wi-Fi P2P con esta conexión para enviar un hash de identidad largo al dispositivo receptor. Si el hash de identidad largo coincide con el hash de una persona conocida en la app Contactos del destinatario, el destinatario responde con sus hashes de identidad largos.

Si los hashes se verifican, el nombre y la foto del destinatario (si se encuentra en Contactos) se muestran en la hoja de compartir de AirDrop del emisor. En iOS y iPadOS, se muestran en la sección Personas o Dispositivos. Los dispositivos que no están verificados o autenticados se muestran en la hoja de compartir de AirDrop con un ícono de silueta y el nombre del dispositivo, como se define en Configuración > General > Información > Nombre. En iOS y iPadOS, se colocan en la sección Otras personas de la hoja de compartir de AirDrop.

El usuario emisor entonces puede seleccionar con quién quiere compartir. Después de la selección del usuario, el dispositivo emisor inicia una conexión encriptada (TLS) con el dispositivo receptor, que intercambia sus certificados de identidad de iCloud. La identidad de los certificados se coteja con la información disponible en la app Contactos de cada usuario.

Si los certificados se verifican, se solicita al usuario receptor que acepte la transferencia entrante del usuario o el dispositivo identificados. Si se eligieron varios destinatarios, este proceso se repite para cada destino.

Seguridad al compartir contraseñas de Wi-Fi en iPhone y iPad

Los dispositivos iOS y iPadOS que permiten compartir contraseñas de Wi-Fi usan un mecanismo similar a AirDrop para enviar una contraseña de Wi-Fi de un dispositivo a otro.

Cuando un usuario selecciona una red Wi-Fi (solicitante) y se le pide que ingrese la contraseña de la red Wi-Fi, el dispositivo Apple inicia una solicitud mediante Bluetooth de baja energía (BLE) para indicar que requiere la contraseña de la red Wi-Fi. Otros dispositivos de Apple que estén activados, cerca y que tengan la contraseña de la red Wi-Fi seleccionada, se conectan al dispositivo solicitante mediante BLE.

El dispositivo que tiene la contraseña de Wi-Fi (otorgante) requiere la información de contacto del solicitante, y el solicitante debe verificar su identidad utilizando un mecanismo similar al de AirDrop. Después de verificar la identidad, el otorgante envía al solicitante el código que sirve para unirse a la red.

Las organizaciones pueden restringir la opción de compartir contraseñas de Wi-Fi en dispositivos o apps administradas mediante una solución de administración de dispositivos móviles (MDM).

Seguridad del firewall en macOS

macOS incluye un firewall integrado para proteger la Mac de ataques de acceso a la red y de denegación de servicio. Se puede configurar desde el panel Seguridad y privacidad de Preferencias del Sistema, y es compatible con la siguiente configuración:

- Bloquear todas las conexiones entrantes, independientemente de la app.
- Permitir automáticamente que el software integrado reciba conexiones entrantes.
- Permitir automáticamente que el software descargado y firmado reciba conexiones entrantes.
- Agregar o denegar el acceso según las apps especificadas por el usuario.
- Evitar que la Mac responda a las solicitudes de sondeo y escaneo de puertos ICMP (protocolo de mensajes de control de Internet).

Seguridad de los kits para desarrolladores

Descripción general de la seguridad de los kits para desarrolladores

Apple proporciona diversas infraestructuras “kit” para permitirles a los desarrolladores externos extender los servicios de Apple. Estas infraestructuras están diseñadas contemplando la privacidad y la seguridad del usuario como su base:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

Seguridad de HomeKit

Seguridad de la comunicación en HomeKit

HomeKit proporciona una infraestructura de automatización doméstica que utiliza la seguridad de iOS, iPadOS, macOS y iCloud para proteger y sincronizar los datos privados, sin exponerlos a Apple.

La identidad y la seguridad de HomeKit se basan en pares de claves pública y privada Ed25519. En el dispositivo iOS, iPadOS y macOS se genera un par de claves Ed25519 para cada usuario de HomeKit, que pasa a ser su identidad de HomeKit. Dicho par se utiliza para autenticar la comunicación entre dispositivos iOS, iPadOS y macOS, y entre accesorios y dispositivos iOS, iPadOS y macOS.

Las claves, almacenadas en el llavero e incluidas sólo en los respaldos encriptados del llavero, se mantienen actualizados entre dispositivos mediante el llavero de iCloud, cuando está disponible. HomePod y Apple TV reciben claves mediante el modo de configuración que requiere tocar para configurar o mediante el modo de configuración que se describe abajo. Las claves se comparten desde un iPhone a un Apple Watch mediante el servicio de identidad (IDS) de Apple.

Comunicación entre accesorios de HomeKit

Los accesorios de HomeKit generan su propio par de claves Ed25519 para la comunicación con dispositivos iOS, iPadOS y macOS. Si el accesorio se restaura con la configuración original de fábrica, se genera un par de claves nuevo.

Para establecer una relación entre un dispositivo iOS, iPadOS o macOS, y un accesorio de HomeKit, las claves se intercambian utilizando el protocolo de contraseña remota segura (3072 bits) y un código de 8 dígitos proporcionado por el fabricante del accesorio, que el usuario ingresa en el dispositivo iOS o iPadOS y que después se encripta con ChaCha20-Poly1305 AEAD mediante claves derivadas de HKDF-SHA512. La certificación MFi del accesorio también se verifica durante la configuración. Los accesorios que no cuentan con un chip MFi pueden integrar soporte para la autenticación del software en iOS 11.3 y versiones posteriores.

Cuando el dispositivo iOS, iPadOS o macOS, y el accesorio de HomeKit se comunican durante el uso, se autentican entre sí mediante las claves intercambiadas en el proceso descrito más arriba. Todas las sesiones se establecen con el protocolo STS y se encriptan con claves derivadas de HKDF-SHA512 basadas en claves Curve25519 por sesión. Esto se aplica tanto a los accesorios basados en IP como a los accesorios Bluetooth de baja energía (BLE).

En el caso de los dispositivos con BLE que son compatibles con las notificaciones de transmisión, el accesorio recibe una clave de encriptación para transmisión de un dispositivo iOS, iPadOS y macOS enlazado a través de una sesión segura. Esta clave se utiliza para encriptar los datos sobre los cambios de estado en el accesorio, los cuales se notifican mediante BLE. La clave de encriptación para transmisión es una clave derivada de HKDF-SHA512, y los datos se encriptan utilizando el algoritmo AEAD con ChaCha20-Poly1305. El dispositivo iOS, iPadOS y macOS modifica de forma periódica la clave de encriptación para transmisión y la actualiza en otros dispositivos utilizando iCloud, como se describe en Seguridad de los datos de HomeKit.

HomeKit y Siri

Siri se puede utilizar para enviar consultas a los accesorios y controlarlos, y para activar ambientaciones. A Siri se le proporciona de forma anónima una cantidad mínima de información sobre la configuración de la casa para proporcionar nombres de habitaciones, accesorios y ambientaciones necesarias para el reconocimiento de comandos. El audio enviado a Siri podría indicar accesorios o comandos específicos; sin embargo, estos datos de Siri no se asocian con otras funciones de Apple, tales como HomeKit.

Accesorios de HomeKit compatibles con Siri

Mediante la app Casa, los usuarios pueden activar nuevas funciones, como Siri, y otras funciones del HomePod, como temporizadores, alarmas, interfono y timbre, en accesorios compatibles con Siri. Cuando estas funciones están activadas, el accesorio se coordina con un HomePod enlazado en la red local que aloja estas funciones de Apple. El audio se intercambia entre los dispositivos a través de canales encriptados usando los protocolos de HomeKit y AirPlay.

Cuando está activada la función Oye Siri, el accesorio escucha la frase “Oye Siri” utilizando un motor de detección de frases de activación que se ejecuta localmente. Si este motor detecta la frase, envía los cuadros de audio directamente a un HomePod enlazado utilizando HomeKit. El HomePod realiza una segunda comprobación del audio y puede cancelar la sesión de audio si la frase no parece contener la frase de activación.

Cuando la función Toca para usar Siri está activada, el usuario puede presionar un botón dedicado en el accesorio para iniciar una conversación con Siri. Los cuadros de audio se envían directamente al HomePod enlazado.

Después de detectar una invocación exitosa de Siri, el HomePod envía el audio a los servidores de Siri y cumple la intención del usuario utilizando las mismas salvaguardas de seguridad, privacidad y encriptación que el HomePod aplica a las invocaciones del usuario hechas directamente al HomePod. Si Siri tiene una respuesta de audio, esta se envía a través de un canal de audio de AirPlay al accesorio. Algunas peticiones de Siri requieren información adicional por parte del usuario (por ejemplo, se le pregunta si quiere escuchar más opciones). En caso afirmativo, el accesorio recibe una indicación de que se debe preguntar al usuario, y el audio adicional se transmite al HomePod.

El accesorio debe tener un indicador visual (por ejemplo, un indicador LED) para indicarle al usuario cuando se está escuchando activamente. El accesorio no tiene conocimiento de la intención de la petición de Siri, salvo el acceso a las transmisiones de audio, y no se almacenan datos del usuario en el accesorio.

Seguridad de los datos de HomeKit

Los datos de HomeKit se pueden actualizar de manera segura entre los dispositivos iOS, iPadOS y macOS de un usuario mediante iCloud y el llavero de iCloud. Durante este proceso, los datos de HomeKit se encriptan usando claves derivadas de la identidad de HomeKit del usuario y un valor único aleatorio, y se maneja como un objeto grande binario opaco, conocido como *blob*. El BLOB más reciente se almacena en iCloud, pero no se utiliza para ningún otro fin. Además, dado que está encriptado con claves que sólo están disponibles en los dispositivos iOS, iPadOS y macOS del usuario, no es posible acceder a su contenido durante la transmisión y el almacenamiento en iCloud.

Los datos de HomeKit también se sincronizan entre varios usuarios de la misma casa. Este proceso utiliza los mismos métodos de autenticación y encriptación que se usan entre un dispositivo iOS, iPadOS y macOS, y un accesorio de HomeKit. La autenticación se basa en las claves públicas Ed25519 que se intercambian entre dispositivos al agregar un usuario a una casa. Después de agregar un usuario nuevo a una casa, todas las comunicaciones futuras se autentican y encriptan con el protocolo STS y claves por sesión.

Sólo el usuario que creó el grupo de casa en HomeKit, u otro usuario que tenga permiso de edición, puede agregar usuarios nuevos. El propietario del dispositivo configura los accesorios con la clave pública del nuevo usuario, de modo que el accesorio pueda autenticar y aceptar los comandos de dicho usuario. Cuando un usuario con permisos de edición agrega un usuario nuevo, el proceso se delega a una central de casa para completar la operación.

