Segurança da Plataforma Apple

Maio de 2022

Conteúdo

Segurança da Plataforma Apple

Introdução à segurança da plataforma Apple

A Apple coloca a segurança no centro de suas plataformas. Aproveitando a experiência obtida com a criação do sistema operacional mais avançado do mundo para dispositivos móveis, a Apple criou arquiteturas de segurança que atendem aos requisitos especiais de dispositivos móveis, relógios, computadores e casas.

Cada dispositivo Apple combina *hardware*, *software* e *serviços* projetados para trabalhar em conjunto e proporcionar o máximo de segurança e uma experiência transparente para o usuário, a serviço do objetivo final de manter informações pessoais seguras. Por exemplo, o silício e o hardware de segurança projetados pela Apple disponibilizam recursos de segurança críticos. E as proteções de software trabalham para manter o sistema operacional e apps de terceiros protegidos. Por fim, serviços fornecem um mecanismo para atualizações de software seguras e pontuais, disponibilizam um ecossistema de apps protegido e facilitam comunicações e pagamentos seguros. Como resultado, os dispositivos Apple protegem não apenas o dispositivo e seus dados, mas também todo o ecossistema, incluindo tudo o que os usuários fazem localmente, em redes e nos principais serviços de internet.

Assim como projetamos nossos produtos para serem simples, intuitivos e poderosos, os projetamos para serem seguros. Recursos importantes de segurança, como a criptografia do dispositivo com base no hardware, não podem ser desativados por engano. Outros recursos, como o Face ID e o Touch ID, melhoram a experiência do usuário tornando a segurança do dispositivo mais simples e intuitiva. E como muitos desses recursos são ativados por padrão, os usuários ou departamentos de TI não precisam realizar configurações extensas.

Esta documentação fornece detalhes de como a tecnologia e os recursos de segurança são implementados nas plataformas Apple. Ela também ajuda as organizações a combinar a tecnologia e os recursos de segurança da plataforma Apple com as suas próprias políticas e procedimentos para atender às suas necessidades de segurança específicas.

O conteúdo está organizado nos seguintes temas:

- **Segurança de hardware e biometria:** o silício e o hardware que formam a base da segurança nos dispositivos Apple, incluindo o Apple Silicon, o Secure Enclave, mecanismos criptográficos, o Face ID e o Touch ID
- **Segurança do sistema:** as funções integradas de hardware e software que proporcionam segurança na inicialização, atualização e operação dos sistemas operacionais da Apple
- **Criptografia e Proteção de Dados:** a arquitetura e o design que protegem os dados do usuário caso o dispositivo seja perdido ou roubado ou se uma pessoa ou processo não autorizado tentar usá-lo ou modificá-lo
- **Segurança de apps:** o software e os serviços que fornecem um ecossistema seguro de apps e permitem que os apps sejam executados em segurança e sem comprometer a integridade da plataforma
- **Segurança de serviços:** os serviços da Apple para identificação, gerenciamento de senhas, pagamentos, comunicações e busca de dispositivos perdidos
- **Segurança de rede:** protocolos de rede padrão do setor que fornecem autenticação e criptografia segura de dados em transmissões
- **Segurança do kit para desenvolvedores:** "kits" de frameworks para o gerenciamento seguro e privado da casa e saúde, além da extensão de recursos de serviços e dispositivos Apple para apps de terceiros
- **Gerenciamento seguro de dispositivos:** métodos que permitem o gerenciamento de dispositivos Apple, ajudam a impedir o uso não autorizado e ativam o apagamento remoto caso o dispositivo seja perdido ou roubado

Um compromisso com a segurança

A Apple está comprometida a ajudar na proteção de clientes usando tecnologias de privacidade e segurança de ponta — criadas para o resguardo de informações pessoais — e métodos abrangentes para ajudar a proteger dados corporativos em ambientes empresariais. A Apple oferece o Apple Security Bounty, recompensando pesquisadores pelo trabalho realizado na descoberta de vulnerabilidades. Detalhes do programa e categorias de recompensas estão disponíveis em https://developer.apple.com/security-bounty/ (em inglês).

Nós mantemos uma equipe de segurança exclusiva para oferecer suporte a todos os produtos da Apple. A equipe realiza auditorias e testes de segurança dos produtos, tanto os que estão em desenvolvimento quanto os já lançados. A equipe da Apple também fornece ferramentas e treinamento de segurança e monitora ativamente em busca de ameaças e relatórios de novos problemas de segurança. A Apple é membro do Forum of Incident Response and Security Teams (FIRST).

A Apple continua rompendo as barreiras do que é possível na privacidade e segurança. Ela usa silício personalizado em toda a linha de produtos — desde o Apple Watch, iPhone e iPad, ao chip T2 Security e Apple Silicon no Mac — possibilitando não só uma computação eficiente como também segurança. Por exemplo, o Apple Silicon forma a base da inicialização segura, do Face ID e Touch ID e da Proteção de Dados. Além disso, os recursos de segurança nos dispositivos com Apple Silicon — como a Proteção da Integridade do Kernel, Códigos de Autenticação de Ponteiros e Restrições de Permissões Rápidas — ajudam a impedir tipos comuns de ataques virtuais. Portanto, mesmo que o código invasor seja executado de alguma forma, os danos que pode causar são drasticamente reduzidos.

Para tirar o máximo de proveito dos apurados recursos de segurança integrados às nossas plataformas, as organizações são encorajadas a analisar suas políticas de TI e segurança, visando fazer o melhor uso possível das camadas de tecnologia de segurança oferecidas por essas plataformas.

Para saber mais sobre como comunicar problemas à Apple e assinar notificações de segurança, consulte Relatar vulnerabilidades de segurança ou privacidade.

A Apple acredita que a privacidade é um direito humano fundamental e oferece diversos controles e opções integradas para permitir que os usuários decidam como e quando apps usam suas informações, além de quais informações são usadas. Para saber mais sobre a abordagem da Apple em relação à privacidade, controles de privacidade em dispositivos Apple e a política de privacidade da Apple, consulte https://www.apple.com/br/privacy.

Nota: salvo indicação em contrário, esta documentação abrange as seguintes versões destes sistemas operacionais: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 e watchOS 8.5.

Segurança de hardware e biometria

Visão geral da segurança do hardware

Para que o software seja seguro, ele deve estar em um hardware com segurança integrada. É por isso que dispositivos Apple — com iOS, iPadOS, macOS, tvOS e watchOS — têm capacidades de segurança projetadas no silício. Essas capacidades incluem uma CPU que fornece recursos de segurança do sistema, além de silício adicional dedicado a funções de segurança. O hardware com enfoque em segurança segue o princípio de oferecer suporte a funções definidas de maneira limitada e discreta para minimizar a superfície de ataque. Esses componentes incluem uma ROM de inicialização que forma uma raiz de confiança de hardware para a inicialização segura, mecanismos AES dedicados para criptografia e descriptografia eficientes e seguras, e um Secure Enclave. O *Secure Enclave* é um sistema no chip (SoC) incluído em todos os dispositivos iPhone, iPad, Apple Watch, Apple TV e HomePod recentes, e em um Mac com Apple Silicon, além daqueles com o chip Apple T2 Security. O Secure Enclave em si segue os mesmos princípios de design do SoC, contendo sua própria ROM de inicialização discreta e mecanismo AES. O Secure Enclave também fornece a fundação para gerar e armazenar com segurança as chaves necessárias para criptografar os dados em repouso, além de proteger e avaliar os dados biométricos do Face ID e Touch ID.

A criptografia do armazenamento deve ser rápida e eficiente. Ao mesmo tempo, ela não pode expor os dados (ou *materiais de criação de chaves*) usados para estabelecer os relacionamentos de chaves criptográficas. O mecanismo de hardware do AES resolve esse problema ao realizar uma rápida criptografia e descriptografia em linha, *conforme os arquivos são gravados ou lidos*. Um canal especial para o Secure Enclave oferece os materiais de criação de chaves necessários para o mecanismo AES sem expor essas informações ao Processador de Aplicativos (ou CPU) ou ao sistema operacional no geral. Isso ajuda a garantir que as tecnologias de Proteção de Dados e do FileVault da Apple protejam os arquivos de usuários sem expor chaves de criptografia de vida longa.

A Apple projetou a inicialização segura para proteger os níveis mais baixos do software contra a adulteração e para permitir que apenas o software confiável do sistema operacional da Apple seja carregado durante a inicialização. A inicialização segura começa no código imutável chamado de ROM de Inicialização que é colocado durante a fabricação do SoC da Apple e conhecido como *raiz de confiança do hardware*. Em computadores Mac com um chip T2, a confiança da inicialização segura do macOS começa com o T2 (o chip T2 e o Secure Enclave também usam suas próprias ROMs de inicialização independentes para executar seus processos de inicialização — de maneira exatamente análoga à inicialização segura dos chips da série A e família M1).

O Secure Enclave também processa os dados de rosto e impressão digital dos sensores do Face ID e Touch ID em dispositivos Apple. Isso fornece uma autenticação segura ao mesmo tempo que mantém os dados biométricos do usuário privados e seguros. Isso também permite que usuários se beneficiem da segurança de códigos e senhas mais longos e complexos e, em muitos casos, com a conveniência de uma autenticação ágil para acesso ou compras.

Segurança do SoC da Apple

O silício projetado pela Apple forma uma arquitetura comum entre todos os produtos da Apple e agora também alimenta o Mac, além do iPhone, iPad, Apple TV e Apple Watch. Por mais de uma década, a equipe de design do silício de alto nível da Apple tem criado e refinado os sistemas no chip (SoCs) da Apple. O resultado é uma arquitetura escalável projetada para todos os dispositivos lideram a indústria quanto às capacidades de segurança. Essa fundação comum para recursos de segurança é possível apenas quando uma empresa projeta seu próprio silício para que funcione com seu software.

O Apple Silicon foi projetado e fabricado para permitir especificamente os recursos de segurança do sistema detalhados abaixo.

Recurso	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Família M1
Proteção da Integridade do Kernel	✓	✓	✓	✓	✓	✓
Restrições de Permissões Rápidas		✓	✓	✓	✓	✓
Proteção da Integridade do Coprocessador do Sistema			✓	✓	✓	✓
Códigos de Autenticação de Ponteiros			✓	✓	✓	✓
Camada de Proteção de Página		✓	✓	✓	✓	Veja a nota abaixo.

Nota: a Camada de Proteção de Página (PPL) requer que a plataforma execute *apenas* o código assinado e confiado; esse é um modelo de segurança que não se aplica ao macOS.

O silício projetado pela Apple também permite especificamente as capacidades de Proteção de Dados detalhadas abaixo.

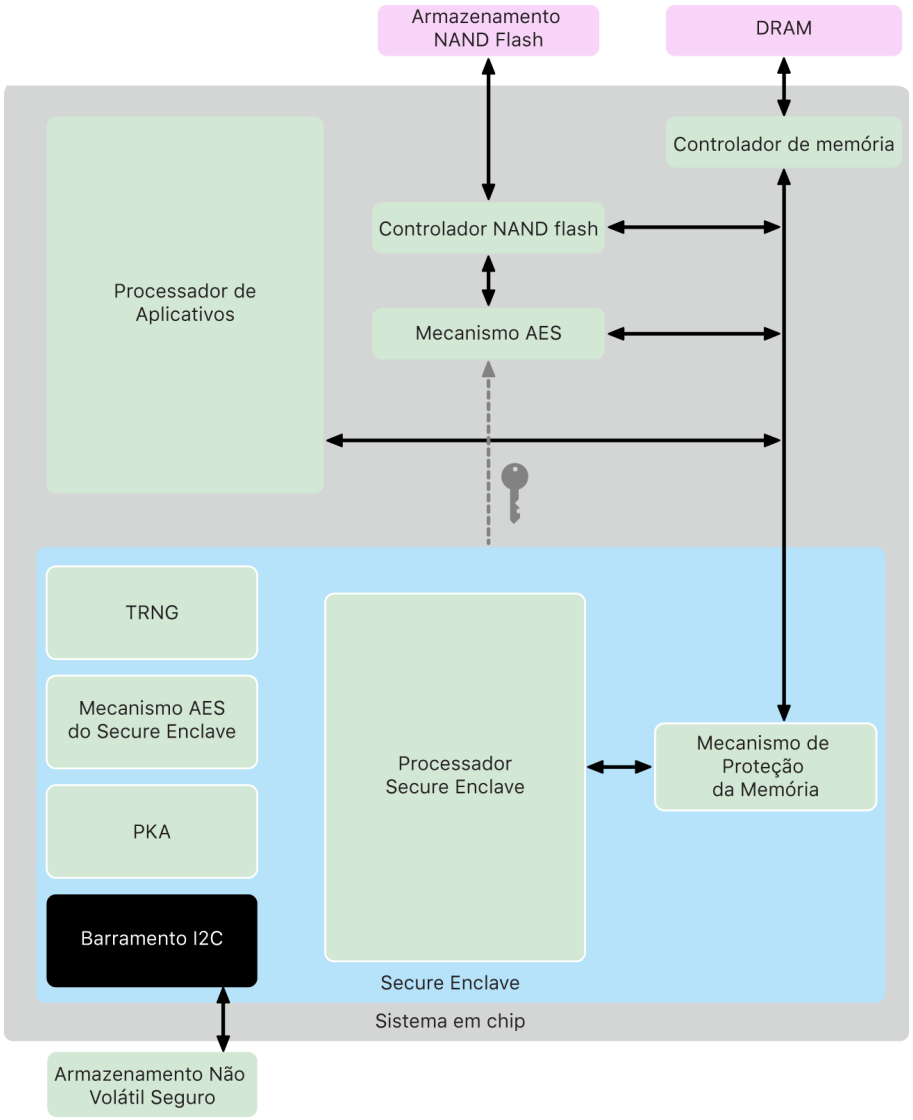
Recurso	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, Família M1
Proteção de Chave Selada (SKP)	✓	✓	✓	✓	✓
recoveryOS - proteção de todas as Classes de Proteção de Dados	✓	✓	✓	✓	✓
Inicializações alternativas de DFU, Diagnóstico e Atualização - proteção de dados das Classes A, B e C			✓	✓	✓

Secure Enclave

O Secure Enclave é um subsistema seguro dedicado nas versões mais recentes do iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch e HomePod.

Visão geral

O Secure Enclave é um subsistema seguro dedicado, integrado aos sistemas no chip (SoCs) da Apple. O Secure Enclave é isolado do processador principal para fornecer uma camada de segurança extra e projetado para manter dados sensíveis do usuário em segurança mesmo quando o kernel do Processador de Aplicativos é comprometido. Ele segue os mesmos princípios de design do SoC: uma ROM de inicialização para estabelecer uma raiz de confiança de hardware, um mecanismo AES para operações criptográficas eficientes e seguras, e memória protegida. Embora o Secure Enclave não inclua armazenamento, ele possui um mecanismo para armazenar informações com segurança em um armazenamento anexo, separado do armazenamento flash NAND usado pelo Processador de Aplicativos e o sistema operacional.



O Secure Enclave é um recurso de hardware presenta na maioria das versões de iPhone, iPad, Mac, Apple TV, Apple Watch e HomePod, especificamente:

- iPhone 5s ou posterior
- iPad Air ou posterior
- Computadores MacBook Pro com Touch Bar (2016 e 2017) que contêm o chip Apple T1
- Computadores Mac baseados em Intel que contêm o chip Apple T2 Security
- Computadores Mac com Apple Silicon
- Apple TV HD ou posterior
- Apple Watch Series 1 ou posterior
- HomePod e HomePod mini

Processador do Secure Enclave

O Processador do Secure Enclave fornece a energia computacional principal para o Secure Enclave. Para proporcionar o isolamento mais forte, o Processador do Secure Enclave é dedicado exclusivamente ao uso do Secure Enclave. Isso ajuda a impedir ataques de canal lateral que dependem de um software malicioso que compartilha o mesmo núcleo de execução de um software alvo sendo atacado.

O Processador do Secure Enclave executa uma versão do microkernel L4 personalizado pela Apple. Ele é projetado para operar eficientemente em uma velocidade de relógio menor, o que ajuda a protegê-lo contra ataques de relógio e energia. O Processador do Secure Enclave, a partir do A11 e S4, inclui um mecanismo de memória protegida e memória criptografada com capacidades antirreprodução, inicialização segura, um gerador de números aleatórios dedicado e seu próprio mecanismo AES.

Mecanismo de Proteção de Memória

O Secure Enclave opera a partir de uma região dedicada da memória DRAM do dispositivo. Diversas camadas de proteção isolam a memória protegida do Secure Enclave do Processador de Aplicativos.

Quando o dispositivo é inicializado, a ROM de Inicialização do Secure Enclave gera uma chave de proteção de memória efêmera aleatória para o Mecanismo de Proteção de Memória. Sempre que o Secure Enclave grava em sua região de memória dedicada, o Mecanismo de Proteção de Memória criptografa o bloco da memória com AES no modo XEX (xor-encrypt-xor) do Mac e calcula uma etiqueta de autenticação de Código de Autenticação de Mensagem baseado em Cifra (CMAC) para a memória. O Mecanismo de Proteção de Memória armazena a etiqueta de autenticação junto com a memória criptografada. Quando o Secure Enclave lê a memória, o Mecanismo de Proteção de Memória verifica a etiqueta de autenticação. Se a etiqueta de autenticação for idêntica, o Mecanismo de Proteção de Memória descriptografa o bloco da memória. Se a etiqueta não for idêntica, o Mecanismo de Proteção de Memória indica um erro ao Secure Enclave. Depois de um erro de autenticação de memória, o Secure Enclave para de aceitar pedidos até que o sistema seja reinicializado.

A partir dos SoCs A11 e S4 da Apple, o Mecanismo de Proteção de Memória adiciona proteção contra reprodução à memória do Secure Enclave. Para ajudar a impedir a reprodução de dados de segurança críticos, o Mecanismo de Proteção de Memória armazena um número de utilização única, chamado de *nonce*, para o bloco da memória, além de uma etiqueta de autenticação. O nonce é usado como um ajuste adicional para a etiqueta de autenticação CMAC. Os nonces de todos os blocos de memória são protegidos por uma árvore de integridade cuja raiz se encontra em uma SRAM dedicada dentro do Secure Enclave. Em gravações, o Mecanismo de Proteção de Memória *atualiza* o nonce e cada nível da árvore de integridade até a SRAM. Em leituras, o Mecanismo de Proteção de Memória *verifica* o nonce e cada nível da árvore de integridade até a SRAM. Incongruências de nonces são gerenciadas de maneira similar às incongruências em etiquetas de autenticação.

Nos SoCs A14, A15, família M1 e posteriores da Apple, o Mecanismo de Proteção de Memória oferece suporte a duas chaves de proteção de memória efêmera. A primeira é usada para dados privados do Secure Enclave e a segunda é usada para os dados compartilhados com o Mecanismo Neural Seguro.

O Mecanismo de Proteção de Memória opera em linha e de forma transparente para o Secure Enclave. O Secure Enclave lê e grava memória como se ela fosse uma DRAM normal não criptografada, enquanto um observador fora do Secure Enclave vê apenas a versão criptografada e autenticada da memória. O resultado é uma forte proteção da memória sem concessões de desempenho ou complexidade de software.

ROM de Inicialização do Secure Enclave

O Secure Enclave inclui uma ROM de Inicialização do Secure Enclave dedicada. Como a ROM de Inicialização do Processador de Aplicativos, a ROM de Inicialização do Secure Enclave é um código imutável que estabelece a raiz de confiança do hardware para o Secure Enclave.

Ao inicializar o sistema, o iBoot atribui uma região da memória dedicada ao Secure Enclave. Antes de usar a memória, a ROM de Inicialização do Secure Enclave inicializa o Mecanismo de Proteção de Memória para fornecer a proteção criptográfica da memória protegida do Secure Enclave.

O Processador de Aplicativos envia então a imagem sepOS à ROM de Inicialização do Secure Enclave. Depois de copiar a imagem sepOS na memória protegida do Secure Enclave, a ROM de Inicialização do Secure Enclave confere o hash criptográfico e a assinatura da imagem para verificar se o sepOS está autorizado a ser executado no dispositivo. Se a imagem sepOS estiver devidamente assinada para ser executada no dispositivo, a ROM de Inicialização do Secure Enclave transfere o controle ao sepOS. Se a assinatura não for válida, a ROM de Inicialização do Secure Enclave é projetada para impedir qualquer uso adicional do Secure Enclave até a próxima redefinição do chip.

Nos SoCs A10 e posteriores da Apple, a ROM de Inicialização do Secure Enclave bloqueia um hash do sepOS em um registro dedicado a esse propósito. O Acelerador de Chave Pública usa esse hash para as chaves destinadas ao sistema operacional (destino-OS).

Monitor de Inicialização do Secure Enclave

Nos SoCs A13 e posteriores da Apple, o Secure Enclave inclui um Monitor de Inicialização projetado para garantir uma integridade mais forte ao hash do sepOS inicializado.

Ao inicializar o sistema, a configuração da Proteção da Integridade do Coprocessador do Sistema (SCIP) do Processador do Secure Enclave ajuda a impedir que o Processador do Secure Enclave execute qualquer outro código diferente da ROM de Inicialização do Secure Enclave. O Monitor de Inicialização ajuda a impedir que o Secure Enclave modifique a configuração da SCIP diretamente. Para fazer com que o sepOS carregado seja executável, a ROM de Inicialização do Secure Enclave envia ao Monitor de Inicialização um pedido com o endereço e o tamanho do sepOS carregado. Ao receber o pedido, o Monitor de Inicialização redefine o Processador do Secure Enclave, cria um hash do sepOS carregado, atualiza os ajustes da SCIP para permitir a execução do sepOS carregado e inicia a execução dentro do código recém-carregado. Conforme a inicialização do sistema continua, esse mesmo processo é usado sempre que um código novo se torna executável. A cada vez, o Monitor de Inicialização atualiza um hash em execução do processo de inicialização. O Monitor de Inicialização também inclui parâmetros críticos de segurança no hash em execução.

Quando a inicialização é concluída, o Monitor de Inicialização finaliza o hash em execução e o envia ao Acelerador de Chave Pública para o uso com chaves destinadas ao OS. Esse processo é projetado para que o vínculo de chaves do sistema operacional não possa ser contornado mesmo com uma vulnerabilidade na ROM de Inicialização do Secure Enclave.

Gerador de Números Aleatórios Verdadeiro

O Gerador de Números Aleatórios Verdadeiro (TRNG) é usado para gerar dados aleatórios seguros. O Secure Enclave usa o TRNG sempre que gera uma chave criptográfica aleatória, núcleo de chave aleatória ou outra entropia. O TRNG é baseado em diversos osciladores de anel pós-processados com CTR_DRBG (um algoritmo que se baseia em cifras de bloco no Modo de Contagem).

Chaves Criptográficas de Raiz

O Secure Enclave inclui uma chave criptográfica de raiz de ID exclusivo (UID). O UID é exclusivo a cada dispositivo e não está relacionado a nenhum outro identificador no dispositivo.

Um UID gerado aleatoriamente é fundido ao SoC durante a manufatura. Desde os SoCs A9, o UID é gerado pelo TRNG do Secure Enclave durante a manufatura e gravado nos fusíveis em um processo de software executado inteiramente no Secure Enclave. Esse processo protege a visualização do UID a partir de fora do dispositivo durante o processo de manufatura e, portanto, não está disponível para acesso ou armazenamento pela Apple nem nenhum de seus fornecedores.

O sepOS usa o UID para proteger segredos específicos do dispositivo. O UID permite que os dados sejam criptograficamente atrelados a um dispositivo específico. Por exemplo, a hierarquia de chaves que protege o sistema de arquivos inclui o UID; então, se o armazenamento SSD interno for movido fisicamente de um dispositivo para outro, os arquivos ficam inacessíveis. Entre outros segredos protegidos específicos do dispositivo estão os dados do Face ID ou Touch ID. Em um Mac, apenas o armazenamento totalmente interno vinculado ao mecanismo AES recebe esse nível de criptografia. Por exemplo, dispositivos de armazenamento externo conectados via USB ou armazenamentos baseados em PCIe adicionados ao Mac Pro de 2019 não são criptografados dessa forma.

O Secure Enclave também tem um ID de grupo (GID), comum a todos os dispositivos que usam um certo SoC (por exemplo, todos os dispositivos que usam o SoC A15 da Apple compartilham o mesmo GID).

O UID e GID não estão disponíveis através do Grupo de Ação de Teste Conjunto (JTAG) nem por outras interfaces de depuração.

Mecanismo AES do Secure Enclave

O Mecanismo AES do Secure Enclave é um bloco de hardware usado para realizar criptografia simétrica baseada na cifra AES. O Mecanismo AES é projetado para resistir ao vazamento de informações ao usar tempo e Análise de Energia Estática (SPA). A partir do SoC A9, o Mecanismo AES também inclui contramedidas de Análise de Energia Dinâmica (DPA).

O Mecanismo AES é compatível com chaves de hardware e software. As chaves de hardware são derivadas do UID ou GID do Secure Enclave. Essas chaves permanecem dentro do Mecanismo AES e não são expostas nem mesmo ao software do sepOS. Embora o software possa solicitar operações de criptografia e descriptografia com chaves de hardware, ele não pode extrair as chaves.

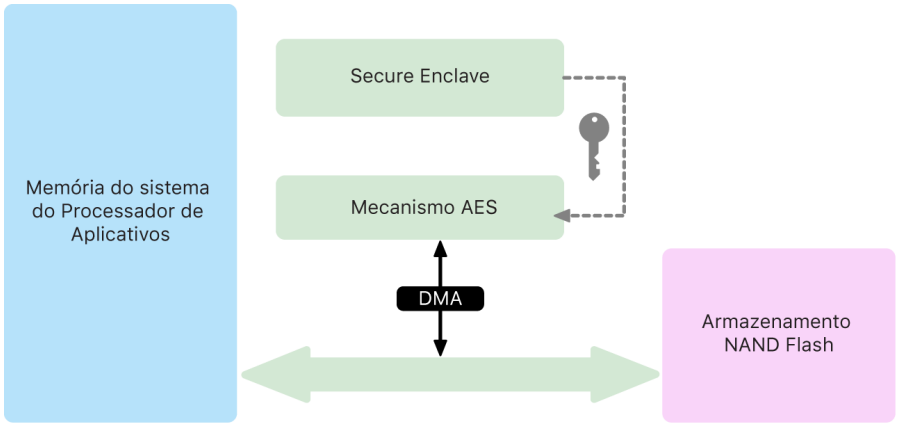
Nos SoCs A10 e mais recentes da Apple, o Mecanismo AES inclui bits de núcleo bloqueáveis que diversificam as chaves derivadas do UID ou GID. Isso permite o condicionamento do acesso aos dados no modo de operação do dispositivo. Por exemplo, bits de núcleo bloqueáveis são usados para negar o acesso a dados protegidos por senha ao inicializar a partir do modo de Atualização do Firmware do Dispositivo (DFU). Para obter mais informações, consulte Códigos e senhas.

Mecanismo AES

Todos os dispositivos Apple com um Secure Enclave também possuem um mecanismo de criptografia AES256 dedicado (o “Mecanismo AES”) integrado ao caminho de acesso direto à memória (DMA), entre o armazenamento flash NAND (não volátil) e a memória principal do sistema, fazendo com que a criptografia de arquivos seja altamente eficiente. Em processadores A9 ou posteriores da série A, o subsistema de armazenamento flash encontra-se em um barramento isolado que recebe acesso apenas à memória que contém os dados do usuário pelo mecanismo de criptografia DMA.

No momento da inicialização, o sepOS usa o TRNG para gerar uma chave de embalamento efêmera. O Secure Enclave usa fios dedicados para transmitir essa chave ao Mecanismo AES, projetados para impedir que ela seja acessada por qualquer software fora do Secure Enclave. O sepOS pode então usar a chave de embalamento efêmera para embalar as chaves de arquivos para uso por parte do driver do sistema de arquivos do Processador de Aplicativos. Quando o driver do sistema de arquivos lê ou grava um arquivo, ele envia a chave embalada ao Mecanismo AES, o qual desembala a chave. O Mecanismo AES nunca expõe a chave desembalada ao software.

Nota: o Mecanismo AES é um componente separado tanto do Secure Enclave quanto do Mecanismo AES do Secure Enclave, mas sua operação está intimamente ligada ao Secure Enclave conforme mostrado abaixo.



Acelerador de Chave Pública

O Acelerador de Chave Pública (PKA) é um bloco de hardware usado para realizar operações de criptografia de curva elíptica. O PKA oferece suporte aos algoritmos de criptografia e assinatura RSA e ECC (Criptografia de Curva Elíptica). O PKA é projetado para resistir ao vazamento de informações de ataques que usam canal lateral e tempo, como SPA e DPA.

O PKA é compatível com chaves de software e hardware. As chaves de hardware são derivadas do UID ou GID do Secure Enclave. Essas chaves permanecem dentro do PKA e não são expostas nem mesmo ao software do sepOS.

A partir dos SoCs A13, as implementações de criptografia do PKA foram matematicamente comprovadas através do uso de técnicas de verificação formais.

Nos SoCs A10 ou posteriores da Apple, o PKA é compatível com chaves destinadas ao OS, algo também chamado de Proteção de Chave Selada (SKP). Essas chaves são geradas por uma combinação do UID do dispositivo e o hash do sepOS em execução no dispositivo. O hash é fornecido pela ROM de Inicialização do Secure Enclave ou pelo Monitor de Inicialização do Secure Enclave em SoCs A13 e posteriores da Apple. Essas chaves também são usadas para verificar a versão do sepOS ao fazer pedidos a certos serviços da Apple, assim como para aumentar a segurança de dados protegidos por código ao ajudar a impedir o acesso a materiais de criação de chaves caso mudanças críticas sejam feitas ao sistema sem a autorização do usuário.

Armazenamento não volátil seguro

O Secure Enclave é equipado com um dispositivo de armazenamento não volátil seguro. O armazenamento não volátil seguro usa um barramento I2C dedicado para se conectar ao Secure Enclave para que ele possa ser acessado apenas pelo Secure Enclave. Todas as chaves de criptografia de dados do usuário têm como raiz a entropia armazenada no armazenamento não volátil seguro do Secure Enclave.

Em dispositivos com SoCs A12, S4 e posteriores, o Secure Enclave é emparelhado com um Componente de Armazenamento Seguro para armazenamento da entropia. O Componente de Armazenamento Seguro é projetado com um código de ROM imutável, um gerador de números aleatórios de hardware, uma chave criptográfica exclusiva por dispositivo, mecanismos de criptografia e detecção de adulteração física. Para se comunicar, o Secure Enclave e o Componente de Armazenamento Seguro usam um protocolo criptografado e autenticado que fornece acesso exclusivo à entropia.

Dispositivos lançados inicialmente no Outono de 2020 ou depois são equipados com um Componente de Armazenamento Seguro de 2ª geração. A 2ª geração do Componente de Armazenamento Seguro adiciona caixas-fortes de contagem. Cada caixa-forte de contagem armazena um sal de 128 bits, um verificador de código de 128 bits, um contador de 8 bits e um valor máximo de tentativa de 8 bits. O acesso às caixas-fortes de contagem dá-se através de um protocolo criptografado e autenticado.

As caixas-fortes de contagem contêm a entropia necessária para desbloquear os dados de usuário protegidos por código. Para acessar os dados de usuário, o Secure Enclave emparelhado deve derivar o valor de entropia de código certo do código do usuário e do UID do Secure Enclave. O código do usuário não pode ser descoberto por tentativas de desbloqueio enviadas de uma fonte diferente do Secure Enclave emparelhado. Se o limite de tentativas de código for excedido (10 tentativas no iPhone, por exemplo), os dados protegidos por código são completamente apagados pelo Componente de Armazenamento Seguro.

Para criar uma caixa-forte de contagem, o Secure Enclave envia o valor de entropia do código e o valor de contagem máximo ao Componente de Armazenamento Seguro. O Componente de Armazenamento Seguro usa seu gerador de números aleatórios para gerar o valor de sal. Depois, ele deriva um valor do verificador de código e um valor de entropia de caixa-forte a partir da entropia do código fornecido, da chave criptográfica exclusiva do Componente de Armazenamento Seguro e do valor de sal. O Componente de Armazenamento Seguro inicializa a caixa-forte de contagem com uma contagem de 0, o valor máximo de tentativa fornecido, o valor do verificador de código e o valor de sal. O Componente de Armazenamento Seguro retorna então o valor de entropia da caixa-forte gerado ao Secure Enclave.

Para obter o valor de entropia de caixa-forte de uma caixa-forte de contagem posteriormente, o Secure Enclave envia a entropia do código ao Componente de Armazenamento Seguro. Primeiro, o Componente de Armazenamento Seguro aumenta o contador da caixa-forte. Se o contador aumentado exceder o valor máximo de tentativa, o Componente de Armazenamento Seguro apaga completamente a caixa-forte de contagem. Se a contagem máxima de tentativas não tiver sido atingida, o Componente de Armazenamento Seguro tenta derivar o valor do verificador de código e o valor de entropia da caixa-forte com o mesmo algoritmo usado para criar a caixa-forte de contagem. Se o valor do verificador de código derivado coincidir com o valor do verificador de código armazenado, o Componente de Armazenamento Seguro retorna o valor de entropia da caixa-forte ao Secure Enclave e redefine o contador em 0.

As chaves usadas para acessar dados protegidos por senha têm suas raízes na entropia armazenada nas caixas-fortes de contagem. Para obter mais informações, consulte Visão geral da Proteção de Dados.

O armazenamento não volátil seguro é usado para todos os serviços antirreprodução no Secure Enclave. Os serviços antirreprodução no Secure Enclave são usados para a revogação de dados em eventos que marcam limites antirreprodução, incluindo, dentre outros, o seguinte:

- Alteração do código
- Ativação ou desativação do Face ID ou Touch ID
- Adição ou remoção de um rosto do Face ID ou impressão do Touch ID
- Redefinição do Face ID ou Touch ID
- Adição ou remoção de um cartão do Apple Pay
- Uso da opção “Apagar Conteúdo e Ajustes”

Em arquiteturas sem um Componente de Armazenamento Seguro, a EEPROM (memória somente leitura programável e eletricamente apagável) é usada para fornecer serviços de armazenamento seguro para o Secure Enclave. Da mesma maneira que os Componentes de Armazenamento Seguro, a EEPROM é conectada e acessível apenas a partir do Secure Enclave, embora ela não contenha recursos de segurança de hardware dedicados, não garanta acesso exclusivo à entropia (além de suas características físicas de conexão) nem ofereça funcionalidade de caixa-forte de contagem.

Mecanismo Neural Seguro

Em dispositivos com Face ID, o Mecanismo Neural Seguro converte imagens e mapas de profundidade 2D em uma representação matemática do rosto de um usuário.

Nos SoCs A11 ao A13, o Mecanismo Neural Seguro é integrado ao Secure Enclave. O Mecanismo Neural Seguro usa o acesso direto à memória (DMA) para alto desempenho. Uma unidade de gerenciamento de entrada e saída de memória (IOMMU) sob controle do kernel do sepOS limita esse acesso direto às regiões autorizadas da memória.

A partir do A14 e da família M1, o Mecanismo Neural Seguro é implementado como um modo seguro no Mecanismo Neural do Processador de Aplicativos. Um controlador de segurança de hardware dedicado alterna entre tarefas do Processador de Aplicativos e Secure Enclave, redefinindo o estado do Mecanismo Neural a cada transição para manter os dados do Face ID seguros. Um mecanismo dedicado aplica criptografia na memória, autenticação e controle de acesso. Ao mesmo tempo, ele usa uma chave criptográfica separada e um intervalo de memória para limitar o Mecanismo Neural Seguro às regiões autorizadas da memória.

Monitores de energia e relógio

Todos os eletrônicos são projetados para operar dentro de um limite de voltagem e envelope de frequência. Quando operados fora desse envelope, os eletrônicos podem funcionar indevidamente e os controles de segurança podem ser contornados. Para ajudar a garantir que a voltagem e a frequência permaneçam em um intervalo seguro, o Secure Enclave é projetado com circuitos de monitoramento. Esses circuitos de monitoramento são projetados para ter um envelope de operação bem mais amplo do que o restante do Secure Enclave. Caso os monitores detectem um ponto de operação ilegal, os relógios no Secure Enclave param automaticamente e não reiniciam até a próxima redefinição do SoC.

Resumo de recursos do Secure Enclave

Nota: produtos A12, A13, S4 e S5 lançados inicialmente no Outono de 2020 têm um Componente de Armazenamento Seguro de 2ª geração, enquanto produtos anteriores baseados nesses SoCs têm um Componente de Armazenamento Seguro de 1ª geração.

SoC	Mecanismo de Proteção de Memória	Armazenamento Seguro	Mecanismo AES	PKA
A8	Criptografia e autenticação	EEPROM	Sim	Não
A9	Criptografia e autenticação	EEPROM	Proteção DPA	Sim
A10	Criptografia e autenticação	EEPROM	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
A11	Criptografia, autenticação e prevenção de reprodução	EEPROM	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS

SoC	Mecanismo de Proteção de Memória	Armazenamento Seguro	Mecanismo AES	PKA
A12 (dispositivos Apple lançados antes do Outono de 2020)	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 1ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
A12 (dispositivos Apple lançados depois do Outono de 2020)	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 2ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
A13 (dispositivos Apple lançados antes do Outono de 2020)	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 1ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS e Monitor de Inicialização
A13 (dispositivos Apple lançados depois do Outono de 2020)	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 2ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS e Monitor de Inicialização
A14, A15	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 2ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS e Monitor de Inicialização
S3	Criptografia e autenticação	EEPROM	Proteção DPA e bits de núcleo bloqueáveis	Sim
S4	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 1ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
S5 (dispositivos Apple lançados antes do Outono de 2020)	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 1ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
S5 (dispositivos Apple lançados depois do Outono de 2020)	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 2ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
S6, S7	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 2ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
T2	Criptografia e autenticação	EEPROM	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS
Família M1	Criptografia, autenticação e prevenção de reprodução	Componente de Armazenamento Seguro 2ª ger.	Proteção DPA e bits de núcleo bloqueáveis	Chaves destinadas ao OS e Monitor de Inicialização

Face ID e Touch ID

Segurança do Face ID e Touch ID

Códigos e senhas são essenciais para a segurança de dispositivos Apple. Ao mesmo tempo, usuários precisam acessar seus dispositivos de uma maneira conveniente, por muitas vezes, mais de cem vezes ao dia. A autenticação biométrica oferece uma maneira de manter a segurança de um código forte — ou até de aumentar a robustez do código ou senha, já que os mesmos não precisam ser digitados manualmente — ao mesmo tempo que oferece a conveniência de pressionar ou olhar para o dispositivo para desbloqueá-lo rapidamente. O Face ID e Touch ID não substituem um código ou senha, mas na maioria das situações eles agilizam e facilitam o acesso.

A arquitetura de segurança biométrica da Apple depende de uma estrita separação de responsabilidades entre o sensor biométrico e o Secure Enclave, e uma conexão segura entre os dois. O sensor captura a imagem biométrica e a transmite com segurança para o Secure Enclave. Durante o registro, o Secure Enclave processa, criptografa e armazena os respectivos dados de modelo do Face ID e Touch ID. Durante a correspondência, o Secure Enclave compara os dados de entrada do sensor biométrico com os modelos armazenados para determinar se o dispositivo será desbloqueado ou para responder que uma correspondência é válida (para o Apple Pay, dentro de apps e para outros usos do Face ID e Touch ID). A arquitetura é compatível com dispositivos que incluem o sensor e o Secure Enclave (como o iPhone, iPad e vários sistemas Mac), assim como a capacidade de separar fisicamente o sensor em um periférico que seja emparelhado com segurança ao Secure Enclave em um Mac com Apple Silicon.

Segurança do Face ID

Com um simples olhar, o Face ID desbloqueia dispositivos Apple compatíveis. Ele fornece uma autenticação intuitiva e segura através do sistema de câmera TrueDepth, que usa tecnologias avançadas para mapear com precisão a geometria do rosto do usuário. O Face ID usa redes neurais para determinar atenção, correspondência e antifalsificação, de modo que o usuário possa desbloquear seu telefone com um olhar, mesmo quando estiver usando uma máscara (em dispositivos compatíveis). O Face ID se adapta automaticamente às mudanças na aparência e resguarda cuidadosamente a privacidade e segurança dos dados biométricos do usuário.

O Face ID é projetado para confirmar a atenção do usuário, fornecer autenticação robusta com uma proporção baixa de identificação falsa e mitigar enganos digitais e físicos.

A câmera TrueDepth busca o rosto do usuário automaticamente quando o usuário desperta um dispositivo Apple que tenha Face ID (ao elevá-los ou tocar na tela), assim como quando tais dispositivos tentam autenticar o usuário a fim de mostrar uma notificação recebida ou quando um app compatível exige autenticação pelo Face ID. Quando um rosto é detectado, o Face ID detecta se os olhos do usuário estão abertos e sua atenção está direcionada para o dispositivo para confirmar a intenção de desbloqueio; na acessibilidade, a verificação de atenção do Face ID é desativada quando o VoiceOver está ativado e, se necessário, pode ser desativada separadamente. A detecção da atenção é sempre necessária ao usar o Face ID com uma máscara.

Depois que a câmera TrueDepth confirma a presença de um rosto atento, ela projeta e lê milhares de pontos infravermelhos para formar um mapa de profundidade do rosto, além de uma imagem infravermelha em 2D. Esses dados são usados para criar uma sequência de imagens 2D e mapas de profundidade, que são assinados digitalmente e enviados para o Secure Enclave. Para combater enganos digitais e físicos, a câmera TrueDepth aleatoriza a sequência de capturas de imagens 2D e mapas de profundidade e projeta um padrão aleatório específico do dispositivo. Uma parte do Mecanismo Neural Seguro — protegida dentro do Secure Enclave — transforma esses dados em uma representação matemática e a compara com os dados faciais registrados. Esses dados faciais registrados são, na verdade, uma representação matemática do rosto capturado em diversas poses.

Segurança do Touch ID

O Touch ID é o sistema de detecção de impressão digital que acelera e facilita o acesso a dispositivos Apple compatíveis. Essa tecnologia lê dados de impressões digitais de qualquer ângulo e, com o passar do tempo, aprende mais informações sobre a impressão digital de um usuário, pois o sensor continua a expandir o mapa de impressão digital conforme nós de sobreposição adicionais são identificados a cada uso.

Os dispositivos Apple que possuem um sensor do Touch ID podem ser desbloqueados usando uma impressão digital. O Touch ID não substitui a necessidade de um código do dispositivo ou uma senha de usuário, que ainda são necessários após a inicialização ou reinicialização do dispositivo, ou encerramento de sessão (no Mac). Em alguns apps, o Touch ID também pode ser usado no lugar do código do dispositivo ou da senha do usuário — por exemplo, para desbloquear notas protegidas por senha no app Notas, sites protegidos pelas chaves e senhas de apps compatíveis. No entanto, um código de dispositivo ou senha de usuário sempre é exigido em alguns cenários (por exemplo, para alterar o código do dispositivo ou a senha de usuário existente ou para remover impressões digitais registradas ou criar novas).

Quando o sensor de impressão digital detecta o toque de um dedo, ele aciona a matriz avançada de leitura para escanear o dedo e envia a digitalização para o Secure Enclave. O canal usado para dar segurança a essa conexão varia, dependendo do sensor do Touch ID ser integrado ao dispositivo com Secure Enclave ou se localizar em um periférico à parte.

Enquanto o escaneamento da impressão digital é vetorizado para análise, o escaneamento de varredura é armazenado temporariamente em uma memória criptografada dentro do Secure Enclave, sendo descartado depois. A análise usa mapeamento de ângulo dos fluxos subdérmicos, um processo com perda que descarta dados de minúcias dos dedos que seriam necessários para reconstruir a impressão digital real do usuário. Durante o registro, o mapa de nós resultante é armazenado em um formato criptografado que pode ser lido apenas pelo Secure Enclave como um modelo para comparar a futuras correspondências, mas sem nenhuma informação de identificação. Os dados nunca saem do dispositivo. Eles não são enviados à Apple nem incluídos nos backups do dispositivo.

Segurança do canal do Touch ID integrado

A comunicação entre o Secure Enclave e o sensor do Touch ID integrado ocorre através de um barramento de interface periférico serial. O processador encaminha os dados para o Secure Enclave, mas é incapaz de lê-los. Eles são criptografados e autenticados com uma chave de sessão negociada usando uma chave compartilhada fornecida para cada sensor do Touch ID e seu respectivo Secure Enclave na fábrica. Para cada sensor do Touch ID, a chave compartilhada é forte, aleatória e diferente. A troca de chaves da sessão usa o embalamento de chaves AES com ambos os lados fornecendo uma chave aleatória que estabelece a chave da sessão e usa a criptografia de transporte que fornece tanto autenticação quanto confidencialidade (usando AES-CCM).

Magic Keyboard com Touch ID

O Magic Keyboard com Touch ID (e o Magic Keyboard com Touch ID e Teclado Numérico) oferece um sensor do Touch ID em um teclado externo que pode ser usado com qualquer Mac com Apple Silicon. O Magic Keyboard com Touch ID realiza a função do sensor biométrico; ele não armazena modelos biométricos, realiza a correspondência biométrica nem exige políticas de segurança (por exemplo, ter que digitar a senha após 48 horas sem desbloquear). O sensor do Touch ID no Magic Keyboard com Touch ID deve ser emparelhado com segurança ao Secure Enclave do Mac antes de ser usado. Depois disso, o Secure Enclave realiza as operações de registro e correspondência e exige as políticas de segurança da mesma maneira que o faria em um sensor do Touch ID integrado. A Apple realiza o processo de emparelhamento na fábrica para um Magic Keyboard com Touch ID fornecido com um Mac. O emparelhamento também pode ser realizado pelo usuário, se necessário. Um Magic Keyboard com Touch ID pode ser emparelhado com segurança apenas a um Mac por vez, mas um Mac pode manter emparelhamentos seguros com até cinco teclados Magic Keyboard com Touch ID diferentes.

O Magic Keyboard com Touch ID e os sensores do Touch ID integrados são compatíveis. Se um dedo registrado no sensor do Touch ID integrado a um Mac for apresentado a um Magic Keyboard com Touch ID, o Secure Enclave do Mac processa a correspondência com sucesso — e vice-versa.

Para oferecer suporte ao emparelhamento seguro e, portanto, à comunicação entre o Secure Enclave do Mac e o Magic Keyboard com Touch ID, o teclado é equipado com um bloco de hardware de Acelerador de Chave Pública (PKA), para oferecer atestados, e com chaves baseadas em hardware, para realizar os processos criptográficos necessários.

Emparelhamento seguro

Antes de usar um Magic Keyboard com Touch ID em operações com Touch ID, ele precisa ser emparelhado com segurança ao Mac. Para emparelhar, o Secure Enclave no Mac e o bloco PKA no Magic Keyboard com Touch ID trocam chaves públicas, com raízes na AC confiável da Apple, e usam chaves de atestado presentes no hardware e ECDH efêmero para atestarem suas identidades com segurança. No Mac, esses dados são protegidos pelo Secure Enclave; no Magic Keyboard com Touch ID, esses dados são protegidos pelo bloco PKA. Depois de emparelhar com segurança, todos os dados do Touch ID comunicados entre o Mac e o Magic Keyboard com Touch ID são criptografados por AES-GCM com uma chave de 256 bits de comprimento e com chaves ECDH efêmeras que usam a curva NIST P-256 baseada nas identidades armazenadas (o pressionamento normal de teclas é comunicado usando a segurança do Bluetooth da mesma forma que em qualquer teclado Bluetooth).

Intenção segura de emparelhamento

Para realizar algumas operações de Touch ID pela primeira vez, como registrar uma impressão digital nova, o usuário deve confirmar fisicamente sua intenção de usar um Magic Keyboard com Touch ID com o Mac. A intenção física é confirmada ao pressionar o botão de força do Mac duas vezes quando solicitado pela interface de usuário ou ao corresponder com sucesso uma impressão digital anteriormente registrada no Mac. Para obter mais informações, consulte Intenção de segurança e conexões ao Secure Enclave.

Transações do Apple Pay podem ser autorizadas com uma correspondência do Touch ID ou ao digitar a senha de usuário do macOS e pressionar o botão do Touch ID duas vezes no Magic Keyboard com Touch ID. Essa última maneira permite que o usuário confirme a intenção física mesmo sem uma correspondência do Touch ID.

Segurança do canal do Magic Keyboard com Touch ID

Para ajudar a garantir um canal de comunicação seguro entre o sensor do Touch ID no Magic Keyboard com Touch ID e o Secure Enclave no Mac emparelhado, exige-se o seguinte:

- Um emparelhamento seguro entre o bloco PKA do Magic Keyboard com Touch ID e o Secure Enclave conforme descrito acima
- Um canal seguro entre o sensor do Magic Keyboard com Touch ID e seu bloco PKA

O canal seguro entre o sensor do Magic Keyboard com Touch ID e seu bloco PKA é estabelecido na fábrica ao usar uma chave exclusiva compartilhada por ambos. (Essa é a mesma técnica usada para criar o canal seguro entre o Secure Enclave no Mac e seu sensor integrado, no caso de computadores Mac com Touch ID integrado.)

Face ID, Touch ID, códigos e senhas

Para usar o Face ID ou o Touch ID, os usuários devem configurar o dispositivo para que um código ou uma senha sejam exigidos para desbloqueá-lo. Quando o Face ID ou o Touch ID fazem uma identificação bem-sucedida, o dispositivo do usuário é desbloqueado sem solicitar o código ou a senha. Isso faz com que o uso de um código ou uma senha mais longa e complexa seja mais prático, já que os usuários não precisam digitá-los com tanta frequência. O Face ID e o Touch ID não substituem o código ou a senha do usuário; em vez disso, eles oferecem acesso fácil ao dispositivo dentro de limites e restrições de tempo cuidadosamente considerados. Isso é importante porque um código ou uma senha forte formam a base de como o iPhone, iPad, Mac ou Apple Watch protegem criptograficamente os dados desse usuário.

Quando um código ou senha do dispositivo são exigidos

Usuários podem usar um código ou senha a qualquer momento em vez do Face ID ou Touch ID, mas há algumas situações em que a biometria não é permitida. As seguintes operações relacionadas à segurança sempre exigem a inserção de um código ou senha:

- Atualização do software
- Apagamento do dispositivo
- Visualização ou alteração dos ajustes de código
- Instalação de perfis de configuração
- Desbloqueio do painel de Segurança e Privacidade nas Preferências do Sistema do Mac
- Desbloqueio do painel de Usuários e Grupos nas Preferências do Sistema do Mac (se o FileVault estiver ativado)

Também é necessário um código ou senha se o dispositivo estiver em qualquer um dos estados seguintes:

- O dispositivo acabou de ser ligado ou reiniciado.
- O usuário encerrou a sessão no Mac (ou ainda não iniciou uma sessão).
- O usuário não desbloqueou o dispositivo por mais de 48 horas.
- O usuário não usou o código ou senha para desbloquear o dispositivo nas últimas 156 horas (seis dias e meio) e o usuário não usou biometria para desbloquear o dispositivo nas últimas 4 horas.
- O dispositivo recebeu um comando de bloqueio remoto.
- O usuário manteve pressionado um dos botões de volume e o botão Repousar/Despertar simultaneamente por 2 segundos e pressionou Cancelar para sair do desligamento/SOS de Emergência.
- Houve cinco tentativas malsucedidas de identificação biométrica (embora, por motivos de usabilidade, o dispositivo possa oferecer a possibilidade de digitação do código ou senha em vez do uso de biometria após um número menor de falhas).

Quando o Face ID com máscara está ativado em um iPhone, ele fica disponível nas próximas 6,5 horas após uma das seguintes ações do usuário:

- Tentativa bem-sucedida de identificação com Face ID (com ou sem máscara)
- Validação do código do dispositivo
- Desbloqueio do dispositivo com o Apple Watch

Quando realizada, qualquer uma dessas ações estende o período por mais 6,5 horas.

Quando o Face ID ou o Touch ID estão ativados no iPhone ou iPad, o dispositivo é bloqueado imediatamente quando o botão Repousar/Despertar é pressionado e sempre que entra em repouso. O Face ID e o Touch ID exigem uma identificação bem-sucedida — ou, opcionalmente, o código — sempre que o dispositivo sai do repouso.

A probabilidade de que uma pessoa aleatória na população possa desbloquear o iPhone ou iPad de um usuário é de menos que 1 em 1.000.000 com o Face ID, incluindo quando o Face ID com máscara está ativado. No caso do iPhone, iPad, modelos de Mac com Touch ID e aqueles com um Magic Keyboard emparelhado, é de menos que 1 em 50.000. Essa probabilidade aumenta quando há várias impressões digitais registradas (até 1 em 10.000 com cinco impressões digitais) ou visuais (até 1 em 500.000 com dois registros visuais). Para ter mais proteção, o Face ID e o Touch ID permitem apenas cinco tentativas malsucedidas de identificação antes que um código ou senha sejam exigidos para obter acesso ao dispositivo ou conta do usuário. Com o Face ID, a probabilidade de uma identificação falsa é maior no caso de:

- Gêmeos e irmãos que se parecem com o usuário
- Crianças com menos de 13 anos (pois suas características faciais distintas podem não ter se desenvolvido completamente)

A probabilidade aumenta ainda mais nesses dois casos quando o Face ID com máscara é usado. Caso uma correspondência falsa seja um motivo de preocupação para um usuário, a Apple recomenda o uso de um código para autenticação.

Segurança da identificação facial

A identificação facial é realizada dentro do Secure Enclave e usa redes neurais treinadas especificamente para esse propósito. Ao desenvolver as redes neurais de identificação facial, a Apple usou mais de um bilhão de imagens, incluindo imagens infravermelhas (IR) e de profundidade coletadas em estudos realizados com o consentimento informado dos participantes. Em seguida a Apple trabalhou com participantes do mundo todo para incluir um grupo expressivo de pessoas levando em conta gênero, idade, etnia e outros fatores. Os estudos foram ampliados conforme o necessário para fornecer um alto grau de precisão para uma ampla gama de usuários. O Face ID foi projetado para funcionar com chapéus, cachecóis, óculos, lentes de contato e muitos tipos de óculos escuros. O Face ID também permite o desbloqueio com máscara em dispositivos iPhone a partir do iPhone 12 e iOS 15.4 ou posterior. Além disso, ele foi projetado para funcionar em ambientes fechados, ambientes abertos e até na escuridão total. Uma rede neural adicional — treinada para identificar e resistir a enganos — defende o dispositivo contra tentativas de desbloqueio com fotos ou máscaras. Os dados do Face ID, incluindo as representações matemáticas do rosto do usuário, são criptografados e disponibilizados somente para o Secure Enclave. Os dados nunca saem do dispositivo. Eles não são enviados à Apple nem incluídos nos backups do dispositivo. Os seguintes dados do Face ID são salvos, criptografados somente para uso pelo Secure Enclave, durante a operação normal:

- As representações matemáticas do rosto do usuário, calculadas durante o registro
- As representações matemáticas do rosto do usuário, calculadas durante algumas tentativas de desbloqueio caso o Face ID as julgue necessárias para melhorar a identificação futura

As imagens de rosto capturadas durante a operação normal não são salvas, e sim imediatamente descartadas depois da representação matemática ser calculada — tanto para o registro inicial quanto para a comparação com os dados do Face ID registrados.

Aprimoramento da identificação do Face ID

Para aprimorar o desempenho da identificação e acompanhar as mudanças naturais de um rosto e da aparência, o Face ID amplia sua representação matemática com o passar do tempo. A partir da identificação bem-sucedida, o Face ID pode usar a nova representação matemática calculada (se sua qualidade for suficiente) para um número finito de identificações adicionais antes de descartar esses dados. Reciprocamente, se o Face ID não conseguir reconhecer um rosto, mas a qualidade da identificação for superior a um certo limite e o usuário digitar o código imediatamente após o não reconhecimento, o Face ID faz uma outra captura e amplia os dados do Face ID registrados com a nova representação matemática calculada. Esses novos dados do Face ID são descartados se o usuário parar de ser identificado com eles ou após um número finito de identificações. Os novos dados também são descartados quando a opção para redefinir o Face ID está selecionada. Esses processos de ampliação permitem que o Face ID acompanhe mudanças dramáticas em pelos faciais ou no uso de maquiagem por parte de um usuário, ao mesmo tempo que minimiza a aceitação falsa.

Usos do Face ID e Touch ID

Desbloqueio de um dispositivo ou conta de usuário

Com o Face ID ou o Touch ID desativados, ao bloquear um dispositivo ou conta, as chaves das classes mais altas da Proteção de Dados (mantidas no Secure Enclave) são descartadas. Os arquivos e os itens das chaves dessa classe ficam inacessíveis até que o usuário digite o código ou a senha para desbloquear o dispositivo ou a conta.

Com o Face ID ou o Touch ID ativados, as chaves não são descartadas quando o dispositivo ou a conta são bloqueados. Ao invés disso, elas são embaladas com uma chave fornecida ao subsistema do Face ID ou Touch ID dentro do Secure Enclave. Quando um usuário tenta desbloquear o dispositivo ou a conta, caso o dispositivo detecte uma identificação bem-sucedida, ele fornece a chave para desembalar as chaves de Proteção de Dados, desbloqueando o dispositivo ou a conta. Esse processo fornece proteção adicional ao exigir a cooperação entre a Proteção de Dados e os subsistemas do Face ID ou Touch ID para desbloquear o dispositivo.

Quando o dispositivo é reinicializado, as chaves exigidas pelo Face ID ou Touch ID para desbloquear o dispositivo ou a conta são perdidas. Elas são descartadas pelo Secure Enclave caso qualquer condição que exija a digitação do código ou senha seja atendida.

Proteção de compras com o Apple Pay

O usuário também pode usar o Face ID e o Touch ID com o Apple Pay para fazer compras em lojas, apps e na web de maneira fácil e segura:

- *Usando o Face ID em lojas:* para autorizar um pagamento em uma loja com o Face ID, primeiro o usuário precisa pressionar o botão lateral duas vezes para confirmar a intenção de fazer o pagamento. Isso captura a intenção do usuário com um gesto físico diretamente relacionado ao Secure Enclave, o que é invulnerável à falsificação por parte de um processo malicioso. Depois, o usuário usa o Face ID para autenticar antes de aproximar o dispositivo do leitor de pagamento por proximidade. Um método de pagamento diferente do Apple Pay pode ser selecionado após a autenticação com o Face ID, o que requer uma nova autenticação, mas o usuário não precisará pressionar novamente o botão lateral duas vezes.
- *Usando o Face ID em apps e na web:* para fazer um pagamento dentro de apps ou na web, o usuário precisa pressionar o botão lateral duas vezes para confirmar a intenção de pagar e autenticar com o Face ID para autorizar o pagamento. Se a transação do Apple Pay não for concluída em 60 segundos depois do botão lateral ter sido pressionado duas vezes, o usuário deve fazer isso novamente para reconfirmar a intenção de pagar.
- *Usando o Touch ID:* com o Touch ID, a intenção de pagar é confirmada com o gesto de ativação do sensor do Touch ID combinado à identificação bem-sucedida da impressão digital do usuário.

Uso das APIs fornecidas pelo sistema

Apps de terceiros podem usar as APIs fornecidas pelo sistema para solicitar que o usuário use o Face ID, o Touch ID, um código ou uma senha para autenticar. Os apps que oferecem suporte ao Touch ID são automaticamente compatíveis com o Face ID sem que nenhuma alteração seja necessária. Ao usar o Face ID ou o Touch ID, o app recebe uma notificação apenas quanto ao êxito da autenticação; ele não pode acessar o Face ID, o Touch ID ou os dados associados ao usuário registrado.

Proteção de itens das chaves

Os itens das chaves também podem ser protegidos pelo Face ID ou Touch ID, sendo liberados pelo Secure Enclave apenas pela identificação bem-sucedida ou com o código do dispositivo ou senha da conta. Os desenvolvedores de apps possuem APIs para verificar se um código ou uma senha foram definidos pelo usuário antes de exigir o Face ID, o Touch ID, um código ou uma senha para desbloquear itens das chaves. Desenvolvedores de apps podem fazer o seguinte:

- Exigir que as operações de autenticação da API não usem a senha de um app ou o código do dispositivo como alternativa. Eles podem consultar se um usuário está registrado, permitindo que o Face ID ou o Touch ID sejam usados como um segundo fator em apps que requerem segurança.
- Gerar e usar chaves de Criptografia de Curva Elíptica (ECC) dentro do Secure Enclave que podem ser protegidas pelo Face ID ou Touch ID. As operações com essas chaves são realizadas sempre dentro do Secure Enclave depois que ele autoriza o uso.

Realização e aprovação de compras

Os usuários também podem configurar o Face ID ou o Touch ID para aprovar compras na iTunes Store, App Store, Apple Books e outros locais, para que não precisem digitar a senha do ID Apple. Quando compras são feitas, o Secure Enclave verifica a ocorrência de uma autorização biométrica e libera então as chaves de ECC usadas para assinar o pedido da loja.

Intenção de segurança e conexões ao Secure Enclave

A intenção de segurança oferece uma maneira de confirmar a intenção de um usuário sem nenhuma interação com o sistema operacional ou Processador de Aplicativos. A conexão é um vínculo físico — de um botão físico para o Secure Enclave — que está disponível nos seguintes:

- iPhone X ou posterior
- Apple Watch Series 1 ou posterior
- iPad Pro (todos os modelos)
- iPad Air (2020)
- Computadores Mac com Apple Silicon

Com esse vínculo, usuários podem confirmar a intenção de concluir uma operação projetada de tal maneira que até um software executado com privilégios de usuário root ou no kernel não possa enganar.

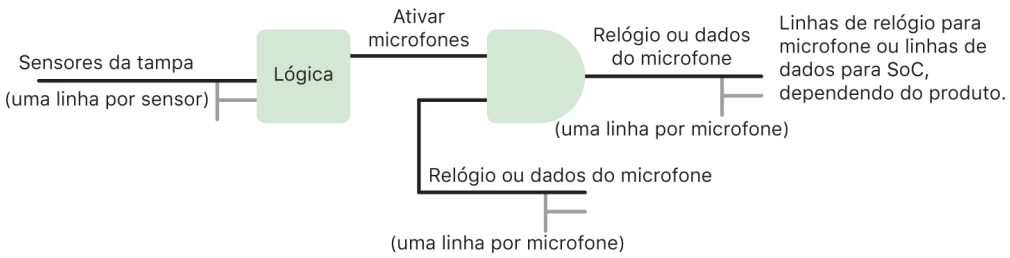
Esse recurso é usado para confirmar a intenção do usuário durante transações do Apple Pay e ao finalizar o emparelhamento do Magic Keyboard com Touch ID a um Mac com Apple Silicon. Ao pressionar duas vezes o botão apropriado (para o Face ID) ou verificar a impressão digital (para o Touch ID) quando solicitado pela interface de usuário, isso sinaliza a confirmação de intenção do usuário. Para obter mais informações, consulte Proteção de compras com o Apple Pay. Um mecanismo similar — baseado no Secure Enclave e firmware do T2 — é compatível com modelos de MacBook com o chip Apple T2 Security e sem Touch Bar.

Desconexão do microfone por hardware

Todos os notebooks Mac baseados em Apple Silicon e notebooks Mac baseados em Intel com o chip Apple T2 Security possuem uma desconexão por hardware que desativa o microfone sempre que a tampa é fechada. Em todos os notebooks MacBook Pro de 13 polegadas e MacBook Air com o chip T2, todos os notebooks MacBook com um chip T2 de 2019 ou posteriores, e notebooks Mac com Apple Silicon, essa desconexão é implementada apenas no hardware. A desconexão é projetada para impedir que qualquer software — mesmo com privilégios de usuário root ou de kernel no macOS, e até mesmo o software no chip T2 ou outro firmware — acione o microfone enquanto a tela estiver fechada (a câmera não é desconectada no hardware porque seu campo de visão fica totalmente obstruído com a tela fechada).

Os modelos de iPad a partir de 2020 também apresentam a desconexão do microfone por hardware. Quando uma capa em conformidade com MFi (incluindo aquelas vendidas pela Apple) é conectada ao iPad e fechada, o microfone é desconectado no hardware. Isso é projetado para impedir que dados de áudio do microfone sejam disponibilizados para qualquer software — mesmo com privilégios de usuário root ou de kernel no iPadOS ou em qualquer firmware do dispositivo.

As proteções nesta seção são implementadas diretamente com lógica de hardware, de acordo com o seguinte digrama de circuitos:



Em cada produto com um corte de hardware do microfone, um ou mais sensores na tela detectam o fechamento físico da tela ou da capa através de alguma propriedade física (um sensor de efeito Hall ou sensor de ângulo da dobradiça, por exemplo) da interação. Em sensores onde a calibragem é necessária, os parâmetros são definidos durante a produção do dispositivo e o processo de calibragem inclui um bloqueio de hardware não reversível que impede qualquer alteração subsequente aos parâmetros sensíveis do sensor. Esses sensores emitem um sinal de hardware direto que passa por um conjunto simples de lógica de hardware não reprogramável. Essa lógica fornece detecção de oscilação, histerese e/ou um atraso de até 500 ms antes de desativar o microfone. Dependendo do produto, esse sinal pode ser implementado ao desativar as linhas que transportam os dados entre o microfone e o Sistema no Chip (SoC) ou ao desativar uma das linhas de entrada do módulo do microfone que o permitem estar ativado, como, por exemplo, a linha do relógio ou um controle efetivo similar.

Cartões Expressos com reserva de energia

Se o iOS não estiver sendo executado porque o iPhone precisa ser carregado, talvez ainda haja energia suficiente na bateria para permitir transações de Cartões Expressos. Dispositivos iPhone compatíveis com este recurso aceitam:

- Um cartão de pagamento ou transporte público designado como o cartão de Transporte Público Expresso
- Carteiras de Estudante com o Modo Expresso ativado
- Chaves de carro com o Modo Expresso ativado
- Chaves de casa com o Modo Expresso ativado
- Cartões de acesso corporativo ou a hotéis com o Modo Expresso ativado

Ao pressionar o botão lateral (ou, no iPhone SE 2ª geração, o botão de Início), o ícone de bateria fraca aparece, bem como o texto indicando que há Cartões Expressos disponíveis para uso. O controlador NFC realiza transações de Cartões Expressos sob as mesmas condições de quando o iOS é executado, exceto pelo fato de as transações serem indicadas somente por uma notificação tátil (nenhuma notificação visível é mostrada). No iPhone SE 2ª geração, as transações concluídas podem demorar alguns segundos para aparecer na tela. Esse recurso não fica disponível quando um desligamento padrão é iniciado pelo usuário.

Segurança do sistema

Visão geral da segurança do sistema

Aproveitando os recursos exclusivos do hardware da Apple, a segurança do sistema é projetada para controlar o acesso aos recursos do sistema operacional em dispositivos Apple sem comprometer a usabilidade. A segurança do sistema abrange o processo de inicialização, as atualizações de software e a proteção dos recursos do sistema do computador, como CPU, memória, disco, programas de software e dados armazenados.

As versões mais recentes dos sistemas operacionais da Apple são as mais seguras. Uma parte importante da segurança da Apple é a *inicialização segura*, que protege o sistema contra infecções de malware no momento da inicialização. A inicialização segura começa no hardware e constrói uma cadeia de confiança pelo software, na qual cada etapa é projetada para garantir que a seguinte esteja funcionando corretamente antes de ceder o controle. Este modelo de segurança funciona não apenas na inicialização padrão de dispositivos Apple, mas também nos diversos modos de recuperação e atualizações pontuais em dispositivos Apple. Subcomponentes, como o chip T2 e o Secure Enclave, também realizam suas próprias inicializações seguras para ajudar a garantir que eles inicializem apenas código validado pela Apple. O sistema de atualização é projetado para impedir ataques de reversão, para que os dispositivos não possam voltar a uma versão mais antiga do sistema operacional (a qual um invasor saiba como comprometer) como método de roubar os dados do usuário.