HomeKit y Apple TV

El proceso de provisión del Apple TV para su uso con HomeKit se realiza de forma automática cuando el usuario inicia sesión en iCloud. La cuenta de iCloud debe tener activada la autenticación de dos factores. El Apple TV y el dispositivo del usuario intercambian temporalmente claves públicas Ed25519 a través de iCloud. Cuando el dispositivo y el Apple TV del propietario están en la misma red local, se usan claves temporales para asegurar la conexión mediante la red local usando el protocolo de estación a estación (STS) y con claves por sesión. Este proceso utiliza los mismos métodos de autenticación y encriptación que se usan entre un dispositivo iOS, iPadOS y macOS, y un accesorio de HomeKit. Mediante esta conexión local segura, el dispositivo del propietario transfiere el par de claves pública-privada Ed25519 del usuario al Apple TV. Estas claves se usan para asegurar la comunicación entre el Apple TV y los accesorios HomeKit, así como entre el Apple TV y otros dispositivos iOS, iPadOS y macOS que sean parte de la casa de HomeKit.

Si un usuario no tiene varios dispositivos y no les otorga acceso a otros usuarios a su casa, los datos de HomeKit no se transmiten a iCloud.

Datos y apps de Casa

El acceso de las apps a los datos de Casa está controlado por la configuración de privacidad del usuario. Para que las apps tengan acceso a estos datos cuando lo solicitan, los usuarios tienen que concedérselo, igual que en el caso de Contactos, Fotos y otras fuentes de datos de iOS, iPadOS y macOS. Si el usuario lo autoriza, las apps tienen acceso a los nombres de las habitaciones, los nombres de los accesorios y la ubicación de cada accesorio, así como a otra información que se detalla en la documentación para desarrolladores de HomeKit que se puede consultar en https://developer.apple.com/homekit/.

Almacenamiento local de datos

HomeKit almacena datos sobre casas, accesorios, ambientaciones y usuarios en los dispositivos iOS, iPadOS y macOS de un usuario. Estos datos almacenados se encriptan con claves derivadas de las claves de identidad de HomeKit del usuario más un valor único aleatorio. Además, los datos de HomeKit se almacenan con la clase de protección de datos Protegido hasta la primera autenticación de usuario. Los datos de HomeKit se guardan sólo en respaldos encriptados, por lo que, por ejemplo, los respaldos no encriptados que se realizan a través de USB por el Finder (macOS 10.15 o versiones posteriores) o en iTunes (macOS 10.14 o versiones anteriores) no contienen datos de HomeKit.

Protección de routers con HomeKit

Los routers compatibles con HomeKit permiten que los usuarios mejoren la seguridad de la red de su hogar al administrar el acceso de los accesorios HomeKit a la red Wi-Fi en su red local o en Internet. Los routers también admiten la autenticación PSK privada (PPSK), de forma que se pueden agregar accesorios a la red Wi-Fi usando una clave que es específica para el accesorio y que se puede revocar de ser necesario. La autenticación PPSK mejora la seguridad al evitar que se exponga la contraseña principal de la red Wi-Fi a los accesorios, así como al permitir que el router identifique de forma segura un accesorio incluso si se cambia su dirección MAC.

Con la app Casa, un usuario puede configurar restricciones de acceso para grupos de accesorios de la siguiente manera:

- *Sin restricciones:* permite acceso sin restricciones a Internet y a la red local.
- *Automático:* esta es la configuración predeterminada. Permite acceso a Internet y a la red local según una lista de sitios de Internet y puertos locales proporcionada a Apple por el fabricante del accesorio. Esta lista incluye todos los sitios y puertos necesarios para que el accesorio funcione correctamente (se utiliza la configuración Sin restricciones hasta que esta lista esté disponible).
- *Limitar a la casa:* no se permite acceso a Internet o a la red local excepto por las conexiones que HomeKit necesita para descubrir y controlar el accesorio desde la red local (incluyendo desde la central de casa para permitir el control remoto).

Una PPSK es una frase de contraseña WPA2 Personal segura y específica para accesorios que HomeKit genera de forma automática y que se revoca si el accesorio se elimina más tarde de la casa. Se usa una PPSK cuando HomeKit agrega un accesorio a la red Wi-Fi en una casa configurada con un router de HomeKit; y esta adición se muestra como Credencial Wi-Fi: administrado por HomeKit en la pantalla de configuración del accesorio en la app Casa. Los accesorios que se agregaron a la red Wi-Fi antes de agregar el router se vuelven a configurar para usar una PPSK si el accesorio es compatible; de lo contrario; conservan sus credenciales existentes.

Como medida de seguridad adicional, los usuarios deben configurar el router de HomeKit usando la app del fabricante de este, de forma que la app pueda validar que los usuarios tienen acceso al router y que pueden agregarlo a la app Casa.

Seguridad de las cámaras de HomeKit

Las cámaras que tienen una dirección de protocolo de Internet (IP) en HomeKit envían transmisiones de video y audio directamente al dispositivo iOS, iPadOS, tvOS o macOS que está en la red local que accede a la transmisión. Las transmisiones están encriptadas utilizando claves generadas aleatoriamente en el dispositivo y una cámara IP, y se intercambian a través de la sesión segura de HomeKit. Cuando un dispositivo no se encuentra en la red local, las transmisiones encriptadas se retransmiten mediante una central de casa al dispositivo. La central de casa no desencripta las transmisiones, sino que únicamente funciona como retransmisor entre el dispositivo y la cámara IP. Cuando la app muestra al usuario la visualización de video de la cámara IP de HomeKit, HomeKit renderiza los cuadros del video de manera segura desde un proceso de sistema separado. Como resultado, la app no puede acceder o almacenar la transmisión de video. Además, las apps no tienen permitido tomar capturas de pantalla de la transmisión.

Video seguro de HomeKit

HomeKit proporciona un mecanismo privado y seguro de extremo a extremo para grabar, analizar y ver clips de cámaras IP de HomeKit sin exponer dicho contenido de video a Apple o a terceros. Cuando una cámara IP detecta movimiento, se envían los clips de video directamente a un dispositivo Apple que funge como central de casa, usando una conexión de red local dedicada entre la central de casa y la cámara IP. La conexión de red local está encriptada con un par de claves derivadas de HKDF-SHA512 creadas para cada sesión que se negocia durante la sesión de HomeKit entre la central de casa y la cámara IP. HomeKit desencripta las transmisiones de video y audio en la central de casa y analiza los cuadros del video de forma local buscando cualquier evento de importancia. Si se detecta uno, HomeKit encripta el clip de video usando AES-256-GCM con una clave AES256 generada de forma aleatoria. HomeKit también genera cuadros póster para cada clip, los cuales se encriptan usando la misma clave AES256. El cuadro póster encriptado y los datos de audio y video se cargan a los servidores de iCloud. Los datos relacionados de cada clip, incluyendo la clave de encriptación, se cargan a CloudKit usando la encriptación de extremo a extremo de iCloud.

Para la clasificación de caras, HomeKit almacena todos los datos utilizados para clasificar la cara de una persona en particular en CloudKit mediante la encriptación de extremo a extremo de iCloud. Los datos almacenados incluyen información sobre cada persona, como el nombre, así como imágenes que representan la cara de esa persona. Estas imágenes faciales se pueden obtener de la app Fotos del usuario si se otorga acceso, o se pueden recopilar a partir de videos previamente analizados de las cámaras IP. Una sesión de análisis de video seguro de HomeKit utiliza estos datos de clasificación para identificar caras en las transmisiones de video seguro que recibe directamente de la cámara IP e incluye esa información de identificación en los metadatos del clip mencionados anteriormente.

Cuando se usa la app Casa para ver los clips de una cámara, se descargan los datos de iCloud y se desencapsulan las claves necesarias para desencriptar las transmisiones de forma local usando la desencriptación de extremo a extremo de iCloud. El contenido de video encriptado se transmite de los servidores y se desencripta de forma local en el dispositivo iOS antes de mostrarlo en el visor. Cada sesión de clip de video podría dividirse en subsecciones, en donde cada subsección encripta la transmisión de contenido con su propia clave única.

Seguridad de HomeKit con dispositivos Apple TV

HomeKit conecta de forma segura algunos accesorios remotos de terceros al Apple TV y permite al propietario del Apple TV de la casa agregar perfiles de usuario.

Usar accesorios de control remoto de terceros con el Apple TV

Algunos accesorios de control remoto de terceros proporcionan eventos de diseño de interfaz humana (HID) y audio de Siri a un Apple TV asociado mediante la app Casa. El control remoto envía los eventos HID a través de la sesión segura al Apple TV. Un control remoto compatible con Siri puede enviar datos de audio al Apple TV cuando el usuario activa manualmente el micrófono del control remoto utilizando el botón de Siri. El control remoto envía los cuadros de audio directamente al Apple TV mediante una conexión de red local dedicada. La conexión de red local está encriptada con un par de claves derivadas de HKDF-SHA512 creadas para cada sesión que se negocia durante la sesión de HomeKit entre el Apple TV y el control remoto. HomeKit decodifica los cuadros de audio en el Apple TV y los reenvía a la app Siri, donde se emplean las mismas medidas de privacidad que con todas las entradas de audio de Siri.

Perfiles de Apple TV para hogares con HomeKit

Cuando un usuario de un hogar con HomeKit agrega su perfil al Apple TV del propietario del hogar, le da a ese usuario acceso a sus programas de TV, música y podcasts. La configuración de cada usuario en cuanto al uso de su perfil en el Apple TV se comparte a la cuenta de iCloud del propietario, usando encriptación de extremo a extremo. Los datos son propiedad de cada usuario y se comparten como datos de sólo lectura con el propietario. Cada usuario del hogar puede cambiar estos valores en la app Casa, y el Apple TV del propietario utiliza esta configuración.

Cuando se activa una configuración, la cuenta de iTunes del usuario queda disponible en el Apple TV. Cuando se desactiva una configuración, toda la información y datos de la cuenta de ese usuario se eliminan del Apple TV. El dispositivo del usuario inicia la primera compartición mediante CloudKit, y el identificador para establecer la compartición se envía a través del mismo canal seguro que se utiliza para sincronizar los datos entre los usuarios del hogar.

Seguridad de SiriKit para iOS, iPadOS y watchOS

Siri utiliza el sistema de extensiones de apps para comunicarse con apps de terceros. En un dispositivo, Siri puede acceder a la información de contacto del usuario y a la ubicación actual del dispositivo. Sin embargo, antes de brindarle datos protegidos a una app, Siri verifica los permisos de acceso de la app controlados por el usuario. De acuerdo con esos permisos, Siri pasa únicamente el fragmento relevante del enunciado original del usuario a la extensión de la app. Por ejemplo, si una app no tiene acceso a la información sobre los contactos, Siri no podrá identificar la relación en una solicitud como "Págale a mi mamá 100 pesos usando [app de pagos]". En este caso, la app sólo vería el término literal "mi mamá".

Sin embargo, si el usuario le ha dado a la app acceso a la información de sus contactos, la app recibiría información resuelta sobre la mamá del usuario. Si se hizo referencia a una relación en el cuerpo de un mensaje, por ejemplo, "Dile a mi mamá por [app de mensajes] que mi hermano es la onda", Siri no podría identificar "mi hermano" a pesar de los permisos de la app.