Os dispositivos Apple também incluem proteções de inicialização e tempo de execução para que mantenham a integridade durante a operação. O silício projetado pela Apple no iPhone, iPad, Apple Watch, Apple TV, HomePod e Mac com Apple Silicon oferece uma arquitetura comum para proteger a integridade do sistema operacional. O macOS também oferece um conjunto configurável de capacidades de proteção compatíveis com seu modelo computacional diferente, assim como capacidades compatíveis com todas as plataformas do hardware Mac.

Inicialização segura

Processo de inicialização de dispositivos iOS e iPadOS

Cada etapa do processo de inicialização contém componentes assinados criptograficamente pela Apple para permitir a verificação da integridade, para que a inicialização prossiga somente após a verificação da cadeia de confiança. Esses componentes incluem gerenciadores de inicialização, kernel, extensões do kernel e firmware de banda base celular. Essa cadeia de inicialização é projetada para verificar que os níveis mais baixos do software não foram adulterados.

Quando um dispositivo iOS ou iPadOS é ligado, o Processador de Aplicativos executa imediatamente o código da memória somente leitura, chamada de ROM de Inicialização. Esse código imutável, conhecido como *raiz de confiança do hardware*, é colocado durante a fabricação do chip e é implicitamente confiável. O código da ROM de Inicialização contém a chave pública da autoridade de certificação (AC) de Raiz da Apple, usada para verificar se o gerenciador de inicialização iBoot está assinado pela Apple antes de permitir que ele seja carregado. Esse é o primeiro passo na cadeia de confiança, na qual cada passo verifica que o próximo esteja assinado pela Apple. Ao terminar suas tarefas, o iBoot verifica e executa o kernel do iOS ou iPadOS. Em dispositivos com processador A9 ou anterior da série A, um estágio adicional do Gerenciador de Inicialização de Baixo Nível (LLB) é carregado e verificado pela ROM de Inicialização, que por sua vez, carrega e verifica o iBoot.

Problemas de carregamento ou verificação dos estágios seguintes são tratados de modo diferente conforme o hardware:

- *O ROM de Inicialização não consegue carregar LLB (dispositivos mais antigos):* modo de Atualização do Firmware do Dispositivo (DFU)
- *LLB ou iBoot:* modo de Recuperação

Nos dois casos, o dispositivo deve estar conectado ao Finder (macOS 10.15 ou posterior) ou iTunes (no macOS 10.14 ou anterior) via USB e ser restaurado aos ajustes padrão de fábrica.

O Registro de Progresso de Inicialização (BPR) é usado pelo Secure Enclave para limitar o acesso a dados de usuário em diversos modos e é atualizado antes de entrar nos modos a seguir:

- *Modo DFU:* definido pela ROM de Inicialização em dispositivos com o A12 ou SoCs posteriores da Apple
- *Modo de recuperação:* definido pelo iBoot em dispositivos com o A10, S2 ou SoCs posteriores da Apple

Em dispositivos com acesso celular, um subsistema de banda base celular também realiza uma inicialização segura adicional ao usar software e chaves assinadas verificadas pelo processador de banda base.

O Secure Enclave também realiza uma inicialização segura que verifica que seu software (sepOS) está verificado e assinado pela Apple.

Implementação do iBoot em memória segura

No iOS 14 e iPadOS 14, a Apple modificou a cadeia de ferramentas do compilador C usada para construir o gerenciador de inicialização do iBoot para melhorar sua segurança. A cadeia de ferramentas modificada implementa código projetado para impedir problemas de segurança de memória e tipo, encontrados normalmente em programas C. Por exemplo, ela ajuda a impedir a maioria das vulnerabilidades nas seguintes classes:

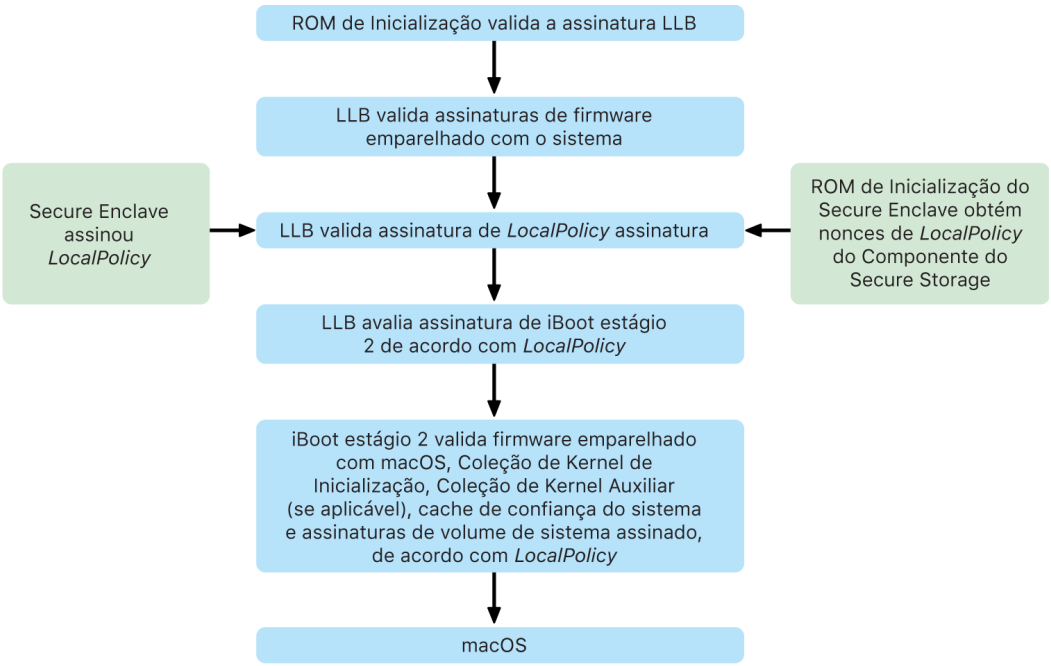
- Sobrecargas de buffer, ao garantir que todos os indicadores carreguem informações de limites verificadas ao acessar a memória
- Exploração da heap, ao separar os dados da heap de seus metadados e detectar condições de erros com precisão, como áreas livres duplas
- Confusão de tipo, ao garantir que todos os indicadores carreguem informações de tipo de tempo de execução verificadas durante as operações de seleção do indicador
- Confusão de tipo causada por erros “usar depois de livre”, ao segregar todas as alocações de memória dinâmica por tipo estático

Essa tecnologia está disponível no iPhone com o Apple A13 Bionic ou posterior e no iPad com o chip A14 Bionic.

Computadores Mac com Apple Silicon

Processo de inicialização para um Mac com Apple Silicon

Quando um Mac com Apple Silicon é ligado, ele realiza um processo de inicialização bem parecido ao do iPhone e iPad.



O chip executa o código da ROM de Inicialização no primeiro passo da cadeia de confiança. A inicialização segura do macOS em um Mac com Apple Silicon verifica não apenas o código do sistema operacional em si, como também as políticas de segurança e até kexts (compatíveis, embora não recomendados) configurados por usuários autorizados.

Quando o LLB (que significa Gerenciador de Inicialização de Baixo Nível) é aberto, ele verifica as assinaturas e carrega os firmwares emparelhados com o sistema de núcleos do intra-SoC, como armazenamento, tela, gerenciamento do sistema e controladores Thunderbolt. O LLB também é responsável por carregar a LocalPolicy, que é um arquivo assinado pelo Processador do Secure Enclave. O arquivo LocalPolicy descreve a configuração escolhida pelo usuário para as políticas de inicialização do sistema e de segurança do tempo de execução. A LocalPolicy tem o mesmo formato de estrutura de dados de todos os outros objetos de inicialização, mas ela é assinada localmente por uma chave privada que está disponível somente dentro do Secure Enclave de um computador em particular, em vez de ser assinada por um servidor central da Apple (como atualizações de software).

Para ajuda a impedir a reprodução de qualquer LocalPolicy anterior, o LLB deve buscar um nonce do Componente de Armazenamento Seguro anexado ao Secure Enclave. Para fazer isso, ele usa a ROM de Inicialização do Secure Enclave e verifica se o nonce na LocalPolicy coincide com o nonce no Componente de Armazenamento Seguro. Isso ajuda a impedir que uma LocalPolicy antiga, que poderia estar configurada para uma segurança mais baixa, seja reaplicada ao sistema depois da segurança ser atualizada. Como consequência, a inicialização segura em um Mac com Apple Silicon ajuda a proteger não apenas contra a reversão das versões do sistema operacional, como também contra a reversão da política de segurança.

O arquivo LocalPolicy captura se o sistema operacional está configurado para segurança Total, Reduzida ou Permissiva.

- *Segurança Total:* o sistema se comporta como o iOS e iPadOS, e permite a inicialização apenas do software sabidamente mais recente disponível no momento da instalação.
- *Segurança Reduzida:* o LLB é direcionado a confiar em assinaturas “globais” incluídas com o sistema operacional. Isso permite que o sistema execute versões mais antigas do macOS. Como versões mais antigas do macOS inevitavelmente têm vulnerabilidades não corrigidas, esse modo é descrito como segurança *Reduzida*. Esse também é o nível de política exigido para oferecer suporte à inicialização de extensões do kernel (kexts).
- *Segurança Permissiva:* o sistema se comporta como a Segurança Reduzida, já que usa a verificação de assinatura global para o iBoot e outros, mas também instrui o iBoot a aceitar alguns objetos de inicialização sendo assinados pelo Secure Enclave com a mesma chave usada para assinar a LocalPolicy. Esse nível de política oferece suporte a usuários que compilam, assinam e inicializam seus próprios kernels XNU personalizados.

Se a LocalPolicy indicar ao LLB que o sistema operacional selecionado está sendo executado em Segurança Total, o LLB avalia a assinatura personalizada do iBoot. Se o sistema operacional estiver sendo executado em Segurança Reduzida ou Segurança Permissiva, ele avalia a assinatura global. Qualquer erro de verificação de assinatura faz com que o sistema seja inicializado no recoveryOS para oferecer opções de reparo.

Depois que o LLB passa para o iBoot, ele carrega os firmwares emparelhados com o macOS, como aqueles para o Mecanismo Neural Seguro, o Processador Sempre Ativo e outros firmwares. O iBoot também analisa as informações sobre a LocalPolicy passadas a ele pelo LLB. Se a LocalPolicy indicar a possível existência de uma Coleção do Kernel Auxiliar (AuxKC), o iBoot a procura no sistema de arquivos, verifica que ela foi assinada pelo Secure Enclave com a mesma chave da LocalPolicy e verifica que seu hash coincide com um hash armazenado na LocalPolicy. Se a AuxKC for verificada, o iBoot a coloca na memória com a Coleção do Kernel de Inicialização antes de bloquear toda a região da memória que abrange a Coleção do Kernel de Inicialização e a AuxKC com a Proteção da Integridade do Coprocessador do Sistema (SCIP). Se a política indicar que uma AuxKC deveria estar presente, mas ela não for encontrada, o sistema continua a inicializar no macOS sem a AuxKC. O iBoot também é responsável por verificar o hash raiz do volume de sistema assinado (SSV) para verificar que o sistema de arquivos a ser montado pelo kernel tenha sua integridade totalmente verificada.

Modos de inicialização para um Mac com Apple Silicon

Um Mac com Apple Silicon possui os modos de inicialização descritos abaixo.

Modo	Combinação de teclas	Descrição
macOS	De um estado desligado, pressione e **solte** o botão de força.	1. A ROM de Inicialização passa para o LLB. 2. O LLB carrega os firmwares emparelhados com o sistema e a LocalPolicy do macOS selecionado. 3. O LLB bloqueia uma indicação no Registro de Progresso de Inicialização (BPR) de que ele está inicializando no macOS e passa para o iBoot. 4. O iBoot carrega os firmwares emparelhados com o macOS, o cache de confiança estático, a árvore do dispositivo e a Coleção do Kernel de Inicialização. 5. Se a LocalPolicy permitir, o iBoot carrega a Coleção do Kernel Auxiliar (AuxKC) de kexts de terceiros. 6. Se a LocalPolicy não a tiver desativado, o iBoot verifica o hash de assinatura raiz do volume de sistema assinado (SSV).
recoveryOS emparelhado	De um estado desligado, mantenha o botão de força **pressionado**.	1. A ROM de Inicialização passa para o LLB. 2. O LLB carrega os firmwares emparelhados com o sistema e a LocalPolicy do recoveryOS selecionado. 3. O LLB bloqueia uma indicação no Registro de Progresso de Inicialização de que ele está inicializando no recoveryOS emparelhado e passa para o iBoot do recoveryOS emparelhado. 4. O iBoot carrega os firmwares emparelhados com o macOS, o cache de confiança, a árvore do dispositivo e a Coleção do Kernel de Inicialização. 5. Se ocorrer um erro na inicialização do recoveryOS emparelhado, é feita uma tentativa de inicializar no recoveryOS Alternativo. *Nota:* reversões de segurança não são permitidas na LocalPolicy do recoveryOS emparelhado.

Modo	Combinação de teclas	Descrição
recoveryOS Alternativo	De um estado desligado, **pressione o botão de força duas vezes e mantenha-o pressionado**.	1. A ROM de Inicialização passa para o LLB. 2. O LLB carrega os firmwares emparelhados com o sistema e a LocalPolicy do recoveryOS selecionado. 3. O LLB bloqueia uma indicação no Registro de Progresso de Inicialização de que ele está inicializando no recoveryOS emparelhado e passa para o iBoot do recoveryOS. 4. O iBoot carrega os firmwares emparelhados com o macOS, o cache de confiança, a árvore do dispositivo e a Coleção do Kernel de Inicialização. *Nota:* reversões de segurança não são permitidas na LocalPolicy do recoveryOS emparelhado.
Modo Seguro	Inicialize no recoveryOS como acima e mantenha a tecla **Shift** pressionada ao selecionar o volume de inicialização.	1. Inicialize no recoveryOS como acima. 2. Manter a tecla Shift pressionada ao selecionar um volume faz com que o app BootPicker aprove o macOS para inicialização, como normalmente, mas também define uma variável `nvram` que diz ao iBoot para não carregar a AuxKC na próxima inicialização. 3. O sistema é reinicializado e inicializa no volume de destino selecionado, mas o iBoot não carrega a AuxKC.

Restrições do recoveryOS emparelhado

No macOS 12.0.1 ou posterior, toda nova instalação do macOS também instala uma versão emparelhada do recoveryOS no grupo de volumes APFS correspondente. Esse projeto é conhecido pelos usuários de computadores Mac com processador Intel, mas no Mac com Apple Silicon, ele fornece segurança adicional e garantias de compatibilidade. Como toda instalação do macOS agora possui um recoveryOS emparelhado dedicado, isso ajuda a assegurar que somente esse recoveryOS emparelhado dedicado possa realizar operações de reversão de segurança. Isso ajuda a proteger as instalações de novas versões do macOS contra adulterações iniciadas a partir de versões mais antigas do macOS e vice-versa.

As restrições de emparelhamento são aplicadas da seguinte forma:

- Todas as instalações do macOS 11 são emparelhadas com o recoveryOS. Se uma instalação do macOS 11 estiver selecionada para inicializar por padrão, deve-se manter pressionada a tecla de força durante a inicialização em um Mac com Apple Silicon para inicializar no recoveryOS. O recoveryOS pode reverter os ajustes de segurança de qualquer instalação do macOS 11, mas não de uma instalação do macOS 12.0.1.
- Se uma instalação do macOS 12.0.1 ou posterior estiver selecionada para inicializar por padrão, deve-se manter pressionada a tecla de força durante a inicialização em um Mac com Apple Silicon para inicializar no recoveryOS emparelhado. O recoveryOS emparelhado pode reverter os ajustes de segurança da instalação do macOS emparelhado, mas não de nenhuma outra instalação do macOS.

Para inicializar em um recoveryOS emparelhado em qualquer instalação do macOS, essa instalação precisa estar selecionada como padrão, o que é feito em “Disco de Inicialização” nas Preferências do Sistema ou ao inicializar qualquer recoveryOS e manter Option pressionada ao selecionar um volume.

Nota: o recoveryOS Alternativo não pode realizar reversões de segurança em nenhuma instalação do macOS.

Controle da política de segurança do Disco de Inicialização para um Mac com Apple Silicon

Visão geral

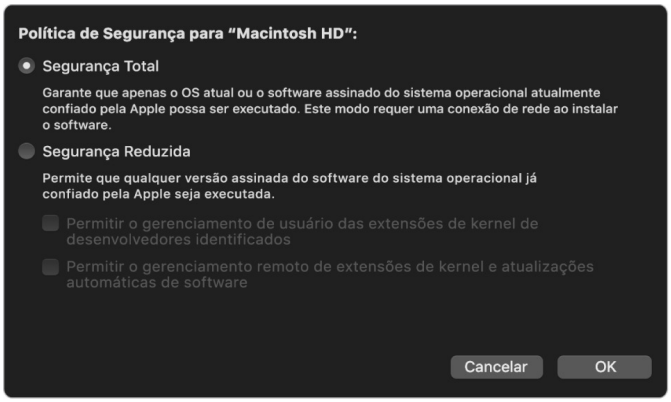
Ao contrário das políticas de segurança em um Mac baseado em Intel, as políticas de segurança em um Mac com Apple Silicon destinam-se a cada sistema operacional instalado. Isso significa que há suporte para várias instâncias instaladas do macOS com versões e políticas de segurança diferentes no mesmo Mac. Por esse motivo, um *seletor de sistema operacional* foi adicionado ao Utilitário de Segurança da Inicialização.

Em um Mac com Apple Silicon, o Utilitário de Segurança do Sistema indica o estado de segurança geral do macOS configurado pelo usuário, como a inicialização de um kext ou a configuração da Proteção da Integridade do Sistema (SIP). Se a alteração de um ajuste de segurança degradar significativamente a segurança ou fizer com que seja mais fácil comprometer o sistema, usuários devem manter o botão de força pressionado (para que apenas um humano com acesso físico possa acionar o sinal, e não um malware) para entrar no recoveryOS e fazer a alteração. Por esse motivo, um Mac baseado em Apple Silicon também não exigirá (nem oferecerá suporte) a uma senha de firmware — todas as alterações críticas já são protegidas pela autorização do usuário. Para obter mais informações sobre a SIP, consulte Proteção da Integridade do Sistema.

As opções de Segurança Total e Segurança Reduzida podem ser definidas ao usar o Utilitário de Segurança da Inicialização a partir do recoveryOS. Mas a Segurança Permissiva pode ser acessada apenas a partir das ferramentas de linha de comando por usuários que aceitem o risco de deixar o Mac muito menos seguro.

Política de Segurança Total

A Segurança Total é o padrão e se comporta como o iOS e iPadOS. Quando um software é baixado e está pronto para ser instalado, em vez de usar a assinatura global fornecida com o software, o macOS contata o mesmo servidor de assinatura da Apple usado para o iOS e iPadOS, e solicita uma nova assinatura "personalizada". Uma assinatura é personalizada quando ela inclui a Identificação Exclusiva de Chip (ECID) — um ID exclusivo específico à CPU da Apple neste caso — como parte do pedido de assinatura. Dessa forma, a assinatura retornada pelo servidor de assinatura é exclusiva e pode ser usada apenas por essa CPU da Apple específica. Quando a política Segurança Total está em vigor, a ROM de Inicialização e o LLB ajudam a garantir que uma determinada assinatura não esteja apenas assinada pela Apple, mas também assinada para esse Mac específico, essencialmente vinculando essa versão do macOS a esse Mac.

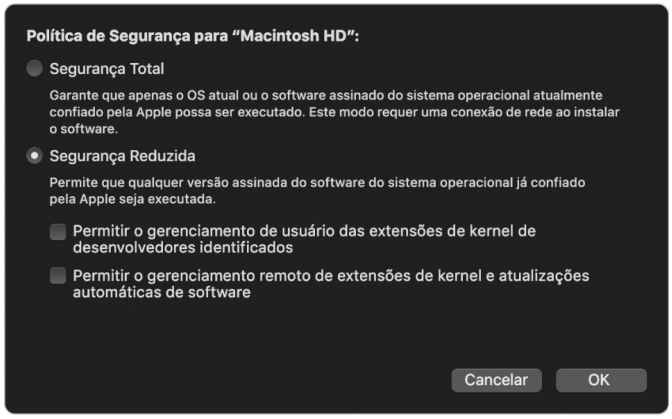


O uso de um servidor de assinatura on-line também oferece uma proteção melhor contra ataques com versões anteriores em comparação a abordagens típicas de assinatura global. Em um sistema de assinatura global, o período de segurança pode ter sido ultrapassado diversas vezes, mas um sistema que nunca viu o firmware mais recente não sabe disso. Por exemplo, um computador que acredite estar no período de segurança 1 aceita software do período de segurança 2, mesmo que o período atual de segurança seja 5. Com um sistema de assinatura on-line do Apple Silicon, o servidor de assinatura pode recusar a criação de assinaturas para softwares que não estejam no período de segurança mais recente.

Além disso, se um invasor descobrir uma vulnerabilidade após uma alteração do período de segurança, ele não pode simplesmente pegar o software vulnerável de um período anterior no sistema A e aplicá-lo ao sistema B para atacá-lo. O fato de que o software vulnerável de um período anterior foi personalizado para o sistema A ajuda a impedir que ele seja transferido e usado para atacar um sistema B. Todos esses mecanismos trabalham em conjunto para fornecer garantias muito maiores para que invasores não possam colocar intencionalmente softwares vulneráveis em um Mac para contornar as proteções oferecidas pelo software mais recente. Mas um usuário que possua um nome de usuário e senha de administrador do Mac sempre pode escolher a política de segurança que se encaixe melhor aos seus casos de uso.

Política de Segurança Reduzida

A Segurança Reduzida é similar ao comportamento da Segurança Média em um Mac baseado em Intel com um chip T2, no qual um fornecedor (neste caso, a Apple) gera uma assinatura digital para o código para aferir a procedência do devido fornecedor. Esse design ajuda a impedir que invasores insiram um código sem assinatura. A Apple chama essa assinatura de "global", pois ela pode ser usada em qualquer Mac, por qualquer período, em um Mac que tenha um conjunto de políticas de Segurança Reduzida definido no momento. A segurança reduzida, em si, não oferece proteção contra ataques de reversão (embora alterações não autorizadas ao sistema operacional possam resultar na inacessibilidade aos dados de usuário). Para obter mais informações, consulte Extensões do kernel em um Mac com Apple Silicon.

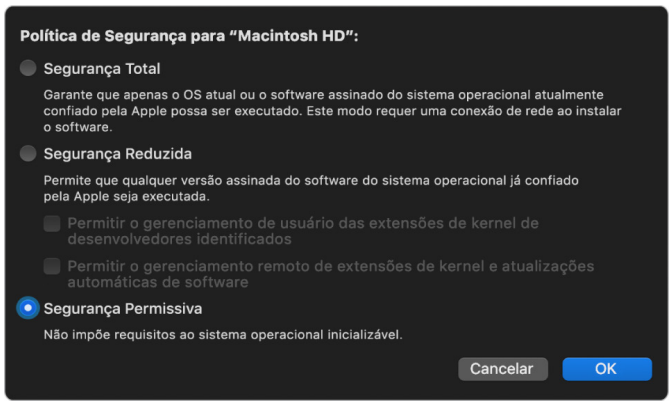


Além de permitir que usuários executem versões mais antigas do macOS, a Segurança Reduzida é exigida por outras ações que possam colocar a segurança do sistema do usuário em risco, como a introdução de extensões de kernel de terceiros (kexts). Kexts têm os mesmos privilégios do kernel e, portanto, qualquer vulnerabilidade em kexts de terceiros pode levar ao comprometimento do sistema operacional inteiro. É por esse motivo que desenvolvedores são fortemente encorajados a adotar extensões do sistema, antes que a compatibilidade com kexts seja removida do macOS em futuros computadores Mac com Apple Silicon. Até mesmo quando kexts de terceiros estão ativados, eles não podem ser carregados no kernel sob demanda. Em vez disso, os kexts são combinados em uma Coleção do Kernel Auxiliar (AuxKC), cujo hash é armazenado na LocalPolicy, exigindo assim, uma reinicialização. Para obter mais informações sobre a geração da AuxKC, consulte Extensões do kernel no macOS.

Política de Segurança Permissiva

A Segurança Permissiva destina-se a usuários que aceitam o risco de colocar o Mac em um estado muito mais inseguro. Esse modo difere do modo Sem Segurança em um Mac baseado em Intel com um chip T2. Com a Segurança Permissiva, a verificação de assinatura ainda é realizada ao longo de toda a cadeia de inicialização de segurança, mas a definição da política como Permissiva indica ao iBoot que ele deve aceitar objetos de inicialização assinados localmente pelo Secure Enclave, como uma Coleção do Kernel de Inicialização gerada pelo usuário, construída a partir de um kernel XNU personalizado. Dessa maneira, a Segurança Permissiva também fornece uma capacidade de arquitetura para executar um kernel arbitrário do tipo "sistema operacional totalmente não confiável". Quando uma Coleção do Kernel de Inicialização ou um sistema operacional totalmente não confiável é carregado no sistema, algumas chaves de descriptografia ficam indisponíveis. Isso é projetado para impedir que sistemas operacionais totalmente não confiáveis acessem dados de sistemas operacionais confiáveis.

Importante: a Apple não fornece ou oferece suporte a kernels XNU personalizados.



Há uma outra maneira na qual a Segurança Permissiva difere da opção Sem Segurança em um Mac baseado em Intel com um chip T2: ela é um pré-requisito para algumas reversões de segurança que, no passado, eram independentemente controláveis. Especificamente, para desativar a Proteção da Integridade do Sistema (SIP) em um Mac com Apple Silicon, um usuário deve reconhecer que ele está colocando o sistema na Segurança Permissiva. Isso é exigido porque a desativação da SIP sempre colocou o sistema em um estado que fazia com que fosse muito mais fácil comprometer o kernel. Em particular, a desativação da SIP em um Mac com Apple Silicon desativa a exigência da assinatura de kexts durante a geração da AuxKC, permitindo assim que qualquer kext arbitrária seja carregada na memória do kernel. Outra melhoria à SIP feita em um Mac com Apple Silicon foi a movimentação do armazenamento da política da NVRAM para a LocalPolicy. Agora, a desativação da SIP requer a autenticação de um usuário que tenha acesso à chave de assinatura da LocalPolicy a partir do recoveryOS (o que pode ser alcançado ao manter o botão de força pressionado). Isso faz com que seja significativamente mais difícil que um invasor via software, ou até mesmo fisicamente presente, desative a SIP.

Não é possível reverter à Segurança Permissiva a partir do app Utilitário de Segurança da Inicialização. Usuários podem reverter apenas ao executar ferramentas de linha de comando a partir do Terminal no recoveryOS, como `csrutil` (para desativar a SIP). Depois que um usuário faz a reversão, sua ocorrência reflete-se no Utilitário de Segurança da Inicialização, o que faz com que um usuário possa definir facilmente a segurança em um modo mais seguro.

Nota: um Mac com Apple Silicon não exige ou oferece suporte a uma política de inicialização de mídia específica porque, tecnicamente, todas as inicializações são realizadas localmente. Se um usuário optar por inicializar a partir de uma mídia externa, a versão do sistema operacional deve ser personalizada primeiro com uma reinicialização autenticada a partir do recoveryOS. Isso cria um arquivo LocalPolicy na unidade interna que é usado para realizar uma inicialização confiável a partir do sistema operacional armazenado na mídia externa. Isso significa que a configuração da inicialização a partir de uma mídia externa é sempre explicitamente ativada de acordo com um sistema operacional específico, e já exige a autenticação do usuário, o que remove a necessidade de qualquer outra configuração adicional de segurança.

Criação e gerenciamento da chave de assinatura da LocalPolicy

Criação

Quando o macOS é instalado pela primeira vez na fábrica ou uma instalação de apagamento com conexão é realizada, o Mac executa o código do disco RAM de restauração temporária para inicializar o estado padrão. Durante esse processo, o ambiente de restauração cria um novo par de chaves pública e privada, as quais são mantidas no Secure Enclave. A chave privada é referida como a *Chave de Identidade do Proprietário (OIK)*. Se uma OIK já existir, ela é destruída como parte desse processo. O ambiente de restauração também inicializa a chave usada para o Bloqueio de Ativação; a *Chave de Identidade do Usuário (UIK)*. Uma parte desse processo exclusiva a um Mac com Apple Silicon dá-se quando uma certificação da UIK é solicitada para o Bloqueio de Ativação e inclui um conjunto de restrições solicitadas que serão exigidas quando da validação na LocalPolicy. Se um dispositivo não puder obter um UIK certificado para o Bloqueio de Ativação (por estar associado no momento a uma conta do Buscar Mac e comunicado como perdido, por exemplo), ele não poderá prosseguir para criar uma LocalPolicy. Se um *Certificado de identidade de usuário (ucrt)* for emitido para o dispositivo, esse ucrt conterá restrições de políticas impostas pelo servidor e restrições de políticas solicitadas pelo usuário em uma extensão X.509 v3.

Quando o Bloqueio de Ativação/`ucrt` é obtido com sucesso, ele é armazenado em um banco de dados do lado do servidor e também retornado ao dispositivo. Depois do dispositivo ter um ucrt, uma solicitação de certificação da chave pública correspondente à OIK é enviada para o servidor da *Autoridade de Atestado Básico (BAA)*. A BAA usa a chave pública do ucrt armazenada no banco de dados acessível da BAA para verificar a solicitação de certificação da OIK. Se a BAA puder verificar a certificação, ela certifica a chave pública e retorna o *Certificado de Identidade do Proprietário (OIC)*, o qual é assinado pela BAA e contém as restrições armazenadas no ucrt. O OIC é enviado de volta para o Secure Enclave. A partir de então, sempre que o Secure Enclave assina uma nova LocalPolicy, ele anexa o OIC ao Image4. O LLB tem confiança integrada no certificado raiz da BAA, o que faz com que ele confie no OIC, o que faz com que ele confie na assinatura geral da LocalPolicy.

Restrições da RemotePolicy

Todos os arquivos Image4, e não apenas LocalPolicies, contêm restrições na avaliação do manifesto Image4. Essas restrições são codificadas com identificadores de objetos especiais (OIDs) no certificado folha. A biblioteca de verificação do Image4 busca o OID de restrição de certificado especial de um certificado durante a avaliação da assinatura e avalia mecanicamente as restrições especificadas neste. As restrições tomam as seguintes formas:

- X deve existir
- X não deve existir
- X deve ter um valor específico

Assim, em assinaturas "personalizadas", por exemplo, as restrições do certificado conterão "ECID deve existir" e, em assinaturas "globais", elas conterão "ECID não deve existir". Essas restrições são projetadas para garantir que todos os arquivos Image4 assinados por uma chave determinada estejam em conformidade com certas exigências para evitar a geração de manifestos Image4 assinados incorretamente.

No contexto de cada LocalPolicy, essas restrições de certificado Image4 são chamadas de *RemotePolicy*. Uma RemotePolicy diferente pode existir para ambientes de inicialização de LocalPolicies diferentes. A RemotePolicy é usada para restringir a LocalPolicy do recoveryOS para que, ao inicializar o recoveryOS, ele possa apenas se comportar como se estivesse inicializando com Segurança Total. Isso aumenta a confiança na integridade do ambiente de inicialização do recoveryOS como um local onde a política possa ser alterada. A RemotePolicy restringe a LocalPolicy a conter a ECID do Mac na qual a LocalPolicy foi gerada e o Hash do Nonce da Política Remota (`rpnh`) específico armazenado no Componente de Armazenamento Seguro desse Mac. O `rpnh` e, portanto, a RemotePolicy, mudam apenas quando ações como registro, cancelamento de registro, bloqueio remoto e apagamento remoto são tomadas para o Buscar Mac e o Bloqueio de Ativação. As restrições da RemotePolicy são determinadas e especificadas no momento da certificação da Chave de Identidade do Usuário (UIK) e assinadas no Certificado de identidade de usuário (ucrt) emitido. Algumas restrições da RemotePolicy são determinadas pelo servidor, como ECID, ChipID e BoardID. Isso é projetado para impedir que um dispositivo assine arquivos LocalPolicy para outros dispositivos. Outras restrições da RemotePolicy podem ser especificadas pelo dispositivo para ajudar a impedir a reversão da Segurança da LocalPolicy sem o fornecimento da autenticação local necessária para acessar a OIK atual e a autenticação remota da conta na qual a ativação do dispositivo está bloqueada.

Conteúdo de um arquivo LocalPolicy para um Mac com Apple Silicon

A LocalPolicy é um arquivo Image4 assinado pelo Secure Enclave. O Image4 é um formato de estrutura de dados codificado com ASN.1 (Notação de Sintaxe Abstrata Um) DER, usado para descrever informações sobre os objetos da cadeia de inicialização segura em plataformas Apple. Em um modelo de inicialização segura baseado em Image4, políticas de segurança são exigidas ao fazer uma instalação de software iniciada por um pedido de assinatura a um servidor de assinatura central da Apple. Se a política for aceitável, o servidor de assinatura retorna um arquivo Image4 assinado, contendo uma variedade de sequências de códigos de 4 caracteres (4CC). Esses arquivos Image4 e 4CCs assinados são avaliados na inicialização por softwares como a ROM de Inicialização ou o LLB.

Passagem de propriedade entre sistemas operacionais

O acesso à Chave de Identidade do Usuário (UIK) é referido como uma “Propriedade”. A Propriedade é exigida para permitir que usuários renunciem a LocalPolicy depois de fazerem alterações de política ou software. A OIK é protegida pela mesma hierarquia de chaves descrita em Proteção de Chave Selada (SKP), com a OIK sendo protegida pela mesma Chave de criptografia de chaves (KEK) da Chave de criptografia do volume (VEK). Isso significa que ela é normalmente protegida pelas senhas do usuário e as medidas do sistema operacional e da política. Há apenas uma única OIK para todos os sistemas operacionais no Mac. Portanto, ao instalar um segundo sistema operacional, é necessário o consentimento explícito dos usuários no primeiro sistema operacional para passar a Propriedade para os usuários no segundo sistema operacional. No entanto, ainda não há usuários no segundo sistema operacional quando o instalador está sendo executado a partir do primeiro sistema operacional. Em sistemas operacionais, é normal que usuários não sejam gerados até que o sistema operacional seja inicializado e o Assistente de Configuração esteja em execução. Assim, duas novas ações são exigidas ao instalar um segundo sistema operacional em um Mac com Apple Silicon:

- Criar uma LocalPolicy para o segundo sistema operacional
- Preparar uma “Instalação de Usuário” para a passagem de Propriedade

Ao executar o Assistente de Instalação e destinar a instalação a um segundo volume vazio, um diálogo pergunta ao usuário se ele deseja copiar um usuário do volume atual para que seja o primeiro usuário do segundo volume. Em caso afirmativo, essa “Instalação de Usuário” criada é, na verdade, uma KEK derivada da senha do usuário selecionado e das chaves de hardware, que então é usada para criptografar a OIK conforme ela é passada para o segundo sistema operacional. Depois, a partir do Assistente de Instalação no segundo sistema operacional, um diálogo solicita a senha desse usuário para permitir que ele acesse a OIK no Secure Enclave para o novo sistema operacional. Caso usuários optem por não copiar um usuário, a Instalação de Usuário ainda é criada da mesma maneira, mas uma senha em branco é usada em vez da senha de um usuário. Esse segundo fluxo existe para certos cenários de administração de sistemas. Entretanto, usuários que desejem ter instalações multivolume e realizar a passagem de Propriedade da maneira mais segura possível sempre devem optar por copiar um usuário do primeiro para o segundo sistema operacional.

LocalPolicy em um Mac com Apple Silicon

Em um Mac com Apple Silicon, o controle da política de segurança local foi delegado a um aplicativo que é executado no Secure Enclave. Esse software pode usar as credenciais do usuário e o modo de inicialização da CPU principal para determinar quem pode alterar a política de segurança e a partir de qual ambiente de inicialização. Isso ajuda a impedir que um software malicioso use os controles de política de segurança contra o usuário ao revertê-los para ganhar mais privilégios.

Propriedades do manifesto LocalPolicy

O arquivo LocalPolicy contém alguns 4CCs arquiteturais encontrados em quase todos os arquivos Image4, como um ID de placa ou modelo (BORD) que indica um chip da Apple em particular (CHIP) ou Identificação Exclusiva de Chip (ECID). Mas os 4CCs abaixo concentram-se apenas nas políticas de segurança que podem ser configuradas por usuários.

Nota: a Apple usa o termo *Um recoveryOS Verdadeiro Emparelhado (1TR)* para indicar uma inicialização no recoveryOS emparelhado ao pressionar uma vez um botão de força físico e mantê-lo pressionado. Isso difere de uma inicialização normal no recoveryOS, que acontece via NVRAM ou ao pressionar duas vezes o botão e manter pressionado, ou que pode acontecer quando ocorrem erros na inicialização. O pressionamento do botão físico de um tipo específico aumenta a confiança de que o ambiente de inicialização não fique ao alcance de um ataque no qual um invasor penetre o macOS via software.

Hash do Nonce da LocalPolicy (lpnh)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* o `lpnh` é usado para a antirreprodução da LocalPolicy. Ele é um hash SHA384 do Nonce da LocalPolicy (LPN), o qual é armazenado no Componente de Armazenamento Seguro e pode ser acessado através da ROM de Inicialização do Secure Enclave ou do Secure Enclave. O nonce não processado nunca pode ser visto pelo Processador de Aplicativos, apenas pelo sepOS. Um invasor que deseje convencer o LLB de que uma LocalPolicy capturada anteriormente é válida teria que colocar um valor no Componente de Armazenamento Seguro que gerasse um hash com o mesmo valor `lpnh` encontrado na LocalPolicy que ele deseja reproduzir. Normalmente, há um único LPN válido no sistema — exceto durante atualizações de software, quando há dois LPNs válidos simultaneamente — para permitir a possibilidade de reverter a inicialização ao software antigo no caso de um erro de atualização. Quando qualquer LocalPolicy de qualquer sistema operacional é alterada, todas as políticas são assinadas novamente com o novo valor *lpnh* correspondente ao novo LPN encontrado no Componente de Armazenamento Seguro. Essa mudança ocorre quando o usuário altera os ajustes de segurança ou cria novos sistemas operacionais com uma nova LocalPolicy para cada um deles.

Hash do Nonce da Política Remota (rpnh)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* o `rpnh` se comporta da mesma maneira que o `lpnh`, mas é atualizado apenas quando a política remota é atualizada, como ao alterar o estado de registro no Buscar. Essa mudança ocorre quando o usuário altera o estado do Buscar em um Mac.

Hash do Nonce do recoveryOS (rpnh)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* o `ronh` se comporta da mesma maneira que o lpnh, mas é encontrado exclusivamente na LocalPolicy do recoveryOS do sistema. Ele é atualizado quando o recoveryOS do sistema é atualizado, como ao fazer atualizações de software. Um nonce separado do `lpnh` e do `rpnh` é usado para que, quando um dispositivo for colocado em um estado desativado pelo Buscar, os sistemas operacionais possam ser desativados (ao remover os respectivos LPN e RPN do Componente de Armazenamento Seguro) e, ao mesmo tempo, o recoveryOS do sistema permaneça inicializável. Dessa maneira, os sistemas operacionais podem ser reativados quando o proprietário do sistema provar seu controle sobre o sistema ao digitar sua senha do iCloud usada para a conta do Buscar. Essa mudança ocorre quando um usuário atualiza o sistema recoveryOS do sistema ou cria novos sistemas operacionais.

Hash do Manifesto Image4 do Estágio Seguinte (nsih)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* o campo *nsih* representa um hash SHA384 da estrutura de dados do manifesto Image4 que descreve o macOS inicializado. O manifesto Image4 do macOS contém as medidas de todos os objetos de inicialização — como o iBoot, o cache de confiança estático, a árvore do dispositivo, a Coleção do Kernel de Inicialização e o hash raiz do volume de sistema assinado (SSV). Quando o LLB é direcionado para inicializar um macOS determinado, ele é projetado para ajudar a garantir que o hash do manifesto Image4 do macOS anexado ao iBoot coincida com aquilo capturado no campo `nsih` da LocalPolicy. Dessa maneira, o `nsih` captura a intenção de para qual sistema operacional o usuário criou uma LocalPolicy. Usuários mudam implicitamente o valor `nsih` quando realizam uma atualização de software.

Hash da Política (auxp) da Coleção do Kernel Auxiliar (AuxKC)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* macOS
- *Descrição:* o `auxp` é um hash SHA384 da política da lista de kexts autorizadas pelo usuário (UAKL). Isso é usado ao gerar a AuxKC para ajudar a garantir que apenas as kexts autorizadas pelo usuário sejam incluídas na AuxKC. `smb2` é um pré-requisito para definir este campo. Usuários mudam implicitamente o valor `auxp` quando alteram a UAKL através da aprovação de uma kext a partir do painel de Segurança e Privacidade das Preferências do Sistema.

Hash do Manifesto Image4 (auxi) da Coleção do Kernel Auxiliar (AuxKC)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* macOS
- *Descrição:* depois que o sistema verifica que o hash da UAKL coincide com aquilo encontrado no campo `auxp` da LocalPolicy, ele pede que a AuxKC seja assinada pelo processador de aplicativos do Secure Enclave responsável pela assinatura da LocalPolicy. Depois, um hash SHA384 da assinatura do manifesto Image4 da AuxKC é colocado na LocalPolicy para impedir a possibilidade de mistura e correspondência de AuxKCs assinadas anteriormente a um sistema operacional no momento da inicialização. Se o iBoot encontrar o campo `auxi` na LocalPolicy, ele tenta carregar a AuxKC no armazenamento e valida sua assinatura. Ele também verifica se o hash do manifesto Image4 anexado à AuxKC coincide com o valor encontrado no campo `auxi`. Se o carregamento da AuxKC falhar por algum motivo, o sistema continua a inicializar sem esse objeto de inicialização e, portanto, sem nenhuma kext de terceiros carregada. O campo `auxp` é um pré-requisito para definir o campo auxi na LocalPolicy. Usuários mudam implicitamente o valor `auxi` quando alteram a UAKL através da aprovação de uma kext a partir do painel de Segurança e Privacidade das Preferências do Sistema.

Hash do Recibo (auxi) da Coleção do Kernel Auxiliar (AuxKC)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* macOS
- *Descrição:* o `auxr` é um hash SHA384 do recibo da AuxKC que indica o conjunto exato de kexts que foram incluídas na AuxKC. O recibo da AuxKC pode ser um subconjunto da UAKL, já que as kexts podem ser excluídas da AuxKC mesmo que estejam autorizadas pelo usuário caso sejam sabidamente usadas para ataques. Além disso, algumas kexts que podem ser usadas para transgredir os limites entre usuário e kernel podem levar a uma redução de funcionalidade, como a incapacidade de usar o Apple Pay ou reproduzir conteúdo 4K e HDR. Usuários que desejem essas capacidades devem optar por uma inclusão de AuxKC mais restrita. O campo `auxp` é um pré-requisito para definir o campo `auxr` na LocalPolicy. Usuários mudam implicitamente o valor `auxr` quando compilam uma nova AuxKC a partir do painel de Segurança e Privacidade das Preferências do Sistema.

Hash do Manifesto CustomOS Image4 (coih)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* 1TR
- *Descrição:* o `coih` é um hash SHA384 do manifesto CustomOS Image4. O payload desse manifesto é usado pelo iBoot (em vez do kernel XNU) para transferir o controle. Usuários mudam implicitamente o valor `coih` quando usam a ferramenta de linha de comando `kmutil configure-boot` no 1TR.

UUID do grupo de volumes APFS (vuid)

- *Tipo:* OctetString (16)
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* o `vuid` indica o grupo de volumes que o kernel deve usar como raiz. Este campo é primariamente informativo e não é usado para restrições de segurança. Esse `vuid` é definido implicitamente pelo usuário ao criar uma nova instalação do sistema operacional.

UUID do Grupo (kuid) da Chave de criptografia de chaves (KEK)

- *Tipo:* OctetString (16)
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* o `kuid` indica o volume que foi inicializado. A chave de criptografia de chaves é usada tipicamente para a Proteção de Dados. Em cada LocalPolicy, ela é usada para proteger a chave de assinatura da LocalPolicy. O `kuid` é definido implicitamente pelo usuário ao criar uma nova instalação do sistema operacional.

Medida de Política de Inicialização Confiável do recoveryOS Emparelhado (prot)

- *Tipo:* OctetString (48)
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* uma Medida de Política de Inicialização Confiável do recoveryOS emparelhado (TBPM) é um cálculo especial de hash SHA384 iterativo feito sobre o manifesto Image4 de uma LocalPolicy, excluindo nonces, para oferecer uma medida consistente com o passar do tempo (já que nonces como `lpnh` são atualizados frequentemente). O campo `prot`, encontrado apenas em cada LocalPolicy do macOS, fornece um emparelhamento para indicar a LocalPolicy do recoveryOS que corresponde à LocalPolicy do macOS.

Política Local do recoveryOS Tem Secure Enclave Assinado (hrlp)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* o `hrlp` indica se o valor `prot` (acima) é ou não a medida de uma LocalPolicy do recoveryOS assinada pelo Secure Enclave. Se não for, a LocalPolicy do recoveryOS é assinada pelo servidor de assinatura on-line da Apple, o qual assina itens como arquivos Image4 do macOS.

Versão do Sistema Operacional Local (love)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR, recoveryOS, macOS
- *Descrição:* O `love` indica a versão do sistema operacional para a qual a LocalPolicy foi criada. A versão é obtida no manifesto do próximo estado durante a criação da LocalPolicy e é usada para impor restrições de emparelhamento do recoveryOS.

Multi-inicialização Segura (smb0)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR, recoveryOS
- *Descrição:* se `smb0` estiver presente e for verdadeira, o LLB permite que o manifesto Image4 do estágio seguinte seja assinado globalmente, em vez de exigir uma assinatura personalizada. Usuários podem alterar este campo com o Utilitário de Segurança da Inicialização ou `bputil` para reverter à Segurança Reduzida.

Multi-inicialização Segura (smb1)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR
- *Descrição:* se `smb1` estiver presente e for verdadeira, o iBoot permite que objetos como uma coleção de kernel personalizada seja assinada pelo Secure Enclave com a mesma chave da LocalPolicy. A presença de `smb0` é um pré-requisito para a presença de `smb1`. Usuários podem alterar este campo com ferramentas de linha de comando como `csrutil` ou `bputil` para reverter à Segurança Permissiva.

Multi-inicialização Segura (smb2)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR
- *Descrição:* se `smb2` estiver presente e for verdadeira, o iBoot permite que a Coleção do Kernel Auxiliar seja assinada pelo Secure Enclave com a mesma chave da LocalPolicy. A presença de `smb0` é um pré-requisito para a presença de `smb2`. Usuários podem alterar este campo com o Utilitário de Segurança da Inicialização ou `bputil` para reverter à Segurança Reduzida e ativar kexts de terceiros.

Multi-inicialização Segura (smb3)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR
- *Descrição:* se `smb3` estiver presente e for verdadeira, um usuário no dispositivo optou pelo controle do gerenciamento de dispositivos móveis (MDM) sobre o sistema. A presença deste campo faz com que o processador de aplicativos do Secure Enclave que controla a LocalPolicy aceite a autenticação do MDM em vez de exigir a autenticação de usuário local. Usuários podem alterar este campo com o Utilitário de Segurança da Inicialização ou `bputil` para ativar o controle gerenciado sobre kexts de terceiros e atualizações de software. (No macOS 11.2 ou posterior, o MDM também pode iniciar uma atualização para a versão mais recente do macOS se o modo de segurança atual for Segurança Total.)

Multi-inicialização Segura (smb4)

- *Tipo:* booleano
- *Ambientes mutáveis:* macOS
- *Descrição:* se `smb4` estiver presente e for verdadeira, o dispositivo optou pelo controle do MDM sobre o sistema operacional através do Apple School Manager, Apple Business Manager ou Apple Business Essentials. A presença deste campo faz com que o aplicativo do Secure Enclave que controla a LocalPolicy aceite a autenticação do MDM em vez de exigir a autenticação de usuário local. Este campo é alterado pela solução MDM quando ela detecta que o número de série de um dispositivo aparece em qualquer daqueles três serviços.

Proteção da Integridade do Sistema (sip0)

- *Tipo:* número inteiro não assinado de 64 bits
- *Ambientes mutáveis:* 1TR
- *Descrição:* a `sip0` contém os bits da política de Proteção da Integridade do Sistema (SIP) existente, armazenados anteriormente na NVRAM. Novos bits de política de SIP são adicionados aqui (em vez de usar os campos de LocalPolicy como os abaixo), se forem usados apenas no macOS e não forem usados pelo LLB. Usuários podem alterar este campo com `csrutil` ou a partir do 1TR para desativar a SIP e reverter à Segurança Permissiva.

Proteção da Integridade do Sistema (sip1)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR
- *Descrição:* se `sip1` estiver presente e for verdadeira, o iBoot permitirá falhas para verificar o hash raiz do volume SSV. Usuários podem alterar este campo com `csrutil` ou `bputil` a partir do 1TR.

Proteção da Integridade do Sistema (sip2)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR
- *Descrição:* se sip2 estiver presente e for verdadeira, o iBoot não bloqueará o registro de hardware da *Região de Texto Somente Leitura Configurável (CTRR)* que marca a memória do kernel como não gravável. Usuários podem alterar este campo com `csrutil` ou `bputil` a partir do 1TR.

Proteção da Integridade do Sistema (sip3)

- *Tipo:* booleano
- *Ambientes mutáveis:* 1TR
- *Descrição:* se `sip3` estiver presente e for verdadeira, o iBoot não exigirá a variável boot-args da NVRAM em sua lista de permissão integrada, o que, de outra maneira, filtraria as opções passadas ao kernel. Usuários podem alterar este campo com `csrutil` ou `bputil` a partir do 1TR.

Certificados and RemotePolicy

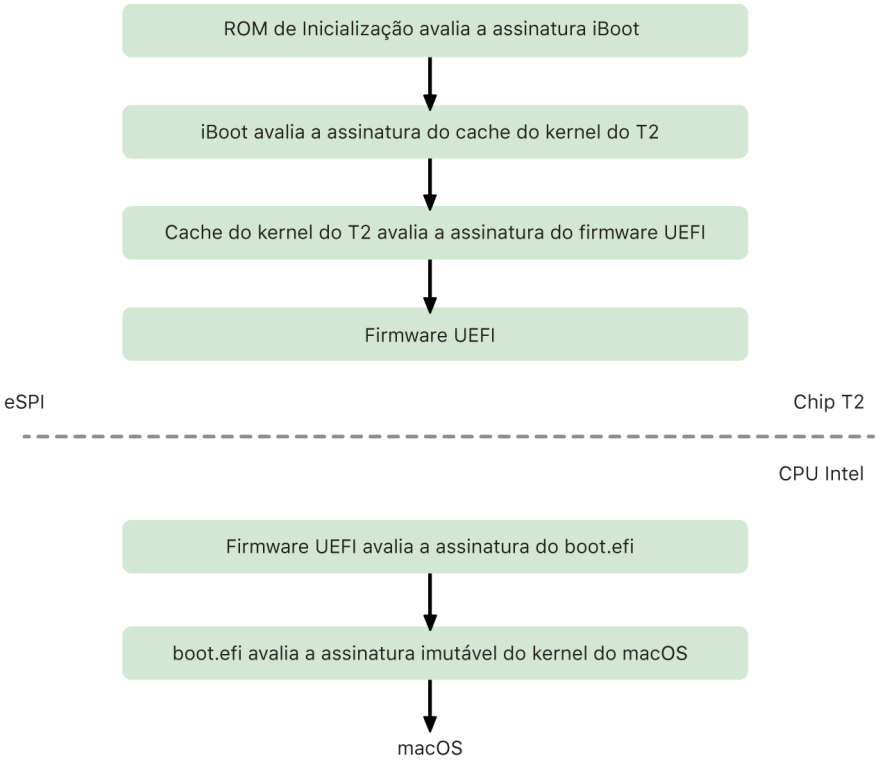
Conforme descrito em Criação e gerenciamento da chave de assinatura da LocalPolicy, o Image4 da LocalPolicy também contém o Certificado de Identidade do Proprietário (OIC) e a RemotePolicy integrada.

Computadores Mac baseados em Intel

Processo de inicialização de um Mac baseado em Intel

Mac baseado em Intel com um chip Apple T2 Security

Quando um computador Mac baseado em Intel com o chip Apple T2 Security é ligado, o chip realiza uma inicialização segura a partir da sua ROM de Inicialização da mesma maneira que um iPhone, iPad e um Mac com Apple Silicon. Isso verifica o gerenciador de inicialização do iBoot, sendo o primeiro passo na cadeia de confiança. O iBoot verifica o kernel e o código de extensão do kernel do chip T2, o qual verifica o firmware da UEFI Intel em seguida. O firmware da UEFI e a assinatura associada ficam disponíveis de início apenas para o chip T2.



Após a verificação, a imagem do firmware da UEFI é mapeada em uma parte da memória do chip T2. Essa memória é disponibilizada para a CPU Intel através da Interface Periférica Serial aprimorada (eSPI). Na primeira inicialização da CPU Intel, ela obtém o firmware da UEFI através da eSPI na cópia mapeada em memória do firmware, localizada no chip T2, cuja integridade foi verificada.

A avaliação da cadeia de confiança continua na CPU Intel, com a avaliação da assinatura do boot.efi (o gerenciador de inicialização do macOS) por parte do firmware da UEFI. As assinaturas da inicialização segura do macOS, residentes no processador Intel, são armazenadas no mesmo formato Image4 usado na inicialização segura do iOS, iPadOS e chip T2. Além disso, o código que analisa os arquivos Image4 é o mesmo código reforçado da implementação atual da inicialização segura do iOS e iPadOS. Em seguida, o boot.efi verifica a assinatura de um novo arquivo, chamado immutablekernel. Quando a inicialização segura está ativada, o arquivo immutablekernel representa o conjunto completo das extensões do kernel da Apple necessárias para inicializar o macOS. A política de inicialização segura é encerrada na passagem para o immutablekernel. Depois disso, as políticas de segurança do macOS (como a Proteção da Integridade do Sistema e as extensões do kernel assinadas) entram em vigor.

Caso haja qualquer erro ou falha nesse processo, o Mac entra no modo de Recuperação, modo de Recuperação do chip Apple T2 Security ou modo de Atualização do Firmware do Dispositivo (DFU) do Chip Apple T2 Security.

Microsoft Windows em um Mac baseado em Intel com um chip T2

Por padrão, um Mac baseado em Intel que oferece suporte à inicialização segura confia apenas no conteúdo assinado pela Apple. Contudo, para melhorar a segurança das instalações do Boot Camp, a Apple também oferece suporte à inicialização segura do Windows. O firmware da Interface de Firmware Extensível Unificada (UEFi) possui uma cópia do certificado Microsoft Windows Production CA 2011 usado para autenticar os carregadores de inicialização da Microsoft.

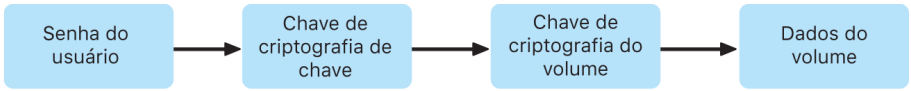
Nota: atualmente, não é fornecida confiança para o Microsoft Corporation UEFI CA 2011, o que permitiria a verificação de código assinado por parceiros da Microsoft. Esta AC da UEFI é comumente usada para verificar a autenticidade dos carregadores de inicialização de outros sistemas operacionais, como variantes de Linux.

O suporte à inicialização segura do Windows não é ativado por padrão. Ele deve ser ativado com o Assistente do Boot Camp (BCA). Quando o usuário executa o BCA, o macOS é reconfigurado para confiar no código assinado pela Microsoft durante a inicialização. Após o término do BCA, se o macOS não tiver êxito na avaliação de confiança da Apple durante a inicialização segura, o firmware da UEFI tenta avaliar a confiança do objeto de acordo com a formatação da inicialização segura da UEFI. Se a avaliação de confiança for bem-sucedida, o Mac dá prosseguimento à inicialização do Windows. Caso contrário, o Mac entra no recoveryOS e informa o usuário sobre a falha na avaliação de confiança.

Computadores Mac baseados em Intel sem um chip T2

Um Mac baseado em Intel sem um chip T2 não oferece suporte à inicialização segura. Dessa forma, o firmware da Interface de Firmware Extensível Unificada (UEFi) carrega o inicializador do macOS (boot.efi) do sistema de arquivos sem verificação e o inicializador carrega o kernel (prelinkedkernel) do sistema de arquivos sem verificação. Para proteger a integridade da cadeia de inicialização, os usuários devem ativar todos os mecanismos de segurança a seguir:

- *Proteção da Integridade do Sistema (SIP):* ativada por padrão, ela protege o inicializador e o kernel contra gravações maliciosas de dentro de um macOS em execução.
- *FileVault:* pode ser ativado de duas formas: pelo usuário ou por um administrador de gerenciamento de dispositivos móveis (MDM). Ele protege contra um invasor fisicamente presente, usando o Modo de Disco de Destino para sobrescrever o inicializador.
- *Senha de firmware:* pode ser ativada de duas formas: pelo usuário ou pelo administrador de um MDM. Isso ajuda a impedir que um invasor fisicamente presente ative modos alternativos de inicialização, como o recoveryOS, Modo de Usuário Único ou Modo Disco de Destino, nos quais o inicializador pode ser sobrescrito. Isso também ajuda a impedir a inicialização a partir de mídias alternativas, método no qual um invasor poderia executar código para sobrescrever o inicializador.



Modos de inicialização de um Mac baseado em Intel com um chip Apple T2 Security

Um Mac baseado em Intel com um chip Apple T2 Security possui uma variedade de modos de inicialização que podem ser acessados no momento da inicialização ao pressionar combinações de teclas reconhecidas pelo firmware da UEFI ou inicializador. Alguns modos de inicialização, como o Modo de Usuário Único, não funcionarão exceto se a política de segurança for alterada para Sem Segurança no Utilitário de Segurança da Inicialização.

Modo	Combinação de teclas	Descrição
Inicialização do macOS	Nenhuma	O firmware da UEFI passa o controle para o inicializador do macOS (um aplicativo da UEFI), que o passa para o kernel do macOS. Na inicialização padrão do Mac com o FileVault ativado, o inicializador do macOS apresenta a interface da Janela de Início de Sessão, que aceita a senha para descriptografar o armazenamento.
Gerenciador de Inicialização	Opção (⌥)	O firmware da UEFI inicia o aplicativo da UEFI integrado que apresenta a interface de seleção do dispositivo de inicialização ao usuário.
Modo de Disco de Destino (TDM)	T	O firmware da UEFI inicia o aplicativo da UEFI integrado que expõe o dispositivo de armazenamento interno como um dispositivo de armazenamento não processado baseado em blocos via FireWire, Thunderbolt, USB ou qualquer combinação dos três (de acordo com o modelo do Mac).
Modo de Usuário Único	Comando (⌘) + S	O kernel do macOS passa a opção –s no vetor de argumentos do launchd, que cria a interface de linha de comando de usuário único no tty do app Console. *Nota:* se o usuário sair da interface de linha de comando, o macOS continua a inicialização até a Janela de Início de Sessão.
recoveryOS	Comando (⌘) + R	O firmware da UEFI carrega um macOS mínimo a partir de uma imagem de disco (.dmg) assinada no dispositivo de armazenamento interno.
recoveryOS via internet	Opção (⌥) + Comando (⌘) + R	A imagem de disco assinada é baixada da internet via HTTP.
Diagnóstico	D	O firmware da UEFI carrega um ambiente de diagnóstico UEFI mínimo a partir de uma imagem de disco assinada no dispositivo de armazenamento interno.
Diagnóstico via Internet	Opção (⌥) + D	A imagem de disco assinada é baixada da internet via HTTP.
Inicialização no Windows	Nenhuma	Se o Windows tiver sido instalado com o Boot Camp, o firmware da UEFI passa o controle para o inicializador do Windows, que o passa para o kernel do Windows.

Utilitário de Segurança da Inicialização em um Mac com um chip Apple T2 Security

Visão geral

Em um Mac baseado em Intel com um chip Apple T2 Security, o Utilitário de Segurança da Inicialização gerencia diversos ajustes de política de segurança. O utilitário pode ser acessado ao inicializar no recoveryOS e selecionar Utilitário de Segurança da Inicialização no menu Utilitários, e protege os ajustes de segurança compatíveis da manipulação fácil por parte de um invasor.

Alterações críticas nas políticas exigem autenticação, mesmo no modo de Recuperação. Na primeira vez que o Utilitário de Segurança da Inicialização é aberto, ele pede ao usuário que digite uma senha de administrador da instalação primária do macOS associada ao recoveryOS inicializado atualmente. Caso não exista nenhum administrador, ele deve ser criado para que a política possa ser alterada. O chip T2 exige que o computador Mac esteja inicializado no recoveryOS e que uma autenticação com uma credencial assegurada pelo Secure Enclave tenha ocorrido para que tal alteração na política possa ser realizada. As alterações nas políticas de segurança possuem dois requisitos implícitos.
O recoveryOS deve:

- Ser inicializada a partir de um dispositivo de armazenamento diretamente conectado ao chip T2, pois as partições de outros dispositivos não possuem credenciais asseguradas pelo Secure Enclave vinculadas ao dispositivo de armazenamento interno.
- Estar em um volume baseado em APFS, pois há suporte apenas para armazenar as credenciais de Autenticação na Recuperação enviadas ao Secure Enclave no volume APFS de “Pré-inicialização” de uma unidade. Os volumes formatados como HFS+ não podem usar a inicialização segura.

Essa política é mostrada apenas no Utilitário de Segurança da Inicialização em um Mac baseado em Intel com um chip T2. Embora a maioria dos casos não deva requerer alterações à política de inicialização segura, o controle final dos ajustes do dispositivo está nas mãos dos usuários, que podem escolher desativar ou reverter a funcionalidade de inicialização segura no Mac de acordo com as suas necessidades.

As alterações na política de inicialização segura feitas dentro deste app são aplicadas apenas à avaliação da cadeia de confiança sendo verificada no processador Intel. A opção "Inicialização segura do chip T2" está sempre ativada.

A política de inicialização segura pode ser configurada como um de três ajustes: Segurança Total, Segurança Média e Sem Segurança. A opção Sem Segurança desativa completamente a avaliação da inicialização segura no processador Intel e permite que o usuário inicialize o que desejar.

Política de inicialização Segurança Total

A Segurança Total é a política de inicialização padrão e se comporta de maneira similar ao iOS e iPadOS ou à Segurança Total em um Mac com Apple Silicon. No momento que um software é baixado e preparado para instalação, ele é personalizado com uma assinatura que inclui a Identificação Exclusiva de Chip (ECID) — um ID exclusivo específico ao chip T2 neste caso — como parte do pedido de assinatura. A assinatura retornada pelo servidor de assinatura é exclusiva e pode ser usada apenas por esse chip T2 específico. O firmware da Interface de Firmware Extensível Unificada (UEFi) é projetado para garantir que quando a política de Segurança Total estiver em vigor, uma determinada assinatura não esteja apenas assinada pela Apple, mas também assinada para esse Mac específico, essencialmente vinculando essa versão do macOS a esse Mac. Isso ajuda a impedir ataques de reversão, conforme descrito em Segurança Total em um Mac com Apple Silicon.

Política de inicialização Segurança Média

A política de inicialização Segurança Média assemelha-se à inicialização segura de UEFI tradicional, na qual um fornecedor (neste caso, a Apple) gera uma assinatura digital para o código para garantir que ele tenha vindo do fornecedor. Dessa forma, os invasores ficam impedidos de inserir um código sem assinatura. Chamamos essa assinatura de "global", pois ela pode ser usada em qualquer Mac, por qualquer período, em um Mac que tenha um conjunto de políticas de Segurança Média definido no momento. Não há suporte para assinaturas globais no iOS, iPadOS ou no próprio chip T2. Este ajuste não tenta impedir ataques de reversão.

Política de inicialização de mídia

A política de inicialização de mídia existe apenas em um Mac baseado em Intel com um chip T2 e é independente da política de inicialização segura. Sendo assim, mesmo que um usuário desative a inicialização segura, o comportamento padrão de impedir a inicialização do Mac a partir de qualquer dispositivo que não seja o dispositivo de armazenamento diretamente conectado ao chip T2 permanece inalterado. A política de inicialização de mídia não é exigida em um Mac com Apple Silicon. Para obter mais informações, consulte Controle da política de segurança do Disco de Inicialização.

Proteção da senha de firmware em um Mac baseado em Intel

O macOS em computadores baseados em Intel com um chip Apple T2 Security é compatível com o uso de uma Senha de Firmware para ajudar a impedir modificações não intencionais nos ajustes de firmware em um Mac específico. A Senha de Firmware é projetada para impedir a seleção de modos de inicialização alternativos, como as inicializações no recoveryOS, Modo de Usuário Único, Modo Disco de Destino ou a partir de um volume não autorizado.

Nota: a senha de firmware não é exigida em um Mac com Apple Silicon porque a funcionalidade de firmware crítica que ela restringia foi movida para o recoveryOS e (quando o FileVault está ativado) o recoveryOS exige a autenticação do usuário para chegar a essa funcionalidade crítica.

O modo mais básico da senha de firmware pode ser alcançado a partir do Utilitário de Senha de Firmware do recoveryOS em um Mac baseado em Intel *sem* um chip T2, e a partir do Utilitário de Segurança da Inicialização em um Mac baseado em Intel *com* um chip T2. Opções avançadas (como a capacidade de solicitar a senha a cada inicialização) estão disponíveis na ferramenta de linha de comando `firmwarepasswd` no macOS.

A definição de uma Senha de Firmware é especialmente importante para reduzir o risco de ataques a computadores Mac baseados em Intel sem o chip T2 realizados por um invasor fisicamente presente. A Senha de Firmware pode ajudar a impedir que um invasor inicialize no recoveryOS, de onde ele poderia, de outra maneira, desativar a Proteção da Integridade do Sistema (SIP). Além disso, a restrição da inicialização de mídias alternativas impede que um invasor execute código privilegiado de outro sistema operacional para atacar o firmware de periféricos.

Existe um mecanismo de redefinição da senha de firmware para ajudar usuários que esqueceram a senha. Os usuários pressionam uma combinação de teclas na inicialização e veem uma string específica do modelo para fornecer ao AppleCare. O AppleCare assina digitalmente um recurso cuja assinatura é verificada pelo Identificador Uniforme de Recursos (URI). Caso a assinatura seja validada e o conteúdo seja para o Mac específico, o firmware da UEFI remove a senha de firmware.

Para usuários que não desejam que mais ninguém possa remover a senha de firmware através do software, exceto o próprio usuário, a opção `–disable–reset–capability` foi acrescentada à ferramenta de linha de comando `firmwarepasswd` no macOS 10.15. Antes de configurar essa opção, os usuários devem aceitar que, caso a senha seja esquecida e precise ser removida, o usuário deverá arcar com o custo da substituição da placa lógica necessária para tal. Organizações que desejam proteger seus computadores Mac de invasores externos e funcionários devem definir uma senha de firmware em sistemas de propriedade da organização. Isso pode ser feito no dispositivo das seguintes maneiras:

- Durante o processo de provisão, usando manualmente a ferramenta de linha de comando `firmwarepasswd`
- Com ferramentas de gerenciamento de terceiros que usam a ferramenta de linha de comando `firmwarepasswd`
- Com o gerenciamento de dispositivos móveis (MDM)

recoveryOS e ambientes de diagnóstico para um computador Mac baseado em Intel

recoveryOS

O recoveryOS é totalmente separado do macOS principal e todo o seu conteúdo é armazenado em um arquivo de imagem de disco chamado BaseSystem.dmg. Também há um BaseSystem.chunklist associado, que é usado para verificar a integridade do BaseSystem.dmg. O chunklist é uma série de hashes de pedaços de 10 MB do BaseSystem.dmg. O firmware da Interface de Firmware Extensível Unificada (UEFi) avalia a assinatura do arquivo chunklist e depois avalia o hash de um pedaço do BaseSystem.dmg por vez. Isso ajuda a garantir que ele corresponda ao conteúdo assinado presente no chunklist. Se algum desses hashes não corresponder, a inicialização a partir do recoveryOS é abortada e o firmware da UEFI tenta inicializar a partir do recoveryOS via internet.

Se a verificação for concluída com sucesso, o firmware da UEFI monta o BaseSystem.dmg como um disco RAM e abre o arquivo boot.efi contido. Não há necessidade do firmware da UEFI realizar uma verificação específica do boot.efi, nem do boot.efi realizar uma verificação do kernel, pois o conteúdo completo do sistema operacional (do qual esses elementos são apenas um subconjunto) já teve sua integridade verificada.

Diagnóstico Apple

O procedimento para inicializar o ambiente de diagnóstico local é basicamente o mesmo do que o para iniciar o recoveryOS. Arquivos AppleDiagnostics.dmg e AppleDiagnostics.chunklist separados são usados, mas eles são verificados da mesma maneira que os arquivos BaseSystem. Em vez de iniciar o boot.efi, o firmware da UEFI abre um arquivo dentro da imagem de disco (arquivo .dmg) chamado diags.efi, que por sua vez é responsável por chamar vários outros drivers da UEFI que podem interagir e verificar erros no hardware.

recoveryOS via internet e ambiente de diagnóstico

Se tiver ocorrido um erro ao iniciar a recuperação local ou os ambientes de diagnóstico, o firmware da UEFI tenta baixar as imagens da internet. (Um usuário também pode solicitar especificamente que as imagens sejam obtidas da internet ao manter sequências especiais de teclas pressionadas durante a inicialização.) A validação da integridade das imagens de disco e chunklists baixados do Servidor de Recuperação do SO é realizada da mesma forma que com as imagens obtidas no dispositivo de armazenamento.

Embora a conexão ao Servidor de Recuperação do OS seja feita via HTTP, o conteúdo completo baixado ainda tem sua integridade verificada da forma descrita anteriormente e, portanto, encontra-se protegido contra a manipulação por um invasor que tenha o controle da rede. Caso a verificação de integridade de um pedaço individual seja malsucedida, ele é solicitado novamente 11 vezes ao Servidor de Recuperação do OS antes que as tentativas sejam interrompidas e um erro seja exibido.

Quando os modos de recuperação e diagnóstico via internet foram adicionados a computadores Mac em 2011, decidiu-se que seria melhor usar o transporte HTTP mais simples e gerenciar a autenticação de conteúdo com o mecanismo de chunklist, em vez de implementar a funcionalidade HTTPS mais complicada no firmware da UEFI e, assim, aumentar a superfície de ataque do firmware.

Segurança do volume de sistema assinado no iOS, iPadOS e macOS

No macOS 10.15, a Apple introduziu um volume de sistema somente leitura, um volume isolado e dedicado ao conteúdo do sistema. O macOS 11 ou posterior adicionam proteções criptográficas fortes ao conteúdo do sistema com um *volume de sistema assinado (SSV)*. O SSV possui um mecanismo de kernel que verifica a integridade do conteúdo do sistema no tempo de execução e rejeita qualquer dado — código ou não — que não tenha uma assinatura criptográfica válida da Apple. A partir do iOS 15 e iPadOS 15, o volume de sistema em um dispositivo iOS e iPadOS também ganha a proteção criptográfica de um volume de sistema assinado.

O SSV ajuda não apenas a impedir a adulteração de qualquer software da Apple que faça parte do sistema operacional, como também faz com que a atualização do software do macOS seja mais confiável e muito mais segura. E já que o SSV usa capturas do Apple File System (APFS), caso uma atualização não possa ser realizada, a versão antiga do sistema pode ser restaurada sem uma reinstalação.

Desde a sua introdução, o APFS tem fornecido integridade aos metadados do sistema de arquivos com somas de verificação não criptográficas no dispositivo de armazenamento interno. O SSV reforça o mecanismo de integridade ao acrescentar hashes criptográficos, ampliando-o assim para abranger cada byte de dados de arquivos. Dados de um dispositivo de armazenamento interno (incluindo metadados do sistema de arquivos) têm seus hashes calculados criptograficamente no caminho de leitura, e os hashes são então comparados a valores esperados nos metadados do sistema de arquivos. No caso de incongruências, o sistema assume que os dados foram adulterados e não os retorna ao software solicitante.

Cada hash SHA256 do SSV é armazenado na árvore de metadados principal do sistema de arquivos, que por sua vez, também tem um hash calculado. E já que cada nó da árvore verifica recursivamente a integridade dos hashes de seus respectivos secundários — de maneira similar a uma árvore de hash binário (Merkle) — o valor de hash do nó raiz, chamado de *selo*, abrange cada bite de dados no SSV, o que significa que a assinatura criptográfica cobre todo o volume de sistema.

Durante a instalação e atualização do macOS, o selo é recalculado a partir do sistema de arquivos no dispositivo e essa medida é comparada com a medida assinada pela Apple. Em um Mac com Apple Silicon, o gerenciador de inicialização verifica o selo antes de transferir o controle ao kernel. Em um Mac baseado Intel com um chip Apple T2 Security, o gerenciador de inicialização encaminha a medida e a assinatura ao kernel, o qual verifica o selo diretamente antes de montar o sistema de arquivos raiz. Em ambos os casos, se a verificação falhar, o processo de inicialização é interrompido e o usuário é solicitado a reinstalar o macOS. Esse procedimento é repetido a cada inicialização, a não ser que o usuário tenha escolhido entrar em um modo de segurança menor e optado, separadamente, por desativar o volume de sistema assinado.

Durante as atualizações de software do iOS e iPadOS, o volume de sistema é preparado e recalculado de forma semelhante. Os carregadores de inicialização do iOS e iPadOS verificam se o selo está intacto e se ele corresponde a um valor assinado pela Apple antes de permitir que o dispositivo inicie o kernel. Se houver alguma discrepância durante a inicialização, o usuário é solicitado a atualizar o software do sistema no dispositivo. Os usuários não têm permissão para desativar a proteção de um volume de sistema assinado no iOS e iPadOS.

SSV e assinatura de código

A assinatura de código ainda está presente e é exigida pelo kernel. O volume de sistema assinado oferece proteção quando qualquer byte, sem exceção, é lido a partir do dispositivo de armazenamento interno. Em contrapartida, a assinatura de código oferece proteção quando objetos Mach são mapeados na memória como executáveis. Tanto o SSV quanto a assinatura de código protegem o código executável em todos os caminhos de leitura e execução.

SSV e FileVault

No macOS 11, uma proteção quando em repouso equivalente para o conteúdo do sistema é fornecida pelo SSV e, sendo assim, o volume de sistema não precisa mais ser criptografado. Qualquer modificação feita ao sistema de arquivos enquanto em repouso será detectada pelo sistema de arquivos quando for lida. Se o usuário ativar o FileVault, o conteúdo do usuário no volume de dados ainda é criptografado com um segredo fornecido pelo usuário.

Se o usuário escolher desativar o SSV, o sistema em repouso ficaria vulnerável à adulteração e essa adulteração poderia permitir que um invasor extraísse dados de usuário criptografados quando da próxima inicialização do sistema. Sendo assim, o sistema não permitirá que o usuário desative o SSV se o FileVault estiver ativado. A proteção enquanto em repouso deve ser ativada ou desativada para ambos os volumes de maneira consistente.

No macOS 10.15 ou anterior, o FileVault protege o software do sistema operacional enquanto em repouso ao criptografar o conteúdo do usuário e do sistema com uma chave protegida por um segredo fornecido pelo usuário. Isso oferece proteção contra o acesso ou modificação efetiva do sistema de arquivos que contém o software do sistema por parte de um invasor com acesso físico ao dispositivo.

SSV e um Mac com um chip Apple T2 Security

Em um Mac com um chip Apple T2 Security, apenas o macOS em si é protegido pelo SSV. O software que é executado no chip T2 e verifica o macOS é protegido pela inicialização segura.

Atualizações seguras de software

A segurança é um processo; não é suficiente inicializar com confiança na versão do sistema operacional instalada na fábrica — também deve haver um mecanismo para obter, de maneira rápida e segura, as atualizações de segurança mais recentes. A Apple lança atualizações de software regularmente para abordar questões de segurança emergentes. Os usuários de dispositivos iOS e iPadOS recebem notificações de atualização no dispositivo. Os usuários de Mac encontram atualizações de software nas Preferências do Sistema. As atualizações são entregues via conexão sem fio para que as correções de segurança mais recentes sejam adotadas rapidamente.

O processo de atualização

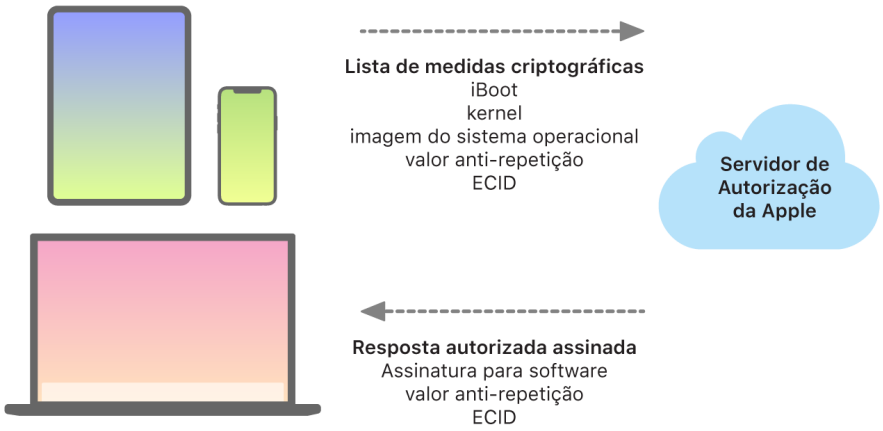
O processo de atualização usa a mesma raiz de confiança baseada em hardware que a inicialização segura, projetada para instalar apenas código assinado pela Apple. O processo de atualização também usa a autorização do software do sistema para verificar que apenas cópias das versões dos sistemas operacionais ativamente assinadas pela Apple possam ser instaladas em dispositivos iOS e iPadOS ou em computadores Mac com o ajuste Segurança Total configurado como a política de inicialização segura no Utilitário de Segurança da Inicialização. Com esses processos seguros dispostos, a Apple pode parar de assinar versões mais antigas de sistemas operacionais com vulnerabilidades conhecidas e ajudar a impedir ataques de reversão.

Para aumentar a segurança das atualizações de software, quando o dispositivo a ser atualizado está fisicamente conectado ao Mac, uma cópia completa do iOS ou iPadOS é baixada e instalada. Mas para as atualizações de software via conexão sem fio (OTA), *apenas os componentes necessários para completar uma atualização são baixados*, melhorando a eficiência da rede por não baixar todo o sistema operacional. Além disso, as atualizações de software podem ser armazenadas em um Mac com o macOS 10.13 ou posterior que tenha o Conteúdo em Cache ativado, para que os dispositivos iOS e iPadOS não precisem baixar novamente a atualização necessária da internet. (Eles ainda precisam contatar os servidores da Apple para concluir o processo de atualização.)

Processo de atualização personalizado

Durante as atualizações, uma conexão é feita ao servidor de autorização de instalações da Apple, o qual inclui uma lista de medidas criptográficas de cada parte do pacote a ser instalado (iBoot, kernel e imagem do sistema operacional, por exemplo), um valor antirreprodução aleatório (o nonce) e o Identificador Exclusivo do Dispositivo (ECID).

O servidor de autorização verifica a lista de medições apresentada e a compara com versões cujas instalações são permitidas. Caso encontre uma correspondência, ele adiciona o ECID à medição e informa o resultado. O servidor passa ao dispositivo um conjunto completo de dados assinados como parte do processo de atualização. A adição do ECID "personaliza" a autorização para o dispositivo solicitante. Ao autorizar e assinar somente as medições conhecidas, o servidor ajuda a garantir que a atualização aconteça exatamente conforme fornecida pela Apple.



A avaliação da cadeia de confiança no momento da inicialização verifica se a assinatura vem da Apple e se a medição do item carregado do dispositivo de armazenamento, combinada com o ECID do dispositivo, corresponde ao que estava coberto pela assinatura. Esses passos são projetados para garantir que, em dispositivos compatíveis com personalização, a autorização seja para um dispositivo específico e que uma versão mais antiga do sistema operacional ou do firmware de um dispositivo não possa ser copiada para outro. O nonce ajuda a impedir que um invasor salve a resposta do servidor e a use para adulterar um dispositivo ou alterar o software do sistema de outra maneira.

O processo de personalização é o motivo pelo qual uma conexão de rede à Apple sempre é exigida para atualizar qualquer dispositivo com um silício projetado pela Apple, incluindo um Mac baseado em Intel com o chip Apple T2 Security.

Por fim, o volume de dados do usuário nunca é montado durante uma atualização de software para ajudar a impedir que qualquer dado seja lido ou gravado nesse volume durante as atualizações.

Em dispositivos com Secure Enclave, esse hardware usa, de maneira similar, a autorização do software do sistema para verificar a integridade do software e é projetado para impedir instalações de versões mais antigas.

Integridade do sistema operacional

O software dos sistemas operacionais da Apple é projetado tendo a segurança como fator fundamental. Esse design inclui uma raiz de confiança de hardware — usada para permitir uma inicialização segura — e um processo de atualização de software que é rápido e seguro. Os sistemas operacionais da Apple também fazem uso das capacidades de hardware propositadamente construídas com base no silício para ajudar a impedir a exploração enquanto o sistema é executado. Esses recursos do tempo de execução protegem a integridade do código confiável enquanto ele é executado. Resumindo, o software dos sistemas operacionais da Apple ajuda a mitigar técnicas de ataque e exploração, sejam essas oriundas de um app malicioso, da web ou de qualquer outro canal. As proteções na lista a seguir estão disponíveis em dispositivos com SoCs compatíveis projetados pela Apple, incluindo o iOS, iPadOS, tvOS, watchOS e, agora, o macOS em um Mac com Apple Silicon.

Recurso	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Família M1
Proteção da Integridade do Kernel	✓	✓	✓	✓	✓	✓
Restrições de Permissões Rápidas		✓	✓	✓	✓	✓
Proteção da Integridade do Coprocessador do Sistema			✓	✓	✓	✓
Códigos de Autenticação de Ponteiros			✓	✓	✓	✓
Camada de Proteção de Página		✓	✓	✓	✓	Veja a nota abaixo.

Nota: a Camada de Proteção de Página (PPL) requer que a plataforma execute *apenas* o código assinado e confiado; esse é um modelo de segurança que não se aplica ao macOS.

Proteção da Integridade do Kernel

Depois que o kernel do sistema operacional completa a inicialização, a Proteção da Integridade do Kernel (KIP) é ativada para ajudar a impedir modificações do código do kernel e de drivers. O controlador de memória fornece uma região protegida de memória física que é usada pelo iBoot para carregar o kernel e as extensões do kernel. Após a conclusão da inicialização, o controlador de memória recusa gravações na região da memória física protegida. A Unidade de Gerenciamento de Memória (MMU) do Processador de Aplicativos é configurada para ajudar a impedir o mapeamento de código privilegiado a partir da memória física fora da região de memória protegida e para impedir mapeamentos graváveis da memória física dentro da região de memória do kernel.

Para impedir a reconfiguração, o hardware usado para ativar a KIP é bloqueado após a conclusão do processo de inicialização.

Restrições de Permissões Rápidas

A partir do Apple A11 Bionic e SoCs S3, uma nova primitiva de hardware foi apresentada. Essa primitiva, Restrições de Permissões Rápidas, inclui um registro de CPU que restringe rapidamente as permissões por thread. Com as Restrições de Permissões Rápidas (também chamadas de registros APRR), sistemas operacionais compatíveis podem remover permissões de execução da memória — sem o custo de uma chamada de sistema e uma consulta ou descarte da tabela de páginas. Esses registros fornecem mais um nível de mitigação de ataques da web, particularmente para o código compilado no tempo de execução (compilação dinâmica), já que a memória não pode ser executada eficientemente ao mesmo tempo que está sendo lida ou gravada.

Proteção da Integridade do Coprocessador do Sistema

O firmware do coprocessador lida com muitas tarefas críticas do sistema — por exemplo, com o Secure Enclave, o processador do sensor de imagens e o coprocessador de movimento. Sendo assim, sua segurança é parte essencial da segurança do sistema como um todo. Para impedir modificações ao firmware do coprocessador, a Apple usa um mecanismo chamado *Proteção da Integridade do Coprocessador do Sistema (SCIP)*.

A SCIP funciona de maneira bem semelhante à Proteção da Integridade do Kernel (KIP): no momento da inicialização, o iBoot carrega o firmware de cada coprocessador em uma região de memória protegida, reservada e separada da região da KIP. O iBoot configura a unidade de memória de cada coprocessador para ajudar a impedir:

- Mapeamentos executáveis fora da sua parte da região de memória protegida
- Mapeamentos graváveis dentro da sua parte da região de memória protegida

Também no momento da inicialização, o sistema operacional do Secure Enclave é usado para configurar a SCIP para o Secure Enclave. Depois que o processo de inicialização é concluído, o hardware usado para ativar a SCIP é bloqueado. Isso é projetado para impedir a reconfiguração.

Códigos de Autenticação de Ponteiros

Códigos de Autenticação de Ponteiros (PACs) são usados para proteger contra a exploração de erros de corrupção de memória. O software do sistema e os apps integrados usam PACs para ajudar a impedir a modificação dos ponteiros de função e endereços de retorno (ponteiros de código). O PAC usa cinco valores secretos de 128 bits para assinar instruções e dados do kernel, e cada processo do espaço do usuário possui suas próprias chaves B. Os itens usam sal e assinaturas conforme indicado a seguir.

Item	Chave	Sal
Endereço de retorno de função	IB	Endereço de armazenamento
Ponteiros de função	IA	0
Função de chamada de bloco	IA	Endereço de armazenamento
Cache de métodos de Objective-C	IB	Endereço de armazenamento + Classe + Seletor
Entradas em tabelas virtuais de C++	IA	Endereço de armazenamento + hash (nome do método truncado)
Etiqueta GoTo calculada	IA	Hash (nome da função)
Estado de threads do kernel	GA	•
Registradores de estado de threads do usuário	IA	Endereço de armazenamento
Ponteiros de tabelas virtuais de C++	DA	0

O valor da assinatura é armazenado nos bits de preenchimento não utilizados no início do ponteiro de 64 bits. A assinatura é verificada antes do uso e o preenchimento é restaurado para ajudar a garantir que o endereço do ponteiro possa ser usado. A falha na verificação resulta em aborto. Essa verificação aumenta a dificuldade de vários ataques, como o de programação orientada a retorno (ROP), o qual procura enganar o dispositivo para que execute um código existente de maneira maliciosa ao manipular endereços de retorno de função armazenados na pilha.

Camada de Proteção de Página

A Camada de Proteção de Página (PPL) no iOS, iPadOS e watchOS é projetada para impedir que o código no espaço do usuário seja modificado após a verificação da assinatura do código ser concluída. Aproveitando a Proteção da Integridade do Kernel e as Restrições de Permissões Rápidas, a PPL gerencia as substituições de permissões da tabela de páginas para garantir que apenas a PPL possa alterar as páginas protegidas que contêm o código do usuário e as tabelas de páginas. O sistema fornece uma enorme redução da superfície de ataque ao oferecer suporte à exigência da integridade do código em todo o sistema, mesmo no caso de um kernel comprometido. Essa proteção não é oferecida no macOS porque a PPL é aplicável apenas a sistemas onde todo o código executado deve ser assinado.

Capacidades de segurança adicionais do sistema macOS

Capacidades de segurança adicionais do sistema macOS

O macOS opera sobre um conjunto mais amplo de hardwares (por exemplo, CPUs baseadas em Intel, CPUs baseadas em Intel com o chip Apple T2 Security e SoCs baseados em Apple Silicon) e oferece suporte a uma gama de casos de uso de computação de propósito geral. Enquanto alguns usuários usam apenas os apps básicos pré-instalados ou aqueles disponíveis na App Store, outros são hackers de kernel que precisam desativar essencialmente todas as proteções da plataforma para executar e testar código com os níveis de confiança mais altos. A maioria encontra-se entre esses dois casos, e grande parte dessa tem periféricos e softwares que requerem níveis de acesso variados. A Apple projetou a plataforma macOS com uma abordagem integrada de hardware, software e serviços — uma plataforma que oferece segurança por design e simplifica a configuração, a implantação e o gerenciamento, mas mantém a configurabilidade esperada por usuários. O macOS também possui as principais tecnologias de segurança que um profissional de TI precisa para ajudar a proteger dados corporativos e integrar a ambientes seguros de redes empresariais.

As capacidades a seguir oferecem suporte e ajudam a manter a segurança para atender as diversas necessidades de usuários do macOS. Elas incluem:

- Segurança do volume de sistema assinado
- Proteção da Integridade do Sistema
- Caches de confiança
- Proteção para periféricos
- Compatibilidade e segurança com o Rosetta 2 (tradução automática) para um Mac com Apple Silicon
- Compatibilidade e proteção para o DMA
- Compatibilidade e segurança para extensões do kernel (kexts)
- Compatibilidade e proteção para a ROM de Opção
- Segurança para o firmware da UEFI para computadores Mac baseados em Intel

Proteção da Integridade do Sistema

O macOS usa permissões do kernel para limitar a possibilidade de gravação de arquivos críticos do sistema com um recurso chamado *Proteção da Integridade do Sistema (SIP)*. Esse recurso é separado e acrescenta à Proteção da Integridade do Kernel (KIP) baseada em hardware disponível em um Mac com Apple Silicon, o que protege o kernel na memória contra modificações. Uma tecnologia de controle de acesso obrigatório é usada para fornecer essa e diversas outras proteções no nível do kernel, incluindo sandbox e Cofre de Dados.

Controles de acesso obrigatórios

O macOS usa controles de acesso obrigatórios — políticas que definem restrições de segurança criadas pelo desenvolvedor e que não podem ser substituídas. Esta abordagem é diferente dos controles de acesso discricionários, que permitem que os usuários substituam as políticas de segurança de acordo com suas preferências.

Os controles de acesso obrigatórios não são visíveis para os usuários, mas são a tecnologia subjacente que ajuda a fornecer vários recursos importantes, como sandbox, controles parentais, preferências gerenciadas, extensões e a Proteção da Integridade do Sistema.

Proteção da Integridade do Sistema

A *Proteção da Integridade do Sistema* restringe componentes a somente leitura em locais específicos e importantes do sistema de arquivos para ajudar a impedir que códigos maliciosos os modifiquem. A Proteção da Integridade do Sistema é um ajuste específico do computador que é ativado por padrão quando um usuário atualiza para o OS X 10.11 ou posterior. Em um Mac baseado em Intel, sua desativação remove a proteção para todas as partições do dispositivo de armazenamento físico. O macOS aplica essa política de segurança a todos os processos em execução no sistema, independentemente de serem executados em sandbox ou com privilégios administrativos.

Caches de confiança

Um dos objetos incluídos na cadeia da Inicialização Segura é o cache de confiança estático, um registro confiado de todos os binários Mach-O masterizados no volume de sistema assinado. Cada Mach-O é representado por um hash de diretório de código. Para ter uma busca eficiente, esses hashes são ordenados antes de serem inseridos no cache de confiança. O diretório de código é o resultado da operação de assinatura realizada por `codesign(1)`. Para exigir o cache de confiança, a SIP deve permanecer ativada. Para desativar a exigência do cache de confiança em um Mac com Apple Silicon, a inicialização segura deve ser configurada como Segurança Permissiva.

Quando um binário é executado (seja como parte da semeação de um novo processo ou para mapear o código executável em um processo existente), seu diretório de código é extraído e tem um hash calculado. Se o hash resultante for encontrado no cache de confiança, os mapeamentos executáveis criados para o binário receberão privilégios de plataforma, o que significa que eles poderão possuir qualquer direito e serem executados sem nenhuma verificação adicional quanto à autenticação da assinatura. Isso contrasta com um Mac baseado em Intel, onde os privilégios de plataforma são passados ao conteúdo do sistema operacional pelo certificado da Apple que assina os binários. (Esse certificado não limita quais direitos o binário pode possuir.)

Binários de fora da plataforma (por exemplo, códigos de terceiros autorizados) devem ter cadeias de certificados válidas para que sejam executados e os direitos que possuem são limitados pelo perfil de assinatura emitido ao desenvolvedor pelo Programa de Desenvolvedor da Apple.

Todos os binários fornecidos com o macOS são assinados com um *identificador de plataforma*. Em um Mac com Apple Silicon, esse identificador é usado para indicar que, mesmo que o binário esteja assinado pela Apple, seu hash de diretório de código deve estar presente no cache de confiança para que seja executado. Em um Mac baseado em Intel, o identificador de plataforma é usado para realizar a revogação direcionada de binários de uma versão mais antiga do macOS; essa revogação direcionada ajuda a impedir que esses binários sejam executados em versões mais recentes.

O cache de confiança estático bloqueia completamente um conjunto de binários a uma versão determinada do macOS. Esse comportamento ajuda a impedir que binários legitimamente assinados pela Apple de sistemas operacionais mais antigos sejam introduzidos em versões mais recentes para que um invasor obtenha vantagens.

Código de plataforma fornecido fora do sistema operacional

A Apple fornece alguns binários, como o Xcode e o conjunto de ferramentas de desenvolvimento, que não são assinados com um identificador de plataforma. Mesmo assim, eles ainda têm permissão de execução com privilégios de plataforma em um Mac com Apple Silicon e naqueles com um chip T2. Por esse software de plataforma ser fornecido independentemente do macOS, ele não está sujeito aos comportamentos de revogação impostos pelo cache de confiança estático.

Caches de confiança carregáveis

A Apple fornece certos pacotes de software com *caches de confiança carregáveis*. Esses caches têm a mesma estrutura de dados dos caches de confiança estáticos. Mas embora haja apenas um cache de confiança estático — e a garantia de que seu conteúdo esteja sempre bloqueado em intervalos somente leitura após a primeira inicialização do kernel ter terminado — caches de confiança carregáveis são adicionados ao sistema no tempo de execução.

Esses caches de confiança são autenticados pelos mesmos mecanismos que autenticam a inicialização do firmware (personalização que usa o serviço de assinatura confiável da Apple) ou como objetos assinados globalmente (cujas assinaturas não os vincula a um dispositivo em particular).

Um exemplo de um cache de confiança personalizado é o cache, fornecido com a imagem de disco usada para realizar o diagnóstico em um Mac com Apple Silicon. Esse cache de confiança é personalizado, junto com a imagem de disco, e carregado no kernel do computador de um Mac enquanto ele está inicializado em um modo de diagnóstico. O cache de confiança permite que o software na imagem de disco seja executado com privilégios de plataforma.

Um exemplo de cache de confiança assinado globalmente é fornecido com as atualizações e software do macOS. Esse cache de confiança permite que um pedaço de código na atualização de software — o *cérebro da atualização* — seja executado com privilégios de plataforma. O cérebro da atualização realiza qualquer trabalho para preparar a atualização de software que o sistema host não tenha a capacidade de realizar de maneira consistente entre as versões.

Segurança do processador de periféricos em computadores Mac

Todos os sistemas de computação modernos possuem vários processadores de periféricos integrados dedicados a tarefas como rede, processamento gráfico, gerenciamento de energia e outros. Geralmente, esses processadores de periféricos têm um objetivo único e são muito menos poderosos que a CPU principal. Periféricos integrados que não implementam segurança suficiente se tornam alvos fáceis para ataques de invasores, através dos quais eles podem infectar persistentemente o sistema operacional. Com um firmware de processador de periférico infectado, um invasor poderia visar o software da CPU principal ou capturar diretamente dados sensíveis (um dispositivo Ethernet poderia ver o conteúdo dos pacotes que não estão criptografados, por exemplo).

Sempre que possível, a Apple trabalha para reduzir o número necessário de processadores de periféricos e evitar designs que exijam firmware. Mas quando processadores separados com seus próprios firmwares são necessários, medidas são tomadas para ajudar a garantir que um invasor não possa persistir nesses processadores. Isso pode ser feito ao verificar o processador de uma das seguintes maneiras:

- Ao executar o processador em um modo para que ele baixe um firmware verificado da CPU principal na inicialização
- Ao fazer com que o processador do periférico implemente sua própria cadeia de inicialização segura para verificar o firmware do processador do periférico sempre que o Mac inicializa

A Apple trabalha com fornecedores para auditar suas implementações e aprimorar seus projetos para incluir as propriedades desejadas, como:

- Garantia de um poder criptográfico mínimo
- Garantia de uma revogação forte do firmware reconhecidamente problemático
- Desativação de interfaces de depuração
- Assinatura do firmware com chaves criptográficas armazenadas nos módulos de segurança de hardware (HSMs) controlados pela Apple

Nos últimos anos, a Apple tem trabalhado com alguns fornecedores externos para adotar as mesmas estruturas de dados "Image4", código de verificação e infraestrutura de assinatura usados pelo Apple Silicon.

Quando nem a operação sem armazenamento nem o armazenamento com a inicialização segura são uma opção, o projeto exige que as atualizações de firmware sejam criptograficamente assinadas e verificadas antes da atualização do armazenamento persistente.

Rosetta 2 em um Mac com Apple Silicon

Um Mac com Apple Silicon é capaz de executar código compilado para o conjunto de instruções x86_64 com um mecanismo chamado *Rosetta 2*. Há dois tipos de tradução oferecidos: dinâmica e antecipada.

Tradução dinâmica

No canal de tradução dinâmica (JIT), um objeto Mach x86_64 é identificado cedo no caminho de execução da imagem. Quando essas imagens são encontradas, o kernel transfere o controle para uma ponta especial de tradução Rosetta em vez de para o editor de links dinâmicos, `dyld(1)`. A ponta de tradução traduz então as páginas x86_64 durante a execução da imagem. A tradução ocorre integralmente dentro do processo. O kernel ainda compara os hashes de código de cada página x86_64 com a assinatura de código anexada ao binário conforme falhas são encontradas na página. No caso de uma incongruência de hash, o kernel exige a política de remediação apropriada para tal processo.

Tradução antecipada

No caminho de tradução antecipada (AOT), os binários x86_64 são lidos do armazenamento em momentos que o sistema considera ideais para a responsividade desse código. Os artefatos traduzidos são gravados no armazenamento como um tipo especial de arquivo de objeto Mach. Esse arquivo se assemelha a uma imagem executável, mas é marcado para indicar ser o produto traduzido de outra imagem.

Nesse modelo, o artefato AOT deriva todas as suas informações de identidade da imagem executável x86_64 original. Para exigir esse vínculo, uma entidade de espaço do usuário privilegiada assina o artefato de tradução com uma chave específica do dispositivo, gerenciada pelo Secure Enclave. A chave é liberada apenas para a entidade de espaço do usuário privilegiada, que é identificada como tal ao usar um direito restrito. O diretório de código criado para o artefato de tradução inclui o hash do diretório de código da imagem executável x86_64 original. A assinatura no artefato de tradução em si é conhecida como *assinatura suplementar*.

O canal AOT começa de maneira similar ao canal JIT, com o kernel transferindo o controle para o tempo de execução Rosetta em vez de para o editor de links dinâmicos, `dyld(1)`. Mas o tempo de execução Rosetta envia uma consulta de comunicação interprocessual (IPC) para o serviço de sistema Rosetta, perguntando se há uma tradução AOT disponível para a imagem executável atual. Se encontrada, o serviço Rosetta fornece um controle para essa tradução, sendo ela mapeada no processo e executada. Durante a execução, o kernel exige os hashes de diretório de código do artefato de tradução, os quais são autenticados pela assinatura com raiz na chave de assinatura específica do dispositivo. Os hashes de diretório de código da imagem x86_64 original não são envolvidos nesse processo.

Os artefatos traduzidos são armazenados em um Cofre de Dados que não pode ser acessado no tempo de execução por nenhuma entidade além do serviço Rosetta. O serviço Rosetta gerencia o acesso ao seu cache ao distribuir descritores de arquivos somente leitura a artefatos de tradução individuais, o que limita o acesso ao cache de artefatos AOT. A comunicação interprocessual e o rastro dependente desse serviço são mantidos intencionalmente estreitos para limitar a superfície de ataque.

Se o hash do diretório de código da imagem x86_64 original não coincidir com o hash codificado na assinatura do artefato de tradução AOT, esse resultado é considerado como uma assinatura de código inválida e ações de exigências apropriadas são tomadas.

Se um processo remoto solicitar ao kernel uma consulta de direitos ou de outras propriedades de identidade de código de um executável AOT traduzido, as propriedade de identidade da imagem x86_64 original são retornadas ao processo.

Conteúdo do cache de confiança estático

O macOS 11 ou posterior é fornecido com binários que contêm partes de código de computador x86_64 e arm64. Em um Mac com Apple Silicon, o usuário pode decidir executar a parte x86_64 de um binário do sistema através do canal Rosetta — para carregar um plug-in que não tenha uma variante arm64 nativa, por exemplo. Para oferecer suporte a essa abordagem, o cache de confiança estático fornecido com o macOS geralmente contém três hashes de diretório de código por arquivo de objeto Mach:

- Um hash do diretório de código da parte arm64
- Um hash do diretório de código da parte x86_64
- Um hash do diretório de código da tradução AOT da parte x86_64

O procedimento de tradução AOT do Rosetta é determinista, no sentido de que ele reproduz uma saída idêntica para qualquer entrada determinada, independentemente de quando a tradução foi realizada ou em qual dispositivo ela foi feita.

Durante a compilação do macOS, todo arquivo de objeto Mach é executado pelo canal de tradução AOT do Rosetta associado à versão do macOS sendo compilada, e o hash de diretório de código resultante é gravado no cache de confiança. Por motivos de eficiência, os produtos traduzidos em si não são fornecidos com o sistema operacional e são reconstituídos sob demanda quando o usuário os solicita.

Quando uma imagem x86_64 está sendo executada em um Mac com Apple Silicon, se o hash de diretório de código dessa imagem estiver no cache de confiança estático, *também* espera-se que o hash de diretório de código do artefato AOT resultante esteja no cache de confiança estático. Tais produtos não são assinados pela chave específica do dispositivo porque a autoridade de assinatura tem suas raízes na cadeia de inicialização segura da Apple.

Código x86_64 não assinado

Um Mac com Apple Silicon não permite a execução do código arm64 nativo sem que uma assinatura válida esteja anexada. Essa assinatura pode ser tão simples quanto uma assinatura de código "ad hoc" (cf. `codesign(1)`) que não tenha nenhuma identidade real da metade secreta de um par de chaves assimétricas (ela é, simplesmente, uma medida não autenticada do binário).

Para oferecer compatibilidade binária, o código x86_64 traduzido tem permissão para ser executado através do Rosetta sem nenhuma informação de assinatura. Nenhuma identidade específica é passada a esse código pelo procedimento de assinatura do Secure Enclave específico do dispositivo, e ele é executado com, precisamente, as mesmas limitações de execução do código nativo não assinado em um Mac baseado em Intel.

Proteções do acesso direto à memória em computadores Mac

Para atingir taxas de transferência altas em interfaces de alta velocidade como PCIe, FireWire, Thunderbolt e USB, os computadores devem oferecer suporte ao acesso direto à memória (DMA) de periféricos. Ou seja, eles devem ser capazes de ler e gravar na RAM sem o envolvimento contínuo da CPU. Desde 2012, computadores Mac implementaram várias tecnologias para se proteger o DMA, resultando no melhor e mais abrangente conjunto de proteções ao DMA em qualquer PC.

Proteções do acesso direto à memória em um Mac com Apple Silicon

Os sistemas no chip da Apple contêm uma Unidade de Gerenciamento de Memória de Entrada/Saída (IOMMU) para cada agente de DMA no sistema, incluindo as portas PCIe e Thunderbolt. Pelo fato de cada IOMMU ter seus próprios conjuntos de tabelas de tradução de endereços para traduzir pedidos de DMA, os periféricos conectados por PCIe ou Thunderbolt podem acessar apenas a memória que tenha sido explicitamente mapeada para seus respectivos usos. Periféricos não podem acessar a memória pertencente a outras partes do sistema, como do kernel ou firmware, ou a memória atribuída a outros periféricos. Se uma IOMMU detectar uma tentativa de um periférico acessar uma memória não mapeada para o uso desse periférico, ela aciona um pânico no kernel.

Proteções do acesso direto à memória em um Mac baseado em Intel

Computadores Mac baseados em Intel com a Tecnologia de Virtualização para E/S Direcionada da Intel (VT-d) inicializam a IOMMU, permitindo o remapeamento e interrupção de mapeamento de DMA bem cedo no processo de inicialização para mitigar diversas classes de vulnerabilidades de segurança. O hardware da IOMMU da Apple começa a operar com uma política "negar por padrão" para que, no instante em que o sistema seja ligado, ele comece a bloquear automaticamente os pedidos de DMA de periféricos. Depois de inicializadas por software, as IOMMUs começam a permitir os pedidos de DMA de periféricos às regiões da memória que tenham sido explicitamente mapeadas para seus respectivos usos.

Nota: a interrupção de remapeamento em PCIe não é necessária em um Mac com Apple Silicon porque cada IOMMU gerencia as MSIs de seus próprios periféricos.

Desde o macOS 11, todos os computadores Mac com um chip Apple T2 Security executam drivers da UEFI que facilitam o DMA em um ambiente restrito de ring 3 quando esses drivers estão emparelhando com dispositivos externos. Essa propriedade ajuda a mitigar vulnerabilidades de segurança que podem ocorrer quando um dispositivo malicioso interage com um driver de UEFI de uma maneira inesperada no momento da inicialização. Particularmente, ela reduz o impacto de vulnerabilidades no gerenciamento de buffers do DMA por parte dos drivers.

Extensões do kernel no macOS

A partir do macOS 11, caso extensões de kernel (kexts) de terceiros estejam ativadas, elas não podem ser carregadas no kernel sob demanda. Em vez disso, elas são combinadas em uma *Coleção do Kernel Auxiliar (AuxKC)*, que é carregada durante o processo de inicialização. Em um Mac com Apple Silicon, a medida da AuxKC é assinada na LocalPolicy (em hardwares anteriores, a AuxKC residia no volume de dados). A reconstrução da AuxKC requer a aprovação do usuário e a reinicialização do macOS para carregar as alterações no kernel, além da configuração da inicialização segura como Segurança Reduzida.

Importante: kexts não são mais recomendadas para o macOS. Kexts colocam em risco a integridade e a confiabilidade do sistema operacional e a Apple recomenda que usuários selecionem soluções que não exijam extensão do kernel.

Extensões do kernel em um Mac com Apple Silicon

Kexts devem ser explicitamente ativadas em um Mac com Apple Silicon através do pressionamento do botão de força ao inicializar para entrar no modo Um recoveryOS Verdadeiro (1TR), reverter para a Segurança Reduzida e selecionar a opção para ativar extensões do kernel. Essa ação também requer que uma senha de administrador seja digitada para autorizar a reversão. A combinação do 1TR com a exigência de senha dificulta que invasores agindo de dentro do macOS via software injetem kexts no macOS que possam ser exploradas para obter privilégios de kernel.

Depois que um usuário autoriza o carregamento de kexts, o fluxo de Carregamento de Extensões do Kernel Aprovado pelo Usuário acima é usado para autorizar a instalação de kexts. A autorização usada para o fluxo acima também é usada para capturar um hash SHA384 da lista de kexts autorizadas pelo usuário (UAKL) na LocalPolicy. O deamon de gerenciamento do kernel (`kmd`) fica então responsável por validar apenas as kexts encontradas na UAKL para incluí-las na AuxKC.

- Se a Proteção da Integridade do Sistema (SIP) estiver ativada, a assinatura de cada kext é verificada antes de ser incluída na AuxKC.
- Se a SIP estiver desativada, a assinatura da kext não é exigida.

Essa abordagem permite fluxos de Segurança Permissiva para que desenvolvedores ou usuários que não façam parte do Programa de Desenvolvedor da Apple possam testar kexts antes de serem assinadas.

Depois que a AuxKC é criada, sua medida é enviada ao Secure Enclave para ser assinada e incluída em uma estrutura de dados Image4 que pode ser avaliada pelo iBoot na inicialização. Como parte da construção da AuxKC, um Recibo de kext também é gerado. Esse recibo contém a lista das kexts realmente incluídas na AuxKC, já que o conjunto poderia ser um subconjunto da UAKL caso kexts banidas fossem encontradas. Um hash SHA384 da estrutura de dados Image4 da AuxKC e o recibo de kext são incluídos na LocalPolicy. O hash Image4 da AuxKC é usado para verificação extra pelo iBoot na inicialização para ajudar a garantir que não seja possível inicializar um arquivo Image4 mais antigo da AuxKC assinado pelo Secure Enclave com uma LocalPolicy mais recente. O recibo de kext é usado por subsistemas como o Apple Pay para determinar se há algum kext carregado no momento que possa interferir com a confiabilidade do macOS. Em caso positivo, as capacidades do Apple Pay podem ser desativadas.

Alternativas a kexts (macOS 10.15 ou posterior)

O macOS 10.15 permite que desenvolvedores estendam as funcionalidades do macOS ao instalar e gerenciar extensões do sistema que são executadas no espaço do usuário, e não no nível do kernel. Por serem executadas no espaço do usuário, as extensões do sistema aumentam a estabilidade e a segurança do macOS. Embora kexts tenham inerentemente acesso total a todo o sistema operacional, as extensões em execução no espaço do usuário recebem apenas os privilégios necessários para realizar suas funções especificadas.

Desenvolvedores podem usar frameworks, incluindo DriverKit, EndpointSecurity e NetworkExtension, para escrever drivers de USB e interface humana, ferramentas de segurança de pontos finais (como para a prevenção de perda de dados ou outros agentes de pontos finais) e ferramentas de VPN e rede — tudo isso sem precisar escrever kexts. Agentes de segurança de terceiros devem ser usados apenas se fizerem uso dessas APIs ou tiverem um planejamento robusto para transicionar em direção a elas e se distanciar de extensões do kernel.

Carregamento de Extensão do Kernel Aprovada pelo Usuário

Para melhorar a segurança, o consentimento do usuário é necessário para o carregamento de extensões do kernel instaladas com o macOS 10.13 ou após sua instalação. Esse processo é conhecido como *Carregamento de Extensões do Kernel Aprovado pelo Usuário*. A autorização do administrador é necessária para aprovar uma extensão do kernel. As extensões do kernel não exigem autorização caso elas:

- Tenham sido instaladas em um Mac com macOS 10.12 ou anterior
- Estejam substituindo extensões aprovadas anteriormente
- Tenham permissão para ser carregadas sem o consentimento do usuário ao usar a ferramenta de linha de comando `spctl`, disponível quando um Mac é inicializado a partir do recoveryOS
- Tenham permissão para serem carregadas usando a configuração do gerenciamento de dispositivos móveis (MDM)

  A partir do macOS 10.13.2, os usuários podem usar o MDM para especificar uma lista de extensões do kernel que podem ser carregadas sem o consentimento do usuário. Essa opção requer um Mac com macOS 10.13.2 que esteja registrado no MDM — através do Apple School Manager, Apple Business Manager ou registro no MDM feito pelo usuário.

Segurança da ROM de Opção no macOS

Nota: No momento, não há suporte para ROMs de Opção em um Mac com Apple Silicon.

Segurança da ROM de Opção em um Mac com o chip Apple T2 Security

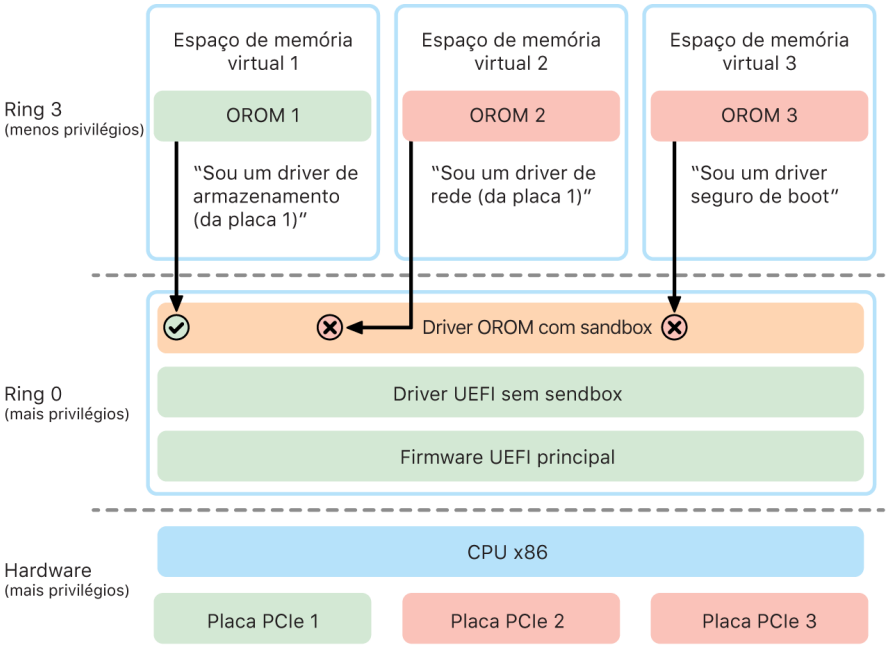
Dispositivos Thunderbolt e PCIe têm uma "ROM de Opção (OROM)" conectada fisicamente ao dispositivo (geralmente ela não é uma ROM de verdade, mas sim um chip regravável que armazena firmware). Em sistemas baseados em UEFI, esse firmware geralmente é um driver de UEFI, que é lido pelo firmware da UEFI e executado. O código executado deve inicializar e configurar o hardware do qual foi obtido, para que o hardware possa ser usado pelo restante do firmware. Essa habilidade é necessária para que hardwares especializados de terceiros possam carregar e operar durante as primeiras fases da inicialização — por exemplo, para inicializar a partir de matrizes RAID externas.

Contudo, como as OROMs geralmente são regraváveis, se um invasor sobrescrevesse a OROM de um periférico legítimo, o código do invasor seria executado no início do processo de inicialização, e poderia adulterar o ambiente de execução e violar a integridade dos softwares carregados posteriormente. Da mesma forma, se o invasor introduzisse seu próprio dispositivo malicioso no sistema, ele também poderia executar um código malicioso.

No macOS 10.12.3, o comportamento de computadores Mac vendidos após 2011 foi alterado para que as OROMs não fossem executadas por padrão durante a inicialização do Mac, a menos que uma combinação especial de teclas fosse pressionada. Essa combinação de teclas ofereceu proteção contra a introdução não intencional de OROMs maliciosas na sequência de inicialização do macOS. O comportamento padrão do Utilitário de Senha de Firmware também foi alterado para que quando o usuário definisse uma senha de firmware, as OROMs não pudessem ser executadas mesmo que a combinação de teclas fosse pressionada. Isso protegia contra a introdução de uma OROM maliciosa por um invasor fisicamente presente. Para os usuários que ainda precisam executar OROMs enquanto uma senha de firmware estiver definida, uma opção não padrão pode ser configurada com a ferramenta de linha de comando `firmwarepasswd` no macOS.

Segurança de sandbox da OROM

No macOS 10.15, o firmware da UEFI foi atualizado para conter um mecanismo de sandbox de OROMs e para retirar os privilégios destas. O firmware da UEFI geralmente executa todo o código, incluindo OROMs, no nível máximo de privilégio da CPU, chamado de ring 0, e tem um único espaço de memória virtual compartilhada para todo o código e dados. Ring 0 é o nível de privilégio no qual o kernel do macOS é executado, enquanto o nível de privilégio mais baixo, ring 3, é onde os apps são executados. O sandbox da OROM usa a separação da memória virtual da mesma forma que o kernel e faz com que as OROMs sejam executadas no ring 3, retirando os privilégios das OROMs.



Além disso, o sandbox restringe significativamente tanto as interfaces que podem ser chamadas pelas OROMs (similarmente ao filtro de chamadas do sistema em kernels) quanto o tipo de dispositivo que uma OROM pode usar para se registrar (similarmente à aprovação de apps). O benefício desse design é que as OROMs maliciosas não podem mais gravar diretamente em nenhum lugar dentro da memória do ring 0. Em vez disso, elas são limitadas a uma interface de sandbox bem definida e estreita. Essa interface limitada reduz significativamente a superfície de ataque e obriga os invasores a primeiro escapar do sandbox e aumentar o privilégio.

Segurança do firmware da UEFI em um Mac baseado em Intel

Um Mac baseado em Intel com um chip Apple T2 Security oferece segurança através do uso do firmware da UEFI (Intel).

Visão geral

Desde 2006, computadores Mac com uma CPU baseada em Intel usam um firmware da Intel baseado na versão 1 ou 2 do kit de desenvolvimento (EDK) da Interface de Firmware Extensível (EFI). O código baseado no EDK2 está em conformidade com a especificação da Interface de Firmware Extensível Unificada (UEFI). Esta seção refere-se ao firmware da Intel como *firmware da UEFI*. O firmware da UEFI era o primeiro código a ser executado no chip Intel.

Em um Mac baseado em Intel sem o chip Apple T2 Security, a raiz de confiança do firmware da UEFI é o chip onde o firmware está armazenado. As atualizações do firmware da UEFI são assinadas digitalmente pela Apple e verificadas pelo firmware antes da atualização do armazenamento. Para ajudar a impedir ataques de reversão, as atualizações sempre devem ter uma versão mais recente que a versão existente. Porém, um invasor que tiver acesso físico ao Mac poderia usar um hardware para se conectar ao chip de armazenamento do firmware e atualizá-lo para que contenha conteúdo malicioso. Da mesma forma, se forem encontradas vulnerabilidades no início do processo de inicialização do firmware da UEFI (antes que ele restrinja as gravações no chip de armazenamento), isso também poderia levar à infecção persistente do firmware da UEFI. Essa limitação da arquitetura do hardware é comum na maioria dos PCs baseados em Intel e está presente em todos os computadores Mac baseados em Intel sem o chip T2.

Para ajudar a impedir ataques físicos que subvertam o firmware da UEFI, computadores Mac foram modificados para colocar a raiz de confiança no firmware da UEFI no chip T2. Nesses computadores Mac, a raiz de confiança do firmware da UEFI é especificamente o firmware do T2, como descrito em Processo de inicialização de um Mac baseado em Intel.

Subcomponente do Mecanismo de Gerenciamento Intel (ME)

Um subcomponente armazenado no firmware da UEFI é o firmware do *Mecanismo de Gerenciamento Intel (ME)*. O ME — um processador e subsistema a parte dentro de chips Intel — é usado primariamente para a proteção do copyright de áudio e vídeo em um Mac que tenha apenas gráficos baseados em Intel. Para reduzir a superfície de ataque desse subcomponente, um Mac baseado em Intel executa um firmware ME personalizado, do qual a maioria dos componentes foi removido. Pelo fato do firmware ME resultante do Mac ser menor que a compilação mínima padrão disponibilizada pela Intel, vários componentes que foram alvo de ataques públicos por pesquisadores de segurança no passado, não estão mais presentes.

Modo de Gerenciamento do Sistema (SMM)

Os processadores Intel possuem um modo especial de execução que é diferente da operação normal. Chamado de *Modo de Gerenciamento do Sistema (SMM)*, ele foi introduzido originalmente para cuidar de operações sensíveis ao tempo, como o gerenciamento de energia. Contudo, para realizar tais ações, computadores Mac usavam historicamente um microcontrolador separado, chamado de *Controlador do Gerenciamento do Sistema (SMC)*. O SMC não é mais um microcontrolador separado e foi integrado ao chip T2.

Segurança do sistema para o watchOS

O Apple Watch usa muitas das mesmas capacidades de segurança da plataforma que o iOS e o iPadOS usam. Por exemplo, o Apple Watch:

- Realiza uma inicialização segura e atualizações de software seguras
- Mantém a integridade do sistema operacional
- Ajuda a proteger dados — tanto no dispositivo e ao comunicar-se com um iPhone emparelhado ou com a internet

As tecnologias compatíveis incluem aquelas na lista de Segurança do Sistema (por exemplo, KIP, SKP e SCIP), assim como Proteção de Dados, chaves e tecnologias de rede.

Atualização do watchOS

O watchOS pode ser configurado para atualizar durante a noite. Para obter mais informações sobre como o código do Apple Watch é armazenado e usado durante a atualização, consulte Keybags.

Detecção de braço

Se a detecção de braço estiver ativada, o dispositivo é bloqueado automaticamente logo após ser removido do braço do usuário. Se a detecção de braço estiver desativada, a Central de Controle oferece uma opção para bloquear o Apple Watch. Quando o Apple Watch está bloqueado, o Apple Pay só pode ser usado ao digitar o código no Apple Watch. A detecção de braço pode ser desativada no app Apple Watch do iPhone. Esse ajuste também pode ser aplicado por meio de uma solução de gerenciamento de dispositivos móveis (MDM).

Bloqueio de Ativação

Quando o Buscar está ativado no iPhone, o respectivo Apple Watch emparelhado pode usar o Bloqueio de Ativação. O Bloqueio de Ativação dificulta o uso ou venda de um Apple Watch perdido ou roubado. O Bloqueio de Ativação requer o ID Apple e a senha do usuário para desemparelhar, apagar ou reativar o Apple Watch.

Emparelhamento seguro com iPhone

O Apple Watch pode ser emparelhado apenas com um iPhone por vez. Quando o Apple Watch é desemparelhado, o iPhone comunica instruções para apagar todo o conteúdo e dados do Apple Watch.

A segurança do emparelhamento do Apple Watch com o iPhone é feita usando um processo fora de banda para trocar chaves públicas, seguido pelo segredo compartilhado do link Bluetooth Low Energy (BLE). O Apple Watch exibe um padrão animado, capturado pela câmera do iPhone. O padrão contém um segredo codificado usado pelo emparelhamento fora de banda BLE 4.1. O padrão de emparelhamento BLE Passkey Entry é usado como método alternativo, se necessário.

Depois de estabelecer a sessão BLE e criptografá-la com o protocolo de segurança mais alto disponível na Especificação Bluetooth Core, o iPhone e o Apple Watch usam um dos seguintes para trocar chaves:

- Um processo adaptado do Serviço de Identidade da Apple (IDS), conforme descrito em Visão geral da segurança do iMessage.
- Uma troca de chaves com IKEv2/IPsec. A troca de chaves inicial é autenticada com a chave de sessão Bluetooth (em casos de emparelhamento) ou as chaves IDS (em casos de atualização do sistema operacional). Cada dispositivo gera um par de chaves Ed25519 de 256 bits pública e privada e, durante o processo inicial de troca de chaves, as chaves públicas são trocadas.

Nota: o mecanismo usado para a troca e criptografia das chaves varia, dependendo de quais versões dos sistemas operacionais estejam no iPhone e no Apple Watch. Dispositivos iPhone com iOS 13 ou posterior quando emparelhados com um Apple Watch com watchOS 6 ou posterior usam apenas IKEv2/IPsec para a troca e criptografia de chaves.

Depois que as chaves forem trocadas:

- A chave da sessão Bluetooth é descartada e todas as comunicações entre o iPhone e o Apple Watch são criptografadas com um dos métodos acima — com os links criptografados de Bluetooth, Wi-Fi e celular oferecendo uma camada de criptografia secundária.
- (Somente IKEv2/IPsec) As chaves são armazenadas nas chaves Sistema e usadas para a autenticação futura de sessões IKEv2/IPsec entre os dispositivos. As demais comunicações entre esses dispositivos são criptografadas e têm sua integridade protegida com AES-256-GCM ou ChaCha20-Poly1305 (chaves de 256 bits) em dispositivos iPhone com iOS 15 ou posterior emparelhados com um Apple Watch Series 4 ou posterior com watchOS 8 ou posterior.

O endereço do dispositivo Bluetooth Low Energy é trocado em intervalos de 15 minutos para reduzir o risco do dispositivo ser rastreado localmente se uma pessoa transmitir um identificador persistente.

Para oferecer suporte a apps que necessitam de dados de transmissão, a criptografia é fornecida com os métodos descritos em Segurança do FaceTime, através do Serviço de Identidade da Apple (IDS) oferecido pelo iPhone emparelhado ou de uma conexão direta à internet.

O Apple Watch implementa o armazenamento criptografado por hardware e a proteção de arquivos e itens das chaves com base em classes. Keybags de acesso controlado também são usadas em itens das chaves. As chaves usadas para as comunicações entre o Apple Watch e o iPhone também são mantidas em segurança através do uso de proteção com base em classes. Para obter mais informações, consulte Keybags para Proteção de Dados.

Desbloqueio Automático e Apple Watch

Para ter mais conveniência ao usar vários dispositivos Apple, alguns dispositivos podem desbloquear outros automaticamente sob certas circunstâncias. O Desbloqueio Automático é compatível com três usos:

- Um Apple Watch pode ser desbloqueado por um iPhone.
- Um Mac pode ser desbloqueado por um Apple Watch.
- Um iPhone pode ser desbloqueado por um Apple Watch quando um usuário é detectado com o nariz e a boca cobertos.

Todos os três casos de uso baseiam-se na mesma fundação básica: um protocolo Station-to-Station (STS) autenticado mutuamente, com Chaves de Longo Prazo trocadas no momento da ativação do recurso e chaves de sessão efêmeras exclusivas, negociadas para cada pedido. Independentemente do canal de comunicação subjacente, o túnel STS é negociado diretamente entre os Secure Enclaves em ambos os dispositivos e todos os materiais criptográficos são mantidos dentro desse domínio seguro (com a exceção de computadores Mac sem um Secure Enclave, que terminam o túnel STS no kernel).

Desbloqueio

Uma sequência completa de desbloqueio pode ser dividida em duas fases. Primeiro, o dispositivo sendo desbloqueado (o “destino ”) gera um segredo criptográfico de desbloqueio e o envia para o dispositivo que realiza o desbloqueio (o “iniciador”). Depois, o iniciador usa o segredo gerado anteriormente para realizar o desbloqueio.

Para armar o desbloqueio automático, os dispositivos usam uma conexão BLE para se conectarem. Depois, um segredo de desbloqueio de 32 bytes gerado aleatoriamente pelo dispositivo de destino é enviado para o iniciador pelo túnel STS. Durante o próximo desbloqueio biométrico ou por código, o dispositivo de destino embala sua chave derivada do código (PDK) com o segredo de desbloqueio e descarta o segredo de desbloqueio da memória.

Para realizar o desbloqueio, os dispositivos iniciam uma nova conexão BLE e usam Wi-Fi peer-to-peer para aproximar a distância entre si com segurança. Se os dispositivos estiverem dentro do intervalo especificado e as políticas de segurança exigidas forem atendidas, o iniciador envia seu segredo de desbloqueio para o destino pelo túnel STS. O destino gera um novo segredo de desbloqueio de 32 bytes e o retorna ao iniciador. Se o segredo de desbloqueio atual enviado pelo iniciador descriptografar o registro de desbloqueio, o dispositivo de destino é desbloqueado e a PDK é reembalada com um novo segredo de desbloqueio. Por fim, o novo segredo de desbloqueio e a PDK são descartados da memória do destino.

Políticas de segurança do Desbloqueio Automático do Apple Watch

Para ter mais conveniência, o Apple Watch pode ser desbloqueado por um iPhone diretamente após a configuração inicial, sem exigir que o usuário digite o código primeiro no Apple Watch. Para atingir isso, o segredo de desbloqueio aleatório (gerado durante a primeira sequência de desbloqueio depois da ativação do recurso) é usado para criar um registro de guarda de longo prazo, que é armazenado na keybag do Apple Watch. O segredo do registro de guarda é armazenado nas chaves do iPhone e usado para compilar automaticamente uma nova sessão após cada reinício do Apple Watch.

Políticas de segurança do Desbloqueio Automático do iPhone

Políticas de segurança adicionais são aplicadas ao Desbloqueio Automático do iPhone com o Apple Watch. O Apple Watch não pode ser usado no lugar do Face ID no iPhone para outras operações, como autorizações do Apple Pay ou de apps. Quando Apple Watch desbloqueia com sucesso um iPhone emparelhado, o Apple Watch mostra uma notificação e reproduz um retorno tátil associado. Se o usuário toca no botão Bloquear iPhone na notificação, o Apple Watch envia ao iPhone um comando de bloqueio via BLE. Quando o iPhone recebe o comando de bloqueio, ele bloqueia o Face ID e o desbloqueio com o Apple Watch. O próximo desbloqueio do iPhone deve ser realizado com o código do iPhone.

O desbloqueio bem-sucedido de um iPhone emparelhado a partir do Apple Watch (quando ativado) requer que os seguintes critérios sejam atendidos:

- O iPhone deve ter sido desbloqueado por um outro método ao menos uma vez depois do Apple Watch ter sido colocado no braço e desbloqueado.
- Os sensores devem ser capazes de detectar que o nariz e a boca estão cobertos.
- A distância medida deve estar entre 2–3 metros ou menos
- O Apple Watch não deve estar no modo hora de dormir.
- O Apple Watch ou o iPhone devem ter sido desbloqueados recentemente, ou o Apple Watch deve ter detectado um movimento físico indicando que a pessoa está ativa (não está dormido, por exemplo).
- O iPhone deve ter sido desbloqueado ao menos uma vez nas últimas 6,5 horas.
- O iPhone deve estar em um estado no qual o Face ID tenha permissão de realizar o desbloqueio do dispositivo. (Para obter mais informações, consulte Face ID, Touch ID, códigos e senhas.)

Aprovação no macOS com o Apple Watch

Quando o Desbloqueio Automático com o Apple Watch está ativado, o Apple Watch pode ser usado no lugar ou em conjunto com o Touch ID para aprovar solicitações de autorização e autenticação de:

- macOS e apps Apple que solicitam autorização
- Apps de terceiros que solicitam autenticação
- Senhas salvas do Safari
- Notas Seguras

Uso seguro de Wi-Fi, celular, iCloud e Gmail

Quando o Apple Watch não está dentro do alcance do Bluetooth, é possível usar Wi-Fi ou dados celulares. O Apple Watch conecta-se automaticamente a redes Wi-Fi que já foram conectadas no iPhone emparelhado e cujas credenciais foram sincronizadas com o Apple Watch enquanto os dispositivos estavam no raio de alcance. Esse comportamento de conexão automática pode então ser configurado por rede, na seção Wi-Fi do app Ajustes do Apple Watch. As redes Wi-Fi que nunca foram conectadas anteriormente em nenhum dos dispositivos podem ser conectadas manualmente na seção Wi-Fi do app Ajustes do Apple Watch.

Quando o Apple Watch e o iPhone estão fora do raio de alcance, o Apple Watch conecta-se diretamente aos servidores do iCloud e Gmail para obter os dados do Mail, em vez de sincronizar os dados do Mail com o iPhone emparelhado pela internet. Para contas do Gmail, o usuário precisa autenticar no Google na seção Mail do app Watch no iPhone. O token do OAuth recebido do Google é enviado ao Apple Watch em formato criptografado pelo Serviço de Identidade da Apple (IDS), para que possa ser usado para obter e-mails. Esse token do OAuth jamais é usado para conectividade com o servidor do Gmail a partir do iPhone emparelhado.

Geração de números aleatórios

Os geradores criptográficos de números pseudoaleatórios (CPRNGs) são um elemento básico importante de um software seguro. Para esse fim, a Apple fornece um software de CPRNG confiável em execução nos kernels do iOS, iPadOS, macOS, tvOS e watchOS. Ele é responsável por agregar a entropia bruta do sistema e fornecer números aleatórios seguros para clientes tanto no kernel quanto no espaço do usuário.

Fontes de entropia

O CPRNG do kernel é alimentado por várias fontes de entropia durante a inicialização e ao longo da vida do dispositivo. Algumas delas são (de acordo com a disponibilidade):

- O TRNG de hardware do Secure Enclave
- Oscilações com base no tempo coletadas durante a inicialização
- Entropia coletada em interrupções de hardware
- Um arquivo inicial usado para persistência da entropia entre inicializações
- Instruções aleatórias da Intel — como RDSEED e RDRAND (somente em um Mac baseado em Intel)

O CPRNG do kernel

O CPRNG do kernel possui um projeto derivado do Fortuna e tem como objetivo um nível de segurança de 256 bits. Ele fornece números aleatórios de alta qualidade para clientes no espaço do usuário através das seguintes APIs:

- A chamada de sistema `getentropy`(2)
- O dispositivo aleatório (/dev/random)

O CPRNG do kernel aceita a entropia fornecida pelo usuário através de gravações no dispositivo aleatório.

Dispositivo de Pesquisa de Segurança da Apple

O Dispositivo de Pesquisa de Segurança da Apple é um iPhone especialmente montado que permite que pesquisadores de segurança realizem pesquisas no iOS sem precisar desmontar ou desativar os recursos de segurança de plataforma do iPhone. Com esse dispositivo, um pesquisador pode carregar "por fora" um conteúdo que é executado com as permissões equivalentes da plataforma, realizando assim a pesquisa em uma plataforma que se aproxima muito mais daquela dos dispositivos de produção.

Para ajudar a garantir que dispositivos de usuários não sejam afetados pela política de execução do dispositivo de pesquisa de segurança, as alterações de política são implementadas em uma variante do iBoot e na Coleção do Kernel de Inicialização. Esses falham quando inicializados em um hardware de usuário. O iBoot de pesquisa verifica um novo estado de montagem e entra em um loop de pânico se estiver sendo executado em um hardware não montado para pesquisa.

O subsistema de cryptex permite que um pesquisador carregue um cache de confiança personalizado e uma imagem de disco com o conteúdo correspondente. Um número de medidas abrangentes de defesa foram implementadas, projetadas para garantir que esse subsistema não permita a execução em dispositivos de usuários:

- O `launchd` não carrega a lista de propriedades `cryptexd` do launchd se detectar um dispositivo normal de clientes.
- O `cryptexd` aborta se detectar um dispositivo normal de clientes.
- `AppleImage4` não oferece o nonce usado para verificar um cryptex de pesquisa em um dispositivo normal de clientes.
- O servidor de assinatura se recusa a personalizar uma imagem de disco de cryptex para um dispositivo fora de uma lista explícita de permitidos.

Para respeitar a privacidade do pesquisador de segurança, apenas as medidas (por exemplo, hashes) dos executáveis ou cache do kernel e os identificadores do dispositivo de pesquisa de segurança são enviados à Apple durante a personalização. A Apple não recebe o conteúdo do cryptex sendo carregado no dispositivo.

Para evitar que um indivíduo malicioso tente mascarar um dispositivo de pesquisa como um dispositivo de usuário para enganar uma vítima a usá-lo corriqueiramente, o dispositivo de pesquisa de segurança apresenta as seguintes diferenças:

- O dispositivo de pesquisa de segurança só inicializa enquanto estiver sendo carregado. Isso pode ser feito com um cabo Lightning ou um carregador Qi compatível. Se o dispositivo não estiver sendo carregado durante a inicialização, ele entra no modo de Recuperação. Se o usuário começar a carregar e reinicializar o dispositivo, ele inicializa como um dispositivo normal. Assim que o XNU é iniciado, o dispositivo não precisa estar carregando para continuar operando.
- As palavras *Dispositivo de Pesquisa de Segurança* aparecem abaixo do logotipo da Apple durante a inicialização do iBoot.
- O kernel XNU inicializa no modo detalhado.
- O dispositivo tem um entalhe na lateral com a mensagem: "Property of Apple. Confidential and Proprietary. Call +1 877 595 1125."

A seguir, medidas adicionais que são implementadas no software que aparece após a inicialização:

- As palavras *Dispositivo de Pesquisa de Segurança* aparecem durante a configuração do dispositivo.
- As palavras *Dispositivo de Pesquisa de Segurança* aparecem na Tela Bloqueada e no app Ajustes.

O Dispositivo de Pesquisa de Segurança oferece a pesquisadores as seguintes capacidades que um dispositivo de usuário não oferece. Os pesquisadores podem:

- Carregar código executável "por fora" no dispositivo com direitos arbitrários com o mesmo nível de permissão dos componente do sistema operacional da Apple.
- Iniciar serviços na inicialização.
- Persistir o conteúdo entre reinicializações.
- Usar o direito `research.com.apple.license-to-operate` para permitir que um processo depure qualquer outro processo no sistema, incluindo processos do sistema.

  O namespace `research.` é respeitado apenas pela variante RESEARCH da extensão de kernel AppleMobileFileIntegrity. Qualquer processo com esse direito é finalizado no dispositivo de um cliente durante a validação da assinatura.
- Personalizar e restaurar um cache de kernel personalizado.