Las apps con SiriKit activado pueden enviar vocabulario específico de la app o del usuario a Siri, como los nombres de los contactos del usuario. Esta información le permite al reconocimiento de voz y comprensión del lenguaje natural de Siri reconocer el vocabulario de esa app y se asocia con un identificador aleatorio. La información personalizada permanece disponible mientras que el identificador esté en uso, o hasta que el usuario desactive la integración en Siri desde Configuración, o hasta que se desinstale la app activada con SiriKit.

Para un enunciado como "Pídeme un auto para ir a casa de mi mamá usando [app de viaje compartido]", la petición requiere los datos de ubicación de los contactos del usuario. Para esa petición solamente, Siri brinda la información requerida a la extensión de la app, independientemente de la configuración de los permisos del usuario en cuanto a la ubicación o la información de contactos para la app.

Seguridad de DriverKit para macOS

DriverKit es la infraestructura que les permite a los desarrolladores crear controladores para dispositivos que el usuario instala en su Mac. Los controladores desarrollados con DriverKit se ejecutan en el espacio del usuario en lugar de en las extensiones de kernel, para mejorar la seguridad y la estabilidad del sistema. Esto facilita la instalación y aumenta la estabilidad y seguridad de macOS.

El usuario simplemente descarga la app (no se requieren instaladores al usar extensiones del sistema o DriverKit) y la extensión sólo se activa cuando es necesario. Esto reemplaza a las kexts en muchos casos de uso, lo que requiere privilegios de administrador para instalar en /Sistema/Biblioteca o /Biblioteca.

Se les aconseja a los administradores de TI que utilizan controladores de dispositivos, soluciones de almacenamiento en la nube o redes y apps de seguridad que requieren extensiones de kernel que se muden a versiones nuevas que estén construidas sobre las extensiones del sistema. Estas versiones nuevas reducen en gran medida la posibilidad de problemas en el kernel de la Mac, así como la superficie de ataque. Estas nuevas extensiones se ejecutan en el espacio del usuario, no requieren privilegios especiales obligatorios para la instalación y se eliminan automáticamente cuando la app que las agrupa se traslada al Basurero.

La infraestructura de DriverKit proporciona clases de C++ para los servicios de E/S, concordancia de dispositivos, descriptores de memoria y filas de envío. También define los tipos adecuados de E/S para números, colecciones, cadenas y otros tipos comunes. El usuario los utiliza con infraestructuras de controladores específicos para familias como USBDriverKit y HIDDriverKit. Usa la infraestructura de extensiones del sistema para instalar y actualizar un controlador.

Seguridad de ReplayKit en iOS y iPadOS

ReplayKit es una infraestructura que permite que los desarrolladores agreguen funcionalidades de grabación y transmisión en vivo a sus apps. Además, permite que los usuarios agreguen notas a sus grabaciones y transmisiones en vivo usando la cámara frontal del dispositivo y el micrófono.

Grabación de video

Existen varias capas de seguridad integradas en la grabación de un video:

- *Cuadro de diálogo de permisos:* antes de comenzar la grabación, ReplayKit le presenta al usuario una alerta de consentimiento que le solicita acreditar su intención de grabar con la pantalla, el micrófono y la cámara frontal. El aviso se presenta una vez por cada proceso de app, y se vuelve a presentar si la app se queda en segundo plano por más de 8 minutos.
- *Captura de audio y pantalla:* la captura de audio y pantalla ocurre fuera del proceso de la app en el daemon replayd de ReplayKit. Esto está diseñado para garantizar que el proceso no tenga acceso al contenido grabado.
- *Captura de audio y pantalla dentro de la app:* esto le permite a una app obtener búfers de muestra y video que están protegidos por el cuadro de diálogo de permisos.
- *Creación y almacenamiento de videos:* el archivo de video se escribe en un directorio al que sólo los subsistemas de ReplayKit pueden acceder, mientras que las apps no pueden. Esto ayuda a evitar que terceros usen las grabaciones sin el consentimiento del usuario.
- *Vista previa y uso compartido del usuario final:* el usuario tiene la habilidad de previsualizar y compartir el video con la interfaz de usuario publicada por ReplayKit. La interfaz de usuario se presenta fuera del proceso mediante la infraestructura de extensiones de iOS y tiene acceso al archivo de video generado.

Transmisión de ReplayKit

Existen varias capas de seguridad integradas en la transmisión de un video:

- *Captura de audio y pantalla:* el mecanismo de captura de audio y pantalla durante la transmisión es idéntico al de la grabación de video y ocurre en `replayd`.
- *Extensiones de transmisión:* para que los servicios de terceros participen en la transmisión de ReplayKit, deben crear dos nuevas extensiones configuradas con el punto final com.apple.broadcast-services:
  - Una extensión de interfaz de usuario que permita al usuario configurar su transmisión.
  - Una extensión de carga que maneje la carga de datos de audio y video en los servidores back-end del servicio.

La arquitectura ayuda a garantizar que las apps de alojamiento no tengan privilegios para transmitir el contenido de audio y video. Sólo ReplayKit y las extensiones de transmisión de terceros tienen acceso.

- *Selector de transmisión:* con el selector de transmisión, los usuarios inician las transmisiones del sistema directamente desde una app utilizando la misma interfaz de usuario definida por el sistema y a la que se puede acceder desde el centro de control. La interfaz se implementa utilizando una API privada, y se trata de una extensión que se encuentra dentro de la infraestructura de ReplayKit. No está incluida en el proceso de la app de alojamiento.
- *Extensión de carga:* la extensión que los servicios de transmisión de terceros implementan para manejar contenido de audio y video durante la transmisión utiliza búfers de muestra decodificados y sin procesar. Durante este modo, los datos de audio y video se serializan y se pasan a la extensión de carga del tercero en tiempo real a través de una conexión XPC directa. Los datos de video se codifican extrayendo el objeto IOSurface del búfer de muestra del video, codificándolo de forma segura como un objeto XPC, enviándolo mediante XPC a la extensión del tercero y decodificándolo nuevamente y de forma segura en un objeto IOSurface.

Seguridad de ARKit en iOS y iPadOS

ARKit es una infraestructura que permite a los desarrolladores producir experiencias de realidad aumentada en su app o juego. Los desarrolladores pueden agregar elementos 2D o 3D usando las cámaras frontal o trasera de un dispositivo iOS o iPadOS.

Apple diseñó las cámaras teniendo en cuenta la privacidad, y las apps de terceros deben obtener el consentimiento del usuario antes de acceder a la cámara. En iOS y iPadOS, cuando un usuario otorga a una app permiso para acceder a la cámara, dicha app puede acceder a imágenes en tiempo real desde las cámaras frontal y posterior. Las apps no pueden usar la cámara sin dejar claro que la cámara está en uso.

Las fotos y videos tomados con la cámara pueden contener otra información, como el lugar y el momento en el que se tomaron, la profundidad del campo y la sobrecaptura. Si los usuarios no quieren que las fotos y los videos tomados con la app Cámara incluyan la ubicación, pueden controlar esto en cualquier momento desde Configuración > Privacidad > Localización > Cámara. Si los usuarios no quieren que sus fotos incluyan la ubicación cuando las comparten, pueden desactivar la localización en el menú Opciones de la hoja de compartir.

Para dar una mejor posición a la experiencia de AR del usuario, las apps que usan ARKit pueden usar información de world-tracking o face-tracking de la otra cámara. World Tracking usa algoritmos en el dispositivo del usuario para procesar la información de estos sensores, a fin de determinar su posición en relación a un espacio físico. World Tracking activa funcionalidades como Optical Heading en Mapas.

Administración segura de dispositivos

Descripción general de la administración segura de dispositivos

iOS, iPadOS, macOS, y tvOS permiten políticas de seguridad flexibles y configuraciones que son fáciles de aplicar y administrar. Gracias a estas políticas, las organizaciones pueden proteger su información corporativa y ayudar a garantizar que sus empleados cumplan con los requisitos de la empresa, incluso si utilizan sus propios dispositivos, por ejemplo, como parte de un programa “trae tu propio dispositivo” (BYOD).

Las organizaciones pueden utilizar recursos como la protección mediante contraseña, los perfiles de configuración, el borrado remoto y las soluciones de administración de dispositivos móviles (MDM) de terceros para administrar conjuntos de dispositivos y ayudar a mantener la seguridad de los datos corporativos, incluso cuando los empleados accedan a dichos datos mediante sus propios dispositivos.

En iOS 13 o versiones posteriores, iPadOS 13.1 o versiones posteriores y macOS 10.15 o versiones posteriores, los dispositivos Apple son compatibles con una nueva opción de inscripción de nuevos usuarios, específicamente diseñada para los programas BYOD. La inscripción de usuarios les brinda más autonomía en sus propios dispositivos, a la vez que aumenta la seguridad de los datos empresariales al almacenarlos en un volumen APFS (Apple File System) separado y criptográficamente protegido. Esto brinda un mejor equilibrio entre la seguridad, la privacidad y la experiencia del usuario en los programas BYOD.

Seguridad del modelo de enlace para iPhone y iPad

iOS y iPadOS usan un modelo de enlace para controlar el acceso a un dispositivo desde una computadora host. El enlace establece una relación de confianza entre el dispositivo y el host conectado, representada mediante el intercambio de claves públicas. iOS y iPadOS utilizan esta señal de confianza para activar otras funcionalidades con el host conectado, como la sincronización de datos. En iOS 9 o versiones posteriores:

- Los servicios que requieren enlace no pueden iniciarse hasta que el usuario haya desbloqueado el dispositivo.
- Lo servicios no se iniciarán a menos que el dispositivo se haya desbloqueado recientemente.
- Los servicios podrían requerir que el dispositivo se desbloquee para comenzar (como en la sincronización de fotos).

Para que el proceso de enlace se lleve a cabo, es necesario que el usuario desbloquee el dispositivo y acepte la solicitud de enlace del host. En iOS 9 o versiones posteriores, el usuario también debe ingresar su código, y después de esto el host y el dispositivo intercambian y guardan claves públicas RSA de 2048 bits. Al host se le proporciona una clave de 256 bits que puede desbloquear un repositorio de claves almacenado en el dispositivo. Las claves intercambiadas se utilizan para comenzar una sesión SSL encriptada, que el dispositivo necesita antes de enviar datos protegidos al host o de iniciar un servicio (sincronización con iTunes o el Finder, transferencias de archivos, desarrollo con Xcode, etc.). Para usar esta sesión encriptada para todas las comunicaciones, el dispositivo necesita conexiones de un host vía Wi-Fi, por lo que se debió haber enlazado anteriormente por USB. Además, el enlace también activa varias funciones de diagnóstico. En iOS 9, un registro de enlaces caduca si no se ha utilizado durante más de seis meses. En iOS 11 o versiones posteriores, este tiempo se redujo a 30 días.

Ciertos servicios de diagnóstico, como com.apple.mobile.pcapd, sólo pueden funcionar mediante USB. Además, el servicio com.apple.file_relay requiere la instalación de un perfil de configuración firmado por Apple. En iOS 11 o versiones posteriores, el Apple TV puede usar el protocolo de contraseña remota segura para establecer inalámbricamente una relación de enlazado.