Criptografia e Proteção de Dados

Visão geral da Criptografia e Proteção de Dados

Os recursos da cadeia de inicialização segura, de segurança do sistema e de apps ajudam a verificar que apenas códigos confiáveis sejam executados em um dispositivo. Os dispositivos Apple possuem recursos de criptografia adicionais para resguardar os dados do usuário, mesmo que outras partes da infraestrutura de segurança tenham sido comprometidas (por exemplo se um dispositivo for perdido ou estiver executando código não confiável). Todos esses recursos beneficiam tanto usuários quanto administradores de TI, protegendo informações pessoais e corporativas, e fornecendo métodos para o apagamento remoto completo e imediato no caso de roubo ou perda do dispositivo.

Dispositivos iOS e iPadOS usam uma metodologia de criptografia de arquivos chamada *Proteção de Dados*, enquanto dados em computadores Mac são protegidos com uma tecnologia de criptografia de volumes chamada *FileVault*. Um Mac com Apple Silicon usa um modelo híbrido com suporte à Proteção de Dados, com duas ressalvas: o nível de proteção mais baixo Classe (D) não é compatível, e o nível padrão (Classe C) usa uma chave de volume e se comporta da mesma maneira que o FileVault em um Mac baseado em Intel. Em todos os casos, as hierarquias de gerenciamento de chaves têm suas raízes no silício dedicado do Secure Enclave, e um Mecanismo AES dedicado oferece suporte à criptografia de velocidade em linha e ajuda a garantir que chaves de criptografia de vida longa não sejam expostas ao sistema operacional do kernel ou CPU (onde podem ser comprometidas). (Um Mac baseado em Intel com um T1 ou que não tenha um Secure Enclave não usa um silício dedicado para proteger suas chaves de criptografia do FileVault.)

Além de usar a Proteção de Dados e o FileVault para ajudar a impedir o acesso não autorizado a dados, a Apple usa *kernels do sistema operacional* para exigir proteção e segurança. O kernel usa controles de acesso para apps com sandbox (os quais restringem quais dados um app pode acessar) e um mecanismo chamado *Cofre de Dados* (o qual, em vez de restringir as chamadas que um app pode fazer, restringe o acesso aos dados de um app de todos os outros apps solicitantes).

Códigos e senhas

Para proteger os dados do usuário de um ataque malicioso, a Apple usa códigos no iOS e iPadOS e senhas no macOS. Quanto mais longo o código ou a senha, mais fortes eles são e mais fáceis de desencorajar ataques de força bruta. Para desencorajar ainda mais os ataques, a Apple impõe tempos de atraso (no iOS e iPadOS) e um número limitado de tentativas de inserção de senha (no Mac).

No iOS e iPadOS, ao configurar um código do dispositivo ou senha, o usuário ativa automaticamente a Proteção de Dados. A Proteção de Dados também é ativada em outros dispositivos que possuem um sistema no chip (SoC) da Apple, como o Mac com Apple Silicon, a Apple TV e o Apple Watch. No macOS, a Apple usa o *FileVault*, um programa integrado de criptografia de volumes.

Como códigos e senhas fortes aumentam a segurança

O iOS e o iPadOS aceitam códigos de seis ou quatro dígitos e códigos alfanuméricos de qualquer tamanho. Além de desbloquear o dispositivo, um código ou senha fornece entropia para certas chaves de criptografia. Isso significa que se um invasor se apossar de um dispositivo, ele não conseguirá acessar os dados em classes de proteção específicas sem o código.

O código ou senha é trançado ao UID do dispositivo, portanto, ataques de força bruta precisam ser realizados no dispositivo sendo atacado. Um grande número de iterações é usado para fazer com que as tentativas sejam cada vez mais lentas. O número de iterações é calibrado de forma que uma tentativa dure aproximadamente 80 milissegundos. Na verdade, seriam necessários mais de cinco anos e meio para tentar todas as combinações de um código alfanumérico de seis caracteres com letras minúsculas e números.

Quanto mais forte for o código do usuário, mais forte se torna a chave de criptografia. E ao usar o Face ID e o Touch ID, o usuário pode estabelecer um código muito mais forte do que seria prático de outra maneira. O código mais forte aumenta a quantidade efetiva de entropia que protege as chaves de criptografia usadas pela Proteção de Dados, sem prejudicar a experiência do usuário ao desbloquear um dispositivo várias vezes ao dia.

Se uma senha longa contendo apenas números for digitada, um teclado numérico é exibido na Tela Bloqueada em vez do teclado completo. Pode ser mais fácil digitar um código numérico longo do que um código alfanumérico curto (a segurança fornecida por ambos é similar).

Os usuários podem selecionar “Código Alfanumérico Personalizado” nas “Opções de Código” em Ajustes > Touch ID e Código ou Ajustes > Face ID e Código para especificar um código alfanumérico maior.

Como o incremento no tempo de atraso desencoraja ataques de força bruta (iOS, iPadOS)

No iOS e iPadOS, para desencorajar ainda mais os ataques de força bruta ao código, há um incremento no tempo de atraso entre as tentativas depois que um código inválido é digitado na Tela Bloqueada, como mostrado na tabela abaixo.

Tentativas	Intervalo aplicado
1–4	Nenhuma
5	1 minuto
6	5 minutos
7–8	15 minutos
9	1 hora

Se Apagar Dados estivar ativado (em Ajustes > Touch ID e Código), após 10 tentativas incorretas consecutivas de digitar o código, todo o conteúdo e ajustes são removidos do armazenamento. Tentativas consecutivas do mesmo código incorreto não são contabilizadas no limite. Esse ajuste também está disponível como política administrativa através de uma solução de gerenciamento de dispositivos móveis (MDM) compatível com esse recurso e do Microsoft Exchange ActiveSync, podendo ser definido em um valor mais baixo.

Em dispositivos com Secure Enclave, os intervalos são exigidos pelo Secure Enclave. Se o dispositivo for reiniciado durante um atraso programado, o atraso ainda é imposto e o timer é reiniciado para o período atual.

Como o incremento no tempo de atraso desencoraja ataques de força bruta (macOS)

Para impedir ataques de força bruta, quando o Mac é inicializado, não são permitidas mais de 10 tentativas de senha na Janela de Início de Sessão ou ao usar o Modo de Disco de Destino, e intervalos de tempo cada vez maiores são impostos após um certo número tentativas incorretas. Os intervalos são exigidos pelo Secure Enclave. Se o Mac for reiniciado durante um intervalo programado, o intervalo ainda é imposto e o timer é reiniciado para o período atual.

A tabela abaixo mostra os intervalos entre tentativas de inserção de senha em um Mac com Apple Silicon e um Mac com o chip T2.

Tentativas	Intervalo aplicado
5	1 minuto
6	5 minutos
7	15 minutos
8	15 minutos
9	1 hora
10	Desativado

Para ajudar a impedir que malwares causem perda permanente de dados ao tentar atacar a senha do usuário, esses limites não são aplicados depois de o usuário ter iniciado uma sessão com sucesso no Mac, mas são impostos novamente após a reinicialização. Se as 10 tentativas forem esgotadas, mais 10 tentativas estão disponíveis após inicializar no recoveryOS. Se elas também forem esgotadas, outras 10 tentativas estão disponíveis para cada mecanismo de recuperação do FileVault (recuperação do iCloud, chave de recuperação do FileVault e chave institucional), totalizando um máximo de 30 tentativas adicionais. Depois que essas tentativas adicionais também são esgotadas, o Secure Enclave não processa mais nenhuma solicitação para descriptografar o volume ou verificar a senha e os dados da unidade tornam-se irrecuperáveis.

Para ajudar a proteger dados em ambientes empresariais, o departamento de TI deve definir e exigir políticas de configuração do FileVault com uma solução MDM. As organizações têm várias opções de gerenciamento de volumes criptografados, como chaves de recuperação institucionais, pessoais (que podem ser opcionalmente armazenadas com o MDM por garantia) ou uma combinação de ambas. A alternância de chaves também pode ser definida como política no MDM.

Em um Mac com o chip Apple T2 Security, a senha cumpre uma função semelhante, com a exceção de que a chave gerada é usada para criptografia do FileVault, em vez da Proteção de Dados. O macOS também oferece opções adicionais de recuperação de senha:

- Recuperação do iCloud
- Recuperação do FileVault
- Chave institucional do FileVault

Proteção de Dados

Visão geral da Proteção de Dados

A Apple usa uma tecnologia chamada Proteção de Dados para proteger os dados guardados no armazenamento flash de dispositivos com um SoC da Apple, como um iPhone, iPad, Apple Watch, Apple TV e um Mac com Apple Silicon. Com a Proteção de Dados, um dispositivo pode responder a eventos comuns, como ligações telefônicas, sem deixar de oferecer um alto nível de criptografia nos dados de usuário. Certos apps do sistema (como Mensagens, Mail, Calendário, Contatos e Fotos) e valores de dados de Saúde usam a Proteção de Dados por padrão. Apps de terceiros recebem essa proteção automaticamente.

Implementação

A Proteção de Dados é implementada pela construção e gerenciamento de uma hierarquia de chaves, aproveitando as tecnologias de criptografia de hardware integradas a dispositivos Apple. A Proteção de Dados é controlada por arquivo, atribuindo uma classe a cada um deles; a acessibilidade é determinada de acordo com a constatação do desbloqueio das chaves de classe. O Apple File System (APFS) permite que o sistema de arquivos subdivida ainda mais as chaves de acordo com um padrão por perímetro (onde partes de um arquivo podem ter chaves diferentes).

Sempre que um arquivo é criado no volume de dados, a Proteção de Dados cria uma nova chave de 256 bits (*a chave única por arquivo*) e a fornece ao Mecanismo AES de hardware, que usa a chave para criptografar o arquivo conforme ele é gravado no armazenamento flash. Em dispositivos com A14, A15 e a família M1, a criptografia usa AES-256 no modo XTS, onde a chave única por arquivo de 256 bits passa por uma Função de Derivação de Chaves (Publicação Especial NIST 800-108) para derivar chaves de ajuste e cifra de 256 bits cada. As gerações de hardware do A9 até o A13, S5, S6 e S7 usam AES-128 no modo XTS, onde a chave única por arquivo de 256 bits é dividida para fornecer chaves de ajuste e cifra de 128 bits cada.

Em um Mac com Apple Silicon, a Proteção de Dados usa a Classe C por padrão (consulte Classes de Proteção de Dados) mas utiliza uma chave de volume em vez de uma chave por perímetro ou por arquivo, o que recria eficientemente o modelo de segurança do FileVault para os dados de usuário. Usuários ainda devem optar por usar o FileVault para receber toda a proteção do trançamento da hierarquia das chaves de criptografia com suas senhas. Desenvolvedores também podem optar por usar uma classe de proteção mais alta que use uma chave por arquivo ou por perímetro.

Proteção de Dados em dispositivos Apple

Em dispositivos Apple com Proteção de Dados, cada dado é protegido com uma chave exclusiva por arquivo (ou por perímetro). A chave, embalada com o algoritmo de embalagem de chaves NIST AED, é ainda embalada por uma de várias chaves de classe, dependendo de como o arquivo deve ser acessado. A chave por arquivo embalada é então armazenada nos metadados do arquivo.

Dispositivos com o formato APFS podem oferecer suporte à clonagem de arquivos (cópias de custo zero que usam a tecnologia "copiar ao gravar"). Se um arquivo for clonado, cada metade do clone recebe uma nova chave para aceitar gravações e permitir que novos dados sejam gravados na mídia com uma nova chave. Com o passar do tempo, o arquivo pode ser composto de várias extensões (ou fragmentos), cada um sendo mapeado a chaves diferentes. Entretanto, todas as extensões que compõem um arquivo são protegidas pela mesma chave de classe.

Quando um arquivo é aberto, seus metadados são descriptografados com a chave do sistema de arquivos, revelando a chave única por arquivo embalada e uma notação de qual classe o protege. A chave única por arquivo (ou por perímetro) é desembalada pela chave de classe e fornecida ao Mecanismo AES de hardware, o qual descriptografa o arquivo conforme ele é lido do armazenamento flash. O gerenciamento de toda a chave de arquivo embalada ocorre no Secure Enclave; a chave do arquivo nunca é exposta diretamente ao Processador de Aplicativos. Na inicialização, o Secure Enclave negocia uma chave efêmera com o Mecanismo AES. Quando o Secure Enclave desembala as chaves de um arquivo, elas são reembaladas pela chave efêmera e enviadas de volta para o Processador de Aplicativos.

Os metadados de todos os arquivos no sistema de arquivos do volume de dados são criptografados com uma chave de volume aleatória, criada na primeira instalação do sistema operacional ou quando o dispositivo é apagado pelo usuário. Essa chave é criptografada e embalada por uma chave de embalamento de chaves conhecida apenas pelo Secure Enclave para armazenamento de longo prazo. A chave de embalamento de chaves é alterada sempre que o usuário apaga o dispositivo. Nos SoCs A9 (e mais recentes), o Secure Enclave faz uso de entropia, assistida por sistemas antirreprodução, para possibilitar o apagamento e proteger sua chave de embalamento de chaves, entre outros materiais. Para obter mais informações, consulte Armazenamento não volátil seguro.

Assim como chaves únicas por arquivo ou por extensão, a chave de metadados do volume de dados nunca é exposta diretamente ao Processador de Aplicativos; o Secure Enclave fornece uma versão efêmera única por inicialização. Quando armazenada, a chave criptografada do sistema de arquivos é embalada ainda por uma "chave apagável" armazenada no Armazenamento Apagável ou com uma chave de embalamento de chave de mídia, protegida pelo mecanismo antirreprodução do Secure Enclave. Essa chave não oferece confidencialidade de dados adicional. Em vez disso, ela é projetada para ser apagada rapidamente sob demanda (por um usuário, por meio da opção "Apagar Todo o Conteúdo e Ajustes", ou por um usuário ou administrador ao emitir um comando de apagamento remoto a partir de uma solução de gerenciamento de dispositivos móveis (MDM), Microsoft Exchange ActiveSync ou iCloud). O apagamento de uma chave dessa maneira deixa todos os arquivos criptograficamente inacessíveis.

O conteúdo de um arquivo pode ser criptografado com uma ou mais chaves únicas por arquivo (ou por extensão) que são embaladas com uma chave de classe e armazenadas nos metadados de um arquivo que, por sua vez, é criptografado com a chave do sistema de arquivos. A chave de classe é protegida pelo UID do hardware e, em algumas classes, pelo código do usuário. Essa hierarquia fornece flexibilidade e bom desempenho. Por exemplo, a alteração da classe de um arquivo requer apenas que a chave única por arquivo seja reembalada e a alteração do código reembala somente a chave de classe.

Classes de Proteção de Dados

Quando um novo arquivo é criado em um dispositivo compatível com a Proteção de Dados, o app que o criou atribui uma classe ao arquivo. Cada classe usa políticas diferentes para determinar quando os dados podem ser acessados. As classes e políticas básicas são descritas nas seções a seguir. Computadores Mac baseados em Apple Silicon não são compatíveis com Classe D: Sem Proteção e um limite de segurança é estabelecido ao redor do início e término da sessão (e não ao bloquear ou desbloquear, como no iPhone, iPad e iPod touch).

Classe	Tipo de proteção
Classe A: Proteção Completa	NSFileProtectionComplete
Classe B: Protegido Exceto se Aberto	NSFileProtectionCompleteUnlessOpen
Classe C: Protegido Até a Primeira Autenticação do Usuário *Nota:* o macOS usa uma chave de volume para recriar as características de proteção do FileVault.	NSFileProtectionCompleteUntilFirstUserAuthentication
Classe D: Sem Proteção *Nota:* incompatível com o macOS.	NSFileProtectionNone

Proteção Completa

NSFileProtectionComplete: a chave de classe é protegida por uma chave derivada do código ou senha do usuário e do UID do dispositivo. Logo depois do usuário bloquear um dispositivo (10 segundos, se o ajuste em Exigir Senha for Imediatamente), a chave de classe descriptografada é descartada, deixando todos os dados nesta classe inacessíveis até que o usuário digite o código novamente ou use o Face ID ou Touch ID para desbloquear (iniciar a sessão) no dispositivo.

No macOS, logo depois que o último usuário finaliza a sessão, a chave de classe descriptografada é descartada, deixando todos os dados nesta classe inacessíveis até que um usuário digite o código novamente ou use o Touch ID para iniciar a sessão no dispositivo.

Protegido Exceto se Aberto

NSFileProtectionCompleteUnlessOpen: talvez seja necessário gravar alguns arquivos enquanto o dispositivo estiver bloqueado ou o usuário não tiver uma sessão iniciada. Um bom exemplo disso é o download em segundo plano de um anexo de e-mail. Esse comportamento é executado através do uso da criptografia assimétrica de curva elíptica (ECDH sobre Curve25519). A chave única por arquivo habitual é protegida por uma chave derivada que usa o Acordo de Chaves Diffie-Hellman de Um Passo, como descrito no NIST SP 800-56A.

A chave pública transitória do Acordo é armazenada em conjunto com a chave única por arquivo embalada. A KDF é a Função de Derivação da Chave de Concatenação (Alternativa Aprovada 1), como descrita em 5.8.1 do NIST SP 800-56A. O AlgorithmID é omitido. PartyUInfo é uma chave pública transitória e PartyVInfo é uma chave pública estática. SHA256 é usado como a função de hash. Assim que o arquivo é fechado, a chave única por arquivo é apagada da memória. Para abri-lo novamente, o segredo compartilhado é recriado usando a chave privada da classe Protegido Exceto se Aberto e a chave pública transitória do arquivo, que são usadas para desembalar a chave única por arquivo, que por sua vez, é usada para descriptografar o arquivo.

No macOS, a parte privada de NSFileProtectionCompleteUnlessOpen é acessível desde que qualquer usuário no sistema tenha uma sessão iniciada ou esteja autenticado.

Protegido Até a Primeira Autenticação do Usuário

NSFileProtectionCompleteUntilFirstUserAuthentication: essa classe se comporta da mesma maneira que a Proteção Completa, exceto pelo fato de que a chave de classe descriptografada não é removida da memória quando o dispositivo é bloqueado ou o usuário finaliza a sessão. A proteção desta classe tem propriedades semelhantes à criptografia de volume completo em computadores de mesa e protege os dados de ataques que envolvem reinicialização. Essa é a classe padrão de todos os dados de apps de terceiros que não tiverem sido atribuídos a uma classe de Proteção de Dados.

No macOS, essa classe usa uma chave de volume que fica acessível desde que o volume esteja montado e age da mesma forma que o FileVault.

Sem Proteção

NSFileProtectionNone: essa chave de classe é protegida apenas pelo UID e é mantida no Armazenamento Apagável. Como todas as chaves necessárias para descriptografar os arquivos desta classe são armazenadas no dispositivo, a criptografia oferece apenas o benefício do apagamento remoto rápido. Se um arquivo não for atribuído a uma classe de Proteção de Dados, ele ainda é armazenado criptografado (como todos os dados em um dispositivo iOS e iPadOS).

Isso não é compatível com o macOS.

Nota: no macOS, em volumes que não correspondem a um sistema operacional inicializado, todas as classes de proteção de dados são acessíveis desde que o volume esteja montado. A classe de proteção de dados padrão é NSFileProtectionCompleteUntilFirstUserAuthentication. A funcionalidade de chave por extensão está disponível tanto a apps Rosetta 2 quanto a apps nativos.

Keybags para Proteção de Dados

As chaves das classes de Proteção de Dados de arquivos e de chaves são coletadas e gerenciadas em keybags no iOS, iPadOS, watchOS e tvOS. Esses sistemas operacionais usam as seguintes keybags: usuário, dispositivo, backup, guarda e Backup do iCloud.

Keybag do usuário

A keybag do usuário é onde as chaves de classe embaladas, usadas em operações normais, são armazenadas. Por exemplo, quando um código é digitado, a *NSFileProtectionComplete* é carregada a partir da keybag do usuário e desembalada. Ela é um arquivo binário de lista de propriedades (.plist) armazenado na classe Sem Proteção.

No caso de dispositivos com SoCs anteriores ao A9, o conteúdo do arquivo .plist é criptografado com uma chave guardada no Armazenamento Apagável. Para oferecer mais segurança às keybags, essa chave é apagada e gerada novamente sempre que um usuário altera seu código.

No caso de dispositivos com os SoCs A9 ou posteriores, o arquivo .plist contém uma chave que indica que a keybag está armazenada em um cofre protegido por um nonce antirreprodução controlado pelo Secure Enclave.

O Secure Enclave gerencia a keybag do usuário e pode ser consultado sobre o estado de bloqueio de um dispositivo. Ele informa que o dispositivo está desbloqueado somente se todas as chaves de classe da keybag do usuário estiverem acessíveis e desembaladas corretamente.

Keybag do dispositivo

A keybag do dispositivo é usada para armazenar as chaves de classe embaladas usadas em operações que envolvem dados específicos do dispositivo. Dispositivos iPadOS configurados para uso compartilhado às vezes precisam de acesso a credenciais antes que um usuário tenha iniciado uma sessão; portanto, é necessária uma keybag que não esteja protegida pelo código do usuário.

O iOS e iPadOS não são compatíveis com a separação criptográfica do conteúdo do sistema de arquivos por cada usuário, o que significa que o sistema usa chaves de classe da keybag do dispositivo para embalar chaves únicas por arquivo. Porém, as chaves usam chaves de classe da keybag do usuário para proteger itens nas chaves do usuário. Em dispositivos iOS e iPadOS configurados para uso de um único usuário (configuração padrão), a keybag do dispositivo e a keybag do usuário são uma só e a mesma, protegidas pelo código do usuário.

Keybag de backup

A keybag de backup é criada quando o Finder (macOS 10.15 ou posterior) ou o iTunes (macOS 10.14 ou anterior) fazem um backup criptografado que é armazenado no computador onde o backup do dispositivo foi feito. Uma nova keybag é criada com um novo conjunto de chaves e os dados do backup são criptografados novamente com essas novas chaves. Como explicado anteriormente, os itens não migratórios das chaves permanecem embalados pela chave derivada do UID, permitindo que eles sejam restaurados para o dispositivo do qual o backup foi feito originalmente, mas deixando-os inacessíveis em um dispositivo diferente.

A keybag — protegida pela senha definida — passa por 10 milhões de iterações da função de derivação de chaves PBKDF2. Apesar dessa contagem de iteração extensa, não há vínculos com um dispositivo específico e, portanto, teoricamente, seria possível tentar um ataque de força bruta à keybag do backup usando vários computadores em paralelo. Essa ameaça pode ser atenuada com uma senha suficientemente forte.

Se um usuário decidir não criptografar o backup, os arquivos não são criptografados, independentemente de suas classes de Proteção de Dados, mas as chaves permanecem protegidas por uma chave derivada do UID. É por isso que os itens das chaves são migrados para um novo dispositivo apenas se uma senha de backup for definida.

Keybag de guarda

A keybag de guarda é usada para sincronizar com o Finder (macOS 10.15 ou posterior) ou iTunes (no macOS 10.14 ou anterior) via USB e gerenciamento de dispositivos móveis (MDM). Essa keybag permite o backup e a sincronização com o Finder ou o iTunes sem exigir que o usuário digite uma senha, e permite que uma solução MDM limpe o código de um usuário remotamente. Ela é armazenada no computador usado para sincronizar com o Finder ou o iTunes, ou na solução MDM que gerencia o dispositivo remotamente.

A keybag de guarda melhora a experiência do usuário durante a sincronização do dispositivo, o que potencialmente requer acesso a todas as classes de dados. Quando um dispositivo bloqueado por código é conectado pela primeira vez ao Finder ou iTunes, o usuário é solicitado a digitar um código. Em seguida, o dispositivo cria uma keybag de guarda que contém as mesmas chaves de classe usadas no dispositivo, protegida por uma nova chave recém-gerada. A keybag de guarda e a chave que a protege são divididas entre o dispositivo e o host ou servidor, com os dados armazenados no dispositivo na classe Protegido Até a Primeira Autenticação do Usuário. É por isso que o código do dispositivo deve ser digitado antes que o usuário faça um backup no Finder ou iTunes da primeira vez após uma reinicialização.

No caso de uma atualização de software sem fio (OTA), é solicitado que o usuário digite o código ao iniciar a atualização. Isso é feito para criar, de forma segura, um token de desbloqueio único, o qual desbloqueia a keybag do usuário depois da atualização. Esse token não pode ser gerado sem que o código do usuário seja digitado e todos os tokens gerados anteriormente são invalidados se o código do usuário for alterado.

Os tokens de desbloqueio de uso único servem para atualizações de software feitas com ou sem supervisão. Eles são criptografados com uma chave derivada do valor atual de um contador monotônico no Secure Enclave, o UUID da keybag e o UID do Secure Enclave.

Nos SoCs A9 (e posteriores), o token de desbloqueio de uso único não depende mais de contadores ou do Armazenamento Apagável. Em vez disso, ele é protegido pelo nonce antirreprodução controlado pelo Secure Enclave.

O token de desbloqueio de uso único de atualizações de software supervisionadas expira depois de 20 minutos. No iOS 13 e iPadOS 13.1 ou posterior, o token é armazenado em um cofre protegido pelo Secure Enclave. Antes do iOS 13, esse token era exportado do Secure Enclave e gravado no Armazenamento Apagável ou protegido pelo mecanismo antirreprodução do Secure Enclave. Um timer de política aumentava o contador se o dispositivo não tivesse sido reinicializado nos últimos 20 minutos.

Atualizações de software automáticas ocorrem quando o sistema detecta que há uma atualização disponível e quando um dos seguintes é verdadeiro:

- As atualizações automáticas estão configuradas no iOS 12 ou posterior.
- O usuário escolhe “Instalar Mais Tarde” ao receber a notificação sobre a atualização.

Após o usuário digitar seu código, um token de desbloqueio de uso único é gerado e pode permanecer válido no Secure Enclave por até oito horas. Se a atualização ainda não tiver ocorrido, o token de desbloqueio de uso único é destruído a cada bloqueio e recriado a cada desbloqueio subsequente. Cada desbloqueio reinicia a contagem de oito horas. Após oito horas, um timer de política invalida o token de desbloqueio de uso único.

Keybag do Backup do iCloud

A keybag do Backup do iCloud assemelha-se à keybag de backup. Todas as chaves de classe nessa keybag são assimétricas (usando Curve25519, como a classe de Proteção de Dados “Protegido Exceto se Aberto”). Uma keybag assimétrica também é usada para o backup no aspecto de recuperação de chaves das Chaves do iCloud.

Proteção de chaves em modos de inicialização alternativos

A Proteção de Dados é projetada para fornecer acesso aos dados de usuário apenas depois de uma autenticação bem-sucedida e somente para o usuário autorizado. As classes da Proteção de Dados são projetadas para oferecer suporte a diversos casos de uso, como a capacidade de ler e gravar dados mesmo quando um dispositivo está bloqueado (porém depois do primeiro desbloqueio). Passos adicionais são tomados para proteger o acesso aos dados de usuário durante modos de inicialização alternativos, como aqueles usados para o modo de Atualização do Firmware do Dispositivo (DFU), modo de Recuperação, Diagnóstico Apple ou até durante atualizações de software. Essas capacidades baseiam-se em uma combinação de recursos de hardware e software, e foram ampliadas conforme o silício projetado pela Apple evoluiu.

Recurso	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, Família M1
Recuperação: proteção de todas as Classes de Proteção de Dados	✓	✓	✓	✓	✓
Inicializações alternativas do modo DFU, Recuperação e atualizações de software: proteção de dados das Classes A, B e C		✓	✓	✓	✓

O Mecanismo AES do Secure Enclave é equipado com bits de núcleo de software bloqueáveis. Quando chaves são criadas a partir do UID, esses bits de núcleo são incluídos na função de derivação da chave para criar hierarquias de chave adicionais. Como o bit de núcleo é usado e varia de acordo com o sistema no chip:

- Desde os SoCs Apple A10 e S3, um bit de núcleo é dedicado a distinguir chaves protegidas pelo código do usuário. O bit de núcleo é definido para chaves que requerem o código de usuário (incluindo Proteção de Dados para chaves de Classe A, Classe B e Classe C) e removido para chaves que não requerem o código do usuário (incluindo a chave de metadados do sistema de arquivos e chaves da Classe D).
- No iOS 13 ou posterior e iPadOS 13.1 ou posterior em dispositivos com o A10 ou posterior, todos os dados do usuário ficam criptograficamente inacessíveis quando os dispositivos são inicializados no modo de Diagnóstico. Isso é feito por meio da introdução de um bit de núcleo adicional cuja definição governa a capacidade de acesso à chave de mídia, que por sua vez é necessária para acessar os metadados (e portanto, o conteúdo de todos os arquivos) no volume de dados criptografado com a Proteção de Dados. Esta proteção engloba os arquivos protegidos em todas as classes (A, B, C e D), não apenas aqueles que exigem o código do usuário.
- Em SoCs A12, a ROM de Inicialização do Secure Enclave bloqueia o bit de núcleo do código se o Processador de Aplicativos tiver entrado no modo de Atualização do Firmware do Dispositivo (DFU) ou modo de recuperação. Quando o bit de núcleo está bloqueado, nenhuma operação de alteração é permitida. Isso é projetado para impedir o acesso a dados protegidos pelo código do usuário.

A restauração de um dispositivo depois que ele entra no modo DFU o leva novamente a um estado conhecidamente bom, com a certeza de que apenas código não modificado e assinado pela Apple está presente. O modo DFU pode ser acessado manualmente.

Consulte o artigo do Suporte da Apple a seguir para saber como colocar um dispositivo no modo DFU:

Dispositivo	Artigo
iPhone, iPad, iPod touch	Se você esqueceu o código do iPhone
Apple TV	Se você vir um símbolo de aviso na Apple TV
Um Mac com Apple Silicon	Revive or restore a Mac with Apple silicon (em inglês)

Proteção de dados do usuário diante de um ataque

Invasores que tentam extrair dados de usuários, normalmente usam várias técnicas diferentes: extração de dados criptografados para outro meio para ataque por força bruta, manipulação da versão do sistema operacional ou enfraquecimento da política de segurança no dispositivo para facilitar a invasão. O ataque aos dados em um dispositivo normalmente requer o uso de uma interface física para comunicação com o dispositivo, como Lightning ou USB. Dispositivos Apple incluem recursos para impedir tais invasões.

Dispositivos Apple são compatíveis com uma tecnologia chamada *Proteção de Chave Selada (SKP)* que é projetada para garantir que materiais criptográficos sejam inutilizáveis quando fora do dispositivo, ou que é usada caso manipulações sejam feitas às versões do sistema operacional ou aos ajustes de segurança sem a devida autorização do usuário. Esse recurso *não* é fornecido pelo Secure Enclave; em vez disso, ele é amparado por registros de hardware que existem em uma camada mais baixa, para que seja possível oferecer uma camada de proteção adicional às chaves necessárias para descriptografar os dados de usuário independentemente do Secure Enclave.

Nota: a SKP está disponível apenas em dispositivos com um SoC projetado pela Apple.

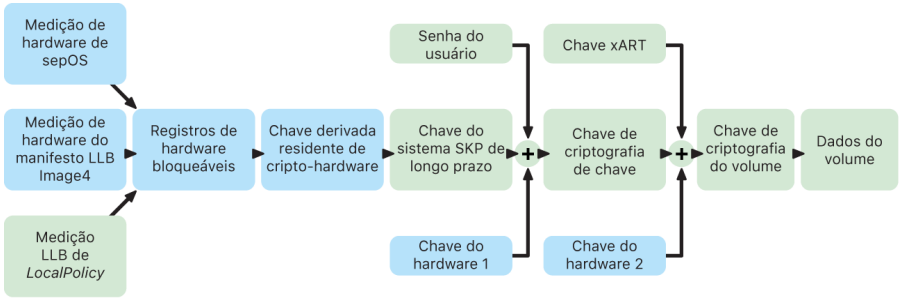
Recurso	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, Família M1
Proteção de Chave Selada	✓	✓	✓	✓	✓

O iPhone e o iPad também podem ser configurados para ativar conexões de dados apenas em condições mais prováveis que indiquem que o dispositivo ainda esteja sob o controle físico do proprietário autorizado.

Proteção de Chave Selada (SKP)

Em dispositivos Apple compatíveis com a Proteção de Dados, a chave de criptografia de chaves (KEK) é protegida (ou selada) com medidas do software no sistema, além de ser atrelada ao UID disponível somente a partir do Secure Enclave. Em um Mac com Apple Silicon, a proteção da KEK é reforçada ainda mais ao incorporar informações sobre a política de segurança no sistema, dado que o macOS oferece suporte a mudanças de política de segurança críticas (desativação da inicialização segura ou SIP, por exemplo), o que não acontece em outras plataformas. Em um Mac com Apple Silicon, essa proteção abrange as chaves do FileVault, já que o FileVault usa a Proteção de Dados (Classe C) para ser implementado.

A chave que resulta do trançamento da senha do usuário, chave SKP de longo prazo e chave 1 de Hardware (o UID do Secure Enclave) é camada de *chave derivada da senha*. Essa chave é usada para proteger a keybag do usuário (em todas as plataformas compatíveis) e a KEK (somente no macOS), e então ativar o desbloqueio biométrico ou o desbloqueio automático com outros dispositivos, como o Apple Watch.



A ROM de Inicialização do Secure Enclave captura a medida do OS do Secure Enclave que está carregado. Quando a ROM de Inicialização do Processador de Aplicativos mede o manifesto Image4 anexado ao LLB, esse manifesto contém uma medida de todos os outros firmwares emparelhados ao sistema que também se encontram carregados. A LocalPolicy contém as configurações de segurança elementares para o macOS que são carregadas. A LocalPolicy também contém o campo `nsih`, o qual é um hash do manifesto Image4 do macOS. O manifesto Image4 do macOS contém medidas de todos os firmwares emparelhados com o macOS e objetos de inicialização elementares do macOS, como a Coleção do Kernel de Inicialização ou o hash raiz do volume de sistema assinado (SSV).

Se um invasor puder alterar inesperadamente qualquer um dos componentes medidos de firmware, software ou configuração de segurança mencionados acima, ele modifica as medidas armazenadas nos registros de hardware. A modificação das medidas faz com que a *chave raiz da medida do sistema (SMRK)* derivada do hardware de criptografia derive um valor diferente, efetivamente rompendo o selo na hierarquia de chaves. Isso faz com que a *chave de medida do sistema do dispositivo (SMDK)* fique inacessível, a qual, por sua vez, faz com que a KEK, e portanto, os dados, fiquem inacessíveis.

Entretanto, quando o sistema não se encontra sob ataque, ele precisa acomodar atualizações de software legítimas que alteram as medidas do firmware e do campo `nsih` na LocalPolicy para que apontem para novas medidas do macOS. Em outros sistemas que tentam incorporar medidas de firmware, mas que não têm uma fonte de confiança conhecida, o usuário é requisitado a desativar a segurança, atualizar o firmware e depois reativar, para que uma nova linha base de medida possa ser capturada. Isso aumenta significativamente o risco de um invasor adulterar o firmware durante uma atualização de software. O sistema é auxiliado pelo fato do manifesto Image4 conter todas as medidas necessárias. O hardware que descriptografa a SMDK com a SMRK quando as medidas coincidem durante uma inicialização normal, também pode criptografar a SMDK para uma futura SMRK proposta. Ao especificar as medidas que são esperadas após uma atualização de software, o hardware pode criptografar uma SMDK que esteja acessível em um sistema operacional atual para que ela permaneça acessível em um sistema operacional futuro. De maneira semelhante, quando um cliente altera legitimamente seus ajustes de segurança na LocalPolicy, a SMDK deve ser criptografada para a SMRK futura com base na medida da LocalPolicy, que o LLB calcula na reinicialização seguinte.

Ativação segura de conexões de dados no iOS e iPadOS

Em dispositivos iOS ou iPadOS, se nenhuma conexão de dados tiver sido estabelecida recentemente, usuários devem usar o Face ID, Touch ID ou código para ativar conexões de dados via Lightning, USB ou interface do Smart Connector. Isso limita a superfície de ataque contra dispositivos conectados fisicamente, como carregadores maliciosos, ao mesmo tempo que permite o uso de outros acessórios dentro de limites de tempo razoáveis. Caso tenha se passado mais de uma hora desde que o dispositivo iOS ou iPadOS foi bloqueado ou desde que uma conexão de dados de um acessório foi terminada, o dispositivo não permitirá quaisquer conexões de dados novas até que o dispositivo seja desbloqueado. Durante esse período de uma hora, serão permitidas somente conexões de dados de acessórios que já tenham sido conectados anteriormente em estado desbloqueado. Esses acessórios são memorizados por 30 dias depois da última vez em que foram conectados. Tentativas de um acessório desconhecido para abrir uma conexão de dados durante esse período desativarão todas as conexões de dados por meio de Lightning, USB ou Smart Connector até que o dispositivo seja desbloqueado novamente. Esse período de uma hora:

- Ajuda a garantir que usuários frequentes de conexões a um Mac ou PC, a acessórios ou que usem conexão por fio ao CarPlay, não precisem digitar o código sempre que conectam o dispositivo
- É necessário porque o ecossistema de acessórios não oferece uma maneira criptograficamente confiável de identificar acessórios antes de estabelecer uma conexão de dados

Além disso, se tiverem se passado mais de três dias desde o estabelecimento de uma conexão de dados a um acessório, o dispositivo desautorizará novas conexões de dados imediatamente após o bloqueio. Isso aumenta a proteção de usuários que não costumam usar tais acessórios com frequência. As conexões de dados via Lightning, USB e Smart Connector também são desativadas sempre que o dispositivo está em um estado em que requer um código para reativar a autenticação biométrica.

O usuário tem a opção de reativar conexões de dados sempre ativas nos Ajustes (a configuração de alguns dispositivos assistivos faz isso automaticamente).

Função do Apple File System

O Apple File System (APFS) é um sistema de arquivos proprietário que foi projetado levando em consideração a criptografia. O APFS funciona em todas as plataformas da Apple: no iPhone, iPad, iPod touch, Mac, Apple TV e Apple Watch. Otimizado para armazenamento Flash/SSD, ele possui criptografia forte, metadados copiados na gravação, compartilhamento de espaço, clonagem de arquivos e diretórios, capturas, dimensionamento rápido de diretórios, primitivas atômicas de salvamento seguro e elementos básicos aprimorados de sistemas de arquivos, além de um projeto exclusivo de "copiar ao gravar" que usa aglutinação de E/S para proporcionar desempenho máximo sem deixar de garantir a confiabilidade dos dados.

Compartilhamento de espaço

O APFS aloca o espaço de armazenamento sob demanda. Quando um único contêiner APFS possui vários volumes, o espaço livre do contêiner é compartilhado e pode ser alocado a qualquer volume conforme necessário. Cada volume usa apenas parte do contêiner total, portanto o espaço disponível é o tamanho total do contêiner menos o espaço usado em todos os volumes nele contidos.

Volumes múltiplos

No macOS 10.15 ou posterior, um contêiner APFS usado para inicializar o Mac deve conter pelo menos cinco volumes, sendo os três primeiros ocultados do usuário:

- *Volume de Pré-inicialização:* este volume não é criptografado e contém os dados necessários para inicializar cada volume do sistema no contêiner.
- *Volume de VM:* este volume não é criptografado, sendo usado pelo macOS para armazenar arquivos de troca criptografados.
- *Volume de Recuperação:* este volume não é criptografado e deve estar disponível sem o desbloqueio de um volume do sistema para inicializar no recoveryOS.
- *Volume do Sistema:* contém o seguinte:
  - Todos os arquivos necessários para inicializar o Mac
  - Todos os apps instalados nativamente pelo macOS (apps que costumavam ficar na pasta /Aplicativos agora ficam na pasta Sistema/Aplicativos)

  Nota: por padrão, nenhum processo pode gravar no volume de Sistema, até mesmo processos do sistema da Apple.
- *Volume de Dados:* contém os dados sujeitos a mudança, como:
  - Qualquer dado dentro da pasta do usuário, incluindo fotos, músicas, vídeos e documentos
  - Apps instalados pelo usuário, incluindo aplicativos do AppleScript e do Automator
  - Frameworks e daemons personalizados instalados pelo usuário, organização ou apps de terceiros
  - Outros locais de propriedade do usuário e nos quais ele pode gravar, como /Aplicativos, /Biblioteca, /Usuários, /Volumes, /usr/local, /private, /var e /tmp

Um volume de dados é criado para cada volume de sistema adicional. Os volumes de pré-inicialização, VM e recuperação são compartilhados, e não duplicados.

No macOS 11 ou posterior, uma captura do volume de sistema é criada. O sistema operacional inicializa a partir de uma captura do volume de sistema, não apenas de uma montagem somente leitura do volume de sistema mutável.

No iOS e iPadOS, o armazenamento é dividido em, ao menos, dois volumes APFS:

- Volume do sistema
- Volume de dados

Proteção de Dados das Chaves

Muitos apps precisam gerenciar senhas e outros dados simples, porém sensíveis, como chaves e tokens de acesso. As chaves oferecem uma maneira segura de armazenar esses itens. Os diversos sistemas operacionais da Apple usam mecanismos diferentes para exigir as garantias associadas às várias classes de proteção das chaves. No macOS (incluindo um Mac com Apple Silicon), a Proteção de Dados não é usada diretamente para exigir essas garantias.

Visão geral

Os itens das Chaves são criptografados usando duas chaves AES-256-GCM diferentes: uma chave de tabela (metadados) e uma chave por linha (chave secreta). Os metadados das Chaves (todos os atributos que não sejam kSecValue) são criptografados com a chave dos metadados para acelerar buscas, e o valor secreto (kSecValueData) é criptografado com a chave secreta. A chave dos metadados é protegida pelo Secure Enclave, mas é armazenada em cache no Processador de Aplicativos para permitir consultas rápidas às chaves. A chave secreta sempre requer uma passagem completa pelo Secure Enclave.

As chaves são implementadas na forma de um banco de dados SQLite, armazenado no sistema de arquivos. Existe apenas um banco de dados e o daemon `securityd` determina quais itens das chaves cada processo ou app pode acessar. As APIs de Acesso às Chaves resultam em chamadas ao daemon, que consulta os direitos “grupos-acesso-Chaves”, “identificador-aplicativo” e “grupo-aplicativo” do app. Ao invés de limitar o acesso a um único processo, os grupos de acesso permitem que os itens das chaves sejam compartilhados entre apps.

Os itens das chaves podem ser compartilhados apenas entre apps do mesmo desenvolvedor. Para compartilhar os itens das chaves, apps de terceiros usam grupos de acesso com um prefixo a eles alocados através do Programa de Desenvolvedor da Apple em seus respectivos grupos de aplicativos. A exigência do prefixo e a exclusividade do grupo do aplicativo são aplicadas através da assinatura de código, perfis de provisão e o Programa de Desenvolvedor da Apple (em inglês).

Os dados das Chaves são protegidos usando uma estrutura de classes semelhante à usada na Proteção de Dados de arquivos. Essas classes apresentam comportamentos equivalentes às classes de Proteção de Dados de arquivos, mas usam chaves e funções distintas.

Disponibilidade	Proteção de dados de arquivos	Proteção de Dados das Chaves
Quando desbloqueado	NSFileProtectionComplete	kSecAttrAccessibleWhen Unlocked
Enquanto bloqueado	NSFileProtectionCompleteUnlessOpen	NA
Depois do primeiro desbloqueio	NSFileProtectionCompleteUntilFirstUser Authentication	kSecAttrAccessibleAfterFirst Unlock
Sempre	NSFileProtectionNone	kSecAttrAccessibleAlways
Código ativado	NA	kSecAttrAccessibleWhen PasscodeSetThisDeviceOnly

Os apps que usam serviços de atualização em segundo plano podem usar *kSecAttrAccessibleAfterFirstUnlock* para itens das chaves que precisam ser acessados durante atualizações em segundo plano.

A classe *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* se comporta da mesma maneira que *kSecAttrAccessibleWhenUnlocked*, mas fica disponível apenas quando o dispositivo está configurado com um código. Essa classe existe somente na keybag do sistema e:

- Não é sincronizada nas Chaves do iCloud;
- Não recebe backup;
- Não é incluída em keybags de guarda segura.

Se o código for removido ou redefinido, os itens serão inutilizados por meio do descarte das chaves de classe.

Outras classes de chaves têm uma contraparte “Somente este dispositivo”, a qual está sempre protegida pelo UID ao ser copiada do dispositivo durante um backup, inutilizando-a caso ela seja restaurada em um dispositivo diferente. A Apple equilibrou segurança e usabilidade cuidadosamente, escolhendo classes de chaves que dependem do tipo de informação sendo protegida e de quando o iOS e iPadOS precisam dela. Por exemplo, um certificado VPN deve estar sempre disponível para que o dispositivo mantenha uma conexão contínua, mas é classificado como “não migratório” para que não possa ser movido para outro dispositivo.

Proteções de classes de dados das Chaves

As proteções de classes na lista abaixo são exigidas para itens das chaves.

Item	Acessível
Senhas de Wi-Fi	Depois do primeiro desbloqueio
Contas do Mail	Depois do primeiro desbloqueio
Contas do Microsoft Exchange ActiveSync	Depois do primeiro desbloqueio
Senhas de VPN	Depois do primeiro desbloqueio
LDAP, CalDAV, CardDAV	Depois do primeiro desbloqueio
Tokens de contas de redes sociais	Depois do primeiro desbloqueio
Chaves de criptografia de anúncio de Handoff	Depois do primeiro desbloqueio
Token do iCloud	Depois do primeiro desbloqueio
Chaves do iMessage	Depois do primeiro desbloqueio
Senha do compartilhamento pessoal	Quando desbloqueado
Senhas do Safari	Quando desbloqueado
Favoritos do Safari	Quando desbloqueado
Backup do Finder/iTunes	Quando desbloqueado, não migratória
Chaves privadas instaladas por um perfil de configuração	Quando desbloqueado, não migratória
Certificados de VPN	Sempre, não migratória
Chaves do Bluetooth®	Sempre, não migratória
Token do serviço de Notificações Push da Apple (APNs)	Sempre, não migratória
Certificados e chaves privadas do iCloud	Sempre, não migratória
PIN do SIM	Sempre, não migratória
Certificados instalados por um perfil de configuração	Sempre
Token do Buscar	Sempre
Voicemail	Sempre

Controle de acesso às Chaves

As Chaves podem usar listas de controle de acesso (ACLs) para definir políticas de acessibilidade e requisitos de autenticação. Os itens podem estabelecer condições que exijam a presença do usuário, especificando que os mesmos não poderão ser acessados a menos que o usuário tenha autenticado através do Face ID, Touch ID ou pela digitação do código ou senha do dispositivo. O acesso a itens também pode ser limitado ao especificar que os registros do Face ID ou Touch ID não tenham sido alterados desde que o item foi adicionado. Essa limitação ajuda a impedir que um invasor adicione sua própria impressão digital para acessar um item das chaves. As ACLs são avaliadas no Secure Enclave e liberadas ao kernel somente se as restrições especificadas forem atendidas.

Arquitetura das Chaves no macOS

O macOS também oferece acesso às chaves para armazenar de forma conveniente e segura nomes de usuário e senhas, incluindo identidades digitais, chaves de criptografia e notas seguras. Ele pode ser acessado por meio do app Acesso às Chaves em /Aplicativos/Utilitários/. O uso das Chaves elimina a necessidade de digitar (ou mesmo de lembrar) as credenciais de cada recurso. Um conjunto inicial e padrão de chaves é criado para cada usuário do Mac, embora os usuários possam criar outros conjuntos com objetivos específicos.

Além de contar com chaves de usuário, o macOS conta com uma série de chaves no nível do sistema que mantêm materiais de autenticação não específicos ao usuário, como credenciais de rede e identidades de infraestrutura de chave pública (PKI). Uma dessas chaves, Raízes do Sistema, é imutável e armazena certificados de autoridades de certificação (AC) raiz de PKI da internet para a realização de tarefas comuns, como transações bancárias on-line e de comércio eletrônico. De forma semelhante, o usuário pode implantar certificados de AC fornecidos internamente em computadores Mac gerenciados para ajudar a validar sites e serviços internos.

FileVault

Criptografia do volume com FileVault no macOS

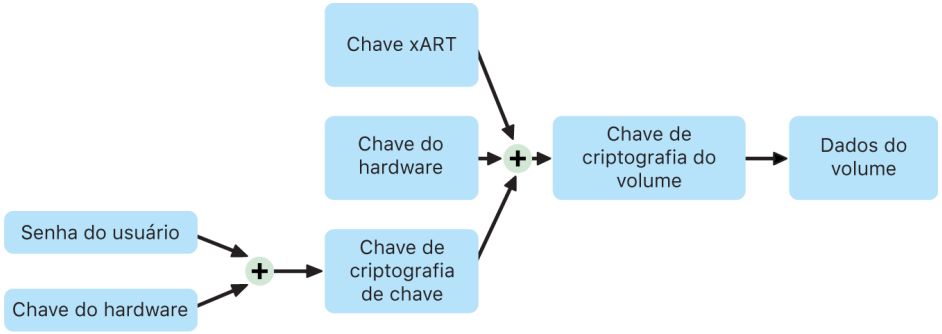
Computadores Mac oferecem o FileVault, um recurso integrado de criptografia para proteger todos os dados em repouso. O FileVault usa o algoritmo de criptografia de dados AES-XTS para proteger volumes inteiros em dispositivos de armazenamento internos e removíveis.

O FileVault em um Mac com Apple Silicon usa a Classe C da Proteção de Dados com uma chave de volume para implementação. Em um Mac com o chip Apple T2 Security, assim como em um Mac com Apple Silicon, os dispositivos de armazenamento interno criptografados conectados diretamente ao Secure Enclave fazem uso dos recursos de segurança de hardware deste, além daqueles do mecanismo AES. Depois que um usuário ativa o FileVault no Mac, suas credenciais são exigidas durante o processo de inicialização.

Armazenamento interno com FileVault ativado

Sem credenciais de início de sessão válidas ou uma chave de recuperação criptográfica, os volumes APFS internos permanecem criptografados e protegidos contra acesso não autorizado, mesmo que o dispositivo de armazenamento físico seja removido e conectado a outro computador. No macOS 10.15, isso inclui os volumes de sistema e de dados. A partir do macOS 11, o volume de sistema é protegido pelo recurso de volume de sistema assinado (SSV), mas o volume de dados continua sendo protegido por criptografia. A criptografia de volumes internos em um Mac com Apple Silicon, assim como naqueles com o chip T2, é implementada pela construção e gerenciamento de uma hierarquia de chaves, aproveitando as tecnologias de criptografia de hardware integradas ao chip. Esta hierarquia de chaves é projetada para cumprir simultaneamente quatro objetivos:

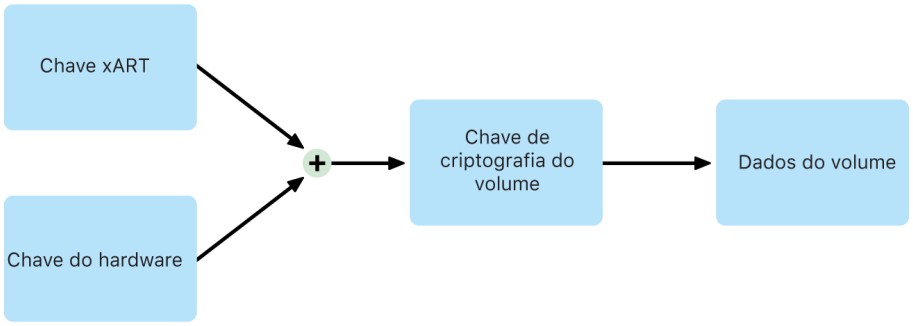
- Exigir a senha do usuário para descriptografia
- Proteger o sistema contra um ataque de força bruta diretamente contra mídias de armazenamento removidas do Mac
- Fornecer um método ágil e seguro para apagar conteúdos por meio do apagamento de materiais criptográficos necessários
- Permitir que os usuários alterem suas senhas (e, com isso, as chaves criptográficas usadas para proteger seus arquivos) sem a necessidade de criptografar novamente todo o volume



Em um Mac com Apple Silicon e naqueles com o chip T2, todo o gerenciamento de chaves do FileVault ocorre no Secure Enclave; as chaves de criptografia nunca são expostas diretamente à CPU Intel. Todos os volumes APFS são criados com uma chave de criptografia do volume por padrão. O conteúdo do volume e os metadados são criptografados com essa chave de criptografia do volume, que é embalada com a chave de classe. A chave de classe é protegida por uma combinação da senha do usuário e do UID do hardware quando o FileVault está ativado.

Armazenamento interno com FileVault desativado

Se o FileVault não estiver ativado em um Mac com Apple Silicon ou em um Mac com o chip T2 durante o processo inicial do Assistente de Configuração, o volume ainda é criptografado, mas a chave de criptografia do volume é protegida apenas pelo UID do hardware no Secure Enclave.



Se o FileVault for ativado posteriormente — um processo que é imediato, já que os dados já foram criptografados — um mecanismo antirreprodução ajuda a impedir que a chave antiga (baseada apenas no UID do hardware) seja usada para descriptografar o volume. Assim, o volume é protegido por uma combinação da senha do usuário e do UID do hardware, como descrito anteriormente.

Apagamento de volumes com FileVault

Ao apagar um volume, a respectiva chave de criptografia do volume é apagada com segurança pelo Secure Enclave. Isso ajuda a impedir o acesso futuro com essa chave, mesmo pelo Secure Enclave. Além disso, todas as chaves de criptografia do volume são embaladas com uma chave de mídia. A chave de mídia não fornece nenhuma confidencialidade adicional dos dados; em vez disso, ela é projetada para proporcionar o apagamento ágil e seguro dos dados porque, sem ela, é impossível descriptografá-los.

Em um Mac com Apple Silicon e naqueles com o chip T2, o apagamento da chave de mídia é garantido pela tecnologia de suporte do Secure Enclave, através comandos remotos do MDM, por exemplo. O apagamento da chave de mídia dessa maneira deixa o volume criptograficamente inacessível.

Dispositivos de armazenamento removíveis

A criptografia de dispositivos de armazenamento externos não usa as capacidades de segurança do Secure Enclave, e ela é realizada da mesma maneira que em um Mac baseado em Intel sem o chip T2.

Gerenciamento do FileVault no macOS

No macOS, organizações podem usar um SecureToken ou Bootstrap Token para gerenciar o FileVault.

Uso do Secure Token

O Apple File System (APFS) no macOS 10.13 ou posterior altera a forma como as chaves de criptografia do FileVault são geradas. Nas versões anteriores do macOS em volumes CoreStorage, as chaves usadas no processo de criptografia do FileVault eram criadas quando um usuário ou organização ativava o FileVault em um Mac. No macOS em volumes APFS, as chaves são geradas durante a criação do usuário, definindo a primeira senha do usuário, ou durante o primeiro início de sessão realizado por um usuário do Mac. Essa implementação das chaves de criptografia, o momento em que são geradas e a forma como são armazenadas fazem parte de um recurso conhecido como *Secure Token*. Especificamente, um secure token é uma versão embalada de uma chave de criptografia de chaves (KEK) protegida pela senha do usuário.

Ao implantar o FileVault no APFS, o usuário pode continuar a:

- Usar as ferramentas e processos existentes, como uma chave de recuperação pessoal (PRK) que pode ser armazenada em uma solução de gerenciamento de dispositivos móveis (MDM) para guarda
- Criar e usar uma chave de recuperação institucional (IRK)
- Adiar a ativação do FileVault até que um usuário inicie ou encerre uma sessão no Mac

No macOS 11, a definição da senha inicial do primeiro usuário do Mac resulta na concessão de um secure token a esse usuário. Em alguns fluxos de trabalho, esse pode não ser o comportamento desejado, já que, como visto, seria necessário o início de sessão na conta do usuário para que o primeiro secure token fosse concedido. Para impedir que isso aconteça, adicione `;DisabledTags;SecureToken` ao atributo `AuthenticationAuthority` do usuário criado programaticamente antes de definir a senha do usuário, conforme mostrado abaixo:

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

Uso do Bootstrap Token

O macOS 10.15 apresentou um novo recurso, o *Bootstrap Token*, para ajudar na concessão de um secure token tanto para contas móveis quanto para a conta opcional de administrador criada no registro do dispositivo (“administrador gerenciado”). No macOS 11, um bootstrap token pode conceder um secure token a qualquer usuário que inicie a sessão em um computador Mac, incluindo contas de usuário locais. O uso do recurso de Bootstrap Token do macOS 10.15 ou posterior requer:

- Registro do Mac no MDM via Apple School Manager ou Apple Business Manager, o que torna o Mac supervisionado
- Suporte do fornecedor do MDM

No macOS 10.15.4 ou posterior, um bootstrap token é gerado e guardado no MDM quando qualquer usuário que tenha um Secure Token ativado inicia a sessão pela primeira vez, caso a solução MDM seja compatível com o recurso. Um bootstrap token também pode ser gerado e guardado no MDM ao usar a ferramenta de linha de comando `profiles`, se necessário.

No macOS 11, um bootstrap token também pode ser usado para coisas além da concessão do secure token a contas de usuário. Em um Mac com Apple Silicon, um bootstrap token, se disponível, pode ser usado para autorizar a instalação de extensões do kernel e de atualizações de software quando gerenciado por um MDM.

Como a Apple protege os dados pessoais de usuários

Proteção do acesso de apps a dados de usuário

Além de criptografar os dados em repouso, os dispositivos Apple usam várias tecnologias, incluindo Cofre de Dados, para ajudar a impedir que apps acessem as informações pessoais de um usuário sem permissão. Nos Ajustes do iOS e iPadOS ou nas Preferências do Sistema no macOS, os usuários podem ver quais a quais apps eles permitiram acessar certas informações, assim como conceder ou revogar qualquer acesso futuro. O acesso é controlado nos seguintes itens:

- *iOS, iPadOS e macOS:* Calendários, Câmera, Contatos, Microfone, Fotos, Lembretes, Reconhecimento de Fala
- *iOS e iPadOS:* Bluetooth, Casa, Mídia, apps de Mídia e Apple Music, Movimento e Preparo Físico
- *iOS e watchOS:* Saúde
- *macOS:* monitoramento de entrada (por exemplo, teclas pressionadas), solicitações, gravações da tela (por exemplo, capturas de tela estáticas e vídeos), Preferências do Sistema

No iOS 13.4 ou posterior e iPadOS 13.4 ou posterior, todos os apps de terceiros têm seus dados protegidos automaticamente em um Cofre de Dados. O Cofre de Dados ajuda a proteger contra o acesso não autorizado aos dados, mesmo a partir de processos que não usam sandbox. Entre as classes adicionais no iOS 15 ou posterior estão Rede Local, Interações por Perto, Dados de Sensores e Uso para Pesquisa, e Foco.

Se o usuário iniciar a sessão no iCloud, os apps no iOS e iPadOS recebem acesso ao iCloud Drive por padrão. Usuários podem controlar o acesso de cada app na seção iCloud dos Ajustes. O iOS e iPadOS também fornecem restrições projetadas para impedir o movimento de dados entre apps e contas instaladas através de uma solução de gerenciamento de dispositivos móveis (MDM) e aqueles instalados pelo usuário.

Proteção de acesso aos dados de saúde do usuário

O HealthKit oferece um repositório central para dados de saúde e preparo físico no iPhone e no Apple Watch. O HealthKit também funciona diretamente com dispositivos de saúde e preparo físico, como monitores de batimento cardíaco compatíveis com Bluetooth Low Energy (BLE) e o coprocessador de movimento integrado a muitos dispositivos iOS. Todas as interações do HealthKit com apps de saúde e preparo físico, instituições de saúde e dispositivos de saúde e preparo físico exigem a permissão do usuário. Esses dados são armazenados na classe de Proteção de Dados “Protegido Exceto se Aberto”. O acesso aos dados é descontinuado 10 minutos após o bloqueio do dispositivo e os dados se tornam acessíveis na próxima vez que o usuário digitar o código ou usar o Face ID ou Touch ID para desbloquear o dispositivo.

Coleta e armazenamento de dados de saúde e preparo físico

O HealthKit também coleta e armazena dados de gerenciamento, como permissões de acesso de apps, nomes de dispositivos conectados ao HealthKit e informações de programação usadas para abrir apps quando novos dados estiverem disponíveis. Esses dados são armazenados na classe de Proteção de Dados "Protegido Até a Primeira Autenticação do Usuário". Arquivos temporários de registro armazenam registros de saúde gerados quando o dispositivo está bloqueado, como quando o usuário está se exercitando. Esses dados são armazenados na classe de Proteção de Dados "Protegido Exceto se Aberto". Quando o dispositivo é desbloqueado, os arquivos de registro temporário são importados para os bancos de dados de saúde primários e depois apagados quando a combinação é concluída.

Os dados do app Saúde podem ser armazenados no iCloud. A criptografia de ponta a ponta de dados do app Saúde requer o iOS 12 ou posterior e autenticação de dois fatores. Caso contrário, os dados do usuário ainda estarão criptografados no armazenamento e transmissão, mas não estarão criptografados de ponta a ponta. Depois que o usuário ativa a autenticação de dois fatores e atualiza para o iOS 12 ou posterior, seus dados de saúde são migrados para a criptografia de ponta a ponta.

Se o usuário usar o Finder (macOS 10.15 ou posterior) ou o iTunes (no macOS 10.14 ou anterior) para fazer o backup de seu dispositivo, os dados de saúde são armazenados apenas se o backup for criptografado.

Registros de saúde clínica

Usuários podem iniciar uma sessão em sistemas de saúde compatíveis dentro do app Saúde para obter uma cópia de seus registros de saúde clínica. Ao conectar um usuário a um sistema de saúde, o usuário autentica usando credenciais de cliente OAuth 2. Após a conexão, os dados dos registros de saúde clínica são baixados diretamente da instituição de saúde através de uma conexão protegida com TLS 1.3. Uma vez baixados, os registros de saúde clínica são armazenados em segurança juntamente com outros dados de saúde.

Integridade dos dados de saúde

Os dados armazenados no banco de dados incluem metadados para rastrear a proveniência de cada registro. Esses metadados incluem um identificador de app que indica qual app armazenou o registro. Além disso, um item de metadados opcional pode conter uma cópia do registro assinada digitalmente. O objetivo é fornecer integridade de dados para registros gerados por um dispositivo confiável. O formato usado para a assinatura digital é a Sintaxe de Mensagem Criptográfica (CMS), especificado no RFC 5652.

Acesso de apps de terceiros a dados de Saúde

O acesso à API do HealthKit é controlado por direitos e os apps devem atender às restrições sobre como os dados são usados. Por exemplo, apps não têm permissão para usar dados de saúde para publicidade. Os apps também precisam fornecer aos usuários uma política de privacidade que detalhe o uso dos dados de saúde.

O acesso aos dados de saúde por apps é controlado pelos ajustes de Privacidade do usuário. Os usuários são solicitados a conceder acesso aos dados de saúde a pedidos dos apps, de maneira semelhante aos apps Contatos, Fotos e outras fontes de dados do iOS. Entretanto, no caso de dados de saúde, o acesso para ler e gravar é concedido aos apps separadamente, assim como para cada tipo de dado de saúde. Os usuários podem visualizar e revogar as permissões concedidas para acesso aos dados de saúde em Ajustes > Saúde > Acesso a Dados e Dispositivos.

Se a permissão para gravar dados for concedida, os apps também podem ler os dados que gravam. Se a permissão para ler dados for concedida, os apps podem ler dados gravados por todas as fontes. Entretanto, os apps não podem determinar o acesso concedido a outros apps. Além disso, os apps não podem afirmar categoricamente se receberam acesso de leitura aos dados de saúde. Quando um app não possui acesso de leitura, nenhuma consulta retorna dados — a resposta gerada é a mesma que um banco de dados vazio retornaria. Isso é projetado para impedir que apps deduzam o estado de saúde do usuário ao aprender quais tipos de dados o usuário está rastreando.

Ficha Médica de usuários

O app Saúde oferece aos usuários a opção de preencher uma ficha médica com informações que podem ser importantes durante uma emergência médica. As informações são digitadas ou atualizadas manualmente e não são sincronizadas com as informações dos bancos de dados de saúde.

As informações da Ficha Médica podem ser visualizadas ao tocar no botão Emergência, na Tela Bloqueada. As informações são armazenadas no dispositivo usando a classe de Proteção de Dados "Sem Proteção", para que sejam acessadas sem que seja necessário digitar o código do dispositivo. A Ficha Médica é um recurso opcional que permite que os usuários decidam como equilibrar segurança e privacidade. O backup dos dados é feito no Backup do iCloud no iOS 13 ou anterior. No iOS 14, a Ficha Médica usa o CloudKit para a sincronização entre dispositivos e tem as mesmas características criptográficas do restante dos dados de saúde.

Compartilhamento de dados de Saúde

No iOS 15, o app Saúde dá aos usuários a opção de compartilhar os dados de Saúde com outros usuários. Os dados de Saúde são compartilhados entre dois usuários por meio da criptografia de ponta a ponta do iCloud. A Apple não pode acessar os dados enviados por meio do compartilhamento dos dados de Saúde. Para usar esse recurso, tanto o usuário que envia os dados quanto o que recebe devem usar o iOS 15 ou posterior e ter a autenticação de dois fatores ativada.

Os usuários também podem optar por usar o recurso de compartilhamento com o provedor, do app Saúde, para compartilhar os dados de Saúde com seu provedor de saúde. Os dados compartilhados por meio desse recurso são disponibilizados apenas às instituições de saúde selecionadas pelo usuário, com criptografia de ponta a ponta. A Apple não guarda nem possui acesso às chaves de criptografia para decifrar, visualizar ou acessar de outra forma os dados de Saúde compartilhados por meio desse recurso. Mais detalhes de como o projeto deste serviço protege os dados de Saúde dos usuários podem ser encontrados na seção Security and Privacy do Apple Registration Guide for Healthcare Organizations (em inglês).

Assinatura digital e criptografia

Listas de controle de acesso

Os dados das chaves são particionados e protegidos com listas de controle de acesso (ACLs). Assim, as credenciais armazenadas por apps de terceiros não podem ser acessadas por apps com identidades diferentes a menos que o usuário as aprove explicitamente. Essa proteção fornece um mecanismo para a proteção de credenciais de autenticação em dispositivos Apple para uma série de apps e serviços dentro da organização.

Mail

No app Mail, os usuários podem enviar mensagens assinadas e criptografadas digitalmente. O Mail descobre automaticamente, com distinção entre maiúsculas e minúsculas e conformidade com o RFC 5322, o endereço de e-mail, assunto ou nomes alternativos em certificados de assinatura digital e criptografia em tokens de Verificação de Identificação Pessoal (PIV) conectados em smart cards compatíveis. Se uma conta de e-mail configurada corresponder a um endereço de e-mail em um certificado de assinatura digital ou criptografia em um token PIV conectado, o Mail mostra automaticamente o botão de assinatura na barra de ferramentas da janela de nova mensagem. Se o Mail tiver o certificado de criptografia de e-mail do destinatário ou puder descobri-lo na lista de endereços global (GAL) do Microsoft Exchange, um ícone de cadeado desbloqueado aparece na barra de ferramentas da nova mensagem. Um ícone de cadeado bloqueado indica que a mensagem será enviada criptografada com a chave pública do destinatário.

S/MIME por mensagem

O iOS, iPadOS e macOS são compatíveis com S/MIME por mensagem. Isso significa que os usuários de S/MIME têm a opção de sempre assinar e criptografar mensagens por padrão ou selecionar mensagens individuais que desejam assinar e criptografar.

As identidades usadas com S/MIME podem ser disponibilizadas a dispositivos Apple por meio de um perfil de configuração, uma solução de gerenciamento de dispositivos móveis (MDM), o Simple Certificate Enrollment Protocol (SCEP) ou Autoridade de Certificação do Microsoft Active Directory.

Smart cards

O macOS 10.12 ou posterior possui compatibilidade nativa com cartões PIV. Esses cartões são amplamente usados em organizações comerciais e governamentais para autenticação de dois fatores, assinatura digital e criptografia.

Os smart cards possuem uma ou mais identidades digitais que têm um par de chaves públicas e privadas e um certificado associado. O desbloqueio de um smart card com o número de identificação pessoal (PIN) fornece acesso às chaves privadas usadas nas operações de autenticação, criptografia e assinatura. O certificado determina o que uma chave pode fazer, quais atributos são associados a ela e se ela foi validada (assinada) pelo certificado de uma autoridade de certificação (AC).

Os smart cards podem ser usados na autenticação com dois fatores. Os dois fatores necessários para desbloquear um cartão são "algo que o usuário possui" (o cartão) e "algo que o usuário sabe" (o PIN). O macOS 10.12 ou posterior também possui compatibilidade nativa com autenticação em Janelas de Início de Sessão com smart card e autenticação por certificado de cliente em sites no Safari. Ele também é compatível com a autenticação do Kerberos por meio de pares de chaves (PKINIT), para início de sessão único em dispositivos compatíveis com Kerberos. Para saber mais sobre smart cards e macOS, consulte Introdução à integração de smart cards em *Implementação da Plataforma Apple*.

Imagens de disco criptografadas

No macOS, as imagens de disco criptografadas atuam como contêineres seguros nos quais os usuários podem armazenar ou transferir documentos e outros arquivos sigilosos. As imagens de disco criptografadas são criadas com o Utilitário de Disco, localizado em /Aplicativos/Utilitários/. As imagens de disco podem ser criptografadas usando criptografia AES de 128 bits ou 256 bits. Como uma imagem de disco montada é tratada como um volume local conectado ao Mac, os usuários podem copiar, mover e abrir arquivos e pastas armazenados nela. Assim como com o FileVault, o conteúdo de uma imagem de disco é criptografado e descriptografado em tempo real. Para trocar documentos, arquivos e pastas de forma segura com imagens de disco criptografadas, os usuários podem salvar uma imagem de disco criptografada em uma mídia removível, enviá-la como anexo de e-mail ou armazená-la em um servidor remoto. Para obter mais informações sobre imagens de disco criptografadas, consulte o Manual do Usuário do Utilitário de Disco.

Segurança de apps

Visão geral da segurança de apps

Hoje, apps estão entre os elementos mais importantes de uma arquitetura de segurança. Mesmo oferecendo benefícios de produtividade incríveis a usuários, apps também têm o potencial de impactar negativamente a segurança e a estabilidade do sistema, assim como os dados do usuário, se não forem gerenciados corretamente.

Por isso, a Apple fornece camadas de proteção para ajudar a assegurar que os apps estejam livres de malwares conhecidos e que não tenham sido adulterados. Proteções adicionais garantem que o acesso dos apps aos dados dos usuários seja cuidadosamente mediado. Esses controles de segurança proporcionam uma plataforma segura e estável para os apps, permitindo que milhares de desenvolvedores ofereçam centenas de milhares de apps para iOS, iPadOS e macOS — tudo isso sem afetar a integridade do sistema. Os usuários podem acessar esses apps em seus dispositivos Apple sem terem medo de vírus, malware ou ataques não autorizados.

No iPhone, iPad e iPod touch, todos apps são obtidos na App Store (e todos são sandboxed), proporcionando os controles mais restritivos.

No Mac, muitos apps são obtidos na App Store, mas os usuários de Mac também baixam e usam apps da internet. Para que downloads da internet sejam seguros, o macOS tem camadas de controles adicionais. Primeiramente, por padrão no macOS 10.15 ou posterior, todos os apps para Mac precisam ser autenticados pela Apple para iniciar. Esse requisito ajuda a garantir que esses apps estejam livres de malwares conhecidos, sem exigir que os apps sejam fornecidos pela App Store. Além disso, o macOS possui uma proteção antivírus de ponta para bloquear (e, se necessário, remover) malware.

Como um controle adicional nas diferentes plataformas, o sandbox ajuda a proteger os dados dos usuários contra acesso não autorizado de apps. E no macOS, os dados em áreas importantes ficam protegidos, ajudando a garantir que os usuários mantenham o controle do acesso de todos os apps aos arquivos nas pastas Mesa, Documentos, Downloads e em outras áreas, estejam esses apps em sandbox ou não.

Capacidade nativa	**Equivalente de terceiros**
Lista de plug-ins não aprovados, lista de extensões do Safari não aprovadas	Definições de Vírus/Malware
Quarentena de Arquivo	Definições de Vírus/Malware
Assinaturas do XProtect/YARA	Definições de Vírus/Malware; proteção no ponto final
Gatekeeper	Proteção no ponto final; exige a assinatura de apps para ajudar a garantir a execução apenas de softwares confiáveis
eficheck (Necessário para um Mac sem o chip Apple T2 Security)	Proteção no ponto final; detecção de rootkit
Firewall de aplicativo	Proteção no ponto final; firewall
Filtro de Pacotes (pf)	Soluções de firewall
Proteção da Integridade do Sistema	Integrada ao macOS
Controles de Acesso Obrigatórios	Integrada ao macOS
Lista de exclusão de kext	Integrada ao macOS
Assinatura obrigatória do código de apps	Integrada ao macOS
Autenticação de apps	Integrada ao macOS

Segurança de apps no iOS e iPadOS

Introdução à segurança de apps para iOS e iPadOS

Ao contrário de outras plataformas de dispositivos móveis, o iOS e iPadOS não permitem que usuários instalem apps não assinados e potencialmente maliciosos de sites ou executem apps não confiáveis. No tempo de execução, verificações de assinatura de código de todas as páginas de memória executáveis são feitas conforme elas são carregadas para ajudar a garantir que o app não tenha sido modificado desde que foi instalado ou atualizado pela última vez.

Após a confirmação de que o app provém de uma fonte confiável, o iOS e iPadOS aplicam medidas de segurança criadas para impedir que ele comprometa outros apps ou o restante do sistema.

Processo de assinatura do código de apps no iOS e iPadOS

No iOS e iPadOS, a Apple oferece segurança de apps através de medidas como a assinatura obrigatória de código, o registro estrito de desenvolvedores e outras.

Assinatura obrigatória de código

Depois de ser iniciado, o kernel do iOS e iPadOS controla quais processadores e apps podem ser executados. Para ajudar a garantir que todos os apps provenham de uma fonte conhecida e aprovada e que não tenham sido adulterados, o iOS e iPadOS exigem que todos os códigos executáveis sejam assinados por um certificado emitido pela Apple. Os apps fornecidos com o dispositivo, como o Mail e o Safari, são assinados pela Apple. Os apps de terceiros também precisam ser validados e assinados por um certificado emitido pela Apple. A assinatura de código obrigatória estende o conceito de cadeia de confiança do sistema operacional aos apps e ajuda a impedir que apps de terceiros carreguem recursos de código não assinado ou usem código que se modifique sozinho.

Como os desenvolvedores assinam os apps

Desenvolvedores podem assinar seus apps através da validação de certificados (através do Programa de Desenvolvedor da Apple). Eles também podem integrar frameworks a seus apps e ter esse código validado com um certificado emitido pela Apple (através de uma string de identificador da equipe),

- *Validação de certificado:* Para desenvolver e instalar apps em dispositivos iOS e iPadOS, os desenvolvedores devem se registrar na Apple e se associar ao Programa de Desenvolvedor da Apple. A identidade real de cada desenvolvedor, seja ele um indivíduo ou uma empresa, é verificada pela Apple antes da emissão de seu certificado. Esse certificado permite que os desenvolvedores assinem e enviem apps à App Store para distribuição. Como resultado, todos os apps que estão na App Store foram enviados por uma pessoa ou organização identificável, o que mitiga a criação de apps maliciosos. Os apps também foram revisados pela Apple para ajudar a garantir que funcionem de forma geral como descrito e não contenham erros óbvios ou outros problemas marcantes. Além da tecnologia já discutida, esse processo de curadoria permite que os usuários possam confiar na qualidade dos apps que adquirem.

- *Validação da assinatura de código:* o iOS e iPadOS permitem que os desenvolvedores integrem frameworks aos seus apps, que podem ser usados pelo próprio app ou por extensões integradas a ele. Para proteger o sistema e outros apps do carregamento de códigos de terceiros em seu espaço de endereço, o sistema executa uma validação da assinatura de código de todas as bibliotecas dinâmicas das quais um processo depende ao ser aberto. Essa verificação é realizada através do identificador da equipe (ID da Equipe), extraído do certificado emitido pela Apple. O identificador da equipe é uma string alfanumérica de 10 caracteres, como 1A2B3C4D5F, por exemplo. Um programa pode depender de qualquer biblioteca de plataforma fornecida com o sistema ou qualquer biblioteca com o mesmo identificador de equipe na assinatura de código do executável principal. Como os executáveis fornecidos como parte do sistema não possuem um identificador de equipe, eles só podem depender de bibliotecas fornecidas com o próprio sistema.

Verificação de apps proprietários para uso interno

As empresas qualificadas também podem desenvolver apps proprietários para uso interno e distribuí-los aos seus funcionários. As empresas e organizações podem se candidatar ao Programa Empresarial de Desenvolvedor da Apple (ADEP). Para obter mais informações e consultar os requisitos de qualificação, consulte o site do Programa Empresarial de Desenvolvedor da Apple. Após se tornar membro do ADEP, uma organização pode se registrar para obter um perfil de provisão que permite que os apps proprietários desenvolvidos internamente sejam executados nos dispositivos que ela autoriza.

Os usuários precisam ter o perfil de provisão instalado para executar esses apps. Isso ajuda a garantir que apenas usuários autorizados possam carregar os apps em seus dispositivos iOS e iPadOS. Os apps instalados por meio do gerenciamento de dispositivos móveis (MDM) são implicitamente confiáveis porque o relacionamento entre a organização e o dispositivo já está estabelecido. Caso contrário, os usuários precisam aprovar o perfil de provisão do app nos Ajustes. As organizações também podem restringir a aprovação de apps de desenvolvedores desconhecidos por seus usuários. Ao abrir pela primeira vez um app proprietário para uso interno, o dispositivo precisa receber uma confirmação positiva da Apple, indicando que o app tem permissão para ser executado.

Segurança do processo em tempo de execução no iOS e iPadOS

O iOS e iPadOS usam “sandbox”, direitos declarados e Aleatorização do Layout de Espaço de Endereço (ASLR) para ajudar a garantir a segurança no tempo de execução.

Sandbox

Todos os apps de terceiros são “sandboxed” e, portanto, não podem acessar os arquivos armazenados por outros apps ou fazer alterações no dispositivo. O sandbox é projetado para ajudar a impedir que um app colete ou modifique informações armazenadas por outros apps. Cada app possui um diretório inicial exclusivo para seus arquivos, atribuído aleatoriamente quando o app é instalado. Se um app de terceiros precisar acessar informações que não as suas próprias, ele usará os serviços fornecidos explicitamente pelo iOS e iPadOS.

Os arquivos e recursos do sistema também são protegidos dos apps do usuário. A maioria dos arquivos e recursos do sistema do iOS e iPadOS é executada com o usuário não privilegiado “mobile”, assim como todos os apps de terceiros. Toda a partição do sistema operacional é montada como somente leitura. Ferramentas desnecessárias, como serviços de início de sessão remoto, não estão incluídas no software do sistema e as APIs não permitem que apps ampliem seus próprios privilégios para modificar outros apps ou o iOS e iPadOS.

Uso de direitos

O acesso de apps de terceiros a informações do usuário e recursos, como o iCloud e a extensibilidade, é controlado através de direitos declarados. Os direitos são pares chave-valor assinados em um app e permitem a autenticação além dos fatores de tempo de execução, como o ID de usuário UNIX. Os direitos não podem ser alterados, já que são assinados digitalmente. Os direitos são usados extensivamente pelos daemons e apps do sistema para realizar operações privilegiadas específicas que, de outra forma, necessitariam que o processo fosse executado como root. Isso reduz de maneira significativa a possibilidade do aumento de privilégio de um daemon ou app do sistema comprometido.

Além disso, os apps só podem executar processamento em segundo plano através das APIs fornecidas pelo sistema. Isso permite que os apps continuem a funcionar sem prejudicar o desempenho ou afetar drasticamente a duração da bateria.

Aleatorização do Espaço de Endereço

A Aleatorização de Espaço de Endereço (ASLR) ajuda a proteger contra a exploração de erros de corrupção da memória. Os apps integrados usam a ASLR para ajudar a aleatorizar todas as regiões da memória na inicialização. Além do trabalho após a abertura, a ASLR organiza aleatoriamente os endereços de memória do código executável, das bibliotecas do sistema e dos construtos de programação relacionados, reduzindo ainda mais a possibilidade de diversos aproveitamentos. Por exemplo, um ataque return-to-libc tenta enganar um dispositivo para que ele execute um código malicioso através da manipulação dos endereços das bibliotecas de contêineres e do sistema. A aleatorização do posicionamento desses itens dificulta a execução do ataque, especialmente em larga escala. O Xcode e os ambientes de desenvolvimento para iOS ou iPadOS, compilam automaticamente os programas de terceiros com o suporte à ASLR ativo.

Recurso Nunca Executar

O iOS e iPadOS fornecem uma proteção ainda maior através do recurso Nunca Executar (XN) do ARM, o qual marca páginas de memória como não executáveis. As páginas de memória marcadas como graváveis e executáveis podem ser usadas por apps apenas sob condições rigorosamente controladas: o kernel verifica a presença de direitos dinâmicos de assinatura de código somente da Apple. Mesmo assim, apenas uma única chamada `mmap` pode ser feita para solicitar uma página executável e gravável, que recebe um endereço aleatorizado. O Safari usa essa funcionalidade em seu compilador JavaScript Just-in-Time (JIT).

Compatibilidade com extensões no iOS, iPadOS e macOS

O iOS, iPadOS e macOS permitem que os apps forneçam funcionalidade a outros apps através de extensões. As extensões são binários executáveis assinados de finalidade específica, empacotados em um app. Durante a instalação, o sistema detecta automaticamente as extensões e usa um sistema de correspondência para disponibilizá-las a outros apps.

Pontos de extensão

Uma área do sistema que ofereça suporte a extensões é chamada de *ponto de extensão*. Cada ponto de extensão fornece APIs e aplica regras para tal área. O sistema determina quais extensões estão disponíveis com base em regras de correspondência de ponto de extensão específicas. O sistema abre os processos de extensão automaticamente conforme a necessidade e gerencia a sua vida útil. Direitos podem ser usados para restringir a disponibilidade das extensões a certos apps do sistema. Por exemplo, um widget da visualização “Hoje” é exibido apenas na Central de Notificações e uma extensão de compartilhamento só está disponível no painel Compartilhamento. Exemplos de pontos de extensão são: widgets Hoje, Compartilhar, Ações, Edição de Fotos, Provedor de Arquivos e Teclado Personalizado.

Como as extensões se comunicam

As extensões são executadas em seus próprios espaços de endereço. A comunicação entre a extensão e o app a partir do qual ela foi ativada usa comunicações interprocessuais mediadas pelo framework do sistema. Elas não têm acesso aos arquivos ou espaços de memória umas das outras. As extensões são criadas para serem isoladas umas das outras, dos apps que as contêm e dos apps que as usam. Elas são sandboxed como qualquer outro app de terceiro e possuem um contêiner separado do contêiner do app que as contém. Entretanto, elas compartilham o mesmo acesso aos controles de privacidade do app em que estão contidas. Portanto, se um usuário conceder a um app acesso aos Contatos, esse acesso também é concedido às extensões integradas ao app, mas não às extensões ativadas por ele.

Como os teclados personalizados são usados

Os teclados personalizados são um tipo especial de extensão, já que ela é ativada pelo usuário para todo o sistema. Depois de ativada, uma extensão de teclado é usada em qualquer campo de texto, exceto para a digitação do código e em visualizações de texto seguro. Para restringir a transferência de dados do usuário, os teclados personalizados são executados por padrão em um sandbox bastante restritivo que bloqueia o acesso à rede, a serviços que executam operações de rede em nome de um processo e a APIs que poderiam permitir que a extensão extraísse dados digitados. Os desenvolvedores de teclados personalizados podem solicitar Acesso Aberto às suas extensões, o que permite que o sistema execute a extensão no sandbox padrão após obter o consentimento do usuário.

MDM e extensões

No caso de dispositivos inscritos em uma solução de gerenciamento de dispositivos móveis (MDM), as extensões de documento e de teclado seguem as regras “Abrir com Gerenciado”. Por exemplo, a solução MDM ajuda a impedir que usuários exportem um documento de um app gerenciado para um Provedor de Documentos não gerenciado ou ajuda a impedir que eles usem um teclado não gerenciado com um app gerenciado. Além disso, os desenvolvedores de apps podem impedir o uso de extensões de teclado de terceiros em seus apps.

Proteção de apps e grupos de apps no iOS e iPadOS

No iOS e iPadOS, organizações podem usar o SDK do IOS e participar de um Grupo de Apps no Portal Apple Developer para proteger apps.

Adoção da Proteção de Dados em apps

O Kit de Desenvolvimento de Software (SDK) do iOS e iPadOS oferece um conjunto completo de APIs que facilitam a adoção da Proteção de Dados por terceiros e desenvolvedores empresariais e ajudam a garantir o nível mais alto de proteção para seus apps. A Proteção de Dados está disponível para APIs de banco de dados e de arquivos, incluindo NSFileManager, CoreData, NSData e SQLite.

O banco de dados do app Mail (incluindo anexos), livros gerenciados, favoritos do Safari, imagens de abertura do app e dados de localização também são armazenados por meio de criptografia, com chaves protegidas pelo código do usuário no dispositivo. Os apps Calendário (excluindo anexos), Contatos, Lembretes, Notas, Mensagens e Fotos implementam o privilégio de Proteção de Dados "Protegido Até a Primeira Autenticação do Usuário".

Os apps instalados pelo usuário que não optam por uma classe específica de Proteção de Dados recebem "Protegido Até a Primeira Autenticação do Usuário" por padrão.

Participação de um Grupo de Apps

Apps e extensões de propriedade de uma certa conta de desenvolvedor podem compartilhar conteúdo quando configurados como parte de um Grupo de Apps. Cabe ao desenvolvedor criar os grupos apropriados no Portal Apple Developer e incluir o conjunto de apps e extensões desejados. Quando configurados para ser parte de um Grupo de Apps, os apps têm acesso ao seguinte:

- Um contêiner compartilhado no volume para armazenamento, que permanece no dispositivo enquanto houver ao menos um app do grupo instalado;
- Preferências compartilhadas;
- Itens compartilhados das chaves.

O Portal Apple Developer ajuda a garantir a exclusividade dos IDs de grupo (GIDs) de Apps por todo o ecossistema de apps.

Verificação de acessórios no iOS e iPadOS

O programa de licenciamento Made for iPhone, iPad e iPod touch (MFi) fornece a fabricantes de acessórios verificados o acesso ao Protocolo de Acessórios para iPod (iAP) e aos componentes de hardware de suporte necessários.

Quando um acessório MFi usa um conector Lightning ou USB-C ou conexão Bluetooth para se comunicar com um dispositivo iOS ou iPadOS, o dispositivo solicita que o acessório responda com um certificado fornecido pela Apple, o qual é verificado pelo dispositivo, para comprovar ter sido autorizado pela Apple. Então, o dispositivo envia um desafio e o acessório precisa respondê-lo com uma resposta assinada. Esse processo é gerenciado completamente por um circuito integrado (CI) personalizado que a Apple fornece a fabricantes de acessórios aprovados, sendo transparente ao acessório em si.

Os acessórios podem solicitar acesso a diferentes funcionalidades e métodos de transporte, como por exemplo, o acesso a transmissões de áudio digital através do cabo Lightning ou USB-C, ou às informações de localização fornecidas por Bluetooth. Um CI de autenticação é projetado para garantir que apenas os acessórios aprovados possuam acesso total ao dispositivo. Se um acessório não oferecer suporte à autenticação, seu acesso é limitado ao áudio analógico e a um pequeno subconjunto de controles de reprodução de áudio serial (UART).

O AirPlay também usa o CI de autenticação para verificar se os receptores foram aprovados pela Apple. As transmissões de áudio AirPlay e vídeo CarPlay usam o MFi-SAP (Protocolo de Associação Segura), o qual usa AES128 no modo de contagem (CTR) para criptografar a comunicação entre o acessório e o dispositivo. As chaves transitórias são trocadas usando a troca de chaves ECDH (Curve25519) e assinadas usando a chave RSA de 1024 bits do CI de autenticação como parte do protocolo Station-to-Station (STS).

Segurança de apps no macOS

Introdução à segurança de apps para macOS

A segurança de apps no macOS consiste em várias camadas sobrepostas, das quais, a primeira, é a opção de executar apenas apps assinados e confiáveis da App Store. Além disso, o macOS dispõe proteções em camadas para ajudar a garantir que os apps baixados da internet estejam livres de malwares conhecidos. O macOS oferece tecnologias para detectar e remover malware, além de proteções adicionais projetadas para impedir que apps não confiáveis acessem dados de usuários. Os serviços da Apple como atualizações do XProtect e Autenticação são projetados para ajudar a evitar a instalação de malware. Quando necessário, esses serviços localizam malwares que podem ter evitado a detecção a princípio e os removem de forma rápida e eficiente. Em última análise, os usuários do macOS estão livres para operar dentro do modelo de segurança que faz sentido para eles, incluindo a execução de código totalmente não assinado e não confiável.

Processo de assinatura do código de apps no macOS

Todos os apps da App Store são assinados pela Apple. Essa assinatura é projetada para garantir que eles não tenham sido adulterados ou alterados. A Apple assina todos os apps fornecidos com os dispositivos Apple.

No macOS 10.15, todos os apps distribuídos fora da App Store devem ser assinados pelo desenvolvedor com um certificado Developer ID emitido pela Apple (combinado com uma chave privada) e autenticados pela Apple para serem executados com os ajustes padrão do Gatekeeper. Os apps desenvolvidos internamente também devem ser assinados com um Developer ID emitido pela Apple para que os usuários possam validar sua integridade.

No macOS, a assinatura de código e a autenticação funcionam de forma independente — e podem ser realizadas por atores diferentes — para objetivos diferentes. A assinatura de código é realizada pelo desenvolvedor usando o certificado Developer ID (emitido pela Apple) e a verificação dessa assinatura comprova para o usuário que o software do desenvolvedor não foi adulterado desde que o desenvolvedor o compilou e assinou. A autenticação pode ser realizada por qualquer pessoa na cadeia de distribuição de software e comprova que a Apple recebeu uma cópia do código para verificar a existência de malwares e que nenhum malware conhecido foi encontrado. A saída da autenticação é um tíquete, que é armazenado nos servidores da Apple e pode ser opcionalmente grampeado no app (por qualquer pessoa) sem invalidar a assinatura do desenvolvedor.

Os Controles de Acesso Obrigatórios (MACs) requerem a assinatura de código para usar direitos protegidos pelo sistema. Por exemplo, os apps que exigem acesso através do firewall devem ter seu código assinado com o direito MAC correspondente.

Gatekeeper e proteção em tempo de execução no macOS

O macOS oferece a tecnologia Gatekeeper e a proteção no tempo de execução para ajudar a garantir que apenas softwares confiáveis sejam executados no Mac de um usuário.

Gatekeeper

O macOS inclui uma tecnologia de segurança chamada *Gatekeeper*, que é projetada para ajudar a garantir que apenas softwares confiáveis sejam executados no Mac de um usuário. Quando um usuário baixa e abre um app, um plug-in ou um pacote de instalação de fora da App Store, o Gatekeeper verifica se o software provém de um desenvolvedor identificado, é autenticado pela Apple para garantir a ausência de conteúdo malicioso, e não foi alterado. O Gatekeeper também solicita a aprovação do usuário antes de abrir softwares baixados pela primeira vez para garantir que o usuário não tenha sido enganado com o objetivo de abrir um código executável que acreditava ser apenas um arquivo de dados.

Por padrão, o Gatekeeper ajuda a garantir que todo software baixado tenha sido assinado pela App Store ou por um desenvolvedor registrado e tenha sido autenticado pela Apple. Tanto o processo de revisão da App Store quanto o canal de autenticação são proetados para garantir que os apps não contenham malwares conhecidos. Portanto, por padrão, *todo software no macOS é verificado em busca de conteúdo malicioso conhecido na primeira vez que é aberto, independentemente da forma como tenha chegado ao Mac*.

Os usuários e as organizações têm a opção de permitir apenas os softwares instalados a partir da App Store. Opcionalmente, os usuários podem substituir as políticas do Gatekeeper e abrir qualquer software, a menos que isso seja restringido por uma solução de gerenciamento de dispositivos móveis (MDM). As organizações podem usar o MDM para configurar os ajustes do Gatekeeper, incluindo a permissão de softwares assinados com identidades alternativas. Caso necessário, o Gatekeeper também pode ser desativado por completo.

O Gatekeeper também protege contra a distribuição de plug-ins maliciosos com apps benignos. Nesses casos, o uso do app aciona o carregamento de um plug-in malicioso sem o conhecimento do usuário. Quando necessário, o Gatekeeper abre apps a partir de localizações somente leitura aleatorizadas. Isso é projetado para impedir o carregamento automático de plug-ins distribuídos com o app.

Proteção em tempo de execução

Os arquivos de sistema, recursos e o kernel são protegidos do espaço de apps do usuário. Todos os apps da App Store são sandboxed para restringir o acesso a dados armazenados por outros apps. Se um app da App Store precisar acessar dados de outro app, ele só pode fazer isso através do uso de APIs e serviços fornecidos pelo macOS.

Proteção contra malware no macOS

A Apple opera um processo de inteligência de ameaças para identificar e bloquear malware rapidamente.

Três camadas de defesa

As defesas contra malware são estruturadas em três camadas:

1. *Impedir a abertura ou execução de malware:* App Store, ou Gatekeeper combinado com a Autenticação

2. *Bloquear a execução de malware em sistemas de clientes:* Gatekeeper, Autenticação e XProtect

3. *Remediar um malware que tenha sido executado:* XProtect

A primeira camada de defesa é projetada para inibir a distribuição de malware e impedir que ele seja aberto até mesmo uma única vez — esse é o objetivo da App Store e do Gatekeeper combinado com a Autenticação.

A camada de defesa seguinte serve para ajudar a garantir que, caso um malware apareça em qualquer Mac, ele seja identificado e bloqueado rapidamente, tanto para parar sua disseminação quanto para remediar os sistemas Mac nos quais ele já tenha ganhado terreno. O XProtect complementa essa defesa, além do Gatekeeper e da Autenticação.

Por fim, o XProtect age para remediar malwares que tenham conseguido uma execução bem-sucedida.

Essas proteções, descritas em mais detalhes abaixo, são combinadas para oferecer suporte às práticas recomendadas de proteção contra vírus e malware. Há proteções adicionais, particularmente em computadores Mac com Apple Silicon, para limitar o dano em potencial de malwares que consigam ser executados. Consulte Proteção do acesso de apps a dados de usuário para ver as maneiras com as quais o macOS pode ajudar a proteger dados de usuário contra malware, e Integridade do sistema operacional para ver as maneiras com as quais o macOS pode limitar as ações que malwares podem realizar no sistema.

Autenticação

A *Autenticação* é um serviço de análise de malware fornecido pela Apple. Desenvolvedores que desejam distribuir apps para macOS fora da App Store enviam seus apps para análise como parte do processo de distribuição. A Apple analisa esse software em busca de malwares conhecidos e, caso não os encontre, emite um tíquete de Autenticação. Normalmente, desenvolvedores adicionam esse tíquete a seus apps para que o Gatekeeper possa verificar e abrir o app, mesmo off-line.

A Apple também pode emitir uma revogação de tíquete para apps sabidamente maliciosos, mesmo que eles tenham sido autenticados anteriormente. O macOS busca regularmente novos tíquetes de revogação para que o Gatekeeper tenha as informações mais recentes e possa bloquear a abertura desses arquivos. Esse processo pode bloquear apps maliciosos rapidamente porque as atualizações acontecem em segundo plano com uma frequência muito maior do que até das atualizações em segundo plano que enviam novas assinaturas do XProtect. Além disso, essa proteção pode ser aplicada tanto a apps autenticados anteriormente, assim como àqueles que não o foram.

XProtect

O macOS inclui uma tecnologia antivírus integrada, chamada *XProtect*, para a detecção e remoção de malware com base em assinaturas. O sistema usa assinaturas YARA, uma ferramenta usada para conduzir a detecção de malware com base na assinatura que a Apple atualiza regularmente. A Apple monitora novas infecções e variantes de malware, e atualiza automaticamente as assinaturas (independentemente das atualizações do sistema) para ajudar a proteger um Mac contra infecções de malware. O XProtect detecta e bloqueia automaticamente a execução de malwares conhecidos. No macOS 10.15 ou posterior, o XProtect busca conteúdo malicioso conhecido sempre que:

- Um app for aberto pela primeira vez
- Um app tiver sido alterado (no sistema de arquivos)
- As assinatura do XProtect forem atualizadas

Quando o XProtect detecta um malware conhecido, o software é bloqueado e o usuário é notificado, recebendo a opção de movê-lo para o Lixo.

Nota: a Autenticação é eficiente contra arquivos conhecidos (ou hashes de arquivos) e pode ser usada em apps que tenham sido abertos anteriormente. As regras baseadas em assinaturas do XProtect são mais genéricas do que um hash de arquivo específico para que seja possível encontrar variantes não vistas pela Apple. O XProtect analisa apenas apps que foram alterados ou quando são abertos pela primeira vez.

Se um malware conseguir chegar ao Mac, o XProtect também possui uma tecnologia para solucionar as infecções. Por exemplo, ele possui um mecanismo que remedia infecções com base em atualizações fornecidas automaticamente pela Apple (como parte das atualizações automáticas dos arquivos de dados do sistema e das atualizações de segurança). Ele também remove malwares ao receber informações atualizadas e continua buscando infecções periodicamente. O XProtect não reinicializa o Mac automaticamente.

Atualizações automáticas de segurança do XProtect

A Apple lança as atualizações do XProtect automaticamente, com base nas informações mais recentes disponíveis sobre ameaças. Por padrão, o macOS busca essas atualizações diariamente. As atualizações da Autenticação, que são distribuídas por meio da sincronização do CloudKit, são muito mais frequentes.

Como a Apple responde quando um novo malware é descoberto

Quando um novo malware é descoberto, vários passos podem ser tomados:

- Qualquer certificado de Developer ID associado é revogado.
- Os tíquetes de revogação de Autenticação são emitidos para todos os arquivos (apps e arquivos associados).
- Assinaturas do XProtect são desenvolvidas e lançadas.

  Essas assinaturas também são aplicadas retroativamente a qualquer software autenticado anteriormente e qualquer nova detecção pode resultar na ocorrência de uma ou mais das ações anteriores.

Por fim, a detecção de um malware inicia uma série de passos durante os próximos segundos, horas e dias para propagar as melhores proteções possíveis para usuários de Mac.

Controle do acesso de apps a arquivos no macOS

A Apple acredita que os usuários devem ter total transparência, consentimento e controle do que os apps fazem com os seus dados. No macOS 10.15, este modelo é aplicado pelo sistema para ajudar a garantir que todos os apps devam obter o consentimento do usuário antes de acessar arquivos em Documentos, Downloads, Mesa, iCloud Drive e volumes de rede. No macOS 10.13 ou posterior, os apps que exigem acesso a todo o dispositivo de armazenamento devem ser adicionados explicitamente nas Preferências do Sistema. Além disso, as funcionalidades de acessibilidade e automação requerem a permissão do usuário para ajudar a garantir que eles não contornem outras proteções. Dependendo da política de acesso, os usuários podem receber uma solicitação ou serem obrigados a alterar o ajuste em Preferências do Sistema > Segurança e Privacidade > Privacidade:

Item	App faz solicitação ao usuário	Usuário deve editar os ajustes de privacidade do sistema
Acessibilidade		✅
Acesso total ao armazenamento interno		✅
Arquivos e pastas *Nota:* inclui Mesa, Documentos, Downloads, volumes de rede e volumes removíveis	✅	
Automação (eventos da Apple)	✅	

Os itens que estão no Lixo do usuário são protegidos de qualquer app que use o Acesso Total ao Disco; o usuário não é solicitado para o acesso do app. Se o usuário desejar que os apps acessem os arquivos, eles devem ser movidos do Lixo para um outro local.

Os usuários que ativarem o FileVault no Mac são solicitados a fornecer credenciais válidas antes de continuar o processo de inicialização e obter acesso a modos de inicialização especializados. Sem credenciais de início de sessão válidas ou uma chave de recuperação, todo o volume permanece criptografado e protegido contra acesso não autorizado, mesmo que o dispositivo de armazenamento físico seja removido e conectado a outro computador.

Para proteger dados em um ambiente empresarial, a TI deve definir e aplicar políticas de configuração do FileVault usando o gerenciamento de dispositivos móveis (MDM). As organizações têm várias opções de gerenciamento de volumes criptografados, como chaves de recuperação institucionais, pessoais (que podem ser opcionalmente armazenadas com o MDM por garantia) ou uma combinação de ambas. A alternância de chaves também pode ser definida como política no MDM.

Recursos de segurança no app Notas

O app Notas inclui um recurso de notas seguras — no iPhone, iPad, Mac e no site do iCloud — que permite que usuários protejam o conteúdo de notas específicas. Os usuários também podem compartilhar notas com outras pessoas de forma segura.

Notas seguras

As notas seguras são criptografadas de ponta a ponta por meio de uma senha fornecida pelo usuário que é exigida para visualizar as notas em dispositivos iOS, iPadOS e macOS, e no site do iCloud. Cada conta do iCloud (incluindo contas de dispositivos "Em Meu") pode ter uma senha separada.

Quando um usuário utiliza uma nota segura, uma chave de 16 bytes é derivada da senha do usuário por meio de PBKDF2 e SHA256. A nota e todos os seus anexos são criptografados usando AES com Modo Galois/Counter (AES-GCM). Novos registros são criados no Core Data e CloudKit para armazenar a nota criptografada, os anexos, a etiqueta e o vetor de inicialização. Depois da criação dos novos registros, os dados originais não criptografados são apagados. Entre os anexos compatíveis com criptografia estão: imagens, desenhos, tabelas, mapas e sites. Notas que contêm outros tipos de anexos não podem ser criptografadas e anexos incompatíveis não podem ser adicionados a notas seguras.

Para visualizar uma nota segura, o usuário deve inserir a senha ou se autenticar usando o Face ID ou Touch ID. Depois que o usuário é autenticado com sucesso, tanto para visualizar ou criar uma nota segura, o app Notas abre uma sessão segura. Enquanto a sessão segura estiver aberta, o usuário pode visualizar ou proteger outras notas sem autenticação adicional. Contudo, a sessão segura aplica-se somente às notas protegidas com a senha fornecida. O usuário ainda precisa se autenticar no caso de notas protegidas por uma senha diferente. A sessão segura é fechada quando:

- O usuário toca no botão Bloquear Agora no app Notas
- O Notas é enviado para segundo plano por mais de 3 minutos (8 minutos no macOS)
- O dispositivo iOS ou iPadOS é bloqueado

Para alterar a senha de uma nota segura, o usuário deve digitar a senha atual, pois o Face ID e o Touch ID não estão disponíveis ao alterar a senha. Depois de escolher uma nova senha, o app Notas reembala, na mesma conta, as chaves de todas as notas existentes que estão criptografadas pela senha anterior.

Se o usuário digitar a senha incorretamente três vezes seguidas, o app Notas mostra uma dica fornecida pelo usuário, caso ela tenha sido fornecida pelo usuário na configuração. Se ainda assim não se lembrar da senha, o usuário pode redefini-la nos ajustes do app Notas. Esse recurso permite que os usuários criem novas notas seguras com uma nova senha, mas não permitirá que eles vejam notas seguras anteriores. As notas asseguradas anteriormente ainda poderão ser visualizadas se a senha antiga for lembrada. A redefinição da senha requer a frase-senha da conta do iCloud do usuário.

Notas compartilhadas

As notas que não estão criptografadas de ponta a ponta com uma senha podem ser compartilhadas com outras pessoas. As notas compartilhadas ainda usam o tipo de dado criptografado CloudKit para qualquer tipo de texto ou anexo colocado em uma nota pelo usuário. Os materiais sempre são criptografados com uma chave que é criptografada no CKRecord. Metadados, como as datas de criação e modificação, não são criptografados. O CloudKit gerencia o processo pelo qual os participantes podem criptografar e descriptografar os dados uns dos outros.

Recursos de segurança no app Atalhos

No app Atalhos, os atalhos são sincronizados opcionalmente com todos os dispositivos Apple que usam o iCloud. Atalhos também podem ser compartilhados com outros usuários por meio do iCloud. Os atalhos são armazenados localmente em um formato criptografado.

Os atalhos personalizados são versáteis – são similares a scripts ou programas. Ao baixar atalhos da internet, o usuário é avisado de que o atalho não foi revisado pela Apple e recebe a oportunidade de inspecioná-lo. Para proteger contra atalhos maliciosos, definições atualizadas de malware são baixadas para identificar atalhos maliciosos no tempo de execução.

Os atalhos personalizados também podem executar JavaScript especificado pelo usuário em sites no Safari quando chamados a partir da folha de compartilhamento. Para proteger contra códigos JavaScript maliciosos que, por exemplo, enganem o usuário para executar um script em um site de rede social que colete seus dados, o JavaScript é validado em relação às definições de malware mencionadas anteriormente. Na primeira vez que um usuário executa JavaScript em um domínio, o usuário é solicitado a permitir que atalhos contendo JavaScript sejam executados na página atual desse domínio.

Segurança de serviços

Visão geral da segurança dos serviços

A Apple criou um conjunto robusto de serviços para que os seus dispositivos sejam muito mais úteis para os usuários e os ajudem a ser mais produtivos. Esses serviços oferecem capacidades poderosas para armazenamento na nuvem, sincronização, armazenamento de senhas, autenticação, pagamento, mensagem, comunicações e muito mais, tudo isso enquanto protege a privacidade do usuário e a segurança de seus dados.

Este capítulo aborda tecnologias de segurança usadas no iCloud, Iniciar sessão com a Apple, Apple Pay, iMessage, Apple Messages for Business, FaceTime, Buscar e Continuidade.

Nota: nem todos os serviços e conteúdos da Apple estão disponíveis em todos os países ou regiões.

ID Apple e ID Apple Gerenciado

Visão geral da segurança do ID Apple

Um ID Apple é a conta usada para iniciar a sessão em serviços da Apple. É importante que os usuários mantenham seus IDs Apple em segurança para ajuda a impedir o acesso não autorizado às suas contas. Para ajudar com isso, os IDs Apple requerem senhas fortes que:

- Devem ter pelo menos oito caracteres
- Devem conter tanto letras quanto números
- Não devem conter três ou mais caracteres idênticos consecutivos
- Não podem ser senhas usadas com frequência

Os usuários são encorajados a exceder essas diretrizes através da adição de caracteres extras e sinais de pontuação para tornar suas senhas ainda mais fortes.

A Apple também notifica os usuários por e-mail ou notificações push (ou ambos) quando alterações importantes são feitas às suas contas; por exemplo, se uma senha ou informação de cobrança for alterada ou se o ID Apple for usado para iniciar a sessão em um novo dispositivo. Se algo estiver fora do esperado, os usuários são instruídos a alterar a senha do ID Apple imediatamente.

Além disso, a Apple emprega diversas políticas e procedimentos feitos para proteger as contas dos usuários. Isso inclui limitar o número de tentativas de início de sessão e redefinição de senha, o monitoramento ativo contra fraude para ajudar na identificação de ataques à medida que ocorrem e revisões regulares das políticas, o que permite à Apple adaptar-se a quaisquer informações novas que possam afetar a segurança do usuário.

Nota: a política de senha do ID Apple Gerenciado é definida por um administrador do Apple School Manager ou Apple Business Manager.

Autenticação de dois fatores

Para ajudar usuários a dar ainda mais segurança às suas contas, por padrão a Apple usa a *autenticação de dois fatores*, uma camada extra de segurança para IDs Apple. Ela foi desenvolvida para garantir que somente o proprietário da conta possa acessar a conta, mesmo que mais alguém saiba a senha. Com a autenticação de dois fatores, a conta do usuário pode ser acessada apenas em dispositivos autorizados, como o iPhone, iPad, iPod touch ou Mac do usuário, ou em outros dispositivos após uma verificação feita a partir de um desses dispositivos autorizados ou de um número de telefone autorizado. Para iniciar a sessão pela primeira vez em qualquer dispositivo novo, são necessárias duas informações: a senha do ID Apple e um código de verificação de seis dígitos que é exibido nos dispositivos autorizados do usuário ou enviado para um número de telefone autorizado. Ao digitar o código, o usuário confirma que autoriza o dispositivo novo e que é seguro iniciar a sessão. Como apenas uma senha não é mais suficiente para acessar a conta de um usuário, a autenticação de dois fatores melhora a segurança do ID Apple do usuário e de todas as informações pessoais que ele armazena junto à Apple. Ela é integrada diretamente ao iOS, iPadOS, macOS, tvOS, watchOS e aos sistemas de autenticação usados pelos sites da Apple.

Quando o usuário inicia uma sessão em um site da Apple com um navegador, uma solicitação de segundo fator é enviada a todos os dispositivos autorizados associados à conta do iCloud do usuário, solicitando a aprovação da sessão web. Se o usuário estiver iniciando a sessão no site da Apple a partir de um navegador em um dispositivo autorizado, ele vê o código de verificação exibido localmente no dispositivo sendo usado. Quando o usuário digita o código nesse dispositivo, a sessão web é aprovada.

Redefinição de senhas e recuperação de contas

Se a senha de uma conta do ID Apple for esquecida, um usuário pode redefini-la em um dispositivo autorizado. Se um dispositivo autorizado não estiver disponível e a senha for conhecida, o usuário pode usar um número de telefone autorizado para autenticar através da verificação por SMS. Além disso, para fornecer uma recuperação imediata para um ID Apple, um código usado anteriormente pode ser usado para a redefinição, em conjunto com o SMS. Se essas opções não forem possíveis, o processo de recuperação da conta deve ser seguido. Para obter mais informações, consulte o artigo do Suporte da Apple Como usar a recuperação de conta quando você não consegue redefinir a senha do ID Apple.

Segurança do ID Apple Gerenciado

Os IDs Apple Gerenciados funcionam de maneira bem semelhante a um ID Apple, mas são de propriedade e controle de empresas ou organizações de ensino. Essas organizações podem redefinir senhas, limitar compras e comunicações como FaceTime e Mensagens, além de configurar permissões por cargo para funcionários, professores e alunos.

Em IDs Apple Gerenciados, alguns serviços são desativados (por exemplo, Apple Pay, Chaves do iCloud, HomeKit e Buscar).

Inspeção de IDs Apple Gerenciados

Os IDs Apple Gerenciados também oferecem suporte à *inspeção*, o que permite que organizações atendam a regulamentações legais e de privacidade. Um administrador, gerente ou professor do Apple School Manager pode inspecionar contas específicas de ID Apple Gerenciado.

Os inspetores podem monitorar apenas as contas que estão abaixo deles na hierarquia da organização. Por exemplo, professores podem monitorar alunos, gerentes podem inspecionar professores e alunos, e administradores podem inspecionar gerentes, professores e alunos.

Quando credenciais de inspeção são solicitadas através do Apple School Manager, é gerada uma conta especial que dá acesso somente ao ID Apple Gerenciado para o qual a inspeção foi solicitada. Assim, o inspetor pode ler e modificar o conteúdo do usuário armazenado no iCloud ou em apps compatíveis com o CloudKit. Todas as solicitações de acesso de auditoria são registradas no Apple School Manager. Os registros mostram quem foi o inspetor, o ID Apple Gerenciado para o qual ele solicitou acesso, a hora da solicitação e se a inspeção foi realizada.

IDs Apple Gerenciados e dispositivos pessoais

Os IDs Apple Gerenciados também podem ser usados em dispositivos iOS e iPadOS e computadores Mac de propriedade individual. Para iniciar a sessão no iCloud, os alunos usam o ID Apple Gerenciado emitido pela instituição e uma senha adicional para uso doméstico que serve como o segundo fator do processo de autenticação de dois fatores do ID Apple. Enquanto um aluno estiver usando um ID Apple Gerenciado em um dispositivo pessoal, as Chaves do iCloud não ficam disponíveis e a instituição pode restringir outros recursos, como FaceTime ou Mensagens. Qualquer documento do iCloud criado por alunos enquanto tiverem uma sessão iniciada está sujeito à auditoria, conforme descrito anteriormente nesta seção.

iCloud

Visão geral da segurança do iCloud

O iCloud armazena contatos, calendários, fotos, documentos e outros itens de um usuário, mantendo as informações atualizadas em todos os dispositivos do usuário automaticamente. O iCloud também pode ser usado por apps de terceiros para armazenar e sincronizar documentos, assim como valores essenciais de dados de apps, conforme definido pelo desenvolvedor. Para configurar o iCloud, o usuário inicia a sessão com um ID Apple e escolhe quais serviços deseja usar. Certos recursos do iCloud, como o iCloud Drive e o Backup do iCloud podem ser desativados por administradores de TI com perfis de configuração de gerenciamento de dispositivos móveis (MDM).

O iCloud usa métodos de segurança fortes e aplica políticas rígidas para proteger os dados do usuário. A maioria dos dados do iCloud é criptografada primeiro no dispositivo do usuário, com chaves do iCloud geradas no dispositivo, antes de ser enviada aos servidores do iCloud. No caso de dados que não são criptografados de ponta a ponta, o dispositivo do usuário envia com segurança essas chaves do iCloud para os Módulos de Segurança de Hardware do iCloud nos centros de processamento de dados da Apple. Isso permite que a Apple ajude o usuário com a recuperação de dados e descriptografe os dados em nome do usuário sempre que isso for necessário (como ao iniciar a sessão em um novo dispositivo, restaurar usando um backup ou acessar dados do iCloud na web). Os dados sendo passados entre os dispositivos do usuário e os servidores do iCloud são criptografados separadamente enquanto em trânsito com TLS, e os servidores do iCloud armazenam os dados do usuário com uma camada adicional de criptografia enquanto em repouso.

As chaves de criptografia, quando disponibilizadas à Apple, são armazenadas em segurança nos centros de processamento de dados da Apple. Ao processar dados armazenados em um centro de processamento de dados de terceiros, essas chaves criptográficas são acessadas apenas pelo software da Apple em execução em servidores seguros e apenas durante a condução do processamento necessário. Para ter privacidade e segurança adicionais, muitos serviços da Apple usam criptografia de ponta a ponta, o que significa que apenas o usuário pode acessar seus respectivos dados do iCloud e somente em dispositivos de confiança nos quais tenha uma sessão iniciada com seu ID Apple.

A Apple oferece aos usuários duas opções para criptografar e proteger os dados armazenados no iCloud:

- **Proteção de dados padrão (o ajuste padrão):** os dados do iCloud do usuário são criptografados, as chaves de criptografia são armazenadas em segurança nos centros de processamento de dados da Apple, e a Apple pode ajudar na recuperação de dados e da conta. Apenas certos dados do iCloud (14 categorias de dados, incluindo os dados de Saúde e as senhas nas Chaves do iCloud) são criptografados.
- **Proteção Avançada de Dados do iCloud:** um ajuste opcional que oferece o nível mais alto da Apple na segurança de dados na nuvem. Se um usuário opta por ativar a Proteção Avançada de Dados, seus dispositivos de confiança mantêm o acesso exclusivo às chaves de criptografia para a maioria dos dados do iCloud, o que os protege com a criptografia de ponta a ponta. Quando a Proteção Avançada de Dados é ativada, o número de categorias de dados que usam criptografia de ponta a ponta aumenta para 23 e inclui o Backup do iCloud, Fotos, Notas e outros.

As categorias específicas de dados do iCloud protegidos com criptografia de ponta a ponta são relacionadas no artigo do Suporte da Apple Visão geral da segurança de dados do iCloud.

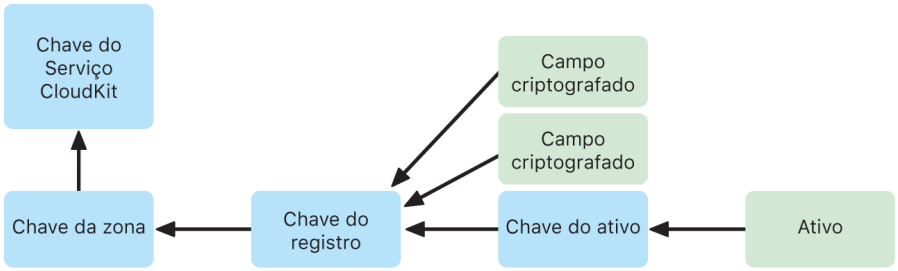
Criptografia do iCloud

A criptografia de dados no iCloud está intimamente associada ao modelo de armazenamento de dados, a começar pelos frameworks e APIs do CloudKit que permitem que os apps e o software do sistema armazenem dados no iCloud em nome do usuário e mantenham tudo atualizado nos dispositivos e na web.

Criptografia do CloudKit

O CloudKit é um framework que permite que desenvolvedores de apps armazenem dados de valores de chaves, dados estruturados e materiais (dados grandes armazenados separadamente do banco de dados, como imagens ou vídeos) no iCloud. O CloudKit é compatível com bancos de dados públicos e privados, agrupados em contêineres. Os bancos de dados públicos são compartilhados globalmente (normalmente usados para materiais genéricos) e não são criptografados. Os bancos de dados privados armazenam os dados do iCloud de cada usuário.

O CloudKit usa uma hierarquia de chaves que coincide com a estrutura dos dados. O banco de dados privado de cada contêiner é protegido por uma hierarquia de chaves que tem raízes em uma chave assimétrica chamada de *chave de Serviço do CloudKit*. Essas chaves são exclusivas para cada usuário do iCloud e são geradas no dispositivo de confiança do usuário. Quando os dados são gravados no CloudKit, todas as chaves de registro são geradas no dispositivo de confiança do usuário e embaladas na hierarquia de chaves apropriada antes que qualquer dado seja enviado.



Muitos serviços da Apple, relacionados no artigo do Suporte da Apple Visão geral da segurança de dados do iCloud, usam criptografia de ponta a ponta com uma chave de serviço do CloudKit protegida pela sincronização das Chaves do iCloud. Nesses contêineres do CloudKit, as chaves de serviço são armazenadas nas Chaves do iCloud do usuário e compartilham as características de segurança das Chaves do iCloud; as chaves de serviço só estão disponíveis nos dispositivos de confiança do usuário e não podem ser acessadas pela Apple nem por nenhum terceiro. No caso da perda de um dispositivo, o usuário pode recuperar os dados das Chaves do iCloud via Recuperação segura das Chaves do iCloud, Contatos para Recuperação de Conta ou uma Chave de Recuperação da Conta.

Gerenciamento de chaves de criptografia

A segurança dos dados criptografados no CloudKit dependem da segurança das chaves de criptografia correspondentes. As chaves de serviço do CloudKit são divididas em duas categorias: criptografadas de ponta a ponta e disponíveis depois da autenticação.

- **Chaves de serviço criptografadas de ponta a ponta:** nos serviços do iCloud criptografados de ponta a ponta, as chaves privadas relevantes ao serviço do CloudKit nunca são disponibilizadas aos servidores da Apple. Pares de chaves de serviço, incluindo as chaves privadas, são criadas localmente em um dispositivo de confiança do usuário e transferidas para os outros dispositivos do usuário com a segurança das Chaves do iCloud. Embora os fluxos de recuperação e sincronização das Chaves do iCloud sejam mediados pelos servidores da Apple, esses servidores são criptograficamente impedidos de acessar qualquer dado das chaves do usuário. No pior cenário de perda de acesso às Chaves do iCloud e todos os seus mecanismos de recuperação, os dados criptografados de ponta a ponta no CloudKit são perdidos. A Apple não pode ajudar a recuperar esses dados.
- **Chaves de serviço disponíveis depois da autenticação:** nos outros serviços, como Fotos e iCloud Drive, as chaves de serviço são armazenadas nos Módulos de Segurança de Hardware do iCloud nos centros de processamento de dados da Apple e podem ser acessadas por alguns serviços da Apple. Quando um usuário inicia a sessão no iCloud em um novo dispositivo e autentica o ID Apple, essas chaves podem ser acessadas pelos servidores da Apple sem nenhuma interação ou entrada adicional do usuário. Por exemplo, depois de iniciar a sessão em iCloud.com, o usuário pode visualizar imediatamente suas fotos online. Essas chaves de serviço são chaves *disponíveis depois da autenticação*.

Proteção Avançada de Dados do iCloud

A Proteção Avançada de Dados do iCloud é um ajuste opcional que oferece o nível de segurança de dados na nuvem mais alto da Apple. Quando o usuário ativa a Proteção Avançada de Dados, os dispositivos de confiança mantêm o acesso exclusivo às chaves de criptografia da maioria dos dados do iCloud, o que os protege com a *criptografia de ponta a ponta*. No caso de usuários que ativam a Proteção Avançada de Dados, o número de categorias de dados protegidas pela criptografia de ponta a ponta aumenta de 14 para 23 e inclui o Backup do iCloud, Fotos, Notas e outras.

A Proteção Avançada de Dados do iCloud estará disponível para usuários dos EUA no final de 2022 e começará a ser lançada no restante do mundo no início de 2023.

Conceitualmente, a Proteção Avançada de Dados é simples: todas as chaves de serviço do CloudKit que foram geradas no dispositivo e posteriormente enviadas aos Módulos de Segurança de Hardware do iCloud (HSMs) *disponíveis depois da autenticação* nos centros de processamento de dados da Apple são apagadas desses HSMs e mantidas integralmente dentro do domínio de proteção das Chaves do iCloud da conta. Elas são gerenciadas como as chaves de serviço *criptografadas de ponta a ponta* existentes, o que significa que a Apple não pode mais ler nem acessar essas chaves.

A Proteção Avançada de Dados também protege automaticamente os campos do CloudKit que outros desenvolvedores optam por marcar como criptografados e todos os materiais do CloudKit.

Ativação da Proteção Avançada de Dados

Quando o usuário ativa a Proteção Avançada de Dados, seu respectivo dispositivo de confiança realiza duas ações: primeiro, ele comunica a intenção do usuário de ativar a Proteção Avançada de Dados aos outros dispositivos que participam da criptografia de ponta a ponta. Para fazer isso, ele grava um novo valor, assinado por chaves locais no dispositivo, em seus metadados de dispositivo nas Chaves do iCloud. Os servidores da Apple não podem remover nem modificar esse atestado enquanto ele é sincronizado com os outros dispositivos do usuário.

O dispositivo incia então a remoção das chaves de serviço *disponíveis depois da autenticação* dos centros de processamento de dados da Apple. Como essas chaves são protegidas pelos HSMs do iCloud, esse apagamento é imediato, permanente e irrevogável. Depois que as chaves são apagadas, a Apple não pode mais acessar *nenhum* dos dados protegidos pelas chaves de serviço do usuário. Nesse estágio, o dispositivo inicia uma operação de rotação de chave assíncrona, que cria uma nova chave de serviço para cada serviço cuja chave estivera disponível anteriormente aos servidores da Apple. Se a rotação da chave falhar (devido a uma interrupção na rede ou qualquer outro erro), o dispositivo tentará realizar novamente a rotação da chave até que ela seja bem-sucedida.

Depois que a rotação da chave de serviço for bem-sucedida, qualquer novo dado gravado no serviço não poderá ser descriptografado com a chave de serviço antiga. Ele será protegido pela nova chave, controlada exclusivamente pelos dispositivos de confiança do usuário, e nunca disponibilizada à Apple.

Proteção Avançada de Dados e acesso via web a iCloud.com

Quando um usuário ativa a Proteção Avançada de Dados pela primeira vez, o acesso via web aos dados em iCloud.com é desativado automaticamente. Isso se dá porque os servidores web do iCloud não têm mais acesso às chaves necessárias para descriptografar e mostrar os dados do usuário. O usuário pode optar por reativar o acesso via web e usar a participação do dispositivo de confiança para acessar os dados do iCloud criptografados na web.

Depois de ativar o acesso via web, o usuário deve autorizar o início de sessão na web em um de seus dispositivos de confiança sempre que acessar iCloud.com. A autorização “arma” o dispositivo para o acesso via web. Durante a próxima hora, o dispositivo aceitará pedidos de servidores específicos da Apple para enviar chaves de serviço individuais, mas somente daqueles que estiverem em uma lista de serviços permitidos normalmente acessíveis em iCloud.com. Em outras palavras, mesmo depois que o usuário autorizar um início de sessão na web, um pedido ao servidor será incapaz de induzir o dispositivo do usuário a enviar chaves de serviço para dados que não se destinam à visualização em iCloud.com (como dados de Saúde ou senhas nas Chaves do iCloud). Os servidores da Apple solicitam apenas as chaves de serviço necessárias para descriptografar os dados específicos solicitados pelo usuário para acesso na web. Sempre que uma chave de serviço é enviada, ela é criptografada com uma chave efêmera destinada à sessão web autorizada pelo usuário e uma notificação é exibida no dispositivo do usuário, mostrando o serviço do iCloud cujos dados estão sendo temporariamente disponibilizados aos servidores da Apple.

Preservação das escolhas do usuário

Os ajustes da Proteção Avançada de Dados e do acesso via web a iCloud.com podem ser modificados apenas pelo usuário. Esses valores são armazenados nos metadados do dispositivo das Chaves do iCloud do usuário e só podem ser alterados em um dos dispositivos de confiança do usuário. Os servidores da Apple não podem modificar esses ajustes em nome do usuário nem revertê-los a uma configuração anterior.

Implicações de segurança do compartilhamento e colaboração

Na maioria dos casos, quando usuários compartilham conteúdo para colaborar entre si (como Notas compartilhadas, Lembretes compartilhados, pastas compartilhadas no iCloud Drive ou uma Fototeca Compartilhada do iCloud, por exemplo) e todos os participantes têm a Proteção Avançada de Dados ativada, os servidores da Apple são usados apenas para estabelecer o compartilhamento e não têm acesso às chaves de criptografia dos dados compartilhados. O conteúdo permanece criptografado de ponta a ponta e acessível somente nos dispositivos de confiança dos participantes. Em cada operação de compartilhamento, um título e uma miniatura representativa podem ser armazenados pela Apple com a proteção de dados padrão, visando mostrar uma prévia para os destinatários.

A seleção da opção "qualquer pessoa com o link" ao ativar a colaboração faz com que o conteúdo seja disponibilizado aos servidores da Apple com a proteção de dados padrão, já que os servidores precisam fornecer acesso a qualquer pessoa que venha a abrir o URL.

A colaboração no iWork e o recurso de Álbuns Compartilhados no app Fotos não são compatíveis com a Proteção Avançada de Dados. Quando usuários colaboram em um documento do iWork ou abrem um documento do iWork de uma pasta compartilhada no iCloud Drive, as chaves de criptografia do documento são enviadas com segurança aos servidores do iWork nos centros de processamento de dados da Apple. Isso se dá porque a colaboração em tempo real no iWork requer mediação por parte do servidor para coordenar as alterações feitas pelos participantes no documento. As fotos adicionadas a Álbuns Compartilhados são armazenadas com a proteção de dados padrão, já que esse recurso permite que os álbuns sejam compartilhados publicamente na web.

Desativação da Proteção Avançada de Dados

O usuário pode desativar a Proteção Avançada de Dados a qualquer momento. Caso decida fazer isso:

1. O dispositivo do usuário registra essa nova escolha nos metadados de participação nas Chaves do iCloud e a sincroniza com segurança em todos os dispositivos.

2. O dispositivo do usuário envia com segurança as chaves de serviço de todos os serviços *disponíveis depois da autenticação* aos HSMs do iCloud nos centros de processamento de dados da Apple. Isso nunca inclui as chaves dos serviços criptografados de ponta a ponta sob a proteção de dados padrão, como as Chaves do iCloud e os dados de Saúde.

O dispositivo envia tanto as chaves de serviço originais (geradas antes da desativação da Proteção Avançada de Dados) quanto as novas chaves de serviço geradas depois que o usuário ativa esse recurso. Isso faz com que todos os dados nesses serviços possam ser acessados depois da autenticação e retorna a conta à proteção de dados padrão, em que a Apple pode novamente ajudar o usuário a recuperar a maior parte dos dados no caso de perda de acesso à conta.

Dados do iCloud não cobertos pela Proteção Avançada de Dados

Dada a necessidade de interoperabilidade dos sistemas de e-mail, contatos e calendário, o Mail do iCloud e os apps Contatos e Calendário não são criptografados de ponta a ponta.

O iCloud armazena alguns dados sem a proteção de chaves de serviço do CloudKit específicas do usuário, mesmo quando a Proteção Avançada de Dados está ativada. Os campos de Registro do CloudKit devem ser explicitamente declarados como "criptografados" no esquema do contêiner para que sejam protegidos, e a leitura e gravação de campos criptografados requerem o uso de APIs dedicadas. A data e a hora em que um arquivo ou objeto foi modificado são usadas para ordenar as informações de um usuário, enquanto as somas de verificação dos dados de arquivos ou fotos são usadas para ajudar a Apple a remover duplicatas e otimizar o armazenamento do iCloud e do dispositivo do usuário; tudo sem precisar acessar os arquivos e as fotos em si. Os detalhes sobre como a criptografia é usada para categorias específicas de dados estão disponíveis no artigo do Suporte da Apple Visão geral da segurança de dados do iCloud.

Decisões, como o uso de somas de verificação para a remoção de duplicatas (uma técnica bem estabelecida, chamada *criptografia convergente*) fizeram parte do projeto original dos serviços do iCloud quando esses foram lançados. Esses metadados sempre são criptografados, mas as chaves de criptografia são armazenadas pela Apple com a proteção de dados padrão. Para continuar reforçando as proteções de segurança para todos os usuários, a Apple está comprometida a garantir que mais dados, incluindo esses tipos de metadados, sejam criptografados de ponta a ponta quando a Proteção Avançada de Dados for ativada.

Requisitos da Proteção Avançada de Dados

Os requisitos para ativar a Proteção Avançada de Dados do iCloud incluem os seguintes:

- A conta do usuário precisa ser compatível com a criptografia de ponta a ponta. A criptografia de ponta a ponta requer a autenticação de dois fatores no ID Apple e um código ou senha definido nos dispositivos de confiança do usuário. Para obter mais informações, consulte o artigo do Suporte da Apple Autenticação de dois fatores do ID Apple.
- Os dispositivos em que o usuário tem uma sessão iniciada com o ID Apple devem estar atualizados com o iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 e a versão mais recente do iCloud para Windows. Esse requisito impede que uma versão anterior do iOS, iPadOS, macOS, tvOS ou watchOS lide incorretamente com as recém-criadas chaves de serviço ao reenviá-las aos HSMs *disponíveis depois da autenticação* em uma tentativa equivocada de reparar o estado da conta.
- O usuário precisa configurar ao menos um método de recuperação alternativo (um ou mais contatos de recuperação ou uma chave de recuperação) que possa ser usado para recuperar os dados do iCloud no caso de perda de acesso à conta.

Se o método de recuperação falhar (se as informações do contato de recuperação estiverem desatualizadas ou o usuário as esquecer), a Apple não poderá ajudar a recuperar os dados do iCloud criptografados de ponta a ponta.

A Proteção Avançada de Dados do iCloud pode ser ativada somente para IDs Apple. IDs Apple Gerenciados e contas de crianças (variam de acordo com o país ou região) não são compatíveis.

Segurança do Backup do iCloud

O iCloud faz o backup de informações (incluindo informações do dispositivo, dados de apps, fotos e vídeos no Rolo da Câmera, e conversas no app Mensagens) diariamente via Wi-Fi. O Backup do iCloud ocorre apenas quando o dispositivo está bloqueado, conectado a uma fonte de alimentação e com acesso à internet via Wi-Fi. Considerando a criptografia de armazenamento usada no iOS e iPadOS, o Backup do iCloud é projetado para manter os dados seguros e, ao mesmo tempo, permitir que backups incrementais não supervisionados e restaurações ocorram. Por padrão, o backup da chave de serviço do Backup do iCloud é feito com segurança nos Módulos de Segurança de Hardware do iCloud nos centros de processamento de dados da Apple e faz parte da categoria de dados disponíveis depois da autenticação. No caso de usuários que ativam a Proteção Avançada de Dados do iCloud, a chave de serviço do Backup do iCloud é protegida com criptografia de ponta a ponta e disponibilizada apenas nos dispositivos de confiança dos usuários.

Quando arquivos são criados em classes de Proteção de Dados que não estão acessíveis quando o dispositivo está bloqueado, suas chaves únicas por arquivo são criptografadas pelas chaves de classe da keybag do Backup do iCloud, o que cria um backup dos arquivos no iCloud em seus estados originais criptografados. Todos os arquivos são criptografados durante o transporte e, quando armazenados, criptografados com chaves baseadas em conta, conforme descrito em Criptografia do CloudKit.

A keybag do Backup do iCloud contém chaves assimétricas (Curve25519) para as classes de Proteção de Dados que não estão acessíveis quando o dispositivo está bloqueado. O conjunto de backups é armazenado na conta do iCloud do usuário e consiste em uma cópia dos arquivos do usuário e a keybag do Backup do iCloud. A keybag do Backup do iCloud é protegida por uma chave aleatória, também armazenada no conjunto de backups. Como a senha do iCloud do usuário não é usada para criptografia, a alteração da senha do iCloud não invalida os backups existentes.

Ao restaurar, os arquivos que têm um backup, a keybag do Backup do iCloud e a chave da keybag são obtidos da conta do iCloud do usuário. A keybag do Backup do iCloud é descriptografada com sua própria chave. Em seguida, as chaves únicas por arquivo na keybag são usadas para descriptografar os arquivos no conjunto de backups, que são gravados no sistema de arquivos como novos arquivos, sendo criptografados novamente de acordo com suas classes de Proteção de Dados.

O Backup do iCloud faz o backup do conteúdo a seguir:

- Registros de músicas, filmes, programas de TV, apps e livros comprados. O Backup do iCloud de um usuário inclui informações sobre o conteúdo comprado presente no dispositivo, mas não o conteúdo comprado em si. Ao restaurar usando um Backup do iCloud, o conteúdo comprado do usuário é baixado automaticamente da iTunes Store, App Store, app Apple TV ou Apple Books. Alguns tipos de conteúdo não são baixados automaticamente em todos os países ou regiões, e as compras anteriores podem estar indisponíveis caso tenham sido ressarcidas ou não estejam mais disponíveis nas respectivas lojas. O histórico de compras completo é associado ao ID Apple do usuário.
- Fotos e vídeos nos dispositivos do usuário. Observe que, se o usuário ativar as Fotos do iCloud no iOS 8.1, iPadOS 13.1 ou OS X 10.10.3 ou posteriores, as fotos e vídeos já estarão armazenados no iCloud e não serão incluídos no Backup do iCloud do usuário.
- Contatos, eventos do calendário, lembretes e notas

- Ajustes do dispositivo
- Dados de apps
- Tela de Início e organização dos apps
- Configuração do HomeKit
- Dados da Ficha Médica
- Senha das Gravações (se necessário; requer o cartão SIM físico usado durante o backup)
- Mensagens, Apple Messages for Business, mensagens de texto (SMS) e MMS (se necessário; requer o cartão SIM físico usado durante o backup)

O Backup do iCloud também é usado para fazer o backup das chaves do dispositivo local, criptografado com uma chave derivada da chave criptográfica de raiz do UID do Secure Enclave do dispositivo. Essa chave é exclusiva do dispositivo e não é de conhecimento da Apple. Isso permite que o banco de dados seja restaurado apenas no mesmo dispositivo de onde tenha sido originado e significa que ninguém, nem mesmo a Apple, pode lê-lo. Para obter mais informações, consulte Secure Enclave.

Mensagens no iCloud

As Mensagens no iCloud mantêm o histórico completo de mensagens do usuário atualizado e disponível em todos os dispositivos.

Com a proteção de dados padrão, as Mensagens no iCloud são criptografadas de ponta a ponta quando o Backup do iCloud está desativado. Quando o Backup do iCloud está ativado, o backup inclui uma cópia da chave de criptografia das Mensagens no iCloud para que a Apple possa ajudar o usuário a recuperar mensagens mesmo que ele perca acesso às Chaves do iCloud e seus dispositivos de confiança. Se o usuário desativa o Backup do iCloud, uma nova chave é gerada no dispositivo para proteger futuras Mensagens no iCloud. A chave nova é armazenada apenas nas Chaves do iCloud, disponíveis apenas para o usuário nos dispositivos de confiança. Os novos dados gravados no contêiner não podem ser descriptografados com a chave do contêiner antigo.