El usuario puede borrar la lista de hosts de confianza con las opciones Restablecer configuración de red o Restablecer localización y privacidad.

Administración de dispositivos móviles

Descripción general de la administración de dispositivos móviles

Los sistemas operativos de Apple son compatibles con la administración de dispositivos móviles (MDM), lo que les permite a las organizaciones configurar y administrar de forma segura las implementaciones de dispositivos escalados de Apple.

Cómo la administración de dispositivos móviles (MDM) funciona de manera segura

Las funciones MDM están integradas en las tecnologías de sistema operativo actuales, tales como los perfiles de configuración, la inscripción OTA y el servicio de notificaciones push de Apple (APNs). Por ejemplo, el APNs se utiliza para activar el dispositivo de manera que pueda comunicarse directamente con la solución MDM a través de una conexión segura. El APNs no permite que se transmita información confidencial ni privada.

Con ayuda de la MDM, los departamentos de TI pueden inscribir dispositivos Apple en un entorno empresarial, configurar los parámetros y actualizarlos mediante una red inalámbrica, supervisar el cumplimiento de políticas corporativas, administrar políticas de actualización de software e incluso borrar o bloquear de forma remota los dispositivos administrados.

Además de las inscripciones tradicionales de dispositivos compatibles con iOS, iPadOS, macOS y tvOS, se agregó un nuevo tipo de inscripción en iOS 13 o versiones posteriores, iPadOS 13.1 o versiones posteriores, y macOS 10.15 o versiones posteriores: la inscripción de usuarios. Las inscripciones de usuarios son inscripciones MDM que se enfocan específicamente en despliegues de “trae tu propio dispositivo” (BYOD), en donde el dispositivo es de propiedad personal, pero se utiliza en un entorno administrado. Las inscripciones de usuarios le otorgan a la solución MDM más privilegios limitados que la inscripción de dispositivos no supervisados, y ofrecen separación criptográfica de los datos corporativos y los del usuario.

Tipos de inscripciones

- *Inscripción automatizada de dispositivos:* la inscripción automatizada de dispositivos les permite a las organizaciones configurar y administrar dispositivos desde el momento en el que los sacan de su empaque (en un proceso conocido como *implementación de avance automático*). A estos dispositivos se les conoce como *supervisados*; y los usuarios tienen la opción de impedir que un usuario elimine el perfil MDM. La inscripción automatizada de dispositivos está diseñada para dispositivos propiedad de la organización.
- *Inscripción de dispositivos:* la inscripción de dispositivos les permite a las organizaciones dejar que los usuarios inscriban dispositivos de forma manual y luego administrar diversos aspectos del uso de estos, incluida la capacidad de borrarlos. La inscripción de dispositivos también tiene un conjunto más amplio de cargas útiles y restricciones que se pueden aplicar a los dispositivos. Cuando un usuario elimina un perfil de inscripción, también se borran todos los perfiles de configuración, sus ajustes y las apps administradas según el perfil de registro.
- *Inscripciones de usuarios:* la inscripción de usuarios está diseñada para dispositivos que son propiedad del usuario, y se integra en el Apple ID administrado para establecer una identidad de usuario en el dispositivo. Los Apple ID administrados son parte del perfil de inscripción de usuario, y el usuario debe autenticarse correctamente para que se complete el proceso de inscripción. Los Apple ID administrados se pueden usar junto con un Apple ID personal con el que el usuario ya ha iniciado sesión. Las apps y cuentas administradas usan un Apple ID administrado, y las apps y cuentas personales usan un Apple ID personal.

Restricciones de dispositivos

Los administradores pueden activar o desactivar restricciones para ayudar a impedir que los usuarios accedan a apps, funciones o servicios específicos de un dispositivo iPhone, iPad, Mac o Apple TV que esté inscrito en una solución de administración de dispositivos móviles (MDM). Las restricciones se envían a los dispositivos en una carga de restricciones, que forma parte de un perfil de configuración. Es posible que algunas restricciones aplicadas a un iPhone se apliquen también a un Apple Watch enlazado.

Administración de la configuración de códigos y contraseñas

De forma predeterminada, el código del usuario se puede definir como un PIN numérico. En dispositivos iOS y iPadOS con Face ID o Touch ID, la extensión mínima del código es de cuatro dígitos. Se recomienda usar códigos largos y complejos, ya que son más difíciles de adivinar o atacar.

Los administradores pueden aplicar requisitos de uso de códigos complejos y otras políticas mediante la MDM o Exchange ActiveSync de Microsoft, o bien pidiendo a los usuarios que instalen perfiles de configuración manualmente. Se necesita una contraseña de administrador para la instalación de la carga útil de la política de códigos para macOS. Algunas políticas de códigos pueden requerir cierta longitud, composición u otros atributos para el código.

Aplicación del perfil de configuración

Los perfiles de configuración son la forma principal en que una solución MDM puede entregar y administrar políticas y restricciones en dispositivos administrados. Si una organización requiere configurar una gran cantidad de dispositivos o proporcionar muchas configuraciones personalizadas de correo electrónico, red o certificados a una gran cantidad de dispositivos, los perfiles de configuración son una forma segura de hacerlo.

Perfiles de configuración

Un *perfil de configuración* es un archivo XML (con extensión .mobileconfig) que contiene cargas útiles que cargan las configuraciones y la información de autorización en dispositivos Apple. Los perfiles de configuración automatizan el establecimiento de configuraciones, cuentas, restricciones y credenciales. Estos archivos se pueden crear con una solución MDM o con Apple Configurator para Mac, o manualmente. Antes de enviar un perfil de configuración a un dispositivo Apple, la organización debe inscribir el dispositivo en la solución MDM mediante un perfil de inscripción.

Perfiles de inscripción

Un *perfil de inscripción* es un perfil de configuración que cuenta con una carga MDM que inscribe el dispositivo en la solución MDM especificada para el dispositivo. Esto permite que la solución MDM envíe comandos y perfiles de configuración al dispositivo, así como consultar ciertos aspectos de este. Cuando un usuario elimina un perfil de inscripción, también se borran todos los perfiles de configuración, sus ajustes y las apps administradas según el perfil de registro. Sólo puede haber un perfil de inscripción en un dispositivo a la vez.

Parámetros del perfil de configuración

Un perfil de configuración contiene varias configuraciones en cargas útiles precisas que se pueden especificar, que incluyen, pero no se limitan a lo siguiente:

- Políticas para códigos y contraseñas
- Restricciones de funcionalidades de los dispositivos (por ejemplo, desactivar la cámara)
- Configuración de red y VPN
- Configuración de Microsoft Exchange
- Configuración de correo electrónico
- Configuración de cuentas
- Configuración del servicio de directorio LDAP
- Configuración del servicio de calendario CalDAV
- Credenciales y claves
- Actualizaciones de software

Firma del perfil y encriptación

Los perfiles de configuración se pueden firmar para validar su origen, y encriptar para ayudar a garantizar su integridad y proteger su contenido. Los perfiles de configuración para iOS y iPadOS se encriptan mediante la sintaxis de mensajes criptográficos (CMS) especificada en RFC 5652, compatible con 3DES y AES128.

Instalación del perfil

Los usuarios pueden instalar perfiles de configuración directamente en sus dispositivos utilizando Apple Configurator para Mac, o bien pueden descargarlos mediante Safari, adjuntarlos a un mensaje de correo, transferirlos mediante AirDrop o la app Archivos en iOS o iPadOS, o descargarlos de forma inalámbrica usando una solución de administración de dispositivos móviles (MDM). Cuando un usuario configura un dispositivo en Apple School Manager o Apple Business Manager, el dispositivo descarga e instala un perfil de inscripción en una solución de MDM. Para obtener información sobre cómo eliminar perfiles, consulta Introducción a la administración de dispositivos móviles en la guía Implementación de las plataformas de Apple.

Nota: en dispositivos supervisados, los perfiles de configuración también se pueden bloquear en un dispositivo, lo que está diseñado para impedir su eliminación o permitirla sólo mediante un código. Dado que muchas organizaciones son dueñas de sus propios dispositivos iOS y iPadOS, se pueden eliminar los perfiles de configuración que vinculan un dispositivo con una solución MDM, pero a la vez se elimina toda la información de configuración administrada, los datos y las apps.

Inscripción automatizada de dispositivos

Las organizaciones pueden inscribir automáticamente dispositivos iOS, iPadOS, macOS y tvOS en la administración de dispositivos móviles (MDM) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban. Después de inscribirse en uno de los servicios, los administradores inician sesión en el sitio web del servicio y enlazan el programa con su solución MDM. A continuación, los dispositivos que hayan comprado se pueden asignar a los usuarios mediante el servidor MDM. Durante el proceso de configuración del dispositivo, se puede incrementar la seguridad de los datos confidenciales al asegurarse de tomar las medidas de seguridad adecuadas. Por ejemplo:

- Hacer que los usuarios se autentiquen como parte del flujo de configuración inicial del dispositivo Apple durante la activación.
- Proporcionar una configuración preliminar con acceso limitado y solicitar configuración adicional en el dispositivo para acceder a datos confidenciales.

Después de asignar el dispositivo a un usuario, todas las configuraciones, restricciones o controles específicos de MDM se instalan automáticamente. Todas las comunicaciones entre los dispositivos y los servidores de Apple se encriptan mediante HTTPS (TLS).

El proceso de configuración se puede simplificar todavía más para los usuarios al eliminar determinados pasos en el Asistente de Configuración de dispositivos, de modo que los usuarios puedan poner sus dispositivos en funcionamiento rápidamente. Los administradores también pueden controlar si los usuarios tienen permitido borrar el perfil MDM del dispositivo, y ayudan a garantizar que las restricciones del dispositivo estén establecidas a lo largo del ciclo de vida de este. Una vez que se ha desempacado y activado el dispositivo, se puede inscribir en la solución MDM de la organización, de manera que se instalen todos los parámetros de administración, apps y libros, según lo definido por el administrador de la MDM.

Apple School Manager, Apple Business Manager, y Apple Business Essentials

Apple School Manager, Apple Business Manager, y Apple Business Essentials son servicios para administradores de TI que permiten implementar los dispositivos Apple que una organización ha adquirido directamente de Apple, o mediante un distribuidor autorizado de Apple o una empresa telefónica participante.

Cuando se usa con una solución MDM, los administradores pueden simplificar el proceso de configuración para los usuarios, ajustar la configuración del dispositivo y distribuir apps y libros comprados en estos tres servicios. Apple School Manager también se integra en los sistemas de información estudiantil (SIS) directamente o mediante SFTP; estos tres servicios pueden usar el sistema para la administración de identidades entre dominios (SCIM) o la autenticación federada con Azure Active Directory de Microsoft (Azure AD) de forma que los administradores puedan crear cuentas rápidamente.