Com a Proteção Avançada de Dados, as Mensagens no iCloud sempre são criptografadas de ponta a ponta. Quando o Backup do iCloud está ativado, todo seu conteúdo é criptografado de ponta a ponta, incluindo a chave de criptografia das Mensagens no iCloud. A chave de serviço do Backup do iCloud, assim como a chave do contêiner das Mensagens no iCloud, são adiantadas quando o usuário ativa a Proteção Avançada de Dados. Para obter mais informações, consulte o artigo do Suporte da Apple Visão geral da segurança de dados do iCloud.

Segurança de contatos de recuperação de conta

Usuários podem adicionar até cinco pessoas em quem confiam como contatos para recuperação de conta para ajudar na recuperação da conta e dados do iCloud, incluindo todos os dados criptografados de ponta a ponta, independentemente de essas pessoas terem ou não ativado a Proteção Avançada de Dados. Nem a Apple nem o contato de recuperação têm as informações necessárias para recuperar os dados do iCloud criptografados de ponta a ponta do usuário.

O Contato de Recuperação é projetado com base na privacidade do usuário. Os contatos de recuperação de um usuário não são de conhecimento da Apple. Os servidores da Apple só tomam conhecimento das informações sobre um contato de recuperação no final do processo de uma tentativa de recuperação, depois que o usuário pede ajuda ao contato e o contato começa realmente a ajudar na recuperação. Essas informações não são retidas depois que a recuperação é concluída.

Processo de segurança do contato de recuperação

Quando um usuário configura um Contato para Recuperação de Conta, a chave para acessar os dados do usuário no iCloud (incluindo os dados do CloudKit criptografados de ponta a ponta) é criptografada com uma chave aleatória forte. Essa chave aleatória é dividida entre o contato de recuperação e a Apple. No momento da recuperação, apenas quando as duas partes das chaves são recombinadas, é que a chave original pode ser recuperada e os dados do iCloud do usuário acessados.

Para configurar um Contato para Recuperação de Conta, o dispositivo do usuário se comunica com os servidores da Apple para enviar a parte das informações de chaveamento que a Apple reterá. Depois, ele estabelece um contêiner do CloudKit criptografado de ponta a ponta com o contato de recuperação para compartilhar a parte que o contato de recuperação precisa. A Apple e o contato de recuperação também recebem o mesmo segredo de autorização do usuário, necessário mais tarde para a recuperação. A comunicação para convidar e aceitar contatos de recuperação ocorre por um canal IDS com autenticação mútua. O contato de recuperação armazena automaticamente as informações recebidas nas suas respectivas Chaves do iCloud. A Apple não pode acessar o conteúdo do contêiner do CloudKit nem as Chaves do iCloud que armazenam essas informações. Quando o compartilhamento é realizado, os servidores da Apple veem apenas um ID anônimo do contato de recuperação.

Posteriormente, quando um usuário precisa recuperar sua conta e dados do iCloud, ele pode pedir ajuda ao contato de recuperação. Nesse momento, um código de recuperação é gerado pelo dispositivo do contato de recuperação, que fornece o código ao usuário fora da banda (pessoalmente ou por telefone, por exemplo). O usuário digita o código de recuperação em seu dispositivo para estabelecer uma conexão segura entre os dispositivos com o protocolo SPAKE2+, cujo conteúdo não pode ser acessado pela Apple. Essa interação é orquestrada pelos servidores da Apple, mas a Apple não pode iniciar o processo de recuperação.

Depois de estabelecer a conexão segura e realizar todas as verificações de segurança necessárias, o dispositivo do contato de recuperação devolve a sua parte das informações de chaveamento para o usuário que está solicitando a recuperação, assim como o segredo de autorização previamente estabelecido. O usuário apresenta esse segredo de autorização a um servidor da Apple, que concede acesso às informações de chaveamento que a Apple guarda. O fornecimento do segredo de autorização também autoriza a redefinição da senha da conta para restaurar o acesso à conta.

Por fim, o dispositivo do usuário recombina as informações de chaveamento recebidas da Apple e do Contato para Recuperação de Conta, e as usa para descriptografar e recuperar seus dados do iCloud.

Existem medidas de segurança efetivas para impedir que um contato de recuperação inicie uma recuperação sem o consentimento do usuário, que incluem uma verificação de atividade na conta do usuário. Se a conta está em uso ativo, a recuperação com um Contato de Recuperação também exige o conhecimento de um código de dispositivo recente ou o Código de Segurança do iCloud.

Segurança de Contatos de Legado

Se um usuário deseja que seus dados do iCloud possam ser acessados por beneficiários designados após seu falecimento, ele pode configurar os Contatos de Legado na sua conta. Um Contato de Legado beneficiário ganha acesso a todos os dados do iCloud do falecido, incluindo quase todos os dados criptografados de ponta a ponta, mas excluindo os dados das Chaves do iCloud, como as senhas de contas. A tecnologia subjacente ao Contato de Legado funciona de forma similar ao Contato de Recuperação: uma chave aleatória forte que é dividida entre a Apple e o contato de legado, de forma que nenhum dos dois possa descriptografar nenhum dado individualmente. O beneficiário recebe as mesmas classes de dados, independentemente do usuário ter ou não ativado a Proteção Avançada de Dados.

As informações de chaveamento que o beneficiário recebe são chamadas de chave de acesso na documentação fornecida a usuários e são salvas automaticamente nos dispositivos compatíveis, mas também podem ser impressas e armazenadas off-line para uso. Para obter mais informações, consulte o artigo do Suporte da Apple Como adicionar um Contato de Legado ao ID Apple.

Após o falecimento do usuário, os Contatos de Legado iniciam uma sessão no site de reivindicação da Apple para iniciar o acesso. Isso requer uma certidão de óbito e é autorizado em parte com o segredo de autorização mencionado na seção anterior. Depois de realizar todas as verificações de segurança, a Apple emite um nome de usuário e uma senha para a nova conta e libera as informações de chaveamento necessárias para o Contato de Legado.

Para facilitar a inserção da chave de acesso quando necessário, ela é apresentada como um código alfanumérico com um código QR associado. Depois de inseri-la, o acesso aos dados do iCloud da pessoa falecida é restaurado. Isso pode ser feito em um dispositivo ou o acesso pode ser estabelecido on-line. Para obter mais informações, consulte o artigo do Suporte da Apple Solicitar acesso a uma conta da Apple como contato herdeiro.

Segurança da Retransmissão Privada do iCloud

A Retransmissão Privada do iCloud ajuda a proteger usuários principalmente ao navegar na web com o Safari, mas também inclui todos os pedidos de resolução de nomes do DNS. Isso ajuda a garantir que nenhuma entidade, nem mesmo a Apple, possa correlacionar o endereço IP do usuário à atividade de navegação. Isso é feito por meio do uso de dois servidores proxy diferentes: um proxy de entrada, gerenciado pela Apple, e um proxy de saída, gerenciado por um provedor de conteúdo. Para usar a Retransmissão Privada do iCloud, o usuário deve ter o iOS 15, iPadOS 15 ou macOS 12.0.1 ou posteriores e ter uma sessão iniciada na conta do iCloud+ com seu respectivo ID Apple. Dado isso, a Retransmissão Privada do iCloud poderá ser ativada em Ajustes > iCloud ou Preferências do Sistema > iCloud.

Para obter mais informações, consulte iCloud Private Relay Overview (em inglês).

Gerenciamento de código e senha

Visão geral da segurança de senha

O iOS, iPadOS e macOS facilitam que usuários autentiquem em apps de terceiros e sites que usam senhas. A melhor maneira de gerenciar senhas é não ter que usar uma senha. O recurso Iniciar sessão com a Apple permite que os usuários iniciem uma sessão em apps e sites de terceiros sem precisar criar e gerenciar outra conta ou senha ao mesmo tempo que protege o início de sessão com a autenticação de dois fatores do ID Apple do usuário. No caso de sites que não são compatíveis com o recurso Iniciar sessão com a Apple, o recurso de Senha Automática Forte permite que os dispositivos do usuário criem, sincronizem e insiram, de forma automática, senhas fortes e exclusivas em sites e apps. No iOS e iPadOS, as senhas são salvas em chaves de Preenchimento Automático de Senha especiais que o usuário pode controlar e gerenciar em Ajustes > Senhas.

No macOS, as senhas salvas podem ser gerenciadas nas preferências de Senhas do Safari. Esse sistema de sincronização também pode ser usado para sincronizar senhas criadas manualmente pelo usuário.

Segurança do recurso Iniciar sessão com a Apple

O recurso Iniciar sessão com a Apple é uma alternativa que oferece privacidade fácil quando comparado a outros sistemas de início de sessão único. Ele fornece a conveniência e eficiência do início de sessão com um toque ao mesmo tempo que oferece ao usuário mais transparência e controle sobre suas informações pessoais.

O recurso Iniciar sessão com a Apple permite que os usuários configurem uma conta e iniciem a sessão em apps e sites com o ID Apple que já possuem, oferecendo aos usuários mais controle sobre suas informações pessoais. Apps podem solicitar apenas o nome e endereço de e-mail do usuário ao configurar uma conta, e o usuário sempre pode escolher: ele pode compartilhar seu endereço de e-mail pessoal com um app ou manter seu e-mail pessoal privado e usar o novo serviço de retransmissão de e-mail privado da Apple. Esse serviço de retransmissão de e-mail compartilha um endereço de e-mail anônimo e exclusivo com encaminhamento para o endereço pessoal do usuário, de forma que ele ainda possa receber comunicações úteis do desenvolvedor sem deixar de manter um grau de privacidade e controle das suas informações pessoais.

O recurso Iniciar sessão com a Apple é projetado para ser seguro. Cada usuário do recurso Iniciar sessão com a Apple é obrigado a ter a autenticação de dois fatores ativada em seu respectivo ID Apple. A autenticação de dois fatores ajuda a proteger não apenas o ID Apple do usuário, mas também as contas estabelecidas com os apps. Além disso, a Apple desenvolveu e integrou um sinal antifraude que respeita a privacidade ao recurso Iniciar sessão com a Apple. Esse sinal dá confiança a desenvolvedores de que os novos usuários adquiridos sejam pessoas de verdade, e não bots ou contas criadas a partir de scripts.

Senhas automáticas fortes

Quando as Chaves do iCloud estão ativadas, o iOS, iPadOS e macOS criam senhas fortes, aleatórias e exclusivas quando o usuário se inscreve ou altera a senha em um site no Safari. No iOS e iPadOS, a geração de senhas automáticas fortes também está disponível em apps. Para não usar senhas fortes, os usuários devem desativá-las. As senhas geradas são salvas nas chaves e mantidas atualizadas em dispositivos com as Chaves do iCloud, quando essas estão ativadas.

Por padrão, as senhas geradas pelo iOS e iPadOS têm 20 caracteres. Elas contêm um dígito, um caractere maiúsculo, dois hifens e 16 caracteres minúsculos. Tais senhas geradas são fortes, com 71 bits de entropia.

As senhas são geradas com base em uma heurística que determina se uma experiência no campo de senha destina-se à criação de senhas. Se a heurística não conseguir reconhecer uma senha de contexto específico sendo usada ao criar uma senha, os desenvolvedores de apps podem definir `UITextContentType.newPassword` no campo de texto e os desenvolvedores da web podem definir `autocomplete= "new-password"` nos elementos <input>.

Para ajudar a garantir que as senhas geradas sejam compatíveis com o serviço relevante, apps e sites podem fornecer regras. Os desenvolvedores fornecem essas regras ao usar `UITextInputPasswordRules` ou o atributo `passwordrules` em elementos de entrada. Depois, os dispositivos geram a senha mais forte possível que satisfaça essas regras.

Segurança do Preenchimento Automático de Senha

O Preenchimento Automático de Senha preenche automaticamente credenciais armazenadas nas chaves. O gerenciador de senhas das Chaves do iCloud e Preenchimento Automático de Senhas oferecem os recursos seguintes:

- Preenchimento de credenciais em apps e sites;
- Geração de senhas fortes;
- Salvamento de senhas tanto em apps quanto em sites no Safari;
- Compartilhamento seguro de senhas para os contatos de um usuário;
- Fornecimento de senhas a uma Apple TV próxima que solicite credenciais.

As ações de gerar e salvar senhas em apps, além de fornecer senhas à Apple TV, estão disponíveis apenas no iOS e iPadOS.

Preenchimento Automático de Senha em apps

O iOS e iPadOS permitem que os usuários insiram nomes de usuário e senhas salvas em campos relacionados a credenciais em apps, de forma semelhante ao Preenchimento Automático de Senha do Safari. No iOS e iPadOS, os usuários devem tocar em um elemento de chave na barra QuickType do teclado de software. No macOS, os apps compilados com Mac Catalyst exibem um menu expansível de Senhas abaixo de campos relacionados a credenciais.

Quando há uma forte associação entre um app e um site que usam o mesmo mecanismo de associação de apps e sites disponibilizada pelo arquivo apple-app-site-association, a barra QuickType do iOS e iPadOS, e o menu expansível do macOS sugerem credenciais diretamente ao app, caso haja uma salva nas Chaves de Preenchimento Automático de Senha. Isso permite que os usuários optem por revelar credenciais salvas pelo Safari a apps com as mesmas propriedades de segurança, sem que esses apps tenham que adotar uma API.

O Preenchimento Automático de Senha não expõe nenhuma informação de credenciais a um app até que o usuário consinta em liberar uma credencial para o app. As listas de credenciais são extraídas ou apresentadas fora do processo do app.

Quando um app e um site têm um relacionamento de confiança e um usuário envia credenciais dentro de um app, talvez o iOS e iPadOS perguntem ao usuário se deseja salvar tais credenciais nas chaves de Preenchimento Automático de Senha para uso futuro.

Acesso de apps a senhas salvas

Apps para iOS, iPadOS e macOS podem pedir ajuda às chaves de Preenchimento Automático de Senha para iniciar a sessão de um usuário através do uso de `ASAuthorizationPasswordProvider` e `SecAddSharedWebCredential`. O fornecedor da senha e sua solicitação podem ser usados em conjunto com o recurso Iniciar sessão com a Apple, de forma que a mesma API seja chamada para ajudar usuários a iniciar a sessão em um app, independentemente de a conta do usuário usar uma senha ou ter sido criada com o recurso Iniciar sessão com a Apple.

Apps podem acessar as senhas salvas somente se o desenvolvedor do app e o administrador do site concederem aprovação e o usuário autorizar. Para expressar a intenção de acessar as senhas salvas do Safari, os desenvolvedores de apps incluem um direito no app. A lista de direitos contém os nomes de domínio de sites associados, e os sites devem colocar um arquivo em seu servidor listando os identificadores exclusivos de app referentes aos apps aprovados pela Apple.

Quando um app com o direito com.apple.developer.associated-domains está instalado, o iOS e iPadOS fazem uma solicitação TLS para cada site listado, pedindo um destes arquivos:

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

Caso o arquivo liste o identificador do app sendo instalado, o iOS e iPadOS assinalam que o site e o app têm uma relação confiável. Somente com uma relação de confiança as chamadas a essas duas APIs resultam em uma solicitação ao usuário, o qual deve concordar antes que qualquer senha seja liberada ao app, atualizada ou apagada.

Recomendações de segurança de senha

A lista de senhas do Preenchimento Automático de Senha no iOS, iPadOS e macOS indica quais senhas salvas do usuário serão *reutilizadas* em outros sites, as senhas que são consideradas *fracas* e as senhas que foram comprometidas por um *vazamento de dados*.

Visão geral

O uso da mesma senha em mais de um serviço pode tornar essas contas vulneráveis a um ataque de inserção em massa de credenciais. Se um serviço for violado e senhas vazarem, os invasores podem tentar usar as mesmas credenciais em outros serviços para atacar outras contas.

- Senhas são marcadas como *reutilizadas* se a mesma senha for vista mais de uma vez em domínios diferentes.
- Senhas são marcadas como fracas se puderem ser adivinhadas com facilidade por um invasor. O iOS, iPadOS e macOS detectam padrões comuns usados na criação de senhas fáceis de memorizar, como o uso de palavras encontradas em um dicionário, substituições comuns de caracteres (como usar “s3nh4” em vez de “senha”), padrões encontrados em um teclado (como “q12we34r” em um teclado QWERTY) ou sequências repetidas (como “123123”). Esses padrões são usados com frequência para criar senhas que satisfaçam requisitos mínimos de serviços, mas também são comumente usados por invasores ao tentar obter uma senha através de força bruta.

  Como muitos serviços exigem especificamente um código PIN de quatro ou seis dígitos, essas senhas curtas são avaliadas com regras diferentes. Os códigos PIN são considerados fracos se estiverem entre os códigos PIN mais comuns, se forem uma sequência crescente ou decrescente como “1234” ou “8765” ou se seguirem um padrão repetitivo, como “123123” ou “123321”.
- Senhas são marcadas como *vazadas* se o recurso de Monitoração de Senhas puder comprovar sua presença em um vazamento de dados. Para obter mais informações, consulte Monitoração de Senhas.

Senhas fracas, reutilizadas e vazadas são indicadas na lista de senhas (macOS) ou constam da interface dedicada de Recomendações de Segurança (iOS e iPadOS). Se o usuário usar uma senha muito fraca ou que tenha sido comprometida por um vazamento de dados para iniciar a sessão em um site no Safari, ele recebe um alerta que o encoraja a atualizá-la para uma senha automática forte.

Atualização da segurança de autenticação de contas no iOS e iPadOS

Apps que implementam uma Extensão de Modificação de Autenticação de Conta (na estrutura Serviço de Autenticação) podem oferecer, facilmente e com o toque de um botão, atualizações de contas baseadas em senhas; especificamente, eles podem mudá-las para usar o recurso Iniciar sessão com a Apple ou para que usem uma senha automática forte. Esse ponto de extensão está disponível no iOS e iPadOS.

Se um app tiver implementado o ponto de extensão e estiver instalado no dispositivo, o usuário vê opções de atualização da extensão ao visualizar as Recomendações de Segurança das credenciais associadas ao app no gerenciador de senhas das Chaves do iCloud nos Ajustes. As atualizações também são oferecidas quando o usuário inicia a sessão no app sob risco de ataque às credenciais. Apps têm a capacidade de dizer ao sistema para não avisar usuários sobre as opções de atualização depois de iniciar a sessão. Com a nova API AuthenticationServices, apps também podem chamar suas extensões e realizar atualizações por conta própria, idealmente, a partir de uma tela de ajustes da conta ou de gerenciamento da conta no app.

Apps também pode optar pela compatibilidade com atualizações de senha forte, atualizações com o recurso Iniciar sessão com a Apple ou ambos. Em uma atualização de senha forte, o sistema gera uma senha automática forte para o usuário. Se necessário, o app pode fornecer regras personalizadas de senha que devem ser seguidas ao gerar a senha nova. Quando um usuário muda uma conta para que ela use o recurso Iniciar sessão com a Apple, o sistema fornece uma nova credencial do recurso Iniciar sessão com a Apple à extensão para associação com a conta. O e-mail do ID Apple do usuário não é fornecido como parte da credencial. Depois da atualização bem-sucedida para o recurso Iniciar sessão com a Apple, o sistema apaga das chaves do usuário as credenciais de senha usadas anteriormente, caso elas estejam salvas nesse local.

As Extensões de Modificação de Autenticação de Conta têm a oportunidade de realizar autenticações de usuário adicionais antes de realizar uma atualização. Para atualizações iniciadas dentro do gerenciador de senhas ou depois de iniciar a sessão em um app, a extensão fornece o nome de usuário e a senha para que a conta seja atualizada. Para atualizações dentro de apps, apenas o nome de usuário é fornecido. Se a extensão exigir autenticações adicionais do usuário, ela pode solicitar a exibição de uma interface de usuário personalizada antes de continuar com a atualização. O caso de uso pretendido ao mostrar essa interface de usuário é fazer com que o usuário digite um segundo fator de autenticação para autorizar a atualização.

Monitoração de Senhas

A Monitoração de Senhas é um recurso que compara as senhas armazenadas nas chaves de Preenchimento Automático de Senha do usuário com uma lista continuamente atualizada e selecionada de senhas notoriamente expostas em vazamentos de diversas organizações on-line. Se o recurso estiver ativado, o protocolo de monitoração compara continuamente as chaves de Preenchimento Automático de Senha do usuário com a lista de seleções.

Como a monitoração funciona

O dispositivo do usuário verifica continuamente todas as entradas, umas contra as outras, nas senhas do usuário, fazendo consultas em um intervalo que independe das senhas do usuário ou dos padrões de uso do gerenciador de senhas. Isso ajuda a garantir que os estados de verificação permaneçam atualizados com a lista atual de seleções de senhas vazadas. Para ajudar a impedir o vazamento de informações relacionadas a quantas senhas únicas o usuário tem, os pedidos são feitos em lote e em paralelo. Um número fixo de senhas é verificado em paralelo a cada verificação e, caso o usuário tenha um número menor do que esse, senhas aleatórias são geradas e adicionadas às consultas para compensar tal diferença.

Como as senhas são correspondidas

A correspondência de senhas é feita em um processo de duas partes. As senhas vazadas mais comumente ficam contidas em uma lista local no dispositivo do usuário. Se houver uma ocorrência de senha nessa lista, o usuário é notificado imediatamente sem nenhuma interação externa. Isso é projetado para garantir que nenhuma informação seja vazada sobre as senhas que um usuário tenha e estejam sujeitas a um risco maior devido a uma violação de senhas.

Se a senha não constar da lista de senhas mais frequentes, ela é comparada às senhas vazadas com menor frequência.

Comparação das senhas do usuário com uma lista de seleções

A verificação da ocorrência de uma senha que não esteja na lista local envolve alguma interação com servidores da Apple. Para ajudar a garantir que senhas legítimas de usuários não sejam enviadas à Apple, uma forma de interseção do *conjunto criptográfico privado* é implantado para comparar as senhas do usuário com um grande conjunto de senhas vazadas. Isso é projetado para garantir que, no caso de senhas com menor risco de violação, poucas informações sejam compartilhadas com a Apple. No caso da senha de um usuário, essas informações limitam-se a um prefixo de 15 bits de um hash criptográfico. A remoção das senhas mais frequentemente vazadas desse processo interativo, com o uso da lista local das senhas mais comumente vazadas, reduz o delta da frequência relativa das senhas nos baldes de serviços da web, o que torna impraticável deduzir senhas de usuário a partir dessas pesquisas.

O protocolo subjacente particiona a lista de senhas selecionadas — no momento deste escrito esta lista contém aproximadamente 1,5 bilhão de senhas — em 2^{15} baldes diferentes. O balde ao qual uma senha pertence é baseado nos primeiros 15 bits do valor do hash SHA256 da senha. Adicionalmente, cada senha vazada, ou pw, é associada a um ponto de curva elíptica na curva NIST P256: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, onde α é uma chave aleatória secreta conhecida somente pela Apple e H_{SWU} é uma função oráculo aleatória que mapeia senhas a pontos de curva com base no método Shallue-van de Woestijne-Ulas. Essa transformação é projetada para ocultar computacionalmente os valores de senhas e ajuda a impedir o desvendamento de senhas recém-vazadas através da Monitoração de Senhas.

Para calcular a interseção do conjunto privado, o dispositivo do usuário usa λ, o prefixo de 15 bits do SHA256(upw), onde upw é uma das senhas do usuário, para determinar o balde ao qual a senha do usuário pertence. O dispositivo gera sua própria constante aleatória, β, e envia o ponto $P_c = \beta \cdot H_{SWU}(upw)$ para o servidor, junto com um pedido do balde correspondente a λ. Aqui, β oculta informações sobre a senha do usuário e limita a λ as informações da senha expostas à Apple. Por fim, o servidor usa o ponto enviado pelo dispositivo, calcula $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$ e retorna o resultado junto com o balde de pontos apropriado — $B\lambda = \{ P_{pw} \mid \text{SHA256(pw) começa com prefixo } \lambda\}$ — para o dispositivo.

As informações retornadas permitem que o dispositivo calcule $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$ e certifica que a senha do usuário foi vazada se $\alpha P_c \in B'_\lambda$.

Envio de senhas para outros usuários ou dispositivos Apple

A Apple envia senhas com segurança para outros usuários ou dispositivos Apple com o AirDrop e na Apple TV.

Salvamento de credenciais em outro dispositivo com AirDrop

Quando o iCloud está ativado, os usuários podem utilizar o AirDrop para enviar uma credencial salva a outro dispositivo. A credencial inclui o nome e a senha do usuário e os sites para quais está salva. O envio de credenciais via AirDrop sempre opera no modo Somente Contatos, independentemente de quais sejam os ajustes do usuário. No dispositivo receptor, após o consentimento do usuário, as credenciais são armazenadas nas Chaves de Preenchimento Automático de Senha do usuário.

Preenchimento de credenciais na Apple TV

O Preenchimento Automático de Senhas está disponível para preencher senhas em apps na Apple TV. Quando o usuário põe o foco em um nome de usuário ou campo de senha no tvOS, a Apple TV começa a anunciar uma solicitação de Preenchimento Automático de Senha por meio de Bluetooth Low Energy (BLE).

Qualquer iPhone, iPad ou iPod touch por perto mostra um aviso convidando o usuário a compartilhar uma credencial com a Apple TV. O método de criptografia é estabelecido desta maneira:

- Se o dispositivo e a Apple TV usarem e mesma conta do iCloud, a criptografia entre os dispositivos acontece automaticamente.
- Se o dispositivo tiver uma sessão iniciada em uma conta do iCloud diferente daquela usada na Apple TV, o usuário é solicitado a estabelecer uma conexão criptografada através do uso de um código PIN. Para receber essa solicitação, o iPhone deve estar desbloqueado e perto do Siri Remote emparelhado com a Apple TV.

Após o estabelecimento da conexão criptografada usando a criptografia do link BLE, a credencial é enviada à Apple TV e automaticamente preenchida nos campos de texto correspondentes no app.

Extensões de provedor de credenciais

No iOS, iPadOS e macOS, usuários podem designar um app de terceiros como provedor de credenciais do Preenchimento Automático de Senha nos ajustes de Senhas (iOS e iPadOS) ou nos ajustes de Extensões nas Preferências do Sistema (macOS). Esse mecanismo funciona por meio de extensões de apps. A extensão do provedor de credenciais deve fornecer uma visualização para a escolha de credenciais e a extensão pode fornecer opcionalmente metadados sobre as credenciais salvas, de modo que possam ser oferecidas diretamente na barra QuickType (iOS e iPadOS) ou em uma sugestão de preenchimento automático (macOS). Os metadados incluem o site da credencial e o nome de usuário associado, mas não a senha. O iOS, iPadOS e macOS se comunicam com a extensão para obter a senha quando o usuário opta por preencher uma credencial em um app ou site no Safari. Os metadados de credenciais são armazenados dentro do contêiner do app provedor de credenciais e são removidos quando um app é desinstalado.

Chaves do iCloud

Visão geral da segurança das Chaves do iCloud

O iCloud permite que usuários sincronizem suas senhas com segurança entre dispositivos iOS e iPadOS e computadores Mac sem expor essas informações à Apple. Os objetivos que influenciaram fortemente o design e a arquitetura das Chaves do iCloud (além do enfoque forte em privacidade e segurança) foram a facilidade de uso e a possibilidade de recuperação das chaves. As Chaves do iCloud são compostas de dois serviços: sincronização das chaves e recuperação das chaves.

A Apple projetou as Chaves do iCloud e a recuperação de chaves para que as senhas de um usuário estejam protegidas mesmo em circunstâncias em que:

- A conta do iCloud de um usuário seja comprometida.
- O iCloud seja comprometido por um ataque externo ou de um funcionário.
- Terceiros acessem contas de usuários.

Integração do gerenciador de senhas com as Chaves do iCloud

O iOS, iPadOS e macOS podem gerar automaticamente sequências aleatórias criptograficamente fortes para usar como senhas de contas no Safari. O iOS e o iPadOS também podem gerar senhas fortes para apps. As senhas geradas são armazenadas nas chaves e sincronizadas com outros dispositivos. Os itens das Chaves são transferidos de dispositivo para dispositivo através de servidores da Apple, mas são criptografados de tal maneira que nem a Apple e nem outros dispositivos possam ler seu conteúdo.

Sincronização segura das chaves

Quando um usuário ativa as Chaves do iCloud pela primeira vez, o dispositivo estabelece um círculo de confiança e cria uma identidade de sincronização para si. A identidade de sincronização consiste em uma chave privada e uma chave pública, sendo armazenada nas chaves do dispositivo. A chave pública da identidade de sincronização é colocada no círculo e o círculo é assinado duas vezes: primeiro pela chave privada da identidade de sincronização e depois por uma chave elíptica assimétrica (usando P-256) derivada da senha da conta do iCloud do usuário. Também armazenados no círculo estão os parâmetros (sal aleatório e iterações) usados para criar a chave baseada na senha do iCloud do usuário.

No caso de contas com autenticação de dois fatores, outro círculo de sincronização semelhante é criado e armazenado no CloudKit. As identidades de dispositivos nesse sistema consistem em dois pares de chaves elípticas assimétricas (usando P-384), que também são armazenadas nas chaves. Cada dispositivo mantém sua própria lista de identidades confiáveis e assina essa lista usando uma de suas chaves de identidade.

Armazenamento do círculo de sincronização no iCloud

O círculo de sincronização assinado é armazenado na área de armazenamento de valores de chaves do iCloud do usuário. Ele não pode ser lido sem o conhecimento da senha do iCloud do usuário nem pode ser modificado legalmente sem a chave privada da identidade de sincronização do seu integrante.

No caso de contas com autenticação de dois fatores, a lista de sincronização de cada dispositivo é armazenada no CloudKit. As listas não podem ser lidas sem o conhecimento da senha do iCloud do usuário nem podem ser modificadas sem as chaves privadas do dispositivo que as possui.

Como outros dispositivos de um usuário são adicionados ao círculo de sincronização

Novos dispositivos, ao iniciarem sessão no iCloud, passam a integrar o círculo de sincronização das Chaves do iCloud de uma entre duas formas possíveis: ou se emparelhando e sendo patrocinados por um dispositivo existente das Chaves do iCloud, ou por meio da recuperação das Chaves do iCloud.

Durante os fluxos de emparelhamento, o dispositivo solicitante cria novas identidades de sincronização tanto para o círculo de sincronização quanto para as listas de sincronização (no caso de contas com autenticação de dois fatores) e as apresenta ao patrocinador. O patrocinador adiciona a chave pública do novo integrante ao círculo de sincronização e a assina novamente com a identidade de sincronização e a chave derivada da senha do iCloud do usuário. O novo círculo de sincronização é colocado no iCloud, onde é assinado pelo novo integrante do círculo de maneira semelhante. Em contas com autenticação de dois fatores, o dispositivo patrocinador também fornece ao novo dispositivo um *voucher* assinado por suas chaves de identidade, mostrando que o dispositivo solicitante deve ser confiável. Em seguida ele atualiza sua lista de identidades de sincronização confiáveis para incluir o solicitante.

Agora há dois integrantes no círculo de sincronização e cada integrante possui a chave pública do outro dispositivo. Eles começam a trocar itens individuais das chaves através do armazenamento de valores de chaves do iCloud ou os armazenam no CloudKit, seja qual for o mais apropriado à situação. Se os dois integrantes do círculo tiverem atualizações para o mesmo item, uma ou outra é escolhida, resultando em consistência. Cada item sincronizado é criptografado, de modo que possa ser descriptografado somente por um dispositivo dentro do círculo de confiança do usuário; ele não pode ser descriptografado por nenhum outro dispositivo ou pela Apple.

Conforme novos dispositivos passam a integrar o círculo de sincronização, esse "processo de integração" é repetido. Por exemplo, quando um terceiro dispositivo se junta, ele pode ser emparelhado com qualquer um dos dispositivos atuais. Conforme novos dispositivos são adicionados, cada um é sincronizado ao novo. Isso é projetado para garantir que todos os integrantes tenham os mesmos itens das chaves.

Apenas certos itens são sincronizados

Alguns itens das chaves são específicos de um dispositivo, como as chaves do iMessage, e portanto devem permanecer no dispositivo. Dessa forma, todo item a ser sincronizado deve ser marcado explicitamente com o atributo `kSecAttrSynchronizable`.

A Apple define esse atributo para os dados de usuário do Safari (incluindo nomes de usuários, senhas e números de cartão de crédito), além de senhas de Wi-Fi, chaves de criptografia do HomeKit e outros itens das chaves compatíveis com criptografia de ponta a ponta do iCloud.

Além disso, os itens das chaves adicionados por apps de terceiros não são sincronizados por padrão. Os desenvolvedores devem definir o atributo `kSecAttrSynchronizable` ao adicionar itens às chaves.

Recuperação segura das Chaves do iCloud

As Chaves do iCloud guardam os dados das chaves de usuários com a Apple, *sem* permitir que a Apple leia as senhas ou outros dados contidos. Mesmo que o usuário tenha um único dispositivo, a recuperação das chaves oferece uma camada de segurança contra a perda de dados. Isso é particularmente importante quando o Safari é usado para gerar senhas fortes e aleatórias para contas da web, pois o único registro dessas senhas encontra-se nas chaves.

Um dos pilares da recuperação das chaves é a autenticação secundária e um serviço de guarda segura, criado pela Apple para oferecer suporte a esse recurso especificamente. As chaves do usuário são criptografadas usando um código forte e o serviço de guarda fornece uma cópia das chaves somente se um conjunto de condições específicas for atendido.

Uso de uma autenticação secundária

Há diversas maneiras de estabelecer um código forte:

- Se a autenticação de dois fatores estiver ativada na conta do usuário, o código do dispositivo é usado para recuperar chaves guardadas.
- Se a autenticação de dois fatores não estiver configurada, o usuário é solicitado a fornecer um código de seis dígitos para criar um código de segurança do iCloud. Opcionalmente, sem a autenticação de dois fatores, os usuários podem especificar seus próprios (e maiores) códigos ou permitir que seus dispositivos criem um código criptograficamente aleatório que possa ser registrado e mantido em separado.

Processo de guarda das chaves

Depois que o código é estabelecido, as chaves são guardadas na Apple. Primeiro, o dispositivo iOS, iPadOS ou macOS exporta uma cópia das chaves do usuário e as criptografa embaladas em chaves dentro de uma keybag assimétrica e as coloca na área de armazenamento de valores de chaves do iCloud do usuário. A keybag é embalada pelo código de segurança do iCloud do usuário e com a chave pública do cluster do módulo de segurança de hardware (HSM) que armazena o registro de guarda. Isso se torna o *registro de guarda do iCloud* do usuário. Em contas com autenticação de dois fatores, as chaves também são armazenadas no CloudKit e embaladas por chaves intermediárias que só podem ser recuperadas com o conteúdo do registro de guarda do iCloud, o que oferece o mesmo nível de proteção.

O conteúdo do registro de guarda também permite que o dispositivo da recuperação volte a integrar as Chaves do iCloud, provando aos dispositivos existentes que o dispositivo da recuperação concluiu com sucesso o processo de guarda e, portanto, está autorizado pelo proprietário da conta.

Nota: Se o usuário decide aceitar um código de segurança criptograficamente aleatório em vez de especificar o seu próprio código ou usar um valor de quatro dígitos, o registro de guarda não é necessário. No lugar disso, a chave aleatória é embalada diretamente pelo código de segurança do iCloud.

Além de estabelecer um código de segurança, usuários devem registrar um número de telefone. Isso fornece um nível de autenticação secundário durante a recuperação das chaves. O usuário recebe uma mensagem SMS que deve ser respondida para que a recuperação prossiga.

Segurança de guarda das Chaves do iCloud

O iCloud proporciona uma infraestrutura segura para a guarda de chaves para ajudar a garantir que apenas os usuários e dispositivos autorizados possam fazer uma recuperação. Os clusters dos módulos de segurança de hardware (HSMs) que armazenam os registros de guarda encontram-se posicionados topograficamente atrás do iCloud. Como descrito anteriormente, cada um possui uma chave que é usada para criptografar os registros de guarda pelos quais são responsáveis.

Para recuperar suas chaves, o usuário deve usar sua conta e senha do iCloud para autenticar e responder a um SMS enviado para o número de telefone registrado. Depois disso, o usuário deve digitar seu código de segurança do iCloud. O cluster HSM usa o protocolo SRP (Secure Remote Password) para verificar se o usuário sabe o seu código de segurança do iCloud; o código em si não é enviado à Apple. Cada integrante do cluster verifica independentemente se o usuário não excedeu o número máximo de tentativas permitidas para recuperar seu registro, conforme descrito abaixo. Havendo consenso da maioria, o cluster abre o registro de guarda e o envia para o dispositivo do usuário.

A seguir, o dispositivo usa o código de segurança do iCloud para desembalar as chaves aleatórias usadas para criptografar as chaves do usuário. Com essa chave, as chaves — obtidas do armazenamento de valores de chaves do iCloud — são descriptografadas e restauradas no dispositivo. O iOS, iPadOS e macOS permitem apenas 10 tentativas para autenticar e recuperar um registro de guarda. Depois de várias tentativas malsucedidas, o registro é bloqueado e o usuário precisará ligar para o Suporte da Apple para obter mais tentativas. Depois da décima tentativa malsucedida, o cluster HSM destrói o registro de guarda e as chaves se perdem para sempre. Isso fornece proteção contra tentativas de aquisição do registro com força bruta, às custas da eliminação dos dados das chaves como consequência.

Essas políticas estão codificadas no firmware HSM. Os cartões de acesso administrativo que permitem a alteração do firmware foram destruídos. Qualquer tentativa de alterar o firmware ou acessar a chave privada faz com que o cluster HSM a destrua. Caso isso ocorra, o proprietário de cada uma das chaves protegidas pelo cluster recebe uma mensagem que o informa sobre a perda do seu registro de guarda. Depois disso, ele pode optar por se inscrever novamente.

Apple Pay

Visão geral da segurança do Apple Pay

Com o Apple Pay, os usuários podem usar dispositivos iPhone, iPad, Mac e Apple Watch compatíveis para fazer pagamentos de maneira fácil, segura e privada em lojas, apps e na web, com o Safari. Os usuários também podem adicionar cartões de transporte público, carteiras de estudante e cartões de acesso compatíveis com o Apple Pay ao app Carteira da Apple. É uma solução simples para os usuários e construída com segurança integrada, tanto no hardware como no software.

O Apple Pay também foi projetado para proteger as informações pessoais do usuário. O Apple Pay não coleta nenhuma informação de transação que possa ser atrelada ao usuário. As transações de pagamentos ocorrem entre o usuário, o comerciante e a administradora do cartão.

Segurança do componente do Apple Pay

O Apple Pay usa vários recursos de hardware e software para proporcionar compras seguras e confiáveis.

Secure Element

O Secure Element é um chip certificado padrão que usa a plataforma Java Card, que está em conformidade com os requisitos da indústria financeira para pagamentos eletrônicos. O CI do Secure Element e a plataforma Java Card são certificados de acordo com o processo de Avaliação de Segurança da EMVCo. Depois da conclusão bem-sucedida da avaliação de segurança, a EMVCo emite certificados exclusivos para o CI e a plataforma.

O CI do Secure Element foi certificado com base no padrão Common Criteria. Para obter mais informações, consulte Certificações de segurança do Processador do Secure Enclave (em inglês) em Apple Platform Certifications.

Controlador NFC

O controlador NFC gerencia os protocolos do tipo “Near Field Communication” e encaminha a comunicação entre o Processador de Aplicativos e o Secure Element, e entre o Secure Element e o terminal de vendas.

Carteira da Apple

O app Carteira da Apple é usado para adicionar e gerenciar cartões de crédito, débito e cartões de lojas, além de fazer pagamentos com o Apple Pay. Na Carteira da Apple, os usuários podem visualizar seus cartões e talvez possam ver informações adicionais fornecidas pela administradora do cartão, como a política de privacidade da administradora, transações recentes etc. Os usuários também podem adicionar cartões ao Apple Pay no:

- Assistente de Configuração e Ajustes do iOS e iPadOS
- App Watch para o Apple Watch
- Carteira e Apple Pay nas Preferências do Sistema de computadores Mac que possuem Touch ID

Além disso, a Carteira da Apple permite que os usuários adicionem e gerenciem cartões de transporte público, cartões de fidelidade, cartões de embarque, ingressos, cartões-presente, carteiras de estudante, cartões de acesso e outros.

Secure Enclave

No iPhone, iPad, Apple Watch, computadores Mac com Touch ID e computadores Mac com Apple Silicon que usam o Magic Keyboard com Touch ID, o Secure Enclave gerencia o processo de autenticação e permite que a transação de pagamento prossiga.

No Apple Watch, o dispositivo deve estar desbloqueado e o usuário precisa clicar duas vezes no botão lateral. Os dois cliques são detectados e encaminhados ao Secure Element (ou Secure Enclave, quando disponível) sem passar pelo Processador de Aplicativos.

Servidores do Apple Pay

Os servidores do Apple Pay gerenciam a configuração e a provisão de cartões de crédito, débito, transporte público, carteiras de estudante e cartões de acesso na Carteira da Apple. Os servidores também gerenciam os Números de Conta do Dispositivo armazenados no Secure Element. Eles se comunicam com o dispositivo e com os servidores da rede de pagamento ou da administradora do cartão. Os servidores do Apple Pay também são responsáveis por criptografar novamente as credenciais de pagamento em pagamentos dentro de apps ou na web.

Como o Apple Pay mantém as compras dos usuários protegidas

Secure Element

O Secure Element hospeda um applet feito especificamente para gerenciar o Apple Pay. Também inclui applets certificados pelas redes de pagamento ou operadoras de cartões. Os dados de cartões de crédito, débito e pré-pagos são criptografados e enviados pela rede de pagamento ou administradora do cartão aos applets usando chaves que são de conhecimento apenas da rede de pagamento ou administradora do cartão e do domínio de segurança dos applets. Esses dados são armazenados nos applets e protegidos com os recursos de segurança do Secure Element. Durante uma transação, o terminal se comunica diretamente com o Secure Element através do controlador da comunicação por campo de proximidade (NFC) em um barramento de hardware dedicado.

Controlador NFC

Como gateway do Secure Element, o controlador NFC ajuda a garantir que todos os pagamentos por proximidade sejam realizados em um terminal de vendas próximo ao dispositivo. Apenas solicitações de pagamento provenientes de um terminal dentro do alcance são marcadas pelo controlador NFC como transações por proximidade.

Após um pagamento com cartão de crédito, débito ou pré-pago (incluindo cartões de lojas) ser autorizado pelo titular do cartão com o Face ID, Touch ID ou código, ou através de dois cliques no botão lateral de um Apple Watch desbloqueado, as respostas de proximidade preparadas pelos applets de pagamento dentro do Secure Element são encaminhadas exclusivamente pelo controlador para o campo NFC. Consequentemente, os detalhes de autorizações de pagamento de transações de pagamento por proximidade ficam contidos no campo NFC local e nunca são expostos ao Processador de Aplicativos. Por outro lado, os detalhes de autorizações de pagamento dentro de apps e na web são encaminhados ao Processador de Aplicativos, mas apenas depois de criptografados pelo Secure Element no servidor do Apple Pay.

Cartões de crédito, débito e pré-pagos

Visão geral da segurança da provisão de cartões

Quando um usuário adiciona um cartão de crédito, débito ou pré-pago (incluindo cartões de lojas) à Carteira da Apple, a Apple envia as informações do cartão com segurança, assim como outras informações sobre a conta e o dispositivo do usuário, à administradora do cartão ou ao provedor de serviços autorizado da administradora do cartão. Por meio do uso dessas informações, a administradora do cartão determina se o cartão será aprovado para uso na Carteira da Apple. Como parte do processo de provisão do cartão, o Apple Pay usa três chamadas do lado do servidor para enviar e receber comunicações com a administradora ou rede do cartão:

- Campos Obrigatórios
- Verificação do Cartão
- Vínculo e Provisão

A administradora do cartão ou a rede usa essas chamadas para verificar, aprovar e adicionar cartões à Carteira da Apple. Essas sessões entre servidor e cliente usam TLS 1.2 para transferir os dados.

Os números completos do cartão não são armazenados no dispositivo ou nos servidores do Apple Pay. Ao invés disso, um Número de Conta do Dispositivo é criado, criptografado e armazenado no Secure Element. Esse Número de Conta do Dispositivo é criptografado de tal maneira que a Apple não consegue acessá-lo. O Número de Conta do Dispositivo é exclusivo e diferente da maioria dos números de cartões de crédito ou débito; a administradora do cartão ou rede de pagamento pode impedir seu uso em um cartão de tarja magnética, por telefone ou em sites. O Número de Conta do Dispositivo no Secure Element nunca é armazenado nos servidores do Apple Pay ou incluído no backup do iCloud, e é isolado de dispositivos iOS, iPadOS e watchOS, e de computadores Mac com Touch ID.

Os cartões para uso com o Apple Watch são fornecidos ao Apple Pay através do uso do app Apple Watch no iPhone ou dentro de um app da administradora do cartão no iPhone. A adição de um cartão ao Apple Watch exige que o relógio esteja dentro da área de comunicação do Bluetooth. Os cartões são registrados especificamente para uso com o Apple Watch e possuem um Número de Conta do Dispositivo próprio, armazenado no Secure Element do Apple Watch.

Quando cartões de crédito, débito ou pré-pagos (incluindo cartões de lojas) são adicionados, eles aparecem em uma lista de cartões durante o Assistente de Configuração em dispositivos que tenham uma sessão iniciada na mesma conta do iCloud. Tais cartões permanecem nessa lista pelo tempo em que estiverem ativos em ao menos um dispositivo. Os cartões são removidos dessa lista após terem sido removidos de todos os dispositivos por sete dias. Esse recurso requer que a autenticação de dois fatores esteja ativada na respectiva conta do iCloud.

Adição de cartões de crédito ou débito ao Apple Pay

Os cartões de crédito podem ser adicionados manualmente ao Apple Pay em dispositivos Apple.

Adição manual de cartões de crédito ou débito

Para adicionar um cartão manualmente, o nome, número, data de validade e CVC do cartão são usados para facilitar o processo de provisão. Essas informações podem ser digitadas pelos usuários ou capturadas pela câmera do dispositivo nos apps Ajustes, Carteira da Apple ou Apple Watch. Quando a câmera captura as informações do cartão, a Apple tenta preencher o nome, número e data de validade do cartão. A foto nunca é salva no dispositivo ou armazenada na fototeca. Após todos os campos serem preenchidos, o processo de Verificação do Cartão confirmará todos os campos, exceto o CVC. Depois, as informações são criptografadas e enviadas ao servidor do Apple Pay.

Se um ID de termos e condições for retornado junto ao processo de Verificação do Cartão, a Apple transfere e exibe os termos e condições da administradora do cartão para o usuário. Caso o usuário aceite os termos e condições, a Apple envia o ID dos termos aceitos, assim como o CVC, para o processo de Vínculo e Provisão. Além disso, como parte do processo de Vínculo e Provisão, a Apple compartilha informações do dispositivo com a administradora ou rede do cartão. Isso inclui informações sobre (a) a atividade da conta da iTunes Store e da App Store do usuário (se ele tem um histórico longo de transações no iTunes, por exemplo), (b) o dispositivo do usuário (por exemplo, número de telefone, nome e modelo do dispositivo, além de qualquer dispositivo Apple complementar necessário para usar o Apple Pay) e (c) a localização aproximada do usuário no momento em que o cartão é adicionado (se os Serviços de Localização estiverem ativados). Por meio do uso dessas informações, a administradora do cartão determina se o cartão será aprovado para uso no Apple Pay.

Dois fatores decorrem do processo de Vínculo e Provisão:

- O dispositivo inicia o download do tíquete da Carteira da Apple que representa o cartão de crédito ou débito.
- O dispositivo inicia o vínculo do cartão ao Secure Element.

O tíquete contém URLs para baixar a imagem ilustrativa do cartão e metadados sobre o cartão (como informações de contato, app relacionado da administradora e recursos compatíveis). Ele também contém o estado do tíquete, que inclui informações sobre a conclusão da personalização do Secure Element, a suspensão vigente do cartão pela administradora ou exigências de verificações adicionais para que o cartão possa fazer pagamentos com o Apple Pay.

Adição de cartões de crédito ou débito de uma conta da iTunes Store

No caso de cartões de crédito e débito já registrados no iTunes, o usuário pode ser solicitado a digitar a senha do seu ID Apple novamente. O número do cartão é obtido do iTunes e o processo de Verificação do Cartão é iniciado. Se o cartão for elegível para o Apple Pay, o dispositivo transfere e exibe os termos e condições para depois enviar o ID dos termos e o código de segurança do cartão para o processo de Vínculo e Provisão. Cartões já registrados em contas do iTunes poderão estar sujeitos a verificações adicionais.

Adição de cartões de crédito ou débito em um app de administradora de cartões

Quando um app está registrado para uso com o Apple Pay, chaves são estabelecidas para o app e para o servidor da administradora do cartão. Essas chaves são usadas para criptografar as informações do cartão enviadas à administradora do cartão. Isso é projetado para impedir que as informações sejam lidas pelo dispositivo Apple. O fluxo de provisão assemelha-se ao usado para cartões adicionados manualmente (descrito anteriormente), exceto pelo fato de que são usadas senhas de uso único em vez do CVC.

Adição de cartões de crédito ou débito do site da administradora de cartões

Algumas administradoras de cartões permitem iniciar o processo de provisão do cartão para a Carteira da Apple diretamente dos seus sites. Nesse caso, para iniciar a tarefa, o usuário seleciona um cartão para provisão no site da administradora. O usuário é direcionado a uma experiência isolada de início de sessão (dentro do domínio da Apple) e é solicitado a iniciar a sessão com o seu ID Apple. Depois de iniciar a sessão, o usuário escolhe um ou mais dispositivos para os quais aprovisionar o cartão e deve confirmar o resultado da provisão em cada dispositivo de destino.

Adição de verificação complementar

A administradora do cartão pode decidir se um cartão de crédito ou débito requer verificação adicional. Dependendo do que for oferecido pela administradora, talvez o usuário possa escolher entre diversas opções de verificação adicional, como mensagem de texto, e-mail, ligação do atendimento ao cliente ou um método em um app de terceiros aprovado para concluir a verificação. No caso de mensagens de texto ou e-mail, o usuário seleciona dentre as informações de contato registradas na administradora. É enviado um código, que deverá ser digitado na Carteira da Apple, nos Ajustes ou no app do Apple Watch. No caso de atendimento ao cliente ou verificação ao usar um app, a administradora realiza o seu próprio processo de comunicação.

Autorização de pagamento com o Apple Pay

Em dispositivos com Secure Enclave, um pagamento pode ser feito apenas depois de receber autorização do Secure Enclave. No iPhone ou iPad, isso envolve a confirmação de que o usuário se autenticou com o Face ID, Touch ID ou o código do dispositivo. Caso disponíveis, o Face ID ou o Touch ID são os métodos padrão, mas o código pode ser usado a qualquer momento. Um código é oferecido automaticamente após três tentativas malsucedidas de identificação de uma impressão digital ou duas tentativas malsucedidas de identificação de um rosto e exigido após cinco tentativas malsucedidas. Um código também é exigido quando o Face ID ou o Touch ID não estão configurados ou ativados para o Apple Pay. Para que um pagamento seja feito no Apple Watch, o dispositivo deve ser desbloqueado com o código e o botão lateral deve ser clicado duas vezes.

Uso de uma chave de emparelhamento compartilhada

A comunicação entre o Secure Enclave e o Secure Element ocorre através de uma interface serial, com o Secure Element conectado ao controlador NFC, que por sua vez encontra-se conectado ao Processador de Aplicativos. Embora não estejam conectados diretamente, o Secure Enclave e o Secure Element podem se comunicar em segurança usando uma chave de emparelhamento compartilhada, fornecida durante o processo de fabricação. A criptografia e a autenticação da comunicação são baseadas em AES, com nonces criptográficos usados em ambos os lados para proteção contra ataques de reprodução. A chave de emparelhamento é gerada dentro do Secure Enclave a partir de sua chave UID e do identificador exclusivo do Secure Element. A chave de emparelhamento é então transferida seguramente do Secure Enclave para um módulo de segurança de hardware (HSM) na fábrica, que possui o material de chave necessário para injetar a chave de emparelhamento no Secure Element.

Autorização de uma transação segura

Quando o usuário autoriza uma transação, que inclui um gesto físico comunicado diretamente ao Secure Enclave, o Secure Enclave envia os dados assinados sobre o tipo de autenticação e os detalhes do tipo de transação (proximidade ou dentro de apps) para o Secure Enclave, atrelados a um valor de Autorização Aleatório (AR). O valor AR é gerado no Secure Enclave na primeira vez que o usuário fornece um cartão de crédito e persiste enquanto o Apple Pay estiver ativado, protegido pela criptografia do Secure Enclave e pelo mecanismo antirreversão. Ele é entregue com segurança ao Secure Element ao usar a chave de emparelhamento como base. Ao receber um novo valor AR, o Secure Element marca qualquer cartão adicionado anteriormente como apagado.

Uso de um criptograma de pagamento para segurança dinâmica

As transações de pagamento originadas de applets de pagamento incluem um criptograma de pagamento e um Número de Conta do Dispositivo. Esse criptograma, um código de uso único, é calculado por um contador de transações e uma chave. O contador de transações aumenta a cada nova transação. A chave é fornecida no applet de pagamento durante a personalização, sendo conhecida pela rede de pagamentos, pela administradora do cartão ou por ambas. Dependendo do esquema de pagamento, outros dados também podem ser usados no cálculo, incluindo:

- Um Número de Terminal Imprevisível, em transações de comunicação por campo de proximidade (NFC)
- Um nonce do servidor do Apple Pay, em transações dentro de apps

Esses códigos de segurança são fornecidos à rede de pagamentos e à administradora do cartão, o que permite ao emissor verificar cada transação. O tamanho desses códigos de segurança pode variar conforme o tipo de transação.

Uso do Apple Pay para pagamentos com cartões

O Apple Pay pode ser usado para fazer compras em lojas, dentro de apps e em sites.

Pagamento com cartões em lojas

Se o iPhone ou Apple Watch estiver ligado e detectar um campo NFC, ele apresenta ao usuário o cartão solicitado (se a seleção automática estiver ativada para esse cartão) ou o cartão padrão, que é gerenciado nos Ajustes. O usuário também pode acessar a Carteira da Apple e escolher um cartão ou, quando o dispositivo estiver bloqueado, ele pode:

- Clicar duas vezes no botão lateral em dispositivos com Face ID
- Clicar duas vezes no botão Início em dispositivos com Touch ID
- Usar os recursos de Acessibilidade que permitem o Apple Pay na Tela Bloqueada

A seguir, antes que as informações sejam transmitidas, o usuário precisa autenticar com o Face ID, o Touch ID ou o código. Quando o Apple Watch está desbloqueado, o cartão de pagamento padrão é ativado ao clicar duas vezes no botão lateral. Nenhuma informação de pagamento é enviada sem a autenticação do usuário.

Depois que o usuário autentica, o Número de Conta do Dispositivo e um código de segurança dinâmico específico à transação são usados ao processar o pagamento. A Apple e o dispositivo do usuário não enviam os números completos do cartão de crédito ou débito para os comerciantes. A Apple pode receber informações anônimas da transação, como a hora e o local aproximado da transação, o que ajuda a melhorar o Apple Pay e outros produtos e serviços da Apple.

Pagamento com cartões dentro de apps

O Apple Pay também pode ser usado para fazer pagamentos em apps no iPhone, iPad, Mac e Apple Watch. Quando os usuários pagam com o Apple Pay dentro de apps, a Apple recebe as informações criptografadas. Antes que essas informações sejam enviadas ao desenvolvedor ou comerciante, a Apple as criptografa novamente com uma chave específica do desenvolvedor. O Apple Pay retém informações anônimas sobre a transação, como o valor aproximado da compra. Essas informações não podem ser atreladas ao usuário e nunca incluem o que o usuário compra.

Quando um app inicia uma transação de pagamento do Apple Pay, os servidores do Apple Pay recebem a transação criptografada do dispositivo antes que o comerciante a receba. Depois, os servidores do Apple Pay criptografam novamente a transação com uma chave específica do comerciante antes de repassá-la ao comerciante.

Quando um app solicita um pagamento, ele chama uma API para determinar se o dispositivo é compatível com o Apple Pay e se o usuário tem cartões de crédito ou débito que podem fazer pagamentos em uma rede de pagamentos aceita pelo comerciante. O app solicita qualquer informação necessária para processar e executar a transação, como o endereço de cobrança e entrega e informações de contato. Em seguida, o app pede para que o iOS, iPadOS ou watchOS apresentem a folha do Apple Pay, que solicita informações para o app, assim como outras informações necessárias, como qual cartão usar.

Nesse momento, informações sobre a cidade, estado e CEP são apresentadas ao app para o cálculo do custo de entrega final. O conjunto completo de informações solicitadas não é fornecido ao app até que o usuário autorize o pagamento com o Face ID, o Touch ID ou o código do dispositivo. Depois que o pagamento é autorizado, as informações apresentadas na folha do Apple Pay são transferidas ao comerciante.

Autorização de pagamento em apps

Quando o usuário autoriza o pagamento, uma ligação é feita aos servidores do Apple Pay para obtenção de um nonce criptográfico (que se assemelha ao valor retornado por terminais NFC usados em transações em lojas). O nonce, assim como outros dados da transação, é passado ao Secure Element para calcular uma credencial de pagamento que é criptografada com uma chave da Apple. A credencial de pagamento criptografada é retornada aos servidores do Apple Pay, que a descriptografam, comparam o nonce da credencial com aquele originalmente enviado pelos servidores do Apple Pay e criptografam a credencial de pagamento novamente com a chave do comerciante associada ao ID do Comerciante. Depois, o pagamento é reenviado ao dispositivo, que o redireciona ao app através da API. O app então a envia ao sistema do comerciante para processamento. O comerciante pode então descriptografar a credencial de pagamento usando sua chave privada para processamento. Isso, juntamente à assinatura dos servidores da Apple, permite que o comerciante verifique que a transação se destina especificamente a esse comerciante.

As APIs requerem um direito que especifique os IDs de Comerciante compatíveis. Um app também pode incluir dados adicionais (como um número de pedido ou identidade do cliente) para enviar ao Secure Element para assinatura, o que impede que a transação seja desviada para outro cliente. Isso é realizado pelo desenvolvedor do app, que pode especificar applicationData em PKPaymentRequest. Um hash desses dados é incluído nos dados de pagamento criptografados. O comerciante fica então responsável por verificar se o hash do applicationData corresponde àquele incluído nos dados de pagamento.

Pagamento com cartões em sites

O Apple Pay pode ser usado para fazer pagamentos em sites no iPhone, iPad, Apple Watch e computadores Mac com Touch ID. As transações do Apple Pay também podem ser iniciadas no Mac e concluídas em um iPhone ou Apple Watch compatível com o Apple Pay que esteja usando a mesma conta do iCloud.

O uso do Apple Pay na web requer que todos os sites participantes registrem-se na Apple. Após o registro do domínio, a validação do nome do domínio é realizada apenas depois que a Apple emite um certificado de cliente TLS. Os sites compatíveis com o Apple Pay são obrigados a fornecer seu conteúdo por HTTPS. Em cada transação de pagamento, os sites precisam usar o certificado de cliente TLS emitido pela Apple para obter uma sessão de comerciante segura e exclusiva. Os dados da sessão do comerciante são assinados pela Apple. Depois da verificação da assinatura da sessão do comerciante, um site pode consultar se o usuário possui um dispositivo compatível com o Apple Pay e se ele tem um cartão de crédito, débito ou pré-pago ativado no dispositivo. Nenhum outro detalhe é compartilhado. Se o usuário não desejar compartilhar essas informações, ele pode desativar as consultas do Apple Pay nos ajustes de privacidade do Safari em dispositivos iPhone, iPad e Mac.

Depois da validação da sessão do comerciante, todas as medidas de privacidade e segurança são idênticas àquelas tomadas ao fazer pagamentos dentro de um app.

Se o usuário estiver transmitindo informações relacionadas a pagamento de um Mac para um iPhone ou Apple Watch, o Handoff do Apple Pay usa o protocolo de Serviço de Identidade da Apple (IDS) com criptografia de ponta a ponta para transmitir as informações relacionadas a pagamento entre o Mac do usuário e o dispositivo autorizador. O cliente do IDS no Mac usa as chaves do dispositivo do usuário para realizar a criptografia, de modo que nenhum outro dispositivo possa descriptografar essas informações. Além disso, as chaves não são disponibilizadas à Apple. A descoberta de dispositivos para o Handoff do Apple Pay contém o tipo e o identificador exclusivo dos cartões de crédito do usuário, além de alguns metadados. O número de conta específico do dispositivo do cartão do usuário não é compartilhado e continua armazenado com segurança no iPhone ou Apple Watch do usuário. A Apple também transmite com segurança os endereços de contato, entrega e cobrança usados recentemente pelo usuário através das Chaves do iCloud.

Depois que o usuário autoriza o pagamento com o Face ID, o Touch ID, o código ou clica duas vezes no botão lateral do Apple Watch, um token de pagamento criptografado exclusivamente para o certificado de comerciante de cada site é transmitido com segurança do iPhone ou Apple Watch para o Mac, sendo então entregue ao site do comerciante.

Apenas dispositivos próximos uns dos outros podem solicitar e concluir pagamentos. A proximidade é determinada através de anúncios de Bluetooth Low Energy (BLE).

Tíquetes por proximidade no Apple Pay

Para transmitir dados de tíquetes compatíveis a terminais NFC compatíveis, a Apple usa o protocolo de Serviços de Valor Agregado (Apple VAS). O protocolo VAS pode ser implementado em terminais por proximidade ou em apps para iPhone e usa NFC para se comunicar com dispositivos Apple compatíveis. O protocolo VAS funciona a distâncias curtas e pode ser usado para apresentação de tíquetes por proximidade, independentemente ou como parte de uma transação do Apple Pay.

Quando o dispositivo é segurado próximo ao terminal NFC, o terminal inicia a recepção das informações do tíquete, solicitando um tíquete. Se o usuário tiver um tíquete com a identidade do emissor do tíquete, ele é solicitado a autorizar seu uso por meio do Face ID, Touch ID ou código. As informações do tíquete, uma marca temporal e uma chave ECDH P-256 aleatória de uso único são usadas com a chave pública do emissor do tíquete para derivar uma chave de criptografia para os dados do tíquete, que é enviada para o terminal.

Do iOS 12.0.1 ao iOS 13 (inclusive), os usuários podem selecionar um tíquete manualmente antes de apresentá-lo ao terminal NFC do comerciante. No iOS 13.1 ou posterior, os emissores de tíquetes podem configurar se os tíquetes selecionados manualmente precisam da autenticação do usuário ou podem ser usados sem autenticação.

Inutilização de cartões com o Apple Pay

Os cartões de crédito, débito e pré-pagos adicionados ao Secure Element podem ser usados somente se uma autorização que use a mesma chave de emparelhamento e valor de Autorização Aleatório (AR) de quando o cartão foi adicionado for apresentada ao Secure Element. Ao receber um novo valor AR, o Secure Element marca qualquer cartão adicionado anteriormente como apagado. Isso permite que o sistema operacional instrua o Secure Enclave a inutilizar os cartões, marcando suas cópias do AR como inválidas nos seguintes casos:

Método	Dispositivo
O código é desativado.	iPhone, iPad, Apple Watch
A senha é desativada.	Mac
O usuário encerra a sessão no iCloud.	iPhone, iPad, Mac, Apple Watch
O usuário seleciona “Apagar Conteúdo e Ajustes”.	iPhone, iPad, Mac, Apple Watch
O dispositivo é restaurado a partir do Modo de Recuperação.	iPhone, iPad, Mac, Apple Watch
Desemparelhamento	Apple Watch

Suspensão, remoção e apagamento de cartões

Os usuários podem usar o Buscar para colocar seus dispositivos no Modo Perdido e suspender o Apple Pay no iPhone, iPad e Apple Watch. Os usuários também podem usar o Buscar, iCloud.com ou a Carteira da Apple (diretamente no dispositivo), para remover e apagar seus cartões do Apple Pay. No Apple Watch, os cartões podem ser removidos através dos ajustes do iCloud, do app Apple Watch no iPhone ou diretamente no relógio. A capacidade de fazer pagamentos usando cartões no dispositivo é suspensa ou removida do Apple Pay pela administradora do cartão ou rede de pagamentos correspondente, mesmo que o dispositivo esteja off-line e desconectado de uma rede celular ou Wi-Fi. Os usuários também podem ligar para a administradora do cartão para suspender ou remover cartões do Apple Pay.

Quando um usuário apaga todo o dispositivo — ao usar “Apagar Conteúdo e Ajustes” ou o app Buscar, ou ao restaurar o dispositivo — o iPhone, iPad, iPod touch, Mac e Apple Watch instruem o Secure Element a marcar todos os cartões como apagados. Isso faz com que os cartões sejam alterados imediatamente para um estado não utilizável até que os servidores do Apple Pay possam ser contatados para apagar completamente os cartões do Secure Element. De forma independente, o Secure Enclave marca o AR como inválido, para que autorizações de pagamento posteriores com cartões previamente registrados não sejam possíveis. Quando o dispositivo estiver on-line, ele tentará contatar os servidores do Apple Pay para ajudar a garantir que todos os cartões no Secure Element sejam apagados.

Segurança do Apple Card

Em modelos compatíveis do iPhone e Mac, um usuário pode solicitar um Apple Card com segurança.

Solicitação do Apple Card

No iOS 12.4 ou posterior, macOS 10.14.6 ou posterior e watchOS 5.3 ou posterior, o Apple Card pode ser usado com o Apple Pay para fazer pagamentos em lojas, apps e na web.

Para inscrever-se para um Apple Card, o usuário deve ter uma sessão iniciada em sua conta do iCloud em um dispositivo iOS ou iPadOS compatível com o Apple Pay e a autenticação de dois fatores configurada na conta do iCloud. Quando a solicitação é aprovada, o Apple Card fica disponível na Carteira da Apple ou em Ajustes > Carteira e Apple Pay em dispositivos qualificados nos quais o usuário tenha uma sessão iniciada com seu ID Apple.

Quando um usuário se inscreve para um Apple Card, as informações de identificação do usuário são verificadas com segurança pelos parceiros provedores de identidade da Apple e compartilhadas com o Goldman Sachs Bank USA para fins de identificação e avaliação de crédito.

As informações fornecidas na inscrição, como o número de previdência social ou a imagem de um documento de identidade, são transmitidas com segurança aos parceiros provedores de identidade da Apple e/ou ao Goldman Sachs Bank USA criptografadas com as suas respectivas chaves. A Apple não pode descriptografar esses dados.

As informações de renda durante a aplicação e as informações de conta bancária usadas para o pagamento de contas são transmitidas com segurança ao Goldman Sachs Bank USA, criptografadas com a chave do banco. As informações sobre a conta bancária são salvas nas chaves. A Apple não pode descriptografar esses dados.

Ao adicionar um Apple Card à Carteira da Apple, as mesmas informações fornecidas ao adicionar um cartão de crédito ou débito podem ser compartilhadas com o banco parceiro da Apple, o Goldman Sachs Bank USA, e com a Apple Payments Inc. Essas informações são usadas somente para a resolução de problemas, prevenção de fraudes e fins regulatórios.

No iOS 14.6 ou posterior, iPadOS 14.6 ou posterior e watchOS 7.5 ou posterior, o organizador de uma família do iCloud com um Apple Card pode compartilhar o cartão com os membros da Família do iCloud que tenham mais de 13 anos. A autenticação do usuário é obrigatória para confirmar o convite. A Carteira da Apple usa uma chave no Secure Enclave para calcular uma assinatura que vincula o proprietário e o convidado. A assinatura é validada nos servidores da Apple.

Como opção, o organizador pode definir um limite de transações para os participantes. Os cartões dos participantes também podem ser bloqueados para pausar os gastos a qualquer momento por meio da Carteira da Apple. Quando um coproprietário ou participante com mais de 18 anos aceita o convite e se inscreve, ele passa pelo mesmo processo de inscrição definido na seção sobre a solicitação do Apple Card na Carteira da Apple.

Uso do Apple Card

Um cartão físico pode ser solicitado em Apple Card na Carteira da Apple. Depois que o usuário recebe o cartão físico, ele é ativado usando a etiqueta NFC que está no envelope do cartão físico. A etiqueta é exclusiva por cartão e não pode ser usada para ativar o cartão de outro usuário. Como opção, o cartão pode ser ativado manualmente nos ajustes da Carteira da Apple. Além disso, o usuário também tem a opção de bloquear ou desbloquear o cartão físico a qualquer momento com a Carteira da Apple.

Detalhes de pagamentos com Apple Card e tíquetes da Carteira da Apple

Os pagamentos devidos na conta do Apple Card podem ser feitos na Carteira da Apple no iOS com Apple Cash e uma conta bancária. Os pagamentos de contas podem ser agendados como recorrentes ou como um pagamento único em uma data específica com o Apple Cash e uma conta bancária. Quando um usuário faz um pagamento, uma ligação é feita para os servidores do Apple Pay para obtenção de um nonce criptográfico, semelhante ao Apple Cash. O nonce, assim como os detalhes da configuração do pagamento, é passado ao Secure Element para calcular uma assinatura. A assinatura é então retornada aos servidores do Apple Pay. A autenticação, integridade e exatidão do pagamento são verificadas pelos servidores do Apple Pay através da assinatura e do nonce, e a ordem é passada ao Goldman Sachs Bank USA para processamento.

O número do Apple Card é recuperado pela Carteira da Apple por meio da apresentação de um certificado. O servidor do Apple Pay valida o certificado para confirmar que a chave foi gerada no Secure Enclave. A seguir, ele usa essa chave para criptografar o número do Apple Card antes de retorná-lo à Carteira da Apple, de forma que somente o iPhone que solicitou o número do Apple Card seja capaz de decifrá-lo. Após a decifração, o número do Apple Card é salvo nas Chaves do iCloud.

Para que os detalhes do número do Apple Card sejam mostrados no tíquete com a Carteira da Apple, o usuário deve se autenticar com o Face ID, o Touch ID ou código. Ele pode ser substituído pelo usuário na seção de informações do cartão, desativando o anterior.

Proteção Avançada Contra Fraude

No iOS 15 ou posterior e iPadOS 15 ou posterior, o usuário do Apple Card pode ativar a Proteção Avançada Contra Fraude na Carteira da Apple. Quando ela está ativada, o Código de Segurança do Cartão é atualizado a cada poucos dias.

Segurança do Apple Cash

No iOS 11.2 ou posterior, iPadOS 13.1 ou posterior e watchOS 4.2 ou posterior, o Apple Pay pode ser usado em um iPhone, iPad ou Apple Watch para enviar, receber e pedir dinheiro a outros usuários. Quando um usuário recebe dinheiro, o dinheiro é adicionado a uma conta do Apple Cash (que pode ser acessada na Carteira da Apple ou em Ajustes > Carteira e Apple Pay) em dispositivos qualificados nos quais o usuário tenha uma sessão iniciada com seu ID Apple.

No iOS 14, iPadOS 14 e watchOS 7, o organizador de uma família do iCloud que tenha verificado sua identidade com o Apple Cash pode ativar o Apple Cash para membros da família com menos de 18 anos. Opcionalmente, o organizador pode restringir as capacidades de envio de dinheiro desses usuários apenas a membros da família ou contatos. Caso o membro da família com menos de 18 anos passe por uma recuperação de conta do ID Apple, o organizador da família deve reativar manualmente o cartão do Apple Cash desse usuário. Caso o membro da família com menos de 18 anos não faça mais parte da família do iCloud, seu respectivo saldo do Apple Cash é transferido automaticamente para o organizador da conta.

Ao configurar o Apple Cash, as mesmas informações fornecidas ao adicionar um cartão de crédito ou débito podem ser compartilhadas com o Green Dot Bank (associado da Apple) ou com a Apple Payments Inc. (uma subsidiária integral criada para proteger a privacidade dos usuários), que armazena e processa informações separadamente do restante da Apple, de maneira que o restante da Apple não tenha conhecimento. Essas informações são usadas somente para a resolução de problemas, prevenção de fraudes e fins regulatórios.

Uso do Apple Cash no iMessage

Para usar pagamentos de pessoa a pessoa e o Apple Cash, o usuário deve ter uma sessão iniciada em sua conta do iCloud em um dispositivo compatível com o Apple Cash e a autenticação de dois fatores configurada na conta do iCloud. Os pedidos de dinheiro e as transferências entre usuários são iniciadas a partir do app Mensagens ou ao pedir à Siri. Quando um usuário tenta enviar dinheiro, o iMessage exibe a folha do Apple Pay. O saldo do Apple Cash sempre é usado primeiro. Se necessário, fundos adicionais são sacados de um segundo cartão de crédito ou débito adicionado pelo usuário à Carteira da Apple.

Uso do Apple Cash em lojas, apps e na web

O cartão do Apple Cash na Carteira da Apple pode ser usado com o Apple Pay para fazer pagamentos em lojas, apps e na web. O dinheiro na conta do Apple Cash também pode ser transferido para uma conta bancária. Além de dinheiro recebido de outro usuário, quantias podem ser adicionadas à conta do Apple Cash a partir de um cartão de débito ou pré-pago na Carteira da Apple.

A Apple Payments Inc. armazena e pode usar os dados de transação do usuário para a resolução de problemas, prevenção de fraudes e fins regulatórios quando uma transação é concluída. O restante da Apple não sabe para quem o dinheiro foi enviado, de quem o dinheiro foi recebido ou onde uma compra foi feita com o cartão do Apple Cash.

Quando o usuário envia dinheiro com o Apple Pay, adiciona dinheiro a uma conta do Apple Cash ou transfere dinheiro para uma conta bancária, uma ligação é feita para os servidores do Apple Pay para obtenção de um nonce criptográfico, o qual é similar ao valor retornado para o Apple Pay dentro de apps. O nonce, assim como outros dados da transação, é passado ao Secure Element para calcular uma assinatura de pagamento. A assinatura é retornada aos servidores do Apple Pay. A autenticação, integridade e exatidão da transação são verificadas pelos servidores do Apple Pay por meio da assinatura de pagamento e do nonce. Em seguida, a transferência do dinheiro é iniciada e o usuário é notificado sobre uma transação concluída.

Se a transação envolver:

- Um cartão de crédito para adicionar dinheiro ao Apple Cash
- Fornecimento suplementar de dinheiro se o saldo do Apple Cash for insuficiente

Uma credencial de pagamento criptografada também é produzida e enviada aos servidores do Apple Pay, de maneira semelhante ao funcionamento do Apple Pay dentro de apps e sites.

Depois que o saldo da conta do Apple Cash excede uma certa quantia ou uma atividade incomum é detectada, o usuário é solicitado a verificar sua identidade. As informações fornecidas para verificar a identidade do usuário — como o número de previdência social ou respostas a perguntas (por exemplo, para confirmar o nome de uma rua onde o usuário morou anteriormente) — são transmitidas com segurança para o associado da Apple e criptografadas com a chave desse associado. A Apple não pode descriptografar esses dados. O usuário é solicitado a verificar sua identidade novamente caso realize uma recuperação de conta do ID Apple antes de reobter acesso ao saldo do Apple Cash.

Segurança do Tap to Pay on iPhone

O recurso Tap to Pay on iPhone, disponível no iOS 15.4, permite que comerciantes dos EUA aceitem Apple Pay e outros pagamentos por proximidade usando um iPhone e um app iOS compatível com parceiros. Com este serviço, os usuários com dispositivos iPhone compatíveis podem aceitar com segurança pagamentos por proximidade e tíquetes do *Apple Pay* com NFC. Com o Tap to Pay on iPhone, os comerciantes não precisam de nenhum hardware adicional para aceitar pagamentos por proximidade.

O recurso Tap to Pay on iPhone foi projetado para proteger as informações pessoais de quem está realizando o pagamento. Este serviço não coleta nenhuma informação de transação que possa ser atrelada a essa pessoa. As informações do cartão de pagamento, como o número do cartão de crédito/débito (PAN), são protegidas pelo Secure Element e não são disponibilizadas ao comerciante. As informações do cartão de pagamento ficam entre o Provedor do Serviço de Pagamento do comerciante, a pessoa que faz o pagamento e a administradora do cartão. Além disso, o serviço Tap to Pay não coleta nomes, endereços ou números de telefone da pessoa que faz o pagamento.

O recurso Tap to Pay on iPhone foi avaliado por um reconhecido laboratório de segurança externo e aprovado pela American Express, Discover, Mastercard e Visa.

Segurança dos componentes do pagamento por proximidade

- *Secure Element:* o Secure Element [link para a seção Secure Element do Apple Pay] contém os kernels de pagamento, que leem e protegem os dados do cartão de pagamento por proximidade.
- *Controlador NFC:* o controlador NFC gerencia os protocolos do tipo “Near Field Communication” e encaminha a comunicação entre o Processador de Aplicativos e o Secure Element, e entre o Secure Element e o cartão de pagamento por proximidade.
- *Servidores do Tap to Pay on iPhone:* os servidores do Tap to Pay on iPhone gerenciam a configuração e a provisão dos kernels de pagamento no dispositivo. Os servidores também monitoram a segurança dos dispositivos com o recurso Tap to Pay on iPhone de forma compatível com o padrão Contactless Payments on COTS (CPoC) do Payment Card Industry Security Standards Council (PCI SSC), tendo conformidade com o PCI DSS.

Como o recurso Tap to Pay lê cartões de crédito, débito e pré-pagos

Visão geral da segurança da provisão

No primeiro uso do recurso Tap to Pay on iPhone com um app que possua direitos suficientes, o servidor do Tap to Pay on iPhone determina se o dispositivo atende aos critérios de qualificação, como o modelo do dispositivo, a versão do iOS e se um código foi definido. Após a conclusão da verificação, o applet de aceitação de pagamentos é baixado do servidor do Tap to Pay on iPhone e instalado no Secure Element, juntamente com a configuração do kernel de pagamento associado. Essa operação é realizada de forma segura entre os servidores do Tap to Pay on iPhone e o Secure Element. O Secure Element valida a integridade e a autenticidade desses dados antes da instalação.

Visão geral da segurança da leitura de cartões

Quando um app com Tap to Pay on iPhone solicita a leitura de um cartão à estrutura ProximityReader, uma folha (controlada pelo iOS) é mostrada e solicita ao usuário que toque em um cartão de pagamento. O iOS inicializa o Leitor de Cartões de Pagamento e solicita os kernels de pagamento no Secure Element para iniciar a leitura do cartão.

Neste momento, o Secure Element assume o controle do Controlador NFC no Modo Leitor. Esse modo permite que apenas os dados do cartão sejam trocados entre o cartão de pagamento e o Secure Element por meio do controlador NFC. Os cartões de pagamento somente podem ser lidos nesse modo.

Depois que o applet de aceitação do Secure Element conclui a leitura do cartão, ele criptografa e assina os dados do cartão. Esses dados permanecem criptografados e autenticados até chegarem ao Provedor do Serviço de Pagamento. Apenas o Provedor do Serviço de Pagamento usado pelo app para solicitar a leitura do cartão pode descriptografar os dados do cartão. O Provedor do Serviço de Pagamento deve solicitar a chave de descriptografia do servidor do Tap to Pay on iPhone. O servidor do Tap to Pay on iPhone emite as chaves de descriptografia para o Provedor do Serviço de Pagamento após a validação da integridade e autenticidade dos dados, e depois de verificar que a leitura do cartão foi feita em até 60 segundos após a leitura do cartão no dispositivo.

Esse modelo ajuda a assegurar que os dados do cartão não possam ser decifrados por nenhuma parte além do Provedor do Serviço de Pagamento, que processa esta transação para o comerciante.

Como usar a Carteira da Apple

Acesso usando a Carteira da Apple

Na Carteira da Apple em dispositivos iPhone e Apple Watch compatíveis, os usuários podem armazenar as chaves da casa, de carros e de quartos de hotel. Eles podem até armazenar crachás corporativos e carteiras de estudante. Quando um usuário chega a uma porta, a chave certa é apresentada automaticamente, permitindo a entrada com apenas um toque por meio da comunicação por campo de proximidade (NFC).

Conveniência para o usuário

Quando uma chave, tíquete, carteira de estudante ou crachá corporativo são adicionados à Carteira da Apple, o Modo Expresso é ativado por padrão. Os cartões no Modo Expresso interagem com terminais compatíveis sem Face ID, Touch ID, autenticação por código ou clique duplo no botão lateral do Apple Watch. Para desativar esse recurso, os usuários podem tocar no botão Mais na frente do cartão na Carteira da Apple e desativar o Modo Expresso. Para ativar o Modo Expresso novamente, eles devem usar Face ID, Touch ID ou código.

Privacidade e segurança

As chaves na Carteira da Apple aproveitam ao máximo a privacidade e a segurança integradas ao iPhone e ao Apple Watch. Nem o horário nem o local em que uma pessoa usa suas chaves na Carteira da Apple são compartilhados com a Apple ou armazenados em servidores da Apple. Além disso, as credenciais são armazenadas com segurança dentro do Secure Element (SE) de dispositivos compatíveis. O SE possui applets especialmente projetados para gerenciar e armazenar com segurança as chaves de acesso, assegurando que elas não possam ser extraídas.

Antes da provisão de qualquer chave de acesso, um usuário deve ter uma sessão iniciada em sua conta do iCloud em um iPhone compatível, bem como ter a autenticação de dois fatores ativada para sua conta do iCloud. A exceção é no caso de uma carteira de estudante, que não exige a autenticação de dois fatores.

Quando um usuário inicia o processo de provisão, ocorrem etapas semelhantes às envolvidas na provisão de cartões de crédito e débito, como vínculo e provisão. Durante uma transação, o leitor se comunica com o Secure Element através do controlador da comunicação por campo de proximidade (NFC) usando um canal seguro estabelecido.

O número de dispositivos, incluindo o iPhone e o Apple Watch, que podem ser aprovisionados com uma chave de acesso é definido e controlado por cada parceiro e pode variar de um parceiro para outro. Essa abordagem permite que cada parceiro tenha controle sobre o número máximo de chaves de acesso aprovisionadas por tipo de dispositivo, atendendo a suas necessidades específicas. Com esse objetivo, a Apple fornece aos parceiros o tipo do dispositivo e identificadores anonimizados de dispositivos. Por motivos de privacidade e segurança, os identificadores são diferentes para cada parceiro.

Os métodos para desativar ou remover as chaves são:

- Apagar o dispositivo remotamente com o Buscar
- Ativar o Modo Perdido com o Buscar
- Receber um comando de apagamento remoto do gerenciamento de dispositivos móveis (MDM)
- Remover todos os cartões da página da conta do ID Apple
- Remover todos os cartões em iCloud.com
- Remover todos os cartões da Carteira da Apple
- Remover o cartão no app da administradora do cartão

No iOS 15.4 ou posterior, quando um usuário clica duas vezes no botão lateral de um iPhone com Face ID ou clica duas vezes no botão de Início de um iPhone com Touch ID, os tíquetes e os detalhes da chave de acesso só são mostrados depois que o usuário se autentica no dispositivo. A autenticação com Face ID, Touch ID ou código é necessária antes que informações específicas do tíquete, como os detalhes de uma reserva de hotel, sejam mostradas na Carteira da Apple.

Tipos de credenciais de acesso

Existem tipos diferentes de acesso na Carteira da Apple, como hotelaria, crachás corporativos, carteiras de estudante, chaves de casas e chaves de carros.

Hotelaria

Chaves de hotéis na Carteira da Apple ajudam a proporcionar uma experiência fácil e sem contato, do check-in ao check-out, além de garantir benefícios adicionais de privacidade e segurança para os hóspedes em relação às chaves tradicionais de cartões de plástico. Para abrir o quarto, os hóspedes de estabelecimentos compatíveis podem tocar a chave na Carteira da Apple em um iPhone e Apple Watch Series 4 ou posterior compatíveis.

Os recursos da Carteira da Apple foram feitos especificamente para facilitar a experiência do cliente:

- Provisão pelo app do hotel, antes da chegada, para adicionar um tíquete à Carteira da Apple antes da estadia
- Quadros de tíquetes de check-in, para iniciar o check-in e a atribuição de quartos na Carteira da Apple
- Atualização das chaves após a provisão, permitindo a extensão ou modificação da estadia atual
- Compatibilidade com chaves para vários quartos com apenas um tíquete na Carteira da Apple
- Arquivamento automático de chaves expiradas na Carteira da Apple

Crachás corporativos

Os crachás de funcionários de parceiros compatíveis podem ser adicionados à Carteira da Apple no iPhone e Apple Watch, fornecendo a funcionários em todo o mundo acesso por proximidade aos locais de trabalho. Para adicionar um crachá, um funcionário precisa da autenticação multifator ativada em sua conta usada para iniciar a sessão no app fornecido pelo empregador.

Os crachás de funcionários fazem uso dos recursos de acesso da Apple, permitindo aos usuários:

- Adicionar automaticamente um crachá de funcionário ao Apple Watch emparelhado por meio da provisão via push, que não exige a instalação do app de um parceiro
- Acesso integrado a comodidades do escritório usando o modo expresso
- Acesso ao local de trabalho mesmo se acabar a bateria do iPhone

Cartões de ID de estudante

No iOS 12 ou posterior, alunos, docentes e funcionários de instituições participantes podem adicionar suas carteiras de estudante à Carteira da Apple em modelos de iPhone e Apple Watch compatíveis para acessar locais e fazer pagamentos em todos os lugares onde o cartão for aceito.

Um usuário adiciona sua carteira de estudante à Carteira da Apple através de um app fornecido pelo emissor do cartão ou escola participante. O processo técnico pelo qual isso ocorre é o mesmo que o descrito na seção Adição de cartões de crédito ou débito em um app de administradora de cartões. Além disso, os apps das administradoras devem ser compatíveis com a autenticação de dois fatores nas contas que guardam o acesso às carteiras de estudante. Um cartão pode estar configurado simultaneamente em até dois dispositivos Apple compatíveis, com sessão iniciada no mesmo ID Apple.

Casas com várias famílias

Os inquilinos e a equipe de prédios parceiros compatíveis podem usar a chave de casa na Carteira da Apple para ter acesso ao prédio, apartamento e áreas comuns. A chave de casa pode ser aprovisionada no app fornecido pelo parceiro. No caso de parceiros que oferecem a provisão facilitada, os administradores do imóvel podem enviar aos inquilinos um link para iniciar a provisão usando o canal de mensagens de sua preferência (por exemplo, e-mail ou SMS), de forma que o inquilino precisa apenas clicar no link para obter a chave. Os Clipes de Apps também oferecem uma experiência segura e integrada, possibilitando a provisão de uma chave sem a instalação do app do parceiro. Para obter mais informações, consulte o artigo do Suporte da Apple Use Clipes de Apps no iPhone.

Chave da casa

Uma chave de casa na Carteira da Apple pode ser usada com fechaduras com NFC compatíveis com um simples toque em um iPhone ou Apple Watch. Para obter mais informações sobre como um usuário pode configurar e utilizar a chave de casa, consulte o artigo do Suporte da Apple Destranque a porta com uma chave de casa no iPhone.

Quando um usuário configura uma chave de casa, todos os moradores da casa também a recebem automaticamente. Para compartilhar a chave da casa com outras pessoas ou remover um membro de uma casa compartilhada, o dono da casa pode usar o app Casa para gerenciar os convites e membros. Quando um usuário opta por aceitar o convite para fazer parte de uma casa com uma chave de casa, é iniciada a provisão da chave da casa à Carteira da Apple em seus dispositivos. Se um usuário desejar sair de uma casa ou se o dono da casa retirar seu acesso, essas ações também removem a chave da casa da Carteira da Apple.

Chave do carro

O armazenamento de chaves de carro digitais na Carteira da Apple tem suporte nativo a dispositivos iPhone compatíveis e dispositivos Apple Watch emparelhados. As chaves de carro são representadas como tíquetes (criados pela Apple em nome do fabricante do automóvel) na Carteira da Apple e são compatíveis com o ciclo de vida completo do cartão Apple Pay (Modo Perdido do iCloud, Apagamento Remoto, apagamento local do tíquete e Apagar Conteúdo e Ajustes). Além do gerenciamento padrão do cartão Apple Pay, chaves de carro compartilhadas podem ser apagadas a partir do iPhone, Apple Watch e Interface Humano-Máquina (HMI) do veículo do proprietário.

Chaves de carro podem ser usadas para trancar e destrancar o veículo, e dar a partida no motor ou colocar o veículo no modo de direção. A “transação padrão” oferece autenticação mútua e é mandatória para dar a partida no motor. As transações de trancamento e destrancamento podem usar a “transação rápida” quando necessária por motivos de desempenho.

As chaves são criadas através do emparelhamento de um iPhone com um veículo compatível e de propriedade do usuário. Todas as chaves são criadas no Secure Element integrado, com base na geração de chave local (ECC-OBKG) de curva elíptica (NIST P-256), e as chaves privadas nunca saem do Secure Element. A comunicação entre os dispositivos e o veículo usa ou o padrão NFC ou uma combinação de Bluetooth LE e UWB, e o gerenciamento de chaves usa uma API do servidor entre a Apple e o fabricante do automóvel com TLS mutuamente autenticado. Depois que uma chave é emparelhada com um iPhone, qualquer Apple Watch emparelhado com esse iPhone também pode receber uma chave. Quando uma chave é apagada no veículo ou no dispositivo, ela não pode ser restaurada. As chaves em dispositivos perdidos ou roubados podem ser suspensas e retomadas, mas para provisioná-las em um novo dispositivo, é necessário um novo emparelhamento ou compartilhamento.

Segurança das chaves de carro no iOS

Os desenvolvedores podem oferecer suporte seguro a maneiras de acessar um veículo sem usar chaves em um iPhone compatível e um Apple Watch emparelhado.

Emparelhamento do proprietário

O proprietário deve provar a posse do veículo (o método depende do fabricante do automóvel) e pode iniciar o processo de emparelhamento no app do fabricante do automóvel ao usar um link no e-mail recebido do fabricante do automóvel ou a partir do menu do veículo. Em todos os casos, o proprietário deve apresentar uma senha de emparelhamento de uso único confidencial ao iPhone, que é usada para gerar um canal de emparelhamento seguro através do protocolo SPAKE2+ com curva NIST P-256. Ao usar o app ou o link no e-mail, a senha é transferida automaticamente para o iPhone, no qual, ao iniciar o emparelhamento a partir do veículo, ela deve ser digitada manualmente.

Compartilhamento de chave

O iPhone emparelhado do proprietário pode compartilhar chaves com dispositivos iPhone de membros da família e amigos elegíveis (e seus dispositivos Apple Watch emparelhados) ao enviar um convite específico ao dispositivo via iMessage e o Serviço de Identidade da Apple (IDS). A troca de todos os comandos de compartilhamento usa o recurso IDS criptografado de ponta a ponta. O iPhone emparelhado do proprietário mantém a imutabilidade do canal IDS durante o processo de compartilhamento para se proteger contra o encaminhamento de convites.

Ao aceitar o convite, o iPhone do membro da família ou amigo cria uma chave digital e envia a cadeia de certificado de criação de chave de volta ao iPhone emparelhado do proprietário para verificar que a chave foi criada em um dispositivo Apple autêntico. O iPhone emparelhado do proprietário assina a chave ECC pública do iPhone do membro da família ou amigo e envia a assinatura de volta ao iPhone do membro da família ou amigo. A operação de assinatura no dispositivo do proprietário requer a autenticação do usuário (Face ID, Touch ID ou digitação de código) e uma intenção segura do usuário, descrita em Usos do Face ID e Touch ID. A autorização é solicitada ao enviar o convite e armazenada no Secure Element para consumo quando o dispositivo do amigo envia o pedido de assinatura de volta. Os direitos da chave são fornecidos ao veículo de forma on-line pelo servidor OEM do veículo ou na primeira vez que a chave compartilhada é usada no veículo.

Apagamento de chaves

Chaves podem ser apagadas no dispositivo de quem possui as chaves a partir do dispositivo do proprietário e no veículo. Os apagamentos no iPhone de quem possui a chave têm efeito imediato, mesmo que a pessoa que possua a chave a esteja usando. Portanto, um aviso contundente é mostrado antes do apagamento. O apagamento de chaves no veículo pode ser possível a qualquer momento ou pode ser possível apenas quando o veículo está on-line.

Em ambos os casos, o apagamento no dispositivo de quem possui as chaves ou veículo é comunicado a um servidor de inventário de chaves (KIS) no lado do fabricante do automóvel, o qual registra as chaves emitidas para um veículo para fins de seguro.

O proprietário pode solicitar um apagamento a partir do verso do tíquete de proprietário. O pedido é enviado primeiro para o fabricante do automóvel para a remoção da chave no veículo. As condições para remover a chave do veículo são definidas pelo fabricante do automóvel. Apenas quando a chave é removida no veículo, o servidor do fabricante do automóvel envia um pedido de término remoto para o dispositivo que possui a chave.

Quando uma chave é eliminada em um dispositivo, o applet que gerencia as chaves digitais de carros cria um atestado de término criptograficamente assinado, o qual é usado como prova de apagamento pelo fabricante do automóvel e usado para remover a chave do KIS.

Transações com o padrão NFC

No caso de veículos com uma chave NFC, um canal seguro entre o leitor e um iPhone é iniciado por meio da geração de pares de chaves efêmeras no leitor e no iPhone. Ao usar um método de acordo de chaves, um segredo compartilhado pode ser derivado em ambos os lados e usado para gerar uma chave simétrica compartilhada com Diffie-Hellman, uma função de derivação de chaves e assinaturas a partir da chave de longo prazo estabelecida durante o emparelhamento.

A chave pública efêmera gerada no lado do veículo é assinada com a chave privada de longo prazo do leitor, o que resulta na autenticação do leitor pelo iPhone. Da perspectiva do iPhone, esse protocolo é projetado para impedir que dados sensíveis e privados sejam revelados a um adversário que intercepte a comunicação.

Por fim, o iPhone usa o canal seguro estabelecido para criptografar seu identificador de chave pública junto com a assinatura calculada em um desafio derivado de dados do leitor e alguns dados adicionais específicos do app. Essa verificação da assinatura do iPhone pelo leitor permite que o leitor autentique o dispositivo.

Transações rápidas

O iPhone gera um criptograma baseado em um segredo compartilhado anteriormente durante uma transação padrão. Esse criptograma permite que o veículo autentique rapidamente o dispositivo em cenários em que o desempenho deva ser considerado. Opcionalmente, um canal seguro entre o veículo e o dispositivo é estabelecido ao derivar chaves de sessão de um segredo compartilhado anteriormente durante uma transação padrão e um novo par de chaves efêmeras. A capacidade do veículo em estabelecer o canal seguro autentica o veículo perante o iPhone.

Transações com o padrão BLE/UWB

No caso de veículos com uma chave UWB, um sessão Bluetooth LE é estabelecida entre o veículo e o iPhone. De forma semelhante à transação NFC, um segredo compartilhado é derivado em ambos os lados e utilizado para estabelecer uma sessão segura. Essa sessão é usada para, a seguir, derivar e combinar uma Chave Secreta de Alcance UWB (URSK, na sigla em inglês). A URSK é fornecida a rádios UWB no dispositivo do usuário e no veículo para possibilitar a localização precisa do dispositivo em uma posição específica próxima ao veículo ou dentro dele. O veículo utiliza a posição do dispositivo para decidir se permite o destravamento ou a partida no veículo. As URSKs têm um TTL predefinido. Para evitar a interrupção da medição da localização quando o TTL expira, as URSKs podem ser derivadas previamente no SE do dispositivo e no HSM/SE do veículo enquanto a localização segura não está ativada mas o BLE está conectado. Isso evita a necessidade de uma transação padrão para derivar uma nova URSK em uma situação em que o tempo seja essencial. A URSK derivada previamente pode ser transferida muito rapidamente aos rádios UWB do carro e do dispositivo para evitar a interrupção da localização via UWB.

Privacidade

O servidor de inventário de chaves (KIS, na sigla em inglês) do fabricante do automóvel não armazena o ID, SEID ou ID Apple do dispositivo. Ele armazena apenas um identificador mutável, a instância do identificador de AC. Esse identificador não está associado a nenhum dado privado no dispositivo ou no servidor e é apagado quando o usuário apaga o dispositivo completamente (ao usar Apagar Todo o Conteúdo e Ajustes).

Adição de cartões de transporte público e eMoney à Carteira da Apple

Em vários mercados do mundo, os usuários podem adicionar cartões de transporte público e eMoney compatíveis à Carteira da Apple em modelos de iPhone e Apple Watch compatíveis. Dependendo da operadora, o usuário pode transferir o valor ou o bilhete único de transporte público (ou ambos) de um cartão físico para representações digitais na Carteira da Apple, ou fornecer um novo cartão de transporte público ou eMoney ao app Carteira a partir da Carteira da Apple ou do app da administradora do cartão. Após a adição dos cartões de transporte público à Carteira da Apple, basta que os usuários mantenham o iPhone ou o Apple Watch próximo ao leitor para usar o transporte público. Alguns cartões de transporte público também podem ser usados para fazer pagamentos.

Como funcionam os cartões de transporte público e eMoney

Os cartões de transporte público e eMoney adicionados são associados à conta do iCloud do usuário. Se o usuário adicionar mais de um cartão à Carteira da Apple, a Apple ou a administradora do cartão podem conseguir associar as informações pessoais do usuário às informações de conta dos cartões. Os cartões de transporte público e eMoney e as transações são protegidas por um conjunto de chaves criptográficas hierárquicas.

Durante o processo de transferência do saldo do cartão físico para a Carteira da Apple, o usuário é solicitado a digitar informações específicas do cartão. Também pode ser necessário que os usuários forneçam informações pessoais como comprovante da propriedade do cartão. Ao transferir tíquetes do iPhone para o Apple Watch, ambos os dispositivos devem estar online.

O saldo pode ser recarregado com fundos de cartões de crédito, débito e pré-pagos por meio da Carteira da Apple ou a partir do app da administradora do cartão de transporte público ou cartão eMoney. Para entender a segurança da recarga do saldo ao usar o Apple Pay, consulte Pagamento com cartões dentro de apps. Para saber como o cartão é aprovisionado a partir do app da administradora do cartão, consulte Adição de cartões de crédito ou débito em um app de administradora de cartões.

Se for possível fazer o provisionamento a partir de um cartão físico, a administradora do cartão de transporte público ou eMoney possui as chaves criptográficas necessárias para autenticar o cartão físico e verificar os dados digitados pelo usuário. Depois de verificar os dados, o sistema cria um Número de Conta do Dispositivo para o Secure Element e ativa o tíquete recém-adicionado na Carteira da Apple com o saldo transferido. No caso de alguns cartões, após a conclusão do provisionamento com o cartão físico, ele é desativado.

No final de qualquer um dos tipos de provisionamento, se o saldo do cartão estiver armazenado no dispositivo, ele é criptografado e armazenado em um applet designado no Secure Element. A operadora possui as chaves para realizar operações criptográficas nos dados do cartão para transações de saldo.

Por padrão, os usuários de cartões de transporte público se beneficiam da experiência integrada do Transporte Público Expresso, o que permite que paguem e usem transportes públicos sem exigir Face ID, Touch ID ou código. Informações como estações visitadas recentemente, histórico de transações e tíquetes adicionais podem ser acessadas por qualquer leitor de cartão por proximidade por perto com o Modo Expresso ativado. Os usuários podem desativar o Transporte Público Expresso para ativar o requisito de autorização com Face ID, Touch ID ou código nos ajustes "Carteira e Apple Pay". Os cartões eMoney não são compatíveis com o modo expresso.

Assim como com outros cartões do Apple Pay, os usuários podem suspender ou remover cartões eMoney, bastando:

- Apagar o dispositivo remotamente com o Buscar
- Ativar o Modo Perdido com o Buscar
- Digitar um comando de apagamento remoto do gerenciamento de dispositivos móveis (MDM)
- Remover todos os cartões da página da conta do ID Apple
- Remover todos os cartões em iCloud.com
- Remover todos os cartões da Carteira da Apple
- Remover o cartão no app da administradora do cartão

Os servidores do Apple Pay notificam a operadora do cartão para suspender ou desativar esses cartões. Se o usuário remover um cartão de transporte público ou eMoney de um dispositivo on-line, ele pode adicioná-lo novamente a um dispositivo com sessão iniciada com o mesmo ID Apple para recuperar o saldo. Se o dispositivo estiver off-line, desligado ou inutilizável, a recuperação pode não ser possível.

Adição de cartões de transporte público e eMoney ao Apple Watch de um membro da família

No iOS 15 e watchOS 8, o organizador de uma família do iCloud pode adicionar cartões de transporte público e eMoney aos dispositivos Apple Watch dos membros da família por meio do app Apple Watch do iPhone deles. Ao aprovisionar um desses cartões ao Apple Watch de um membro da família, o dispositivo deve estar próximo e conectado ao iPhone do organizador por meio de Wi-Fi ou Bluetooth. Para isso ocorrer, os membros da família precisam ter a autenticação de dois fatores ativada para seus IDs Apple.

Os membros da família podem usar o iMessage no Apple Watch para enviar uma solicitação de adição de dinheiro a um cartão de transporte público ou eMoney. O conteúdo da mensagem é protegido por criptografia de ponta a ponta, conforme descrito em Visão geral da segurança do iMessage. A adição de dinheiro a um cartão no Apple Watch de um membro da família pode ser feita remotamente por uma conexão Wi-Fi ou celular. A proximidade não é necessária.

Nota: esse recurso pode não estar disponível em todos os países ou regiões.

Cartões de crédito e débito

Em algumas cidades, leitores de transporte público aceitam cartões EMV (inteligentes) para pagar a tarifa de transportes públicos. Quando usuários apresentam um cartão EMV de crédito ou débito a esses leitores, a autenticação do usuário é solicitada, da mesma maneira que em "Pague com cartões de crédito e débito em lojas".

No iOS 12.3 ou posterior, alguns cartões EMV de crédito/débito existentes na Carteira da Apple podem ser ativados para o Transporte Público Expresso. Com o Transporte Público Expresso, os usuários podem pagar uma viagem em operadoras de transporte público compatíveis sem precisar de Face ID, Touch ID ou código. Quando o usuário aprovisiona um cartão EMV de crédito ou débito, o primeiro cartão aprovisionado na Carteira da Apple é ativado para o Transporte Público Expresso. Para desativar o Transporte Público Expresso desse cartão, o usuário pode tocar no botão Mais na frente do cartão na Carteira da Apple e definir "Ajustes de Transporte Público Expresso" como Nenhum. O usuário também pode usar a Carteira da Apple para selecionar um cartão de crédito ou débito diferente como seu cartão de Transporte Público Expresso. O Face ID, Touch ID ou código são exigidos para reativar ou selecionar um cartão diferente para o Transporte Público Expresso.

O Apple Card e o Apple Cash são qualificados para o Transporte Público Expresso.

Documentos de identidade na Carteira da Apple

No iPhone 8 ou posterior com iOS 15.4 ou posterior e no Apple Watch Series 4 ou posterior com watchOS 8.4 ou posterior, os usuários podem adicionar documentos de identidade estaduais ou carteiras de habilitação à Carteira da Apple e tocar no iPhone ou Apple Watch para apresentá-los de forma integrada e segura em locais participantes.

Nota: este recurso está disponível somente em estados participantes dos EUA.

Os documentos de identidade na Carteira da Apple usam recursos de segurança integrados ao hardware e software do dispositivo do usuário para ajudar a proteger sua identidade e suas informações pessoais.

Adição de uma carteira de habilitação ou documento de identidade estadual à Carteira da Apple

No iPhone, basta tocar no botão Adicionar (+) na parte superior da tela na Carteira da Apple para começar a adicionar a carteira ou documento de identidade. Se os usuários tiverem um Apple Watch emparelhado no momento da configuração, também são solicitados a adicionar a carteira de habilitação ou documento de identidade à Carteira da Apple no Apple Watch.

Primeiro, os usuários são solicitados a usar o iPhone para digitalizar a frente e o verso do documento físico. O iPhone avalia a qualidade e o tipo das imagens para ajudar a assegurar que as imagens fornecidas sejam consideradas aceitáveis pela autoridade emissora do documento. Essas imagens do documento de identidade são criptografadas para a chave da autoridade emissora no dispositivo e enviadas a essa autoridade.

Em seguida, o usuário é solicitado a realizar uma série de movimentos com o rosto e a cabeça. Esses movimentos são avaliados pelo dispositivo do usuário e pela Apple para ajudar a reduzir o risco de que alguém esteja usando uma foto, vídeo ou máscara para tentar adicionar o documento de outra pessoa à Carteira da Apple. O resultado da análise desses movimentos é enviado à autoridade estadual, mas não o vídeo dos movimentos em si.

Para ajudar a assegurar que a pessoa que está adicionando o documento de identidade à Carteira da Apple seja a mesma à qual o pertence documento, os usuários são solicitados a tirar uma selfie. Antes que a foto do usuário seja enviada à autoridade estadual, os servidores da Apple e o dispositivo do usuário comparam a foto com a aparência da pessoa que realizou a série de movimentos com o rosto e a cabeça, ajudando a garantir que a foto a ser enviada é de uma pessoa viva com a mesma aparência da pessoa no documento. Depois de feita a comparação, a foto é criptografada no dispositivo e enviada à autoridade do estado emissor para ser comparada com a imagem do documento de identidade contida nos arquivos da autoridade.

Por fim, os usuários são solicitados a realizar uma autenticação com Face ID ou Touch ID. O dispositivo do usuário vincula essa única biometria do Face ID ou Touch ID ao documento de identidade para ajudar a assegurar que somente a pessoa que adicionou o documento a este iPhone possa apresentá-lo. As outras informações biométricas registradas não podem ser usadas para autorizar a apresentação do documento. Isso ocorre estritamente no dispositivo, não sendo enviado à autoridade que emitiu o documento.

A autoridade emissora receberá as informações necessárias para configurar o documento digital. Isso inclui imagens da frente e do verso do documento do usuário e dados lidos do código de barras PDF417, além da selfie tirada pelo usuário durante o processo de verificação da identidade. O estado emissor também recebe um valor de um dígito, usado no combate a fraude, baseado nos padrões de uso do dispositivo do usuário, nos dados de ajustes e em informações sobre o ID Apple pessoal do usuário. Por fim, fica a cargo do estado aprovar ou negar o documento sendo adicionado à Carteira da Apple.

Depois que a autoridade emissora autorizar a adição do documento de identidade ou carteira de habilitação à Carteira da Apple, um par de chaves é gerado no Secure Element pelo iPhone, ancorando o documento do usuário àquele dispositivo específico. Caso o documento esteja sendo adicionado ao Apple Watch, um par de chaves é gerado no Secure Element pelo Apple Watch.

Depois que o documento está no iPhone, as informações apresentadas no documento do usuário na Carteira da Apple são armazenadas em um formato criptografado protegido pelo Secure Enclave.

Uso de uma carteira de habilitação ou documento de identidade estadual na Carteira da Apple

Para usar o documento na Carteira da Apple, os usuários precisam se autenticar no dispositivo com Face ID ou Touch ID associado ao documento na Carteira da Apple antes do iPhone apresentar as informações ao leitor de identidade.

Para usar o documento na Carteira da Apple no Apple Watch, os usuários precisam desbloquear o iPhone usando a aparência do Face ID ou impressão digital do Touch ID associados, a cada vez que colocam o Apple Watch. Dessa forma, eles podem usar o documento na Carteira da Apple sem se autenticar até tirarem o Apple Watch novamente. Essa funcionalidade faz uso de recursos básicos do Desbloqueio Automático detalhados em Segurança do sistema para o watchOS.

Quando os usuários seguram o iPhone ou Apple Watch perto do leitor de identidade, eles veem uma solicitação no dispositivo mostrando quais informações específicas estão sendo solicitadas, por quem e se há a intenção de armazená-las. Depois de autorizar com o Face ID ou Touch ID associado, as informações de identificação solicitadas são liberadas no dispositivo.

Importante: os usuários não precisam desbloquear, mostrar ou entregar o dispositivo para apresentar o documento.

Se os usuários tiverem um recurso de acessibilidade como Controle por Voz, Controle Assistivo ou AssistiveTouch em vez de terem o Face ID ou o Touch ID ativado, eles podem usar o código para acessar e apresentar suas informações.

A transmissão dos dados da identidade ao leitor de identidade segue o padrão ISO/IEC 18013-5, que fornece diversos mecanismos de segurança capazes de detectar, impedir e mitigar riscos de segurança. Eles consistem em integridade e antifalsificação de dados de identificação, vinculação de dispositivos, consentimento informado e confidencialidade dos dados do usuário em links de rádio.

Integridade e antifalsificação dos dados de identificação

Os documentos na Carteira da Apple usam uma assinatura fornecida pela autoridade emissora, permitindo que qualquer leitor compatível com ISO/IEC 18013-5 verifique o documento de um usuário na Carteira da Apple. Além disso, todos os elementos dos dados do documento na Carteira são protegidos individualmente contra falsificação. Isso permite que o leitor da identidade solicite um subconjunto específico de elementos dos dados presentes no documento na Carteira da Apple e que o documento na Carteira da Apple responda com o mesmo subconjunto, dessa forma compartilhando somente os dados solicitados e protegendo ao máximo a privacidade do usuário.

Vinculação de dispositivos

A autenticação de documentos de identidade na Carteira da Apple usa uma assinatura do dispositivo para proteção contra a clonagem de um documento e a reprodução de uma transação de identificação. Com o armazenamento da chave privada para autenticação do documento no Secure Element do dispositivo iPhone, o documento fica vinculado ao mesmo dispositivo para o qual a autoridade emissora criou o documento.

Consentimento informado

Os leitores de identidade para documentos na Carteira da Apple são autenticados por meio do protocolo definido no padrão ISO/IEC 18013-5. Durante a apresentação, um ícone derivado do certificado do leitor é mostrado, para assegurar o usuário de que está interagindo com a parte pretendida.

Confidencialidade dos dados do usuário em links de rádio

A criptografia da sessão ajuda a assegurar que todas as informações de identificação pessoal (PII) trocadas entre o documento na Carteira da Apple e o leitor de identidade sejam criptografadas. A criptografia é realizada pela camada de aplicativo. Portanto, a segurança da sessão não depende da segurança fornecida pela camada de transmissão (por exemplo, NFC, Bluetooth e Wi-Fi).

Os documentos de identidade na Carteira da Apple ajudam a manter privadas as informações dos usuários

Os documentos de identidade na Carteira da Apple aderam ao processo de “recuperação de dispositivo”, descrito no padrão ISO/IEC 18013-5. A recuperação de dispositivo evita a necessidade de chamadas ao servidor durante a apresentação, protegendo assim os usuários contra rastreamento da Apple e da autoridade emissora.

iMessage

Visão geral da segurança do iMessage

O iMessage da Apple é um serviço de mensagens para dispositivos iOS e iPadOS, Apple Watch e computadores Mac. O iMessage oferece suporte a texto e anexos, como fotos, contatos, localizações, links e anexos diretamente em uma mensagem, como um ícone de sinal de positivo. As mensagens aparecem em todos os dispositivos registrados de um usuário para que a conversa possa ser continuada em qualquer um deles. O iMessage faz amplo uso do serviço de Notificações Push da Apple (APNs). A Apple não registra o conteúdo de mensagens ou anexos, que são protegidos por criptografia de ponta a ponta, para que ninguém, exceto o remetente e o destinatário, possa acessá-los. A Apple não pode descriptografar os dados.

Quando um usuário ativa o iMessage em um dispositivo, o dispositivo gera pares de chaves de criptografia e assinatura para uso com o dispositivo. Para criptografia, há uma chave de criptografia RSA de 1280 bits assim como uma chave de criptografia EC de 256 bits na curva NIST P-256. Para assinaturas, chaves de assinatura de 256 bits do Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA) são usadas. As chaves privadas são salvas nas chaves do dispositivo e ficam disponíveis apenas após o primeiro desbloqueio. As chaves públicas são enviadas para o Serviço de Identidade da Apple (IDS), onde são associadas ao número de telefone ou endereço de e-mail do usuário, juntamente ao endereço APNs do dispositivo.

Conforme os usuários adicionam dispositivos para uso no iMessage, suas chaves de criptografia e assinatura pública, endereços APNs e números de telefone associados são adicionados ao serviço de diretório. Os usuários também podem adicionar outros endereços de e-mail, que são verificados através do envio de um link de confirmação. Os números de telefone são verificados pela rede e SIM da operadora. Em algumas redes, isso requer o uso de SMS (um diálogo de confirmação é apresentado ao usuário se o SMS tiver custo). A verificação do número de telefone pode ser exigida para vários serviços do sistema além do iMessage, como FaceTime e iCloud. Todos os dispositivos registrados do usuário exibem uma mensagem de alerta quando um novo dispositivo, número de telefone ou endereço de e-mail é adicionado.

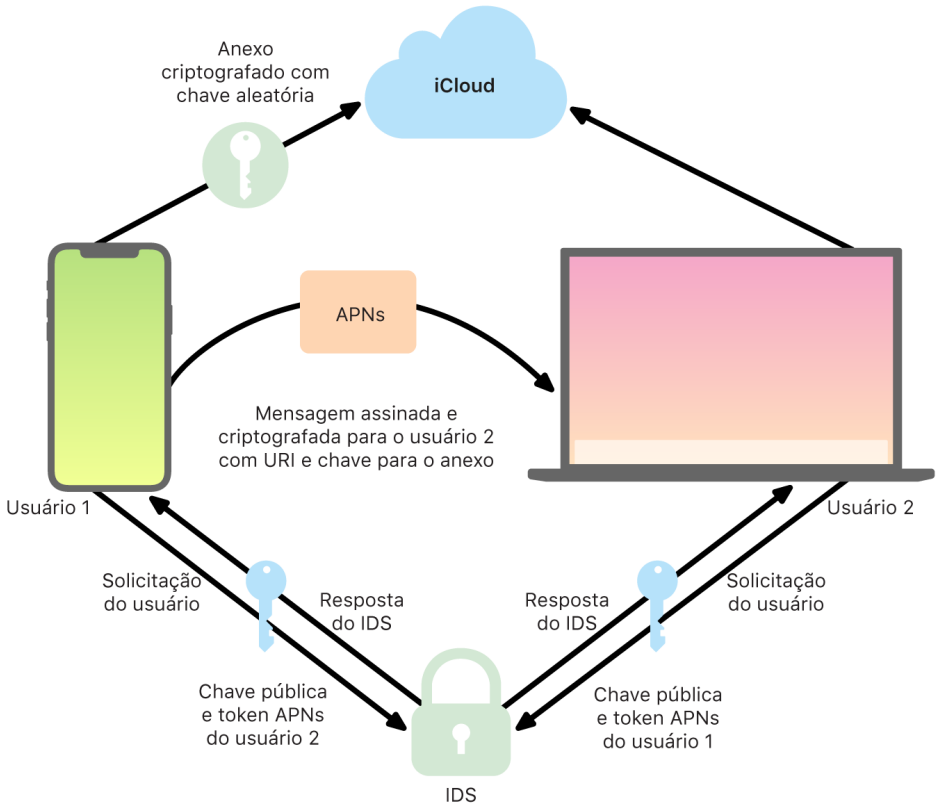
Como o iMessage envia e recebe mensagens com segurança

Para iniciar uma nova conversa do iMessage, os usuários digitam um endereço ou nome. Se um número de telefone ou endereço de e-mail for digitado, o dispositivo contata o Serviço de Identidade da Apple (IDS) para obter as chaves públicas e endereços do APNs de todos os dispositivos associados ao destinatário. Se o usuário digitar um nome, primeiro o dispositivo usa o app Contatos do usuário para coletar números de telefone e endereços de e-mail associados ao nome para depois obter as chaves públicas e endereços APNs do IDS.

A mensagem sendo enviada é criptografada individualmente para cada um dos dispositivos do destinatário. As chaves públicas de criptografia e assinatura dos dispositivos de destino são obtidas do IDS. Para cada dispositivo de destino, o dispositivo remetente gera um valor de 88 bits aleatório e o usa como uma chave HMACSHA256 para construir um valor de 40 bits derivado das chaves públicas do remetente e do destinatário e do texto simples. A concatenação dos valores de 88 bits e 40 bits cria uma chave de 128 bits, que usa AES para criptografar a mensagem no Modo de Contagem (CTR). O valor de 40 bits é usado pelo lado do destinatário para verificar a integridade do texto simples descriptografado. Essa chave AES única por mensagem é criptografada à chave pública do dispositivo de destino usando RSA-OAEP. Depois, o hash SHA-1 é aplicado à combinação do texto e da chave da mensagem criptografada, e o hash é assinado com o Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA) usando a chave de assinatura privada do dispositivo de envio. No iOS 13 ou posterior e iPadOS 13.1 ou posterior, dispositivos podem usar uma criptografia de Esquema de Criptografia Integrada de Curva Elíptica (ECIES) em vez da criptografia RSA.

As mensagens resultantes, uma para cada dispositivo de destino, consistem no texto da mensagem criptografada, chave da mensagem criptografada e assinatura digital do remetente. Elas então são despachadas para o APNs para entrega. Metadados, como a marca temporal e informações de roteamento do APNs, não são criptografados. A comunicação com o APNs é criptografada usando um canal TLS de encaminhamento secreto.

O APNs só pode transmitir mensagens de até 4 KB ou 16 KB, dependendo da versão do iOS ou iPadOS. Se a mensagem de texto for muito longa ou se um anexo (como uma foto) estiver incluído, o anexo é criptografado com AES no modo CTR com uma chave de 256 bits gerada aleatoriamente e enviado para o iCloud. A chave AES do anexo, seu Identificador Uniforme de Recursos (URI) e um hash SHA-1 de sua forma criptografada são enviados para o destinatário na forma de conteúdo de uma iMessage, com suas confidencialidade e integridade protegidas através da criptografia normal do iMessage, como mostrado no diagrama a seguir.



Nas conversas em grupo, este processo é repetido para cada destinatário e seus dispositivos.

No lado recipiente, cada dispositivo recebe sua cópia da mensagem do APNs e, se necessário, obtém o anexo do iCloud. O número de telefone ou endereço de e-mail do remetente é correspondido ao contato do destinatário para que um nome seja exibido, quando possível.

Assim como em todas as notificações push, a mensagem é apagada do APNs quando entregue. No entanto, ao contrário de outras notificações push, as mensagens do iMessage são colocadas em fila para entrega a dispositivos off-line. As mensagens são armazenadas nos servidores da Apple por até 30 dias.

Compartilhamento seguro de nome e foto do iMessage

O compartilhamento de nomes e fotos no iMessage permite que os usuários compartilhem nomes e fotos no iMessage. O usuário pode selecionar informações do “Meu Cartão” ou personalizar o nome e incluir qualquer imagem que desejar. O compartilhamento de nomes e fotos no iMessage usa um sistema de dois estágios para distribuir o nome e a foto.

Os dados são subdivididos em campos, cada um criptografado e autenticado separadamente, e autenticados em conjunto com o processo a seguir. Há três campos:

- Nome
- Foto
- Nome do arquivo da foto

Uma das primeiras etapas da criação de dados é a geração aleatória de uma chave de registro de 128 bits no dispositivo. Em seguida, essa chave de registro é derivada com HKDF-HMAC-SHA256 para criar três subchaves: Chave 1:Chave 2:Chave 3 = HKDF(chave de registro, “apelidos”). Para cada campo, um Vetor de Inicialização (VI) aleatório de 96 bits é gerado e os dados são criptografados com AES-CTR e a Chave 1. Em seguida, um código de autenticação de mensagem (MAC) é calculado com HMAC-SHA256 usando a Chave 2 e abrangendo o nome, o campo IV e o texto cifrado do campo. Por último, o conjunto de valores MAC dos campos individuais é concatenado e seu MAC é calculado com HMAC-SHA256 usando a Chave 3. O MAC de 256 bits é armazenado juntamente com os dados criptografados. Os primeiros 128 bits desse MAC são usados como o ID de Registro.

O registro criptografado é armazenado no banco de dados público do CloudKit com esse ID de Registro. Esse registro nunca é alterado e, sempre que o usuário resolve mudar seu nome e foto, um novo registro criptografado é gerado. Quando o usuário 1 resolve compartilhar seu nome e foto com o usuário 2, ele envia a chave de registro juntamente com o ID de Registro dentro do payload do iMessage, o qual é criptografado.

Quando o dispositivo do usuário 2 recebe esse payload do iMessage, ele percebe que o payload contém um ID de Registro e chave de Apelido e Foto. O dispositivo do usuário 2 acessa o banco de dados público do CloudKit para obter o nome e a foto criptografados no ID de Registro e os envia pelo iMessage.

Depois que mensagem é obtida, o dispositivo do usuário 2 descriptografa o payload e verifica a assinatura usando o próprio ID de Registro. Depois desse estágio, o nome e a foto são apresentados ao usuário 2, que pode optar por adicioná-los aos seus contatos ou usá-los no app Mensagens.

Proteção do Apple Messages for Business

O Apple Messages for Business é um serviço de mensagens que permite que usuários usem o app Mensagens para se comunicarem com uma empresa. Com o Apple Messages for Business, o usuário sempre está no controle da conversa. Ele também pode apagar a conversa e bloquear a empresa para não receber mensagens dela no futuro. Para ter privacidade, a empresa não recebe o número de telefone, endereço de e-mail ou informações da conta do iCloud do usuário. Em vez disso, um identificador exclusivo personalizado, chamado *ID Opaco*, é gerado pelo Serviço de Identidade da Apple (IDS) e compartilhado com a empresa. O ID Opaco é exclusivo ao relacionamento entre o ID Apple do usuário e o ID de Empresa da empresa. Um usuário tem um ID Opaco diferente para cada empresa com a qual se comunica com o Apple Messages for Business. O usuário decide se e quando deseja compartilhar informações de identificação pessoal com a empresa e o serviço do Apple Messages for Business nunca armazena o histórico de conversas.

O Apple Messages for Business é compatível com IDs Apple Gerenciados do Apple Business Manager e determina se eles estão ativados para o iMessage e FaceTime no Apple School Manager.

As mensagens enviadas à empresa são criptografadas entre o dispositivo do usuário e os servidores de mensagens da Apple, usando a mesma segurança e servidores de mensagens da Apple que o iMessage. Os servidores de mensagens da Apple descriptografam essas mensagens na RAM e as retransmitem à empresa por um link criptografado que usa TLS 1.2. As mensagens nunca são armazenadas sem criptografia ao transitar pelo serviço do Apple Messages for Business. As respostas das empresas também usam TLS 1.2 para o envio aos servidores de mensagens da Apple, onde são criptografadas com as chaves públicas exclusivas de cada dispositivo destinatário.

Se os dispositivos do usuário estiverem on-line, a mensagem é entregue imediatamente e não é armazenada em cache nos servidores de mensagens da Apple. Se o dispositivo do usuário não estiver on-line, a mensagem criptografada é armazenada em cache por até 30 dias para permitir que o usuário a receba quando o dispositivo estiver on-line novamente. Assim que o dispositivo estiver on-line novamente, a mensagem é entregue e apagada do armazenamento em cache. Depois de 30 dias, uma mensagem não entregue armazenada em cache expira e é apagada permanentemente.

Segurança do FaceTime

O FaceTime é o serviço de ligações de vídeo e áudio da Apple. De maneira similar ao iMessage, o FaceTime usa o serviço de Notificações Push da Apple (APNs) para estabelecer uma conexão inicial aos dispositivos registrados do usuário. O conteúdo de áudio/vídeo de ligações do FaceTime é protegido por criptografia de ponta a ponta, para que ninguém, exceto o remetente e o destinatário, possa acessá-lo. A Apple não pode descriptografar os dados.

A conexão inicial do FaceTime é feita através de uma infraestrutura de servidores da Apple, que retransmite pacotes de dados entre os dispositivos registrados do usuário. Através do uso de notificações APNs e mensagens STUN (Session Traversal Utilities for NAT) pela conexão de retransmissão, os dispositivos verificam seus certificados de identidade e estabelecem um segredo compartilhado para cada sessão. O segredo compartilhado é usado para derivar chaves de sessão para os canais de mídia transmitidos através do SRTP (Secure Real-time Transport Protocol). Os pacotes SRTP são criptografados com AES256 em Counter Mode e autenticados com HMAC-SHA1. Depois da conexão inicial e da configuração de segurança, o FaceTime usa STUN e ICE (Internet Connectivity Establishment) para estabelecer uma conexão peer-to-peer entre os dispositivos, se possível.

O FaceTime em Grupo estende o FaceTime para oferecer suporte a até 33 participantes simultâneos. Assim como no FaceTime clássico entre dois usuários, as ligações são criptografadas entre os dispositivos dos participantes convidados. Embora o FaceTime em Grupo reutilize a maior parte da infraestrutura e design do FaceTime entre dois usuários, essas ligações em grupo contam com um mecanismo de estabelecimento de chaves construído sobre a autenticidade oferecida pelo Serviço de Identidade da Apple (IDS). Esse protocolo proporciona sigilo avançado, o que significa que o comprometimento do dispositivo de um usuário não permitirá o vazamento do conteúdo de ligações anteriores. As chaves da sessão são embaladas por meio de AES-SIV e são distribuídas entre os participantes usando uma construção ECIES com chaves transitórias P-256 ECDH.

Quando um novo número de telefone ou endereço de e-mail é adicionado a uma ligação em andamento do FaceTime em Grupo, os dispositivos ativos estabelecem novas chaves de mídia e nunca compartilham chaves usadas anteriormente com os dispositivos recém-convidados.

Buscar

Segurança do Buscar

O app Buscar para dispositivos Apple possui uma base de criptografia avançada de chave pública.

Visão geral

O app Buscar combina o Buscar iPhone e o Buscar Amigos em um único app no iOS, iPadOS e macOS. O Buscar pode ajudar usuários a localizar um dispositivo perdido — e até um Mac que esteja off-line. Um dispositivo on-line pode simplesmente comunicar sua localização ao usuário via iCloud. Para funcionar off-line, o Buscar envia sinais Bluetooth de curto alcance do dispositivo perdido, os quais podem ser detectados por outros dispositivos Apple sendo usados por perto. Esses dispositivos por perto retransmitem a localização detectada do dispositivo perdido para o iCloud, de forma que usuários possam localizá-lo no app Buscar — ao mesmo tempo em que protege a privacidade e segurança de todos os usuários envolvidos. O Buscar funciona até mesmo com um Mac que esteja off-line e em repouso.

Ao usar Bluetooth e com milhões de dispositivos iOS, iPadOS e macOS sendo usados em todo o mundo, um usuário pode localizar seu dispositivo perdido, mesmo que o dispositivo não consiga se conectar a uma rede Wi-Fi ou celular. Qualquer dispositivo iOS, iPadOS ou macOS que possui a "busca off-line" ativada nos ajustes do Buscar pode funcionar como um "dispositivo localizador". Isso significa que o dispositivo pode usar Bluetooth para detectar a presença de outro dispositivo off-line perdido e usar sua conexão de rede para informar ao proprietário uma localização aproximada. Quando um dispositivo tem a busca off-line ativada, ele também pode ser localizado por outros participantes da mesma maneira. Toda essa interação é criptografada de ponta a ponta, anônima e feita para ser eficiente no consumo da bateria e no uso dos dados. O impacto na duração da bateria e no uso do plano de dados celulares é mínimo, e a privacidade do usuário fica mais protegida.

Nota: o Buscar pode não estar disponível em todos os países ou regiões.

Criptografia de ponta a ponta

O Buscar possui uma base de criptografia avançada de chave pública. Quando a busca off-line está ativada nos ajustes do Buscar, um par de chaves de criptografia privada de curva elíptica (EC) P-224 indicado por {d,P} é gerado diretamente no dispositivo, em que *d* é a chave privada e *P* a chave pública. Além disso, um SK_0 secreto de 256 bits e um contador $_i$ são inicializados como zero. O par privado de chaves e o segredo nunca são enviados à Apple, sendo sincronizados apenas entre os outros dispositivos do usuário com criptografia de ponta a ponta, usando as Chaves do iCloud. O segredo e o contador são usados para derivar a chave simétrica atual SK_i com esta construção recursiva: $SK_i = KDF(SK_{i-1}, \text{"update"})$.

Com base na chave SK_i, dois inteiros grandes u_i e v_i são calculados com $(u_i,v_i) = KDF(SK_i, \text{"diversify"})$. Tanto a chave privada P-224, chamada *d*, como a chave pública correspondente, chamada *P*, são então derivadas em uma relação afim que envolve os dois números inteiros para calcular um par de chaves de vida curta: a chave privada derivada é d_i, em que $d_i = u_i * d + v_i$ (módulo da ordem da curva P-224) e a parte pública correspondente é P_i e verifica que $P_i = u_i*P + v_i*G$.

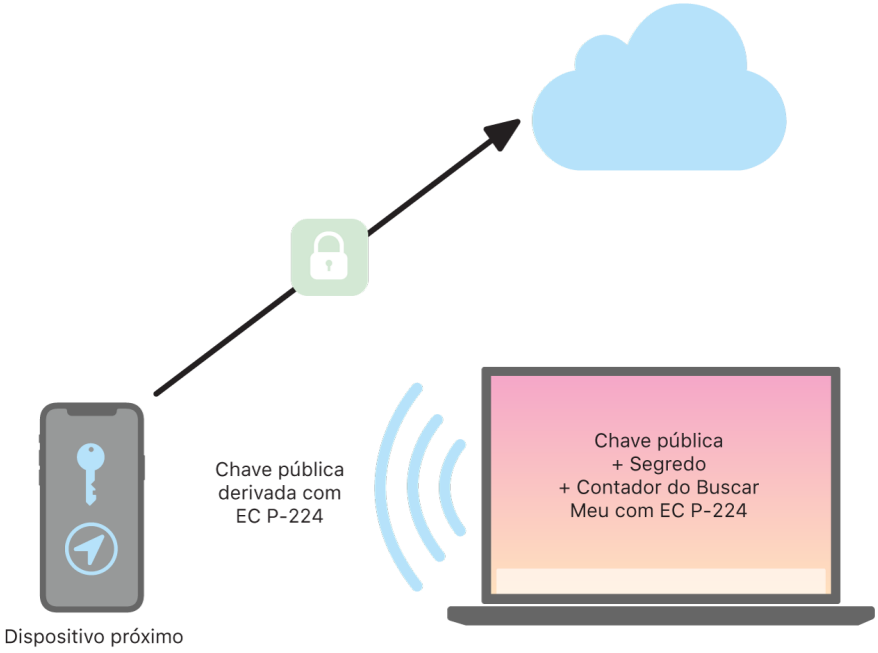
Quando um dispositivo é perdido e não consegue se conectar a uma rede celular ou Wi-Fi (um MacBook Pro deixado sobre o banco de uma praça, por exemplo), ele começa a transmitir periodicamente a chave pública derivada P_i por um período limitado em um payload Bluetooth. Graças ao uso de P-224, a representação da chave pública cabe em um único payload Bluetooth. Para ajudar a localizar o dispositivo off-line, os dispositivos próximos podem criptografar a localização dele com a chave pública. A cada 15 minutos, aproximadamente, a chave pública é substituída por uma nova, usando um valor incrementado do contador e o processo acima, de forma que o usuário não possa ser rastreado por um identificador persistente. O mecanismo de derivação é projetado para impedir que as várias chaves públicas P_i sejam vinculadas ao mesmo dispositivo.

Manutenção da anonimidade de usuários e dispositivos

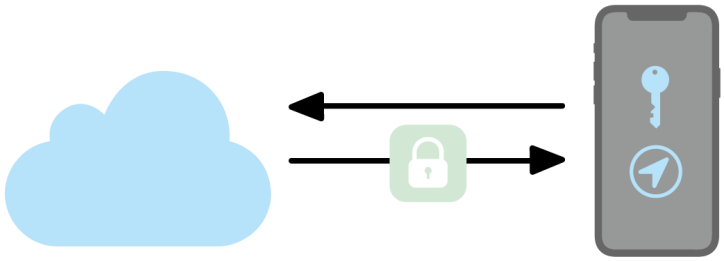
Além de garantir que as informações sobre a localização e outros dados sejam totalmente criptografados, as identidades dos participantes permanecem privadas entre si e com a Apple. O tráfego enviado pelos dispositivos localizadores à Apple não contém nenhuma informação de autenticação no conteúdo ou nos cabeçalhos. Como resultado, a Apple não sabe quem são o localizador ou o proprietário do dispositivo encontrado. Além disso, a Apple não registra informações que revelariam a identidade do localizador nem retém informações que permitiriam a correlação do localizador com o proprietário. O proprietário do dispositivo recebe apenas a informação criptografada sobre a localização, que é descriptografada e mostrada no app Buscar sem indicação de quem encontrou o dispositivo.

Uso do Buscar para localizar dispositivos Apple perdidos

Qualquer dispositivo Apple que esteja dentro do alcance do Bluetooth e tenha a busca off-line ativada pode detectar um sinal de outro dispositivo Apple configurado para permitir o Buscar e ler a chave P_i anunciada no momento. Os dispositivos localizadores usam a construção ECIES e a chave pública P_i da transmissão para criptografar sua localização atual e encaminhá-la à Apple. A localização criptografada é associada a um índice de servidor, que é calculado como o hash SHA256 da chave pública P-224 P_i obtida no payload de Bluetooth. A Apple nunca possui a chave de descriptografia, portanto não consegue ler a localização criptografada pelo localizador. O proprietário do dispositivo perdido pode reconstruir o índice e descriptografar a localização criptografada.



Ao tentar localizar o dispositivo perdido, um intervalo esperado de valores do contador é estimado para o período de busca. Com o conhecimento da chave privada P-224 original *d* e dos valores secretos SK_i no intervalo de valores do contador do período de busca, o proprietário pode reconstruir o conjunto de valores $\{d_i, SHA256(P_i)\}$ de todo o período de busca. O dispositivo do proprietário usado para localizar o dispositivo perdido pode consultar o servidor usando o conjunto de valores de índice $SHA256(P_i)$ e baixar as localizações criptografadas do servidor. Em seguida, o app Buscar descriptografa localmente as localizações criptografadas com as chaves privadas correspondentes d_i e mostra o local aproximado do dispositivo perdido no app. Relatórios de localização de vários dispositivos localizadores são combinados pelo app do proprietário para gerar uma localização mais precisa.



Localização de dispositivos off-line

Se um usuário tiver o Buscar iPhone ativado em seu dispositivo, a busca off-line é ativada por padrão ao atualizar o dispositivo para o iOS 13 ou posterior, iPadOS 13.1 ou posterior e macOS 10.15 ou posterior. Isso é projetado para garantir que todo usuário tenha a melhor chance possível de localizar seu dispositivo caso ele seja perdido. Porém, se em algum momento o usuário preferir não participar, pode desativar a busca off-line nos ajustes do Buscar no dispositivo. Quando a busca off-line está desativada, o dispositivo não atua mais como localizador nem pode ser detectado por outros dispositivos localizadores. Contudo, o usuário ainda pode localizar o dispositivo, desde que ele possa se conectar a uma rede Wi-Fi ou celular.

Quando um dispositivo off-line perdido é localizado, o usuário recebe uma notificação e uma mensagem de e-mail informando que o dispositivo foi encontrado. Para visualizar a localização do dispositivo perdido, o usuário abre o app Buscar e seleciona a aba Dispositivos. Em vez de mostrar o dispositivo em um mapa em branco, como aconteceria antes do dispositivo ser encontrado, o Buscar mostra uma localização no mapa com um endereço aproximado e a informação de há quanto tempo o dispositivo foi detectado. Se houver mais relatórios de localização, a localização e a marca temporal são atualizadas automaticamente. Embora os usuários não possam reproduzir um som em um dispositivo off-line ou apagá-lo remotamente, eles podem usar as informações sobre a localização para refazer seus passos ou tomar outras medidas que ajudem a recuperá-lo.