Apple mantiene certificaciones de conformidad con los estándares 27001 y 27018 de ISO/IEC para permitir que los clientes de Apple cumplan con sus obligaciones regulatorias y contractuales. Estas certificaciones brindan a nuestros clientes una afirmación independiente sobre las prácticas de seguridad y privacidad de la información de Apple para sistemas incluidos. Para obtener más información, consulta Certificaciones de seguridad de los servicios en Internet de Apple en la guía Certificaciones de las plataformas de Apple.

Nota: para saber si un programa de Apple está disponible en algún país o región en específico, consulta el artículo de soporte de Apple: Disponibilidad de los programas de Apple y los métodos de pago para el sector educativo y empresarial.

Supervisión de dispositivos

La *supervisión* por lo general indica que el dispositivo es propiedad de la organización, lo que ofrece un control adicional sobre su configuración y restricciones. Para obtener más información, consulta Acerca de la supervisión de dispositivos de Apple en la guía Implementación de las plataformas de Apple.

Seguridad del bloqueo de activación

La forma en la que Apple aplica el bloqueo de activación depende de si el dispositivo es un iPhone o un iPad, una Mac con Apple Chip, o una Mac basada en procesador Intel y que cuenta con el chip de seguridad T2 de Apple.

Comportamiento en iPhone y iPad

En los dispositivos iPhone y iPad, el bloqueo de activación se aplica a través del proceso de activación después de la pantalla de selección de Wi-Fi del asistente de configuración de iOS y iPadOS. Cuando el dispositivo indica que se está activando, envía una solicitud a un servidor de Apple para obtener un certificado de activación. Los dispositivos con bloqueo de activación solicitan al usuario las credenciales de iCloud del usuario que activó el bloqueo de activación en esta ocasión. El asistente de configuración de iOS y iPadOS no avanzará a menos que se pueda obtener un certificado válido.

Comportamiento en una Mac con Apple Chip

En una Mac con Apple Chip, el LLB verifica que exista una política local, LocalPolicy, válida para el dispositivo y que los valores únicos de este coincidan con los valores almacenados en el componente de almacenamiento seguro. LLB arrancará en recoveryOS si se presentan las siguientes condiciones:

- No hay un LocalPolicy para el macOS actual
- El archivo LocalPolicy no es válido para el macOS en cuestión
- El hash de los valores únicos de LocalPolicy no coincide con los hashes de los valores almacenados en el componente de almacenamiento seguro

recoveryOS detecta que la computadora Mac no está activada y contacta al servidor de activación para obtener un certificado de activación. Si el dispositivo tiene activado el bloqueo de activación, recoveryOS solicita al usuario las credenciales de iCloud del usuario que activó el bloqueo en esta ocasión. Una vez que se cuenta con un certificado de activación válido, se utiliza su clave de certificado de activación para obtener un certificado de RemotePolicy. La computadora Mac usa la clave de certificado de LocalPolicy y RemotePolicy para generar un LocalPolicy válido. LLB impedirá que macOS arranque a menos que se cuente con un LocalPolicy válido.

Comportamiento en computadoras Mac basadas en Intel

En una Mac basada en Intel con el chip de seguridad T2 de Apple, el firmware de este chip verifica que haya un certificado de activación válido antes de permitir que la computadora arranque en macOS. El firmware UEFI que carga el chip de seguridad T2 de Apple es responsable de consultar el estado de activación del dispositivo desde el chip T2 y de arrancar en recoveryOS en lugar de macOS en caso de que no haya un certificado de activación válido. recoveryOS detecta que la Mac no está activada y contacta al servidor de activación para obtener un certificado de activación. Si el dispositivo tiene activado el bloqueo de activación, recoveryOS solicita al usuario las credenciales de iCloud del usuario que activó el bloqueo en esta ocasión. El firmware UEFI impedirá que macOS arranque a menos que se cuente con un certificado de activación válido.

Modo perdido administrado y borrado remoto

El modo perdido administrado se utiliza para localizar dispositivos supervisados que han sido robados. Una vez que se localizan, se pueden bloquear o borrar de forma remota.

Modo perdido administrado

Si un dispositivo iOS o iPadOS supervisado con iOS 9 o versiones posteriores se pierde o es objeto de un robo, un administrador de una administración de dispositivos móviles (MDM) puede activar de forma remota el modo perdido (llamado Modo perdido administrado) en ese dispositivo. Cuando se activa el modo perdido administrado, se cierra la sesión del usuario actual y el dispositivo no se puede desbloquear. La pantalla muestra un mensaje que el administrador puede personalizar, así que podría mostrar un número telefónico al que se puede llamar por si alguien encuentra el dispositivo. El administrador también puede solicitar que el dispositivo envíe su ubicación actual (incluso si la función Localización está desactivada) y, opcionalmente, que reproduzca un sonido. Cuando el administrador desactiva el modo perdido administrado (que es la única forma en la que se puede desactivar este modo), se le informa al usuario a través de un mensaje en la pantalla bloqueada o se muestra un aviso en la pantalla de inicio.

Borrado remoto

Un administrador o usuario puede borrar de forma remota los dispositivos iOS, iPadOS y macOS (el borrado remoto instantáneo está disponible únicamente si la Mac tiene FileVault activado). El borrado remoto instantáneo se consigue al descartar de forma segura la clave de contenido de Effaceable Storage, de modo que los datos ya no se pueden leer. En el caso del borrado remoto mediante Exchange ActiveSync de Microsoft, el dispositivo se registra en Microsoft Exchange Server antes de realizar el borrado.

Cuando la MDM o iCloud activan un comando de borrado remoto, el dispositivo iPhone, iPad, iPod touch o Mac regresa una confirmación a la solución MDM y realiza el borrado.

El borrado remoto no es posible en las siguientes situaciones:

- Con el uso de la inscripción de usuarios.
- Cuando se utiliza Exchange ActiveSync de Microsoft en una cuenta instalada con la inscripción de usuarios.
- Con el uso de Exchange ActiveSync de Microsoft si el dispositivo se supervisa.

Los usuarios también pueden borrar el contenido de sus dispositivos iOS y iPadOS mediante la app Configuración. Por último, como se ha mencionado anteriormente, los dispositivos iOS y iPadOS se pueden configurar para que se realice un borrado automático del contenido después de una serie de intentos fallidos de ingresar el código.

Seguridad de iPad compartido en iPadOS

iPad compartido es un modo multiusuario que se puede usar en implementaciones del iPad. Permite a los usuarios compartir un iPad mientras mantiene los documentos y datos de cada usuario separados. Cada usuario recibe su propia ubicación de almacenamiento reservada y privada, que se implementa como un volumen APFS (Apple File System) protegido por las credenciales del usuario. La función iPad compartido requiere el uso de un Apple ID administrado, el cual es generado por y pertenece a la organización.

Con iPad compartido, un usuario puede iniciar sesión en cualquier dispositivo propiedad de la organización que esté configurado para ser utilizado por varios usuarios. Los datos de los usuarios se dividen en particiones en directorios separados, cada uno en su propio dominio de protección de datos y protegido por permisos UNIX y aislamiento. En iPadOS 13.4 o versiones posteriores, los usuarios también pueden iniciar una sesión temporal. Cuando el usuario cierra una sesión temporal, su volumen APFS se elimina y se devuelve su espacio reservado al sistema.

Iniciar sesión en un iPad compartido

Para iniciar sesión en un iPad compartido es posible usar Apple ID administrados tanto nativos como federados. Al usar una cuenta federada por primera vez, el usuario se redirige al portal de inicio de sesión del proveedor de identidad (IdP). Después de autentificarse, se emite un identificador de acceso de corta duración para los Apple ID administrados de respaldo, y el proceso de inicio de sesión sigue de forma similar al proceso nativo de los Apple ID administrados. Una vez que se haya iniciado sesión, el asistente de configuración del iPad compartido le pide al usuario que establezca un código (credencial) para asegurar los datos locales en el dispositivo, y para autenticarse en la pantalla de inicio de sesión en el futuro. Al igual que en un dispositivo de un solo usuario, en donde el usuario iniciaría sesión una vez en su Apple ID administrado usando su cuenta federada y luego desbloquearía el dispositivo con su código, en un iPad compartido, el usuario inicia sesión una vez usando su cuenta federada y desde ese momento utiliza su código establecido.

Cuando un usuario inicia sesión sin una autenticación federada, el Apple ID administrado se autentica con el servicio de identidad (IDS) de Apple usando el protocolo SRP. Si la autenticación se realiza correctamente, se concede un identificador de corta duración al dispositivo. Si el usuario ha usado el dispositivo anteriormente, entonces ya existe una cuenta de usuario local que se puede desbloquear utilizando las mismas credenciales.

Si el usuario no ha usado el dispositivo antes o está usando una sesión temporal, el iPad compartido proporciona un nuevo ID de usuario UNIX, un volumen APFS para almacenar los datos personales del usuario y un llavero local. Debido a que el almacenamiento está asignado (reservado) para el usuario en el momento en que se crea el volumen APFS, puede que no haya espacio suficiente para crear un volumen nuevo. En tal caso, el sistema identifica a un usuario existente cuyos datos hayan terminado de sincronizarse con la nube y lo retira del dispositivo para permitir que un usuario nuevo inicie sesión. En el improbable caso de que no se hayan terminado de cargar a la nube los datos de ninguno de los usuarios existentes, el inicio de sesión del usuario nuevo fallará. Para iniciar sesión, el usuario nuevo deberá esperar a que se terminen de sincronizar los datos de uno de los usuarios, o deberá solicitarle a un administrador que elimine a la fuerza una cuenta de usuario existente, lo que conlleva un riesgo de pérdida de datos.

Si el dispositivo no está conectado a Internet (por ejemplo, si el usuario no tiene un punto de acceso Wi-Fi), la autenticación se puede llevar a cabo utilizando la cuenta local durante una cantidad limitada de días. En tal caso, sólo podrán iniciar sesión los usuarios que cuenten con una cuenta local o que utilicen una sesión temporal. Una vez que se agotó el tiempo límite, se requerirá que los usuarios se autentiquen en línea, incluso si ya existe una cuenta local.

Después de que la cuenta local del usuario haya sido creada o desbloqueada, y autenticada de forma remota, el identificador de corta duración concedido por los servidores de Apple se convierte en un identificador de iCloud que permite iniciar sesión en iCloud. Después, se restaura la configuración del usuario y se sincronizan sus datos y documentos de iCloud.

Mientras la sesión del usuario esté activa y el dispositivo permanezca en línea, los documentos y datos se almacenan en iCloud a medida que se creen o modifiquen. Además, un mecanismo de sincronización en segundo plano ayuda a garantizar que los cambios se envíen a iCloud o a otros servicios web usando sesiones en segundo plano de NSURLSession después de que se cierre la sesión del usuario. Una vez que se completa la sincronización en segundo plano de ese usuario, se desmonta el volumen APFS de este y no se podrá volver a montar a menos que el usuario vuelva a iniciar sesión.

Las sesiones temporales no sincronizan datos con iCloud, y aunque una sesión temporal pueda iniciar sesión en un servicio de sincronización de terceros, como Box o Google Drive, no existe la posibilidad de continuar sincronizando datos cuando finaliza la sesión temporal.

Cerrar sesión en un iPad compartido

Cuando un usuario cierra sesión en un iPad compartido, el repositorio de claves del usuario se bloquea inmediatamente y se cierran todas las apps. Para acelerar el inicio de sesión de un nuevo usuario, iPadOS aplaza temporalmente algunas acciones de cierre de sesión comunes y presenta una ventana de inicio de sesión al nuevo usuario. Si un usuario inicia sesión durante este tiempo (aproximadamente 30 segundos), el iPad compartido realiza la limpieza aplazada como parte del inicio de sesión en la cuenta del nuevo usuario. Sin embargo, si el iPad compartido permanece inactivo, se activa la limpieza aplazada. Durante la fase de limpieza, la ventana de inicio de sesión se reinicia como si hubiera ocurrido otro cierre de sesión.

Cuando finaliza una sesión temporal, iPad compartido realiza la secuencia completa de cierre de sesión y elimina el volumen APFS de la sesión temporal de forma inmediata.

Seguridad de Apple Configurator

Apple Configurator para Mac tiene un diseño flexible, seguro y centrado en el dispositivo que permite que el administrador configure de forma rápida y sencilla uno o docenas de dispositivos iOS, iPadOS y tvOS conectados a una Mac mediante USB (o dispositivos tvOS enlazados mediante Bonjour) antes de dárselos a los usuarios. Con Apple Configurator para Mac, un administrador puede actualizar software, instalar apps y perfiles de configuración, renombrar y cambiar el fondo de pantalla de los dispositivos, exportar la información y los documentos del dispositivo, y mucho más.

Apple Configurator para Mac también puede revivir o restaurar las computadoras Mac con Apple Chip y las computadoras Mac con el chip de seguridad T2 de Apple. Cuando se reactiva o restaura una Mac de esta manera, el archivo que contiene las más recientes actualizaciones complementarias de los sistemas operativos (macOS, recoveryOS en el caso de Apple Chip, o sepOS en el caso del chip T2) se descarga de forma segura desde los servidores de Apple y se instala directamente en la Mac. Después de una reactivación o restauración satisfactoria, el archivo se elimina de la Mac con Apple Configurator. En ningún momento el usuario puede inspeccionar o usar este archivo fuera de Apple Configurator.

Los administradores también pueden optar por agregar dispositivos a Apple School Manager, Apple Business Manager o Apple Business Essentials usando Apple Configurator para Mac o Apple Configurator para iPhone, incluso si los dispositivos no se adquirieron directamente con Apple, un distribuidor autorizado de Apple, o una empresa telefónica participante. Cuando el administrador configura un dispositivo que se inscribió manualmente, se comporta como cualquier otro dispositivo en uno de esos servicios, con supervisión obligatoria e inscripción en la administración de dispositivos móviles (MDM). En el caso de los dispositivos que no se adquirieron directamente, el usuario tiene un periodo provisional de 30 días para dar de baja al dispositivo de uno de esos servicios, de la supervisión y de la MDM.

Las organizaciones también pueden usar Apple Configurator para Mac con el fin de activar dispositivos iOS, iPadOS y tvOS que no tengan conexión a Internet, para ello, deben conectarlos a una Mac anfitriona con conexión a Internet mientras se realiza la configuración de los dispositivos. Los administradores pueden restaurar, activar y preparar dispositivos con la configuración necesaria, incluidas apps, perfiles y documentos, sin tener que conectarse a redes Wi-Fi o celulares. Esta función no permite que un administrador omita los requisitos existentes del bloqueo de activación que normalmente se requieren durante la activación con conexión a Internet.

Seguridad de Tiempo en pantalla

Tiempo en pantalla es una función integrada que permite consultar y administrar el tiempo que los adultos y sus menores pasan en apps, sitios web y más. Hay dos tipos de usuarios: adultos y menores (administrados).

Aunque Tiempo en pantalla no es una función nueva de seguridad del sistema, es importante entender cómo protege la privacidad y la seguridad de los datos recopilados y compartidos entre los dispositivos. Tiempo en pantalla está disponible en iOS 12 o versiones posteriores, iPadOS 13.1 o versiones posteriores, macOS 10.15 o versiones posteriores, y algunas funciones están disponibles en watchOS 6 o versiones posteriores.

La tabla de abajo describe las funciones principales de Tiempo en pantalla.

Funcionalidad	Sistema operativo compatible
Ver datos de uso	iOS iPadOS macOS
Imponer restricciones adicionales	iOS iPadOS macOS watchOS
Configurar límites de uso de Internet	iOS iPadOS macOS
Configurar límites en las apps	iOS iPadOS macOS watchOS
Configurar tiempos desactivados	iOS iPadOS macOS watchOS

Para los usuarios que administran su propio dispositivo, los datos de uso y los controles de Tiempo en pantalla se pueden sincronizar con los dispositivos asociados con la misma cuenta de iCloud utilizando la encriptación de extremo de CloudKit. La cuenta del usuario debe tener la autenticación de dos factores activada (la sincronización está activada de forma predeterminada). Tiempo en pantalla reemplaza la función Restricciones incluida en versiones anteriores de iOS y iPadOS, así como la función Controles parentales incluida en versiones anteriores de macOS.

En iOS 13 o versiones posteriores, iPadOS 13.1 o versiones posteriores, y macOS 10.15 o versiones posteriores, los usuarios y los menores administrados en Tiempo en pantalla comparten automáticamente su uso a través de varios dispositivos si su cuenta de iCloud tiene activada la autenticación de dos factores. Cuando un usuario borra el historial de Safari o elimina una app, se eliminan los datos de uso correspondientes de ese dispositivo y de todos los dispositivos sincronizados.

Padres y Tiempo en pantalla

Los padres también pueden usar Tiempo en pantalla en sus dispositivos iOS, iPadOS y macOS para entender y controlar el uso que sus hijos hacen de los dispositivos. Si el padre es el organizador de la familia, (en Compartir en familia de iCloud), podrá ver los datos de uso y administrar la configuración de Tiempo en pantalla de sus hijos. Los hijos reciben una notificación cuando los padres activan Tiempo en pantalla y, además, ellos también pueden revisar sus propios datos de uso. Cuando los padres activan Tiempo en pantalla para sus hijos, deben ingresar un código para evitar que sus hijos modifiquen la configuración. Cuando cumplen la mayoría de edad (lo que depende del país o región), los hijos pueden desactivar esta función de monitoreo.

Los datos de uso y la configuración establecida se transfieren entre los dispositivos de los padres y los hijos utilizando un protocolo de servicio de identidad (IDS) de Apple que está encriptado de extremo a extremo. Los datos encriptados pueden permanecer en servidores IDS hasta que el dispositivo receptor esté disponible (por ejemplo, hasta que se encienda un iPhone, iPad, o iPod touch, si estaba apagado). Apple no puede leer estos datos.

Análisis de Tiempo en pantalla

Si el usuario activa Compartir análisis (iPhone y Watch), se recopilarán únicamente datos anónimos para que Apple pueda entender mejor cómo se usa Tiempo en pantalla, por ejemplo:

- Si Tiempo en pantalla se activó durante el Asistente de Configuración o se activó posteriormente en Configuración.
- Si hubo un cambio en el uso de una categoría después de crearle un límite (dentro de 90 días).
- Si Tiempo en pantalla está activado.
- Si Tiempo desactivado está activado.
- El número de veces que se solicitó más tiempo.
- El número de límites para apps.
- El número de veces que los usuarios vieron el uso en la configuración de Tiempo en pantalla, por tipo de usuario y por tipo de visualización (local, remota, widget).
- El número de veces que los usuarios ignoraron un límite, por tipo de usuario.
- El número de veces que los usuarios eliminaron un límite, por tipo de usuario.

Apple no recopila datos de uso de una app o página web específicos. Cuando un usuario ve una lista de apps en los datos de uso de Tiempo en pantalla, los íconos de las apps se obtienen directamente de App Store, la cual no conserva ningún tipo de información de estas solicitudes.

Glosario

Acceso directo a la memoria (DMA) Función que permite a los subsistemas de hardware acceder a la memoria principal directamente, sin pasar por el CPU.

administración de dispositivos móviles (MDM) Un servicio que permite a un administrador gestionar de forma remota los dispositivos inscritos. Una vez que se inscribe un dispositivo, el administrador puede usar el servicio de MDM a través de la red para configurarlo y realizar otras tareas sin la interacción del usuario.

AES (estándar de encriptación avanzado) Un estándar de encriptación global popular utilizado para encriptar datos con el fin de mantenerlos privados.

AES-XTS Un modo de AES definido en el IEEE 1619-2007 diseñado para encriptar los medios de almacenamiento.

Aleatorización del espacio de direcciones (ASLR) Técnica que emplean los sistemas operativos para que sea mucho más complicado conseguir aprovecharse de una vulnerabilidad de seguridad en el software. Al garantizar la impredecibilidad de las direcciones y los desplazamientos de la memoria, el código de ataque no puede incrustar esos valores en el código fuente.

Algoritmo de firma digital de curva elíptica (ECDSA) Algoritmo de firmas digitales basado en criptografía que emplea curvas elípticas.

APFS (Apple File System) El sistema de archivos predeterminado en dispositivos iOS, iPadOS, tvOS y watchOS, así como en computadoras Mac con macOS 10.13 o versiones posteriores. APFS cuenta con una encriptación robusta, uso compartido del espacio, instantáneas, dimensionamiento rápido del directorio y fundamentos del sistema de archivos mejorados.

Apple Business Manager Forma rápida y optimizada de implementar dispositivos Apple que una organización haya comprado directamente de Apple o de un distribuidor o proveedor autorizado de Apple participante. Las organizaciones pueden inscribir automáticamente dispositivos en la administración de dispositivos móviles (MDM) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban.

Apple School Manager Forma rápida y optimizada de implementar dispositivos Apple que una organización haya comprado directamente de Apple o de un distribuidor o proveedor autorizado de Apple participante. Las organizaciones pueden inscribir automáticamente dispositivos en la administración de dispositivos móviles (MDM) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban.

autorización del software del sistema Un proceso que combina las claves criptográficas integradas en el hardware con un servicio en línea para revisar que sólo se proporcione e instale el software legítimo de Apple, adecuado para los dispositivos compatibles, en el momento de la actualización.

bits semilla del software Bits dedicados en el motor AES del Secure Enclave que se agregan al inicio del UID cuando se generan claves del UID. Cada bit semilla del software tiene un bit de bloqueo correspondiente. El sistema operativo y la ROM de arranque del Secure Enclave pueden cambiar independientemente el valor de cada bit semilla del software si aún no se ha establecido el bit de bloqueo correspondiente. Una vez que se ha establecido el bit de bloqueo, no es posible modificar el bit semilla del software o el bit de bloqueo. Los bits semilla del software y sus bloqueos se restablecen cuando Secure Enclave se reinicia.

Boot Camp Utilidad de macOS que permite la instalación de Microsoft Windows en computadoras Mac compatibles.

Bóveda de datos Un mecanismo, impuesto por el kernel, que protege contra el acceso no autorizado a los datos independientemente de si la app que solicita el acceso está en la zona protegida.

circuito integrado (IC) También conocido como *microchip*.

CKRecord Diccionario de pares de clave-valor que contiene datos guardados en CloudKit u obtenidos desde el mismo.

clave de contenido Parte de la jerarquía de la clave de encriptación que ayuda a proporcionar un borrado seguro e instantáneo. En iOS, iPadOS, tvOS y watchOS, la clave de contenido encapsula los metadatos en el volumen de datos (y sin ella, el acceso a todas las claves por archivo es imposible, por lo que no se puede acceder a los archivos protegidos por Protección de datos). En macOS, la clave de contenido encapsula el material de las claves, todos los metadatos y los datos en el volumen protegido por FileVault. En cualquiera de los dos casos, borrar la clave de contenido hace que los datos encriptados sean inaccesibles.

clave del sistema de archivos Clave que encripta los metadatos de cada archivo, incluida la clave de clase correspondiente. Se guarda en la función Effaceable Storage para facilitar el borrado rápido, en lugar de la confidencialidad.

Clave derivada del código (PDK) La clave de encriptado derivada del entrelazamiento de la contraseña del usuario con la clave SKP de largo plazo y el UID del Secure Enclave.

clave por archivo La clave utilizada por la protección de datos para encriptar un archivo en el sistema de archivos. La clave por archivo se encapsula mediante una clave de clase y se almacena en los metadatos del archivo.

Componente de almacenamiento seguro Un chip diseñado con un código de ROM inmutable, un hardware generador de números aleatorios, motores de criptografía y detección de manipulación física. En los dispositivos compatibles, el Secure Enclave se enlaza con un componente de almacenamiento seguro para el almacenamiento del valor único antirreproducciones. Para leer y actualizar los valores únicos, el Secure Enclave y el chip de almacenamiento utilizan un protocolo de protección que ayuda a garantizar el acceso exclusivo a los valores únicos. Hay varias generaciones de esta tecnología con diferentes garantías de seguridad.

controlador de memoria El subsistema en el sistema en chip que controla la interfaz entre el sistema en chip y su memoria principal.

Controlador SSD Subsistema de hardware que administra los medios de almacenamiento (unidad de estado sólido).

correspondencia de ángulos del patrón de arrugas Representación matemática de la dirección y el ancho de las arrugas extraída de una porción de una huella digital.

Effaceable Storage Área del almacenamiento NAND dedicada, utilizada para almacenar claves criptográficas, que se puede identificar directamente y borrar de forma segura. Aunque no ofrezca protección si un atacante dispone del dispositivo físicamente, las claves almacenadas en la función Effaceable Storage se pueden usar como parte de una jerarquía de claves para facilitar el borrado rápido y la consiguiente seguridad.

encapsulación de claves Encriptación de una clave con otra clave. iOS y iPadOS utilizan la encapsulación de claves AES del Instituto Nacional de Estándares y Tecnología (NIST), de acuerdo con la publicación RFC 3394.

Firmware de la interfaz del firmware extensible unificado (UEFi) Tecnología que reemplaza el BIOS para conectar el firmware al sistema operativo de una computadora.

Gatekeeper En macOS, tecnología diseñada para ayudar a garantizar que sólo se ejecute software de confianza en la Mac de un usuario.

Gestor de arranque de bajo nivel (LLB) En las computadoras Mac con arquitectura de arranque de dos fases, LLB contiene el código al que invoca la ROM de arranque y que, a su vez, carga iBoot como parte de la cadena de arranque seguro.

Grupo de acción de pruebas conjuntas (JTAG) Herramienta estándar de depuración de hardware que usan programadores y desarrolladores de circuitos.

HMAC Un código de autentificación de mensajes en clave-hash basado en una función criptográfica hash.

iBoot Gestor de arranque de dos niveles de todos los dispositivos Apple. Código que carga XNU como parte de la cadena de arranque seguro. Dependiendo de la generación del sistema en chip (SoC), el gestor de arranque de bajo nivel puede cargar iBoot, o puede hacerlo la ROM de arranque directamente.

ID de grupo (GID) Como el UID, pero común para todos los procesadores de una clase.

Identificador de chip exclusivo (ECID) Identificador de 64 bits único en el procesador de cada dispositivo iOS y iPadOS. Cuando se responde una llamada en un dispositivo, se detiene el tono de llamada en los dispositivos enlazados con iCloud que estén cerca con un aviso mediante Bluetooth de baja energía (BLE) 4.0. Los bytes de aviso se encriptan usando el mismo método que los avisos de Handoff. Se usa como parte del proceso de personalización y no se considera un secreto.

Identificador de recursos uniforme (URI) Cadena de caracteres que identifica un recurso basado en la web.

identificador único (UID) Clave AES de 256 bits que se graba en cada procesador durante el proceso de fabricación. Ni el firmware ni el software la pueden leer y solamente la usa el motor AES del hardware del procesador. Para obtener la clave real, un atacante tendría que crear un ataque físico muy sofisticado y caro contra el silicio del procesador. El UID no está relacionado con ningún otro identificador del dispositivo como, por ejemplo, el UDID.

Intercambio de claves efímeras con Diffie-Hellman de curva elíptica (ECDHE) Mecanismo de intercambios de claves basado en curvas elípticas. ECDHE permite que dos partes establezcan una clave secreta, esto previene que un tercero no autorizado obtenga la clave al ver los mensajes entre las dos partes.

Interfaz periférica serie mejorada (eSPI) Bus todo en uno diseñado para la comunicación en serie síncrona.

llavero La infraestructura y un conjunto de API usadas por los sistemas operativos de Apple y por apps de terceros para almacenar y recuperar contraseñas, claves y otras credenciales confidenciales.

Modo de actualización del firmware del dispositivo (DFU) Modo en el que el código de la memoria ROM de arranque de un dispositivo espera su recuperación mediante USB. Al estar en este modo, la pantalla se muestra en negro. Sin embargo, al conectarse a una computadora en la que se ejecuta iTunes o el Finder, se muestra el siguiente mensaje: "iTunes (o el Finder) detectó un (iPad, iPhone, o iPod touch) en modo de recuperación. El usuario debe restaurar este (iPhone, iPad iPod touch) para poder usarlo con iTunes (o el Finder)".

Modo de recuperación Un modo que se usa para restaurar muchos dispositivos Apple si no se reconoce el dispositivo del usuario para que se pueda reinstalar el sistema operativo.

módulo de seguridad de hardware (HSM) Computadora especializada en seguridad a prueba de manipulaciones que protege y administra claves digitales.

Motor criptográfico de AES Componente de hardware dedicado que implementa el AES.

NAND Memoria flash no volátil.

perfil de datos Archivo de lista de propiedades (archivo .plist) firmado por Apple que contiene una serie de entidades y autorizaciones que permiten instalar y probar apps en un dispositivo iOS o iPadOS. Un perfil de datos de desarrollo contiene una lista de dispositivos seleccionados por un desarrollador para realizar una distribución a medida, y un perfil de datos de distribución contiene el ID de app de una app desarrollada por una empresa.

Protección de claves selladas (SKP) Una tecnología de la protección de datos que protege, o *sella*, las claves de encriptado con medidas de software del sistema y claves disponibles solamente en el hardware (como el UID del Secure Enclave).

Protección de datos Mecanismo de protección de archivos y del llavero para dispositivos Apple compatibles. También puede referirse a las API que utilizan las apps para proteger los archivos y los elementos del llavero.

Protección de la integridad del coprocesador del sistema (SCIP) Un mecanismo utilizado por Apple que está diseñado para prevenir la modificación del firmware del coprocesador.

Recompensas de seguridad de Apple Recompensa que brinda Apple a los investigadores que reportan vulnerabilidades que afectan a los sistemas operativos más recientes y, cuando es relevante, al hardware más reciente.

Registro del proceso de arranque (BPR) Un conjunto de indicadores de hardware de sistemas en chip (SoC) que indica el software que puede usarse para monitorear los modos de arranque a los que ha entrado el dispositivo, tales como el modo de actualización del firmware del dispositivo (DFU) y el modo de recuperación. Una vez que se establece un indicador en el BPR, no se puede borrar. Esto permite que un software posterior obtenga un indicador confiable del estado del sistema.

repositorios de claves Estructura de datos que se utiliza para almacenar un conjunto de claves de clase. Cada tipo (usuario, dispositivo, sistema, respaldo, custodia o respaldo de iCloud) tiene el mismo formato:

Un encabezado que contiene: la versión (establecido a cuatro en iOS 12 o versiones posteriores), el tipo (sistema, respaldo, custodia o respaldo de iCloud), el UUID del repositorio de claves, una HMAC si el repositorio de claves está firmado, y el método para encapsular las claves de clase, vinculado a la UID o PBKDF2, junto con el valor de sal aleatorio y el conteo de iteraciones.

Una lista de claves de clase: el UUID de la clave, la clase (qué clase de protección de datos de llavero o archivo), el tipo de encapsulación (sólo clave derivada de la UID, o clave derivada de la UID y clave derivada del código), la clave de clase encapsulada y una clave pública para clases asimétricas.

ROM de arranque El primer código que ejecuta el procesador de un dispositivo al arrancar por primera vez. Como parte integral del procesador, ni Apple ni ningún atacante lo puede alterar.

sepOS El firmware del Secure Enclave basado en una versión personalizada de Apple del microkernel L4.

Servicio de identidad (IDS) de Apple Directorio de Apple de claves públicas de iMessage, direcciones de APN, números de teléfono y direcciones de correo electrónico que se usan para buscar las claves y las direcciones de los dispositivos.

Servicio de notificaciones push de Apple (APNs) Servicio ofrecido por Apple a nivel mundial que envía notificaciones push a los dispositivos Apple.

sistema en chip (SoC) Circuito integrado (IC) que incorpora varios componentes en un único chip. El procesador de aplicaciones, el Secure Enclave y otros coprocesadores son componentes del SoC.

Unidad de administración de memoria de entrada/salida (IOMMU) Una unidad de administración de memoria de entrada/salida. Un subsistema en un chip integrado que controla el acceso al espacio de direcciones desde otros dispositivos y periféricos de entrada/salida.

valor único Número único e irrepetible utilizado en varios protocolos de seguridad.

vinculación Proceso mediante el cual el código de un usuario se convierte en una clave encriptada y se fortalece con el UID del dispositivo. Este proceso ayuda a garantizar que un ataque de fuerza bruta deba realizarse en un dispositivo determinado y, por lo tanto, que la velocidad esté limitada y que el ataque no se pueda realizar en paralelo. El algoritmo de vinculación es PBKDF2, que usa AES encriptado con el UID del dispositivo como la función pseudoaleatoria (PRF) para cada iteración.

xART Abreviatura de la tecnología antirreproducciones eXtended. Conjunto de servicios que proporcionan almacenamiento persistente encriptado y autenticado para el Secure Enclave con funcionalidades antirreproducción basadas en la arquitectura del almacenamiento físico. Consulta Componente de almacenamiento seguro.

XNU Kernel ubicado en el corazón de los sistemas operativos de Apple. Se presupone que es de confianza, y refuerza las medidas de seguridad tales como la firma de código, el aislamiento en zona protegida, la comprobación de las autorizaciones y la aleatorización del espacio de direcciones (ASLR).

XProtect En macOS, tecnología antivirus que utiliza firmas para la detección y eliminación de malware.

Historial de revisión del documento

Historial de revisión del documento

Fecha	Resumen
Diciembre de 2022	Temas agregados: • Protección de datos avazada para iCloud Temas actualizados: • Descripción general de la seguridad de iCloud • Encriptación en iCloud • Seguridad del respaldo en iCloud • Seguridad de Contactos de recuperación de cuenta • Seguridad de Contactos para legado

Fecha	Resumen
Mayo de 2022	Actualizado para: • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 Temas agregados: • Restricciones de recoveryOS vinculado • Versión del sistema operativo local (love) • Compartir datos de Salud • Seguridad de Contactos de recuperación de cuenta • Seguridad de Contactos para legado • Seguridad de Tap to Pay on iPhone • Acceder mediante Apple Wallet • Tipos de credenciales de acceso • Identificaciones en Apple Wallet • Accesorios de HomeKit compatibles con Siri Temas actualizados: • Magic Keyboard con Touch ID • Face ID, Touch ID, códigos y contraseñas • Seguridad de la coincidencia facial • Tarjetas express con reserva de energía • Modos de arranque en una Mac con Apple Chip • Contenidos del archivo LocalPolicy en computadoras Mac con Apple Chip • Seguridad del volumen del sistema firmado en iOS, iPadOS y macOS • Seguridad del sistema en watchOS • Dispositivo de investigación de seguridad de Apple • El papel de Apple File System • Protección del acceso de las apps a los datos de usuario • Introducción a la seguridad de las apps en macOS • Protección contra el malware en macOS • Descripción general de la seguridad de iCloud • Sincronización segura del llavero • Seguridad de la recuperación del llavero de iCloud • Pagos con tarjeta mediante Apple Pay • Pases sin contacto en Apple Pay • Inhabilitar las tarjetas con Apple Pay • Solicitud de Apple Card • Seguridad de Apple Cash • Agregar tarjetas de transporte público y de monedero electrónico a Apple Wallet • Seguridad de Apple Messages for Business • Seguridad de FaceTime • Seguridad de la función Llave de auto en iOS • Seguridad de Apple Configurator Temas eliminados: • Accesorios de HomeKit y iCloud

Fecha	Resumen
Mayo de 2021	Actualizado para: • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 Temas agregados: • Magic Keyboard con Touch ID. • Intención segura y conexiones con el Secure Enclave. • Desbloqueo automático con Apple Watch. • Hash del manifiesto de Image4 de CustomOS (coih). Temas editados: • Se agregó información sobre dos nuevas transacciones del modo express en Tarjetas express con reserva de energía. • Se editó la sección Resumen de funciones del Secure Enclave. • Se agregó contenido de la actualización del software a Arranque múltiple seguro (smb3). • Se agregó contenido adicional en Protección de claves selladas (SKP).

Fecha	Resumen
Febrero de 2021	Actualizado para: • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 Temas agregados: • Implementación de iBoot de forma segura para la memoria • Proceso de arranque en una Mac con Apple Chip • Modos de arranque en una Mac con Apple Chip • Control de la política de seguridad del disco de arranque para una computadora Mac con Apple Chip • Administración y creación de claves de firmas para LocalPolicy • Contenidos del archivo LocalPolicy en computadoras Mac con Apple Chip • Seguridad del volumen del sistema firmado en iOS, iPadOS y macOS • Dispositivo de investigación de seguridad de Apple • Monitoreo de contraseñas • Seguridad de iPv6 • Seguridad de la función Llave de auto en iOS Temas actualizados: • Secure Enclave • Desconexión del micrófono de hardware • recoveryOS y entornos de diagnóstico en computadoras Mac basadas en Intel • Protecciones del acceso directo a la memoria en las computadoras Mac • Extensiones de kernel en macOS • Protección de la integridad del sistema • Seguridad del sistema en watchOS • Administración de FileVault en macOS • Acceso de las apps a las contraseñas guardadas • Recomendaciones de seguridad para las contraseñas • Seguridad de Apple Cash • Seguridad de Apple Messages for Business • Privacidad de Wi-Fi • Seguridad del bloqueo de activación • Seguridad de Apple Configurator

Fecha	Resumen
Abril 2020	Actualizado para: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Actualizaciones: • Se agregó información sobre la desconexión del micrófono del iPad a la sección Desconectar el micrófono de hardware. • Se agregó información sobre las bóvedas de datos a la sección Proteger el acceso de las apps a los datos de usuario. • Se actualizaron las secciones Administración de FileVault en macOS y Herramientas de línea de comandos. • Se agregó información sobre la herramienta para la eliminación de malware en la sección Protección contra el malware en macOS. • Se actualizó la sección Seguridad de iPad compartido en iPadOS.
Diciembre de 2019	Se fusionaron la guía de seguridad de iOS, la descripción general de seguridad de macOS, y la descripción general del chip de seguridad T2 de Apple. Actualizado para: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Se eliminaron las secciones Controles de privacidad, Siri y sugerencias de Siri y Prevención inteligente de seguimiento de Safari. Consulta https://www.apple.com/la/privacy/ para obtener información actualizada sobre esas funciones.
Mayo de 2019	Actualizado para iOS 12.3 • Compatibilidad con TLS 1.3 • Descripción revisada de la seguridad de AirDrop • Modo DFU y modo de recuperación • Requisitos de código para conexiones de accesorios
Noviembre de 2018	Actualizado para iOS 12.1 • FaceTime grupal

Fecha	Resumen
Septiembre de 2018	Actualizado para iOS 12 Secure Enclave • Protección de la integridad del sistema operativo • Tarjeta express con reserva de energía • Modo DFU y modo de recuperación • Accesorios de control de TV de HomeKit • Pases sin contacto • Tarjetas de identificación de estudiantes • Sugerencias de Siri • Atajos en Siri • App Atajos • Administración de contraseñas del usuario • Tiempo en pantalla • Certificaciones y programas de seguridad
Julio de 2018	Actualizado para iOS 11.4 • Políticas de credenciales biométricas • HomeKit • Apple Pay • Chat para clientes • Mensajes en iCloud • Apple Business Manager
Diciembre de 2017	Actualizado para iOS 11.2 • Apple Pay Cash
Octubre de 2017	Actualizado para iOS 11.1 • Certificaciones y programas de seguridad • Touch ID/Face ID • Notas compartidas • Encriptación de extremo a extremo de CloudKit • Actualización de TLS • Apple Pay y pagos con Apple Pay en Internet • Sugerencias de Siri • iPad compartido
Julio de 2017	Actualizado para iOS 10.3 • Secure Enclave • Protección de datos de archivo • Repositorios de claves • Certificaciones y programas de seguridad • SiriKit • HealthKit • Seguridad de la red • Bluetooth • iPad compartido • Modo perdido • Bloqueo de activación • Controles de privacidad

Fecha	Resumen
Marzo de 2017	Actualizado para iOS 10 Seguridad del sistema • Clases de protección de datos • Certificaciones y programas de seguridad • HomeKit, ReplayKit y SiriKit • Apple Watch • Wi-Fi, VPN • Inicio de sesión único • Apple Pay y pagos con Apple Pay en Internet • Aprovisionamiento de tarjetas de crédito, débito y prepago • Sugerencias de Safari
Mayo de 2016	Actualizado para iOS 9.3 • Apple ID administrado • Autenticación de dos factores para Apple ID • Repositorios de claves • Certificaciones de seguridad • Modo perdido y bloqueo de activación • Notas seguras • Apple School Manager • iPad compartido
Septiembre de 2015	Actualizado para iOS 9 Bloqueo de activación de Apple Watch • Políticas de código • Compatibilidad API de Touch ID • Protección de datos en A8 mediante AES-XTS • Repositorios de claves para la actualización de software sin supervisión • Actualización de certificados • Modelo de confianza de apps empresariales • Protección de datos para los marcadores de Safari • Seguridad de transporte de las apps • Especificaciones de VPN • Acceso remoto a iCloud para HomeKit • Tarjetas de recompensa de Apple Pay y app de la entidad emisora de la tarjeta de Apple Pay • Indexación de Spotlight en el dispositivo • Modelo de enlace de iOS • Apple Configurator 2 • Restricciones

El uso del logotipo de Apple que se ingresa con el teclado (Opción + Mayúsculas + K) para fines comerciales sin el consentimiento escrito de Apple podría constituir una quebrantamiento de marca registrada y competencia desleal en violación de las leyes federales y estatales.

Apple, el logotipo de Apple, AirDrop, AirPlay, Apple Books, Apple Card, Apple Music, Apple Pay, Apple TV, Apple Wallet, Apple Watch, AppleScript, ARKit, Bonjour, Boot Camp, CarPlay, Face ID, FaceTime, FileVault, Finder, FireWire, Handoff, HealthKit, HomeKit, HomePod, HomePod mini, iMac, iMac Pro, iMessage, iPad, iPadOS, iPad Air, iPad Pro, iPhone, iPod touch, iTunes, Keychain, Lightning, Mac, Mac Catalyst, Mac mini, Mac Pro, MacBook, MacBook Air, MacBook Pro, macOS, Magic Keyboard, Objective-C, OS X, QuickType, Retina, Rosetta, Safari, Siri, Siri Remote, SiriKit, Swift, Spotlight, Touch ID, TrueDepth, tvOS, watchOS y Xcode son marcas comerciales de Apple Inc., registradas en los EE.UU. y en otros países y regiones.

App Clips, Find My y Touch Bar son marcas comerciales de Apple Inc.

App Store, AppleCare, CloudKit, iCloud, iCloud Drive, iCloud Keychain y iTunes Store son marcas de servicio de Apple Inc., registradas en los EE.UU. y en otros países y regiones.

Apple Messages for Business es una marca de servicio de Apple Inc

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

IOS es una marca comercial o marca comercial registrada de Cisco en los EE.UU. y otros países, y se usa bajo licencia.

La marca denominativa y los logotipos de Bluetooth® son marcas comerciales registradas de Bluetooth SIG, Inc., y Apple dispone de licencia para usar dichas marcas.

Java es una marca comercial registrada de Oracle y sus filiales.

UNIX® es una marca comercial registrada propiedad de The Open Group.

Otros nombres de productos y empresas mencionados en el presente documento pueden ser marcas comerciales de sus respectivas empresas.

Se ha hecho todo lo posible para garantizar que la información de este manual sea precisa. Apple no se hace responsable de los errores de impresión o tipográficos.

Algunas apps no están disponibles en todas las regiones. La disponibilidad de las apps está sujeta a cambios.

LA028-00625