Continuidade

Visão geral da segurança da Continuidade

A Continuidade aproveita-se de tecnologias como iCloud, Bluetooth e Wi-Fi para permitir que usuários continuem a atividade de um dispositivo em outro, façam e recebam ligações telefônicas, enviem e recebam mensagens de texto, e compartilhem uma conexão celular à internet.

Segurança do Handoff

A Apple gerencia handoffs com segurança, seja de um dispositivo para outro, entre um app nativo e um site, e até handoffs de grandes quantidades de dados.

Como o Handoff funciona em segurança

Com o Handoff, quando os dispositivos iOS, iPadOS e macOS de um usuário estão próximos, o usuário pode passar aquilo em que estiver trabalhando de um dispositivo para outro. O Handoff permite que o usuário alterne entre dispositivos e continue trabalhando imediatamente.

Quando um usuário inicia a sessão no iCloud em um segundo dispositivo compatível com Handoff, os dois dispositivos estabelecem um emparelhamento Bluetooth Low Energy (BLE) 4.2 fora de banda usando APNs. As mensagens individuais são criptografadas de maneira bem semelhante às mensagens do iMessage. Depois de emparelhados, cada dispositivo gera uma chave AES simétrica de 256 bits que é armazenada nas chaves do dispositivo. A chave pode criptografar e autenticar os anúncios de BLE que comunicam a atividade atual do dispositivo para outros dispositivos emparelhados com o iCloud ao usar AES256 no modo GCM, com medidas de proteção contra reprodução.

Na primeira vez que um dispositivo recebe um anúncio de uma nova chave, ele estabelece uma conexão BLE ao dispositivo originário e realiza uma troca de chaves de criptografia de anúncios. O uso de criptografia padrão BLE 4.2 mantém essa conexão em segurança, assim como a criptografia de mensagens individuais, que assemelha-se à criptografia do iMessage. Em algumas situações, essas mensagens são enviadas usando APNs em vez de BLE. O payload da atividade é protegido e transferido da mesma maneira que uma iMessage.

Handoff entre apps nativos e sites

O Handoff permite que um app nativo do iOS, iPadOS e macOS retome a atividade do usuário em uma página web em domínios controlados legitimamente pelo desenvolvedor do app. Ele também permite que a atividade do usuário do app nativo seja retomada em um navegador.

Para ajudar a impedir que apps nativos reivindiquem a retomada de sites que não sejam controlados pelo desenvolvedor, o app precisa demonstrar controle legítimo sobre os domínios web que deseja retomar. O controle sobre um domínio de site é estabelecido através do mecanismo de credenciais web compartilhadas. Para obter detalhes, consulte Acesso de apps a senhas salvas. O sistema deve validar o controle do nome de domínio de um app antes que o app tenha permissão para aceitar o Handoff da atividade do usuário.

A fonte do Handoff de uma página web pode ser qualquer navegador que tenha adotado as APIs do Handoff. Quando o usuário visualiza uma página web, o sistema anuncia o nome do domínio da página web em bytes de anúncio de Handoff criptografados. Somente os outros dispositivos do usuário são capazes de descriptografar os bytes de anúncio.

No dispositivo de destino, o sistema detecta que um app nativo instalado aceita o Handoff do nome de domínio anunciado e exibe o ícone do app nativo como opção de Handoff. Quando aberto, o app nativo recebe o URL completo e o título da página web. Nenhuma outra informação é passada do navegador para o app nativo.

Em contrapartida, um app nativo pode especificar um URL alternativo quando o dispositivo que estiver recebendo o Handoff não tiver o mesmo app nativo instalado. Nesse caso, o sistema exibe o navegador padrão do usuário como opção de app Handoff (caso o navegador tenha adotado as APIs do Handoff). Quando o Handoff é solicitado, o navegador é aberto e recebe o URL alternativo fornecido pelo app de origem. Não há requisitos para que a URL alternativa seja limitada a nomes de domínios controlados pelo desenvolvedor do app nativo.

Handoff de dados maiores

Além do uso de recursos básicos do Handoff, alguns apps podem optar por usar APIs que oferecem suporte ao envio de uma quantidade maior de dados através da tecnologia Wi-Fi peer-to-peer criada pela Apple (semelhante ao AirDrop). O app Mail, por exemplo, usa essas APIs para que o rascunho de um e-mail (que talvez tenha anexos grandes) possa usar o Handoff.

Quando um app usa essas APIs, a troca entre dois dispositivos é iniciada da mesma forma que no Handoff. Porém, depois de receber o payload inicial usando Bluetooth Low Energy (BLE), o dispositivo receptor inicia uma nova conexão via Wi-Fi. Essa conexão é criptografada (com TLS) e deriva a confiança por meio de uma identidade compartilhada pelas Chaves do iCloud. A identidade nos certificados é comparada com a identidade do usuário para verificá-la. Dados adicionais de payload são enviados por essa conexão criptografada até que a transferência seja concluída.

Área de Transferência Universal

A Área de Transferência Universal baseia-se no Handoff para passar o conteúdo da área de transferência de um usuário entre dispositivos com segurança, o que possibilita que o usuário copie em um dispositivo e cole em outro. O conteúdo é protegido da mesma maneira que outros dados de Handoff e compartilhado por padrão com a Área de Transferência Universal, a não ser que o desenvolvedor do app opte por não permitir o compartilhamento.

Os apps têm acesso aos dados da área de transferência independentemente de o usuário ter colado a área de transferência no app. Com a Área de Transferência Universal, esse acesso aos dados é ampliado a apps nos outros dispositivos do usuário (conforme estabelecido pelo início de sessão no iCloud).

Segurança da retransmissão de ligações celulares do iPhone

Quando o Mac, iPad, iPod touch ou HomePod de um usuário está na mesma rede Wi-Fi de seu iPhone, ele pode usar a conexão celular do iPhone para fazer e receber ligações telefônicas. A configuração requer que os dispositivos tenham uma sessão iniciada no iCloud e no FaceTime usando o mesmo ID Apple.

Quando uma ligação é recebida, todos os dispositivos configurados são notificados por meio do serviço de Notificações Push da Apple (APNs) e cada notificação usa a mesma criptografia de ponta a ponta do iMessage. Os dispositivos que estão na mesma rede mostram a interface de usuário da notificação de ligação. Quando o usuário atende à ligação, o áudio é transmitido continuamente do iPhone do usuário usando uma conexão peer-to-peer segura entre os dois dispositivos.

Quando uma ligação é atendida em um dispositivo, o toque de dispositivos próximos emparelhados com o iCloud é interrompido com um breve anúncio por meio de Bluetooth Low Energy (BLE). Os bytes do anúncio são criptografados pelo mesmo método dos anúncios do Handoff.

As ligações feitas também são retransmitidas para o iPhone através do APNs. De forma semelhante, o áudio é transmitido pela conexão peer-to-peer segura entre os dispositivos. Os usuários podem desativar a retransmissão de ligações telefônicas em um dispositivo, bastando desativar “Ligações via iPhone” nos ajustes do FaceTime.

Segurança do Encaminhamento de Mensagens do iPhone

O Encaminhamento de Mensagens envia automaticamente as mensagens de texto SMS recebidas em um iPhone para um iPad, iPod touch ou Mac registrado do usuário. Cada dispositivo deve ter uma sessão iniciada no iMessage usando o mesmo ID Apple. Quando o Encaminhamento de Mensagens está ativado, o registro se dá automaticamente nos dispositivos dentro do círculo de confiança de um usuário se a autenticação de dois fatores estiver ativada. Caso contrário, o registro é verificado em cada dispositivo através da digitação de um código numérico aleatório de seis dígitos gerado pelo iPhone.

Após os dispositivos estarem conectados, o iPhone criptografa e encaminha as mensagens de texto SMS recebidas para cada dispositivo, usando os métodos descritos em Visão geral da segurança do iMessage. As respostas são enviadas de volta para o iPhone com o mesmo método, e o iPhone envia a resposta como uma mensagem de texto com o mecanismo de transmissão de SMS da operadora. O Encaminhamento de Mensagens pode ser ativado ou desativado nos ajustes do Mensagens.

Segurança do Instant Hotspot

O Instant Hotspot conecta outros dispositivos Apple a um acesso pessoal do iOS e iPadOS. Dispositivos iOS e iPadOS que oferecem suporte ao Instant Hotspot usam Bluetooth Low Energy (BLE) para descoberta e comunicação com dispositivos que tenham uma sessão iniciada na mesma conta individual do iCloud ou contas usadas com o Compartilhamento Familiar (no iOS 13 e iPadOS). Os computadores Mac compatíveis (com OS X 10.10 ou posterior) usam a mesma tecnologia para descoberta e comunicação com dispositivos iOS e iPadOS que usam Instant Hotspot.

Inicialmente, quando um usuário acessa os ajustes de Wi-Fi em um dispositivo, ele emite um anúncio BLE contendo um identificador com o qual todos os dispositivos que tenham uma sessão iniciada na mesma conta do iCloud concordam. O identificador é gerado a partir de um DSID (Identificador de Sinalização de Destino) que é atrelado à conta do iCloud e alternado periodicamente. Quando outros dispositivos que têm uma sessão iniciada na mesma conta do iCloud estão próximos e oferecem suporte ao Acesso Pessoal, eles detectam o sinal e respondem, comunicando a disponibilidade para usar o Instant Hotspot.

Quando um usuário que não faz parte do Compartilhamento Familiar escolhe um iPhone ou iPad para Acesso Pessoal, uma solicitação para ativar o Acesso Pessoal é enviada ao dispositivo. A solicitação é enviada através de um link que usa criptografia BLE e criptografada de forma semelhante ao iMessage. Em seguida, o dispositivo responde através do mesmo link BLE usando a mesma criptografia por mensagem com informações de conexão para o Acesso Pessoal.

Para usuários que fazem parte do Compartilhamento Familiar, as informações de conexão ao Acesso Pessoal são compartilhadas com segurança ao usar um mecanismo similar ao usado por dispositivos HomeKit para sincronizar informações. Especificamente, a segurança da conexão que compartilha as informações do acesso entre os usuários é feita com uma chave efêmera ECDH (Curve25519) que é autenticada com as respectivas chaves públicas Ed25519 específicas do dispositivo do usuário. As chaves públicas usadas são aquelas que foram previamente sincronizadas entre os membros do Compartilhamento Familiar com IDS quando o Compartilhamento Familiar foi estabelecido.

Segurança de rede

Visão geral da segurança de rede

Além das medidas de segurança integradas que a Apple usa para proteger os dados armazenados em dispositivos Apple, há várias medidas que podem ser tomadas por organizações para manter a segurança das informações enquanto em trânsito. Todas essas medidas de segurança tratam da segurança de redes.

Como usuários devem poder acessar redes corporativas de qualquer lugar do mundo, é importante ajudar a garantir que eles estejam autorizados e seus dados protegidos durante a transmissão. Para que esses objetivos de segurança sejam alcançados, o iOS, iPadOS e macOS integram tecnologias comprovadas e os padrões mais recentes de conexões de rede Wi-Fi e dados celulares. É por isso que os nossos sistemas operacionais usam — e fornecem a desenvolvedores o acesso a — protocolos de rede padrão para comunicações autenticadas, autorizadas e criptografadas.

Segurança de TLS

O iOS, iPadOS e macOS oferecem suporte ao Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) e ao Datagram Transport Layer Security (DTLS). O protocolo TLS é compatível com AES128 e AES256, e prefere conjuntos de cifras com encaminhamento secreto. Apps que usam internet, como Safari, Calendário e Mail, usam esse protocolo automaticamente para ativar um canal de comunicação criptografado entre o dispositivo e os serviços de rede. As APIs de alto nível (como CFNetwork) facilitam a adoção do TLS por desenvolvedores em apps, enquanto as APIs de baixo nível (como Network.framework) fornecem um controle mais detalhado. O CFNetwork não permite SSL 3 e os apps que usam WebKit (como o Safari) são proibidos de fazer uma conexão SSL 3.

No iOS 11 ou posterior e no macOS 10.13 ou posterior, os certificados SHA-1 não podem mais fazer conexões TLS sem ter a confiança do usuário. Certificados com chaves RSA com menos de 2048 bits também não são permitidos. O conjunto de cifras simétricas RC4 não é mais usado no iOS 10 e no macOS 10.12. Por padrão, clientes ou servidores TLS implementados com APIs de Transporte Seguro não têm os conjuntos de cifras RC4 ativados e não podem se conectar quando RC4 for o único conjunto de cifras disponível. Para ter mais segurança, serviços ou apps que requeiram RC4 devem ser atualizados para usar conjuntos de cifras seguros. No iOS 12.1, os certificados emitidos após 15 de outubro de 2018 a partir de um certificado-raiz autorizado pelo sistema devem ter uma sessão iniciada em um registro de Transparência de Certificado autorizado para terem acesso a conexões TLS. No iOS 12.2, o TLS 1.3 está ativado por padrão para APIs Network.framework e NSURLSession. Clientes TLS que usam APIs SecureTransport não podem usar TLS 1.3.

Segurança de Transporte em Apps

A Segurança de Transporte em Apps fornece requisitos de conexão padrão para que os apps possam seguir as melhores práticas de conexão segura ao usar as APIs NSURLConnection, CFURL ou NSURLSession. Por padrão, a Segurança de Transporte em Apps limita a seleção de cifras para incluir apenas os conjuntos que fornecem encaminhamento secreto, especificamente:

- ECDHE_ECDSA_AES e ECDHE_RSA_AES no Modo Galois/Counter (GCM)
- Modo de Encadeamento de Bloco de Cifra (CBC)

Apps podem desativar o requisito de encaminhamento secreto por domínio, adicionando, nesse caso, RSA_AES ao conjunto de cifras disponíveis.

Os servidores precisam oferecer suporte ao TLS 1.2 e encaminhamento secreto, e os certificados precisam ser válidos e assinados com SHA256 ou mais forte com, no mínimo, uma chave RSA de 2048 bits ou chave de curva elíptica de 256 bits.

As conexões de rede que não atenderem a esses requisitos falharão, a não ser que o app substitua a Segurança de Transporte em Apps. Certificados inválidos sempre resultarão em falha e falta de conexão. A Segurança de Transporte em Apps é aplicada automaticamente a apps compilados para iOS 9 ou posterior e macOS 10.11 ou posterior.

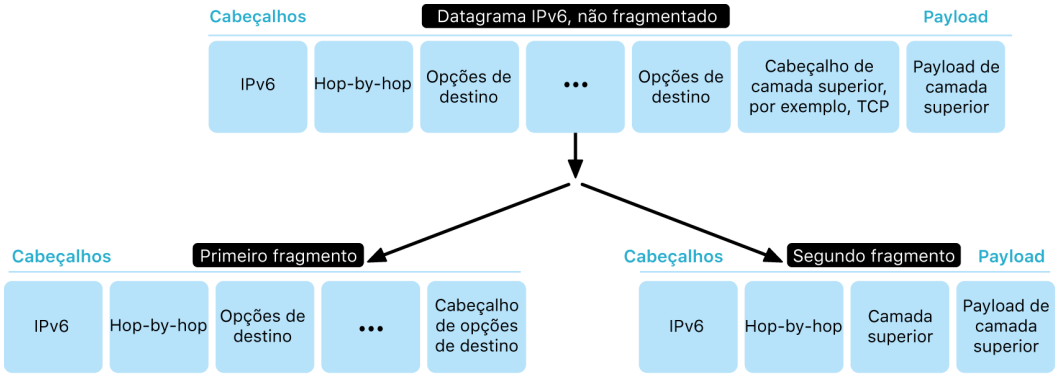
Verificação da validade de certificados

A avaliação do estado de confiança de um certificado TLS é realizada de acordo com padrões de mercado consolidados, conforme definido no RFC 5280 e incorpora padrões novos como o RFC 6962 (Transparência de Certificado). No iOS 11 ou posterior e macOS 10.13 ou posterior, os dispositivos Apple são atualizados periodicamente com uma lista atual de certificados revogados e restringidos. A lista é agregada a partir de listas de revogação de certificados (CRLs) que são publicadas por todas as autoridades de certificação raiz integradas nas quais a Apple confia, assim como por suas ACs emissoras subordinadas. A lista também pode incluir outras restrições a critério da Apple. Essas informações são consultadas sempre que uma função de API de rede é usada para fazer uma conexão segura. Se houver um número grande demais de certificados revogados de uma AC para serem listados individualmente, uma avaliação de confiança pode exigir uma resposta de estado de certificado on-line (OCSP), e ser malsucedida caso a resposta não esteja disponível.

Segurança de IPv6

Todos os sistemas operacionais da Apple são compatíveis com IPv6, implementando diversos mecanismos para proteger a privacidade dos usuários e a estabilidade do conjunto de conexões de rede. Quando a Configuração Automática de Endereço sem Monitoração de Estado (SLAAC) é usada, os endereços IPv6 de todas as interfaces são gerados de uma maneira que ajuda a impedir o rastreamento de dispositivos entre redes e, ao mesmo tempo, permite uma boa experiência de usuário ao garantir a estabilidade do endereço quando nenhuma alteração de endereço ocorre. O algoritmo de geração do endereço é baseado em endereços gerados criptograficamente conforme o RFC 3972, aprimorado por um modificador específico da interface para assegurar que até as interfaces diferentes na mesma rede tenham, eventualmente, endereços diferentes. Além disso, endereços temporários são criados com uma duração preferida de 24 horas, sendo esses usados por padrão para qualquer nova conexão. De acordo com o recurso de endereço Wi-Fi Privado apresentado no iOS 14, iPadOS 14 e watchOS 7, um endereço de link local exclusivo é gerado para cada rede Wi-Fi à qual o dispositivo se conecta. O SSID da rede é incorporado como um elemento adicional para a geração do endereço, de forma similar ao parâmetro Network_ID conforme o RFC 7217. Essa abordagem é usada no iOS 14, iPadOS 14 e watchOS 7.

Para oferecer proteção contra ataques baseados em cabeçalhos de extensão e fragmentação de IPv6, dispositivos Apple implementam as medidas de proteção especificadas no RFC 6980, RFC 7112 e RFC 8021. Entre outras medidas, estas inibem ataques em que o cabeçalho da camada superior é encontrado apenas no segundo fragmento (conforme mostrado abaixo), o qual por sua vez, poderia causar ambiguidades para controles de segurança, como filtros de pacotes sem monitoração de estado.



Além disso, para ajudar a garantir a confiabilidade do conjunto de IPv6 de sistemas operacionais da Apple, dispositivos Apple exigem vários limites em estruturas de dados relacionados ao IPv6, como o número de prefixos por interface.

Segurança de rede privada virtual (VPN)

Serviços seguros de rede, como as redes privadas virtuais, geralmente precisam de pouca configuração para funcionar com dispositivos iOS, iPadOS e macOS.

Protocolos compatíveis

Esses dispositivos funcionam com servidores de VPN compatíveis com os seguintes protocolos e métodos de autenticação:

- IKEv2/IPsec com autenticação por segredo compartilhado, Certificados RSA, Certificados de Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA), EAP-MSCHAPv2 ou EAP-TLS
- VPN-SSL usando o devido app cliente da App Store
- L2TP/IPsec com autenticação do usuário por senha MS-CHAPV2 e autenticação por máquina por segredo compartilhado (iOS, iPadOS e macOS) e RSA SecurID ou CRYPTOCard (apenas macOS)
- Cisco IPsec com autenticação do usuário por senha, RSA SecurID ou CRYPTOCard e autenticação por máquina por segredo compartilhado e certificados (apenas macOS)

Implantações de VPN compatíveis

O iOS, iPadOS e macOS são compatíveis com os itens a seguir:

- *VPN por Demanda:* em redes que usam autenticação baseada em certificado. As políticas de TI especificam, por meio de um perfil de configuração VPN, quais domínios requerem conexão VPN.
- *VPN por App:* para realização de conexões VPN de forma muito mais granular. As soluções de gerenciamento de dispositivos móveis (MDM) podem especificar uma conexão para cada app gerenciado e domínios específicos do Safari. Isso ajuda a garantir que os dados seguros sempre transitem pela rede corporativa, mas não os dados pessoais de usuários.

O iOS e iPadOS são compatíveis com o seguinte:

- *VPN Sempre Ativa:* em dispositivos gerenciados por uma solução MDM e supervisionada com o Apple Configurator para Mac, Apple School Manager ou Apple Business Manager. A VPN Sempre Ativa elimina a necessidade de ativação da VPN pelos usuários para ativar a proteção ao se conectarem a redes Wi-Fi ou celulares. Ela também proporciona a organizações o controle total do tráfego do dispositivo, encapsulando todo o tráfego IP de volta à organização. O IKEv2, a troca padrão de parâmetros e chaves para criptografias subsequentes, dá segurança à transmissão do tráfego com a criptografia de dados. As organizações podem monitorar e filtrar o tráfego de seus dispositivos, proteger os dados de suas redes e restringir o acesso de dispositivos à internet.

Segurança de Wi-Fi

Acesso seguro a redes sem fio

Todas as plataformas Apple oferecem suporte aos protocolos padrão da indústria de autenticação e criptografia de Wi-Fi para fornecer acesso autenticado e confidencialidade na conexão às seguintes redes sem fio seguras:

- WPA2 Pessoal
- WPA2 Empresarial
- WPA2/WPA3 Transitório
- WPA3 Pessoal
- WPA3 Empresarial
- WPA3 Empresarial com segurança de 192 bits

O WPA2 e WPA3 autenticam cada conexão e fornecem criptografia AES de 128 bits para ajudar a garantir a confidencialidade dos dados transferidos sem fio. Isso proporciona aos usuários o maior nível de segurança de dados, que permanecem protegidos durante o envio e recebimento de comunicações em conexões de rede Wi-Fi.

Compatibilidade com WPA3

O WPA3 é compatível com os seguintes dispositivos Apple:

- iPhone 7 ou posterior
- iPad 5ª geração ou posterior
- Apple TV 4K ou posterior
- Apple Watch Series 3 ou posterior
- Computadores Mac (final de 2013 ou posterior, com 802.11ac ou posterior)

Os dispositivos mais novos oferecem suporte à autenticação com WPA3 Empresarial com segurança de 192 bits, incluindo o suporte à criptografia AES de 256 bits em conexões com pontos de acesso (PAs) compatíveis. Isso oferece proteções de confidencialidade ainda maiores para o tráfego transferido sem fio. O WPA3 Empresarial com segurança de 192 bits é compatível com iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max e dispositivos iOS e iPadOS posteriores.

Compatibilidade com PMF

Além de proteger dados transferidos sem fio, as plataformas Apple estendem as proteções do nível de WPA2 e WPA3 a quadros de gerenciamento unicast e multicast por meio do serviço Quadro de Gerenciamento Protegido (PMF) definido no 802.11w. A compatibilidade com PMF está disponível nos seguintes dispositivos Apple:

- iPhone 6 ou posterior
- iPad Air 2 ou posterior
- Apple TV HD ou posterior
- Apple Watch Series 3 ou posterior
- Computadores Mac (final de 2013 ou posterior, com 802.11ac ou posterior)

Com suporte a 802.1X, os dispositivos Apple podem ser integrados a uma grande variedade de ambientes de autenticação RADIUS. Os métodos de autenticação sem fio 802.1X compatíveis incluem EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 e PEAPv1.

Proteções da plataforma

Os sistemas operacionais da Apple protegem o dispositivo contra vulnerabilidades no firmware do processador de rede. Isso significa que os controladores de rede com Wi-Fi têm acesso limitado à memória do Processador de Aplicativos.

- Quando USB ou SDIO (Entrada e Saída Digital Seguras) são usados para criar uma interface com o processador de rede; o processador de rede não pode iniciar transações de acesso direto à memória (DMA) com o Processador de Aplicativos.
- Quando PCIe é usado, cada processador de rede encontra-se isolado em seu próprio barramento PCIe. Uma Unidade de Gerenciamento de Memória de Entrada/Saída (IOMMU) em cada barramento PCIe limita ainda mais o acesso DMA do processador de rede apenas à memória e aos recursos que contêm seus pacotes de rede e estruturas de controle.

Protocolos descontinuados

Os produtos Apple aceitam os seguintes protocolos descontinuados de autenticação e criptografia via Wi-Fi:

- WEP Aberto, tanto com chaves de 40 bits quanto de 104 bits
- WEP Compartilhado, tanto com chaves de 40 bits quanto de 104 bits
- WEP Dinâmico
- Temporal Key Integrity Protocol (TKIP)
- WPA
- WPA/WPA2 Transitório

Esses protocolos não são mais considerados seguros e seu uso é vivamente desaconselhado por motivos de compatibilidade, confiabilidade, desempenho e segurança. Seu suporte é oferecido apenas para fins de compatibilidade com versões anteriores e podem ser removidos em versões futuras do software.

É recomendável que todas as implementações de Wi-Fi sejam migradas para WPA3 Pessoal ou WPA3 Empresarial para fornecer as conexões Wi-Fi mais robustas, seguras e compatíveis possíveis.

Privacidade de Wi-Fi

Aleatorização do endereço MAC

As plataformas Apple usam um endereço de controle de acesso de mídia (endereço MAC) aleatório ao realizar varreduras de Wi-Fi quando não estão associadas a uma rede Wi-Fi. Essas varreduras podem ser realizadas para encontrar e conectar a uma rede Wi-Fi conhecida ou para auxiliar os Serviços de Localização em apps que usam cercas virtuais, como lembretes baseados em localização, ou para fixar uma localização no app Mapas da Apple. Observe que as varreduras de Wi-Fi que acontecem durante a tentativa de conexão a uma rede Wi-Fi preferida não são aleatorizadas. O suporte à aleatorização do endereço MAC do Wi-Fi está disponível no iPhone 5 ou posteriores.

As plataformas Apple também usam um endereço MAC aleatório ao realizar varreduras ePNO (Preferred Network Offload) aprimoradas quando um dispositivo não está associado a uma rede Wi-Fi ou seu processador está em repouso. As varreduras ePNO são executadas quando um dispositivo usa os Serviços de Localização em apps que usam cercas virtuais, como lembretes baseados em localização, que determinam se o dispositivo está próximo a uma localização específica.

Como o endereço MAC de um dispositivo é alterado ao desconectar-se de uma rede Wi-Fi, os observadores passivos de tráfego Wi-Fi não podem usá-lo para rastrear o dispositivo continuamente, mesmo quando ele estiver conectado a uma rede de dados celulares. A Apple informou aos fabricantes de Wi-Fi que as varreduras de Wi-Fi do iOS e iPadOS usam endereços MAC aleatórios e que, nem os fabricantes nem a Apple, podem prevê-los.

No iOS 14 ou posterior, iPadOS 14 ou posterior e watchOS 7 ou posterior, quando um iPhone, iPad, iPod touch ou Apple Watch se conecta a uma rede Wi-Fi, ele se identifica com um endereço MAC exclusivo (aleatório) por rede. Esse recurso pode ser desativado pelo usuário ou ao usar uma nova opção no payload de Wi-Fi. Sob certas circunstâncias, o dispositivo usará o endereço MAC real.

Para obter mais informações, consulte o artigo do Suporte da Apple Usar endereços Wi-Fi privados no iPhone, iPad, iPod touch e Apple Watch.

Aleatorização de números de sequência de quadros de Wi-Fi

Os quadros de Wi-Fi possuem um número de sequência, que é usado pelo protocolo de baixo nível 802.11 para proporcionar comunicações eficientes e confiáveis via Wi-Fi. Como esses números de sequência são incrementados a cada quadro transmitido, eles poderiam ser usados para correlacionar informações transmitidas durante varreduras de Wi-Fi com outros quadros transmitidos pelo mesmo dispositivo.

Para se proteger contra isso, os dispositivos Apple usam números de sequência aleatórios sempre que um endereço MAC é alterado para um novo endereço aleatório. Isso inclui a aleatorização dos números de sequência a cada nova solicitação de varredura iniciada enquanto o dispositivo não está associado. Há suporte para essa aleatorização nos seguintes dispositivos:

- iPhone 7 ou posterior
- iPad 5ª geração ou posterior
- Apple TV 4K ou posterior
- Apple Watch Series 3 ou posterior

- iMac Pro (Retina 5K, 27 polegadas, 2017) ou posterior
- MacBook Pro (13 polegadas, 2018) ou posterior
- MacBook Pro (15 polegadas, 2018) ou posterior
- MacBook Air (Retina, 13 polegadas, 2018) ou posterior
- Mac mini (2018) ou posterior
- iMac (Retina 4K, 21,5 polegadas, 2019) ou posterior
- iMac (Retina 5K, 27 polegadas, 2019) ou posterior
- Mac Pro (2019) ou posterior

Conexões Wi-Fi

A Apple gera endereços MAC aleatórios nas conexões Wi-Fi peer-to-peer usadas para AirDrop e AirPlay. Os endereços aleatórios também são usados no Acesso Pessoal no iOS e iPadOS (com um cartão SIM) e no Compartilhamento de Internet no macOS.

Endereços novos e aleatórios são gerados sempre que essas interfaces de rede são iniciadas. Além disso, endereços exclusivos são gerados de forma independente para cada interface conforme necessário.

Redes ocultas

As redes Wi-Fi são identificadas pelo nome da rede, conhecido como *identificador de conjunto de serviço* (SSID). Algumas redes Wi-Fi são configuradas para ocultar o SSID, fazendo com que o ponto de acesso sem fio não transmita o nome da rede. Essas redes são conhecidas como *redes ocultas*. O iPhone 6s e dispositivos posteriores detectam automaticamente quando uma rede está oculta. Se uma rede estiver oculta, o dispositivo iOS ou iPadOS envia uma sondagem com o SSID incluído na solicitação, mas não de outra forma. Isso ajuda a impedir que o dispositivo transmita o nome de redes ocultas às quais o usuário se conectou anteriormente, garantindo assim mais privacidade.

Segurança de Bluetooth

Existem dois tipos de Bluetooth nos dispositivos Apple, o Bluetooth Classic e o Bluetooth Low Energy (BLE). O modelo de segurança das duas versões de Bluetooth inclui os seguintes recursos de segurança distintos:

- *Emparelhamento:* o processo de criação de uma ou mais chaves de segredo compartilhado
- *Vinculação:* o ato de armazenar as chaves criadas durante o emparelhamento para uso em conexões subsequentes para formar um par de dispositivos confiáveis
- *Autenticação:* verificação de que os dois dispositivos possuem as mesmas chaves
- *Criptografia:* confidencialidade das mensagens
- *Integridade da mensagem:* proteção contra falsificação de mensagens
- *Emparelhamento Simples Seguro:* proteção contra espionagem passiva e ataques man-in-the-middle

O Bluetooth versão 4.1 acrescentou o recurso Conexões Seguras ao transporte físico BR/EDR do Bluetooth Classic.

Os recursos de segurança de cada tipo de Bluetooth estão na lista abaixo.

Compatibilidade	**Bluetooth Classic**	**Bluetooth Low Energy**
Emparelhamento	Curva elíptica P-256	Algoritmos aprovados pelo FIPS (AES-CMAC e curva elíptica P-256)
Vinculação	Emparelhamento de informações armazenadas em um local seguro em dispositivos iOS, iPadOS, macOS, tvOS e watchOS	Emparelhamento de informações armazenadas em um local seguro em dispositivos iOS, iPadOS, macOS, tvOS e watchOS
Autenticação	Algoritmos aprovados pelo FIPS (HMAC-SHA256 e AES-CTR)	Algoritmos aprovados pelo FIPS
Criptografia	Criptografia AES-CCM, realizada no Controlador	Criptografia AES-CCM, realizada no Controlador
Integridade da mensagem	AES-CCM, usada para a integridade da mensagem	AES-CCM, usada para a integridade da mensagem
Emparelhamento Simples Seguro: proteção contra espionagem passiva	Elliptic Curve Diffie-Hellman Exchange Ephemeral (ECDHE)	Elliptic Curve Diffie-Hellman Exchange (ECDHE)
Emparelhamento Simples Seguro: proteção contra ataques man-in-the-middle (MITM)	Dois métodos numéricos assistidos pelo usuário: comparação numérica ou digitação de código	Dois métodos numéricos assistidos pelo usuário: comparação numérica ou digitação de código Os emparelhamentos requerem uma resposta do usuário, incluindo todos os modos de emparelhamento não-MITM
Bluetooth 4.1 ou posterior	iMac (final de 2015 ou posterior) MacBook Pro (início de 2015 ou posterior)	iOS 9 ou posterior iPadOS 13.1 ou posterior macOS 10.12 ou posterior tvOS 9 ou posterior watchOS 2.0 ou posterior

Compatibilidade	Bluetooth Classic	Bluetooth Low Energy
Bluetooth 4.2 ou posterior	iPhone 6 ou posterior	iOS 9 ou posterior iPadOS 13.1 ou posterior macOS 10.12 ou posterior tvOS 9 ou posterior watchOS 2.0 ou posterior

Privacidade do Bluetooth Low Energy

Para ajudar a proteger a privacidade do usuário, o BLE inclui estes dois recursos: aleatorização de endereço e derivação de chave de transporte cruzado.

A *aleatorização de endereço* é um recurso que altera o endereço do dispositivo Bluetooth frequentemente, reduzindo a capacidade de se rastrear um dispositivo BLE por um período de tempo. Para que um dispositivo que use o recurso de privacidade se reconecte a dispositivos conhecidos, o endereço do dispositivo, chamado de *endereço privado*, deve poder ser resolvido pelo outro dispositivo. A geração do endereço privado usa a chave de identidade de resolução do dispositivo trocada durante o procedimento de emparelhamento.

O iOS 13 ou posterior e o iPadOS 13.1 ou posterior têm a capacidade de derivar chaves de links entre transportes, um recurso conhecido como *derivação de chave em transporte cruzado*. Por exemplo, uma chave de link gerada com BLE pode ser usada para derivar uma chave de link de Bluetooth Classic. Além disso, a Apple adicionou suporte de Bluetooth Classic para BLE em dispositivos compatíveis com o recurso Conexões Seguras introduzido na Bluetooth Core Specification versão 4.1 (consulte a Bluetooth Core Specification 5.1 (em inglês)).

Segurança de Banda Ultralarga no iOS

O novo chip U1 criado pela Apple usa tecnologia de banda ultralarga para detecção espacial, permitindo que o iPhone 11, iPhone 11 Pro e iPhone 11 Pro Max ou modelos posteriores de iPhone localizem com precisão outros dispositivos Apple que também possuam o chip U1. A tecnologia de banda ultralarga usa a mesma tecnologia para aleatorizar dados encontrados em outros dispositivos Apple compatíveis:

- Aleatorização do endereço MAC
- Aleatorização de números de sequência de quadros de Wi-Fi

Início de sessão único

Segurança de Início de sessão único

Início de sessão único

O iOS e iPadOS oferecem suporte à autenticação em redes empresariais através do Início de Sessão Único (SSO). O SSO trabalha com redes baseadas em Kerberos para autenticar usuários nos serviços em que são autorizados a acessar. O SSO pode ser usado em uma série de atividades de rede, de sessões seguras do Safari até apps de terceiros. Também há suporte à autenticação baseada em certificados, como PKINIT.

O macOS oferece suporte à autenticação em redes empresariais por meio do Kerberos. Os apps podem usar o Kerberos para autenticar usuários nos serviços que são autorizados a acessar. O Kerberos também pode ser usado em uma série de atividades de rede, de sessões seguras do Safari e autenticação em sistemas de arquivos em rede até apps de terceiros. Há suporte à autenticação baseada em certificados, embora o app seja obrigado a adotar uma API de desenvolvedor.

O SSO do iOS, iPadOS e macOS usa tokens SPNEGO e o protocolo HTTP Negotiate para funcionar com gateways de autenticação baseados em Kerberos e sistemas de Autenticação Integrada do Windows que oferecem suporte a tíquetes do Kerberos. O suporte ao SSO é baseado no projeto Heimdal de código aberto.

Os seguintes tipos de criptografia são aceitos no iOS, iPadOS e macOS:

- AES-128-CTS-HMAC-SHA1-96;
- AES-256-CTS-HMAC-SHA1-96;
- DES3-CBC-SHA1;
- ARCFOUR-HMAC-MD5.

O Safari oferece suporte ao SSO e os apps de terceiros que usam APIs de rede padrão do iOS e iPadOS também podem ser configurados para usá-lo. Para configurar o SSO, o iOS e iPadOS oferecem suporte ao payload de um perfil de configuração que permite que soluções de gerenciamento de dispositivos móveis (MDM) acionem os ajustes necessários. Isso inclui a definição do nome principal do usuário (ou seja, a conta do usuário no Active Directory) e os ajustes do domínio Kerberos, assim como a definição de quais apps e URLs do Safari devem ter permissão para usar o SSO.

Para configurar o Kerberos no macOS, obtenha tíquetes com o Ticket Viewer, inicie uma sessão em um domínio do Active Directory do Windows ou use a ferramenta de linha de comando `kinit`.

Início de sessão único extensível

Os desenvolvedores de apps podem fornecer suas próprias implementações do início de sessão único por meio de extensões do SSO. As extensões SSO são chamadas quando um app nativo ou web precisa usar algum provedor de identidade para autenticação do usuário. Os desenvolvedores podem fornecer dois tipos de extensões: as que redirecionam para HTTPS e as que usam um mecanismo de desafio/resposta, como Kerberos. Isso permite que os esquemas de autenticação do OpenID, OAuth, SAML2 e Kerberos sejam usados com o início de sessão único extensível.

Para usar uma extensão de início de sessão único, um app pode usar a API AuthenticationServices ou o mecanismo de interceptação de URL oferecido pelo sistema operacional. O WebKit e CFNetwork fornecem uma camada de interceptação que permite suporte integrado ao Início de sessão único em qualquer app nativo ou WebKit. Para que uma extensão de início de sessão único seja chamada, uma configuração fornecida por um administrador deve ser instalada por meio de um perfil de gerenciamento de dispositivos móveis (MDM). Além disso, as extensões do tipo redirecionamento devem usar o payload de Domínios Associados para provar que o servidor de identidade ao qual oferecem suporte está ciente da sua existência.

A única extensão fornecida com o sistema operacional é a extensão de SSO do Kerberos.

Segurança do AirDrop

Os dispositivos Apple que oferecem suporte ao AirDrop usam tecnologia Bluetooth Low Energy (BLE) e tecnologia Wi-Fi peer-to-peer criada pela Apple para enviar arquivos e informações para dispositivos próximos, incluindo dispositivos iOS compatíveis com AirDrop e dispositivos iPad com iOS 7 ou posterior e computadores Mac com OS X 10.11 ou posterior. O sinal de rádio Wi-Fi é usado para comunicação direta entre dispositivos, sem usar nenhuma conexão à internet ou ponto de acesso sem fio (PA). Essa conexão é criptografada com TLS.

O AirDrop é configurado com a opção de compartilhamento Apenas Contatos por padrão. Os usuários também podem optar por usar o AirDrop para compartilhar com todos ou desativar o recurso completamente. As organizações podem restringir o uso do AirDrop para dispositivos ou apps sendo gerenciados por uma solução de gerenciamento de dispositivos móveis (MDM).

Operação do AirDrop

O AirDrop usa serviços do iCloud para ajudar na autenticação de usuários. Quando um usuário inicia uma sessão no iCloud, uma identidade RSA de 2048 bits é armazenada no dispositivo. Quando o usuário ativa o AirDrop, um hash de identificação breve do AirDrop é criado com base nos endereços de e-mail e números de telefone associados ao ID Apple do usuário.

Quando um usuário escolhe o AirDrop como método de compartilhamento de um item, o dispositivo de envio emite um sinal AirDrop através de BLE que inclui o hash de identificação breve do AirDrop do usuário. Outros dispositivos Apple que estejam despertos, nas proximidades e que estejam com o AirDrop ativado detectam o sinal e respondem usando Wi-Fi peer-to-peer, de modo que o dispositivo de envio possa descobrir a identidade de quaisquer dispositivos que respondam.

No modo Apenas Contatos, o hash de identificação breve do AirDrop recebido é comparado aos hashes das pessoas incluídas no app Contatos do dispositivo receptor. Se uma correspondência for encontrada, o dispositivo receptor responde por Wi-Fi peer-to-peer com as informações de sua identidade. Se não houver correspondência, o dispositivo não responde.

No modo Todos, o mesmo processo geral é usado. Porém, o dispositivo receptor responde mesmo que não haja nenhuma correspondência no app Contatos do dispositivo.

O dispositivo emissor então inicia uma conexão via AirDrop usando Wi-Fi peer-to-peer, usando essa conexão para enviar um hash de identificação longo para o dispositivo receptor. Se o hash de identificação longo corresponder ao hash de uma pessoa conhecida nos Contatos do receptor, então o receptor responderá com seus hashes de identificação longos.

Se os hashes forem verificados, o nome e a foto do receptor (se existentes no app Contatos) são exibidos na folha de compartilhamento do AirDrop do remetente. No iOS e iPadOS, eles são mostrados na seção “Pessoas” ou “Dispositivos”. Os dispositivos que não foram verificados ou autenticados são mostrados na folha de compartilhamento do AirDrop do remetente com um ícone de silhueta e o nome do dispositivo, como definido em Ajustes > Geral > Sobre > Nome. No iOS e iPadOS, eles aparecem na seção “Outras Pessoas” da folha de compartilhamento do AirDrop.

O usuário remetente pode selecionar com quem deseja compartilhar. Após a seleção do usuário, o dispositivo remetente inicia uma conexão criptografada (TLS) com o dispositivo receptor, que troca seus certificados de identidade do iCloud. A identidade nos certificados é comparada com o app Contatos de cada usuário para verificá-la.

Se os certificados forem verificados, o usuário receptor é solicitado a aceitar a transferência do usuário ou dispositivo identificado. Se vários destinatários forem selecionados, este processo é repetido para cada um deles.

Segurança do compartilhamento de senhas de Wi-Fi no iPhone e iPad

Os dispositivos iOS e iPadOS que oferecem suporte ao compartilhamento de senhas de Wi-Fi usam um mecanismo similar ao AirDrop para enviar uma senha de Wi-Fi de um dispositivo para outro.

Quando um usuário seleciona uma rede Wi-Fi (solicitante) e a senha do Wi-Fi é solicitada ao usuário, o dispositivo Apple inicia um anúncio de Bluetooth Low Energy (BLE), indicando que ele deseja a senha do Wi-Fi. Outros dispositivos Apple que não estão em repouso, encontram-se por perto e têm a senha da rede Wi-Fi selecionada, usam BLE para se conectar ao dispositivo solicitante.

O dispositivo que tem a senha do Wi-Fi (concessor) exige as informações de contato do solicitante, que deve usar um mecanismo similar ao AirDrop para comprovar sua identidade. Depois de comprovar a identidade, o concessor envia o código ao solicitante, o qual pode ser usado para conexão à rede.

Organizações podem restringir o uso do compartilhamento de senhas de Wi-Fi em dispositivos ou apps sendo gerenciados por uma solução de gerenciamento de dispositivos móveis (MDM).

Segurança do firewall no macOS

O macOS possui um firewall integrado para proteger o Mac de acesso à rede e ataques de negação de serviço. Ele pode ser configurado no painel Segurança e Privacidade das Preferências do Sistema e aceita as seguintes configurações:

- Bloquear todas as conexões recebidas, independentemente do app.
- Permitir automaticamente que softwares integrados recebam conexões.
- Permitir automaticamente que softwares baixados e assinados recebam conexões.
- Adicionar ou negar acesso com base em apps especificados pelo usuário.
- Impedir que o Mac responda a pedidos de exame e escaneamento de portas via ICMP (Protocolo de Mensagens de Controle da Internet).

Segurança do kit para desenvolvedores

Visão geral da segurança do kit para desenvolvedores

A Apple fornece diversos “kits” de frameworks para permitir que desenvolvedores externos ampliem os serviços da Apple. Estes frameworks tratam a privacidade e a segurança do usuário como fatores fundamentais:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

Segurança do HomeKit

Segurança de comunicação do HomeKit

O HomeKit oferece uma infraestrutura de automação doméstica que usa a segurança do iCloud e do iOS, iPadOS e macOS para proteger e sincronizar dados privados sem expô-los à Apple.

A segurança e identidade do HomeKit são baseadas em pares de chaves públicas-privadas Ed25519. Um par de chaves Ed25519 é gerado no dispositivo iOS, iPadOS e macOS para cada usuário do HomeKit, definindo sua respectiva identidade HomeKit. Ela é usada para autenticar a comunicação entre dispositivos iOS, iPadOS e macOS e entre dispositivos iOS, iPadOS e macOS e acessórios.

As chaves — armazenadas nas chaves e incluídas apenas em backups criptografados das Chaves — são mantidas sincronizadas entre dispositivos através das Chaves do iCloud, onde disponíveis. O HomePod e a Apple TV recebem chaves por meio de toque para configurar ou do modo de configuração descrito abaixo. As Chaves são compartilhadas a partir de um iPhone para um Apple Watch emparelhado por meio do Serviço de Identidade da Apple (IDS).

Comunicação entre acessórios HomeKit

Os acessórios HomeKit geram seus próprios pares de chaves Ed25519 para uso nas comunicações com dispositivos iOS, iPadOS e macOS. Se o acessório for restaurado aos ajustes de fábrica, um novo par de chaves é gerado.

Para estabelecer um relacionamento entre um dispositivo iOS, iPadOS e macOS e um acessório HomeKit, as chaves são trocadas usando o protocolo Secure Remote Password (3072 bits), utilizando um código de oito dígitos fornecido pelo fabricante do acessório, digitado no dispositivo iOS ou iPadOS pelo usuário e criptografado usando ChaCha20-Poly1305 AEAD com chaves derivadas HKDF-SHA512. A certificação MFi do acessório também é verificada durante a configuração. Acessórios sem um chip MFi podem integrar a compatibilidade com a autenticação de software no iOS 11.3 ou posterior.

Quando o dispositivo iOS, iPadOS e macOS e um acessório HomeKit se comunicam durante o uso, um autentica o outro pelas chaves trocadas no processo acima. Cada sessão é estabelecida usando o protocolo Station-to-Station e criptografada com chaves derivadas HKDF-SHA512, baseadas em chaves Curve25519 únicas por sessão. Isso se aplica tanto a acessórios com base em IP como a acessórios Bluetooth Low Energy (BLE).

Para dispositivos BLE compatíveis com notificações transmitidas, o acessório recebe uma chave de criptografia de transmissão de um dispositivo iOS, iPadOS e macOS emparelhado por meio de uma sessão segura. Essa chave é usada para criptografar os dados sobre mudanças de estado do acessório, que são notificadas por meio de anúncios do BLE. A chave de criptografia de transmissão é uma chave derivada HKDF-SHA512, e os dados são criptografados usando o algoritmo AEAD ChaCha20-Poly1305. A chave de criptografia de transmissão é alterada periodicamente pelo dispositivo iOS, iPadOS e macOS e atualizada para outros dispositivos através do iCloud, conforme descrito em Segurança de dados do HomeKit.

HomeKit e Siri

A Siri pode ser usada para consultar e controlar acessórios e para ativar cenas. Informações mínimas sobre a configuração da casa são fornecidas anonimamente à Siri para fornecer o nome de quartos, acessórios e cenas necessários para o reconhecimento de comandos. O áudio enviado para a Siri pode indicar acessórios ou comandos específicos, mas tais dados da Siri não são associados a outros recursos da Apple, como o HomeKit.

Acessórios do HomeKit compatíveis com a Siri

Os usuários podem ativar novos recursos como a Siri e outros recursos do HomePod, como timers, alarmes, interfone e campainha, em acessórios compatíveis com a Siri no app Casa. Quando esses recursos estão ativados, o acessório trabalha em conjunto com um HomePod emparelhado na rede local que hospeda esses recursos da Apple. O áudio é trocado entre os dispositivos por meio de canais criptografados usando os protocolos HomeKit e AirPlay.

Quando o recurso “Ouvir E aí Siri” está ativado, para ouvir a frase “E aí Siri” o acessório utiliza um mecanismo executado localmente para detecção de frases de acionamento. Se esse mecanismo detectar a frase, ele envia os quadros de áudio diretamente a um HomePod emparelhado usando o HomeKit. O HomePod faz uma segunda verificação do áudio e pode cancelar a sessão de áudio caso não pareça que a frase contenha o trecho de acionamento.

Quando o recurso Pressionar para a Siri está ativado, o usuário pode pressionar um botão dedicado no acessório para iniciar uma conversa com a Siri. Os quadros de áudio são enviados diretamente ao HomePod emparelhado.

Depois que uma chamada bem-sucedida da Siri é detectada, o HomePod envia o áudio aos servidores da Siri e cumpre a solicitação do usuário com as mesmas proteções de segurança, privacidade e criptografia que o HomePod aplica às chamadas que o usuário faz ao próprio HomePod. Se a Siri tiver uma resposta de áudio, essa resposta é enviada ao acessório por meio de um canal de áudio AirPlay. Algumas solicitações à Siri exigem informações adicionais do usuário (por exemplo, perguntar se o usuário deseja ouvir mais opções). Nesse caso, o acessório recebe uma indicação de que deve ser feita uma pergunta ao usuário e o áudio adicional é transmitido ao HomePod.

O acessório é obrigado a ter um indicador visual para mostrar ao usuário quando está ouvindo ativamente (um indicador de LED, por exemplo). O acessório não tem qualquer conhecimento da intenção da solicitação à Siri, exceto pelo acesso às transmissões de áudio. Além disso, nenhum dado do usuário é armazenado no acessório.

Segurança de dados do HomeKit

Os dados do HomeKit podem ser atualizados com segurança entre os dispositivos iOS, iPadOS e macOS de um usuário através do iCloud e das chaves do iCloud. Durante esse processo, os dados do HomeKit são criptografados com chaves derivadas da identidade HomeKit do usuário e um nonce aleatório, sendo gerenciados como um grande objeto binário opaco, ou *bolha*. A bolha mais recente é armazenada no iCloud, mas ela não é usada para nenhum outro propósito. Como os dados são criptografados usando chaves disponíveis apenas nos dispositivos iOS, iPadOS e macOS do usuário, seu conteúdo se torna inacessível durante a transmissão e o armazenamento no iCloud.

Os dados do HomeKit também são sincronizados entre os vários usuários da mesma casa. Esse processo usa a mesma autenticação e criptografia usadas entre um dispositivo iOS, iPadOS e macOS e um acessório HomeKit. A autenticação é baseada em chaves públicas Ed25519, que são trocadas entre os dispositivos quando um usuário é adicionado a uma casa. Depois que um novo usuário é adicionado a uma casa, todas as comunicações posteriores são autenticadas e criptografadas usando o protocolo Station-to-Station e chaves únicas por sessão.

O usuário que criou a casa no HomeKit inicialmente ou outro usuário com permissões de edição pode adicionar novos usuários. O dispositivo do proprietário configura os acessórios com a chave pública do novo usuário para que os acessórios possam autenticar e aceitar comandos do novo usuário. Quando um usuário com permissões de edição adiciona um novo usuário, o processo é delegado a uma central da casa para concluir a operação.

HomeKit e Apple TV

O processo de autorização da Apple TV para uso com o HomeKit é realizado automaticamente quando o usuário inicia a sessão no iCloud. A autenticação de dois fatores deve estar ativada na conta do iCloud. A Apple TV e o dispositivo do proprietário trocam chaves públicas Ed25519 temporárias através do iCloud. Quando o dispositivo do usuário e a Apple TV estão na mesma rede local, as chaves temporárias são usadas para garantir uma conexão através da rede local usando o protocolo Station-to-Station e chaves únicas por sessão. Esse processo usa a mesma autenticação e criptografia usadas entre um dispositivo iOS, iPadOS e macOS e um acessório HomeKit. Por meio dessa conexão local segura, o dispositivo do proprietário transfere os pares de chaves públicas-privadas Ed25519 do usuário para a Apple TV. Essas chaves são então usadas para dar segurança à comunicação entre a Apple TV e os acessórios HomeKit e também entre a Apple TV e outros dispositivos iOS, iPadOS e macOS que façam parte da casa com HomeKit.

Se um usuário não tiver vários dispositivos e não conceder acesso a usuários adicionais em sua casa, nenhum dado do HomeKit é transmitido para o iCloud.

App e dados da casa

O acesso aos dados da casa por apps é controlado pelos ajustes de Privacidade do usuário. Os usuários são solicitados a conceder acesso quando os apps solicitam dados da casa, de maneira semelhante aos apps Contatos, Fotos e outras fontes de dados do iOS, iPadOS e macOS. Se o usuário aprovar, os apps terão acesso aos nomes dos cômodos e acessórios, em qual quarto cada acessório se encontra e outras informações, conforme detalhado na documentação do desenvolvedor do HomeKit em https://developer.apple.com/homekit/ (em inglês).

Armazenamento de dados locais

O HomeKit armazena os dados de casas, acessórios, cenas e usuários em um dispositivo iOS, iPadOS e macOS do usuário. Os dados armazenados são criptografados usando chaves derivadas das chaves de identidade HomeKit do usuário em conjunto com um nonce aleatório. Além disso, os dados do HomeKit são armazenados usando a classe de Proteção de Dados “Protegido Até a Primeira Autenticação do Usuário”. O backup de dados do HomeKit é feito apenas em backups criptografados, portanto, por exemplo, backups não criptografados feitos no Finder (macOS 10.15 ou posterior) ou iTunes (no macOS 10.14 ou anterior) via USB não contêm dados do HomeKit.

Segurança de roteadores com HomeKit

Roteadores compatíveis com o HomeKit permitem que usuários melhorarem a segurança da rede doméstica ao gerenciar o acesso Wi-Fi que os acessórios do HomeKit têm à rede local e à internet. Os roteadores também são compatíveis com a autenticação PSK Privada (PPSK), para que os acessórios possam ser adicionados à rede Wi-Fi com uma chave específica do acessório que possa ser revogada quando necessário. A autenticação PPSK melhora a segurança ao não expor a senha principal do Wi-Fi aos acessórios, assim como ao permitir que o roteador identifique um acessório com segurança, mesmo que seu endereço MAC mude eventualmente.

Com o app Casa, um usuário pode configurar restrições de acesso em grupos de acessórios da seguinte maneira:

- *Sem Restrições:* permite acesso irrestrito à internet e à rede local.
- *Automático:* esse é o ajuste padrão. Permite acesso irrestrito à internet e à rede local com base em uma lista de sites da internet e portas locais fornecidas à Apple pelo fabricante do acessório. Essa lista inclui todos os sites e portas necessários ao acessório para que ele funcione corretamente (Sem Restrições é usado até que tal lista esteja disponível).
- *Restringir à Casa:* nenhum acesso à internet ou à rede local, exceto por conexões exigidas pelo HomeKit para descobrir e controlar o acessório a partir da rede local (incluindo conexões da central da casa para oferecer suporte ao controle remoto).

A PPSK é uma senha WPA2 Pessoal forte, específica do acessório, que é gerada automaticamente pelo HomeKit e revogada se ou quando o acessório for posteriormente removido da Casa. Uma PPSK é usada quando um acessório é adicionado à rede Wi-Fi pelo HomeKit em uma casa configurada com um roteador HomeKit; essa adição reflete-se como uma Credencial Wi-Fi: gerenciada pelo HomeKit na tela de ajustes do acessório no app Casa. Os acessórios que tiverem sido adicionados à rede Wi-Fi antes da adição do roteador são reconfigurados para usar uma PPSK se o acessório for compatível, caso contrário, eles mantêm suas credenciais existentes.

Como uma medida de segurança adicional, usuários devem usar o app do fabricante do roteador HomeKit para configurá-lo, de forma que o app possa validar se os usuários possuem acesso ao roteador e podem adicioná-lo ao app Casa.

Segurança da câmera do HomeKit

As câmeras que têm um endereço de Protocolo de Internet (IP) no HomeKit enviam transmissões de vídeo e áudio diretamente para o dispositivo iOS, iPadOS, tvOS e macOS que estiver acessando a transmissão na rede local. As transmissões são criptografadas com chaves geradas aleatoriamente no dispositivo e na câmera de Protocolo de Internet (ou câmera IP), e são trocadas através da sessão segura do HomeKit com a câmera. Quando um dispositivo não está na rede local, as transmissões são retransmitidas através da central da casa para o dispositivo. A central da casa não descriptografa as transmissões; ela funciona apenas como um retransmissor entre o dispositivo e a câmera IP. Quando um app exibe o vídeo da câmera IP do HomeKit para o usuário, o HomeKit renderiza os fotogramas de vídeo com segurança a partir de um processo do sistema à parte. Como resultado, o app não pode acessar ou armazenar a transmissão de vídeo. Além disso, os apps não têm permissão para fazer capturas de tela dessa transmissão.

Vídeo seguro do HomeKit

O HomeKit oferece um mecanismo seguro e privado de ponta a ponta para gravar, analisar e visualizar clipes de câmeras IP do HomeKit sem expor esse conteúdo de vídeo à Apple ou nenhum terceiro. Quando um movimento é detectado pela câmera IP, os clipes de vídeo são enviados diretamente ao dispositivo Apple que age como central da casa por uma conexão de rede local dedicada entre a central da casa e a câmera IP. A conexão de rede local é criptografada com um par de chaves por sessão derivado de HKDF-SHA512, negociado por uma sessão do HomeKit entre a central da casa e a câmera IP. O HomeKit descriptografa as transmissões de áudio e vídeo na central da casa e analisa os fotogramas de vídeo localmente em busca de eventos significativos. Se um evento significativo for detectado, o HomeKit usa AES-256-GCM com uma chave AES256 gerada aleatoriamente para criptografar o clipe de vídeo. O HomeKit também gera fotogramas-pôster para cada clipe e esses fotogramas-pôster são criptografados com a mesma chave AES256. Os dados de fotogramas-pôster, áudio e vídeo são enviados para os servidores do iCloud. Os respectivos metadados de cada clipe, incluindo a chave de criptografia, usam a criptografia de ponta a ponta do iCloud quando são enviados.

Para a classificação de rostos, o HomeKit armazena todos os dados usados para classificar o rosto de uma pessoa específica no CloudKit com a criptografia de ponta a ponta do iCloud. Os dados armazenados incluem informações sobre cada pessoa, como nome e imagens que representam o rosto dessa pessoa. Essas imagens de rostos podem advir do app Fotos de um usuário, caso ele opte por isso, ou serem coletadas do vídeo analisado anteriormente da câmera IP. Uma sessão de análise de Vídeo Seguro do HomeKit usa esses dados de classificação para identificar rostos na transmissão de vídeo segura recebida diretamente da câmera IP e inclui essas informações de identificação nos metadados do clipe mencionados anteriormente.

Quando o app Casa é usado para visualizar os clipes de uma câmera, os dados são baixados do iCloud e as chaves para descriptografar as transmissões usam a descriptografia de ponta a ponta do iCloud para serem desembaladas localmente. O conteúdo de vídeo criptografado é transmitido dos servidores e descriptografado localmente no dispositivo iOS antes de aparecer no visualizador. Cada sessão de clipe de vídeo pode ser dividida em subseções, na qual cada subseção criptografa a transmissão de conteúdo com sua própria chave única.

Segurança do HomeKit com a Apple TV

O HomeKit conecta com segurança alguns acessórios remotos de terceiros à Apple TV e oferece suporte à adição de perfis de usuário ao proprietário da Apple TV da casa.

Uso de acessórios remotos de terceiros com a Apple TV

Alguns acessórios remotos de terceiros oferecem eventos de Design de Interface de Usuário (HID) e áudio da Siri a uma Apple TV associada, adicionada através do app Casa. O controle remoto envia eventos de HID pela sessão segura para a Apple TV. Um controle remoto de TV compatível com a Siri envia os dados de áudio à Apple TV quando o usuário ativa explicitamente o microfone no Remote ao usar um botão Siri dedicado. O controle remoto envia os quadros de áudio diretamente à Apple TV ao usar uma conexão de rede local a dedicada. Um par de chaves por sessão derivado de HKDF-SHA512 negociado por uma sessão do HomeKit entre a Apple TV e o controle remoto da TV é usado para criptografar a conexão de rede local. O HomeKit descriptografa os quadros de áudio na Apple TV e os encaminha ao app Siri, onde eles são tratados com as mesmas proteções à privacidade de todas as entradas de áudio da Siri.

Perfis da Apple TV para casas com HomeKit

Quando um usuário de uma casa com HomeKit adiciona seu perfil à Apple TV do proprietário da casa, esse usuário recebe acesso aos programas de TV, músicas e podcasts. Os ajustes de cada usuário relacionados ao uso de seu perfil na Apple TV são compartilhados com a conta do iCloud do proprietário usando a criptografia de ponta a ponta do iCloud. Cada usuário é dono de seus dados, que são compartilhados somente para leitura do proprietário. Cada usuário da casa pode alterar esses valores no app Casa para que a Apple TV do proprietário use esses ajustes.

Quando um ajuste está ativado, a conta do iTunes do usuário é disponibilizada na Apple TV. Quando um ajuste está desativado, a conta e os dados referentes a esse usuário são apagados na Apple TV. O compartilhamento inicial do CloudKit é iniciado pelo dispositivo do usuário e o token usado para estabelecer o compartilhamento seguro do CloudKit é enviado através do mesmo canal seguro usado para sincronizar os dados entre usuários da casa.

Segurança do SiriKit para iOS, iPadOS e watchOS

A Siri usa o sistema de extensões de apps para se comunicar com apps de terceiros. Em um dispositivo, a Siri pode acessar as informações de contato do usuário e a localização atual do dispositivo. Mas antes de fornecer dados protegidos a um app, a Siri verifica as permissões de acesso do app, controladas pelo usuário. De acordo com essas permissões, a Siri passa apenas o fragmento relevante do enunciado original do usuário para a extensão do app. Por exemplo, se um app não tiver acesso a informações de contato, a Siri não resolverá um relacionamento em um pedido do usuário como "Use o App de Pagamento para pagar 10 reais à minha mãe". Nesse caso, o app veria apenas o termo literal "minha mãe".

Porém, se o usuário tiver concedido ao app acesso às informações de contato, o app receberia informações resolvidas sobre a mãe do usuário. Se houver referência a um relacionamento no corpo de uma mensagem, como em "Diga à minha mãe no AppMensagens que meu irmão está bem", a Siri não resolve "meu irmão", independentemente das permissões do app.

Os apps que fazem uso do SiriKit podem enviar um vocabulário específico do app ou do usuário à Siri, como os nomes dos contatos do usuário. Essas informações permitem que o reconhecimento de fala e entendimento de linguagem natural da Siri reconheçam o vocabulário desse app, sendo associadas a um identificador aleatório. As informações personalizadas permanecem disponíveis durante todo o uso do identificador ou até que o usuário desative a integração do app à Siri nos Ajustes, ou até que o app que utiliza o SiriKit seja desinstalado.

No caso de um enunciado como "Quero uma viagem até a casa da minha mãe usando o RideShareApp", a solicitação requer dados de localização dos contatos do usuário. Para essa solicitação apenas, a Siri fornece as informações necessárias à extensão do app, independentemente dos ajustes de permissão do usuário relacionados à localização ou às informações de contato para o app.

Segurança do DriverKit para macOS

O DriverKit é o framework que permite que desenvolvedores criem drivers de dispositivo que os usuários podem instalar no Mac. Os drivers criados com o DriverKit são executados no espaço do usuário, não como extensões do kernel, melhorando a segurança e a estabilidade do sistema. Isso facilita a instalação e aumenta a estabilidade e a segurança do macOS.

O usuário simplesmente baixa o app (instaladores não são necessários ao usar extensões do sistema ou o DriverKit) e a extensão é ativada apenas quando necessário. Elas substituem as kexts em vários casos de uso que requerem privilégios de administrador para realizar instalações em /Sistema/Biblioteca ou /Biblioteca.

Recomenda-se que administradores de TI que usam drivers de dispositivos, soluções de armazenamento na nuvem, rede e apps de segurança que exigem extensões de kernel passem para versões mais novas que se baseiem em extensões do sistema. Essas versões mais novas reduzem consideravelmente a possibilidade de pânico no kernel no Mac, além de diminuir a superfície de ataque. Essas novas extensões são executadas no espaço do usuário, não precisam de privilégios especiais para instalação e são removidas automaticamente quando o app associado é movido para o Lixo.

O framework DriverKit fornece classes de C++ para serviços de E/S, correspondência de dispositivos, descritores de memória e filas de despacho. Ele também define tipos de números, coleções, strings e outros tipos comuns adequados para E/S. O usuário os utiliza com frameworks de drivers específicos de famílias como USBDriverKit e HIDDriverKit. Use o framework de Extensões do Sistema para instalar e atualizar um driver.

Segurança de ReplayKit no iOS e iPadOS

O ReplayKit é uma estrutura que permite que desenvolvedores adicionem recursos de gravação e transmissão ao vivo a seus apps. Além disso, ele também permite que usuários usem a câmera frontal e o microfone do dispositivo para comentar em suas gravações e transmissões.

Gravação de filmes

Há várias camadas de segurança integradas à gravação de um filme:

- *Diálogo de permissões:* antes da gravação ser iniciada, o ReplayKit apresenta um alerta de consentimento ao usuário, solicitando que ele reconheça sua intenção de gravar a tela, usar o microfone e a câmera frontal. Esse alerta é apresentado uma vez por processo de app, sendo apresentado novamente se o app permanecer em segundo plano por mais de oito minutos.
- *Captura de tela e áudio:* a captura de tela e áudio ocorre fora do processo do app, no daemon replayd do ReplayKit. Isso é projetado para garantir que o conteúdo gravado nunca fique acessível ao processo do app.
- *Captura de tela e áudio dentro de apps:* permite que um app obtenha buffers de vídeo e amostra, o que é protegido por meio do diálogo de permissões.
- *Criação e armazenamento de filmes:* o arquivo de filme é gravado em um diretório acessível apenas aos subsistemas do ReplayKit e nunca fica acessível a nenhum app. Isso ajuda a impedir que as gravações sejam usadas por terceiros sem o consentimento do usuário.
- *Pré-visualização e compartilhamento pelo usuário final:* o usuário é capaz de pré-visualizar e compartilhar o filme com uma interface de usuário oferecida pelo ReplayKit. A interface de usuário é apresentada fora do processo através da infraestrutura de Extensões do iOS e tem acesso ao arquivo de filme gerado.

Transmissão com ReplayKit

Há várias camadas de segurança integradas à transmissão de um filme:

- *Captura de tela e áudio:* o mecanismo de captura de tela e áudio durante a transmissão é idêntico ao da gravação de filmes, ocorrendo no `replayd`.
- *Extensões de transmissão:* para que serviços de terceiros participem da transmissão do ReplayKit, é necessário que eles criem duas novas extensões que estejam configuradas pelo com.apple.broadcast-services:
  - Uma extensão de interface de usuário que permita ao usuário configurar a transmissão;
  - Uma extensão de envio que gerencie o envio de dados de vídeo e áudio para os servidores de retaguarda do serviço.

A arquitetura ajuda a garantir que os apps hosts não tenham nenhum privilégio sobre o conteúdo de vídeo e áudio da transmissão. Apenas o ReplayKit e as extensões de transmissão de terceiros possuem acesso.

- *Seletor de transmissão:* com o seletor de transmissão, o usuário inicia transmissões do sistema diretamente do app com a mesma interface de usuário definida pelo sistema, que pode ser acessada através da Central de Controle. A interface de usuário é uma extensão que reside dentro do framework ReplayKit, implementada ao usar uma API privada. Ele não pode ser processado pelo app host.
- *Extensão de envio:* a extensão implementada por serviços de transmissão de terceiros para gerenciar conteúdo de vídeo e áudio durante uma transmissão usa buffers de amostra não codificados e não processados. Durante esse modo de gerenciamento, os dados de vídeo e áudio são serializados e passados à extensão de envio do terceiro em tempo real por uma conexão XPC direta. Os dados de vídeo são codificados ao extrair o objeto IOSurface do buffer de amostra do vídeo, codificá-lo com segurança como um objeto XPC, enviá-lo através do XPC para a extensão de terceiros e descodificá-lo com segurança de volta em um objeto IOSurface.

Segurança do ARKit no iOS e iPadOS

O ARKit é um framework que permite que desenvolvedores produzam experiências de realidade aumentada em seus apps ou jogos. Desenvolvedores podem usar a câmera frontal ou traseira de um dispositivo iOS ou iPadOS para adicionar elementos 2D ou 3D.

A Apple projetou câmeras tendo em mente a privacidade, e apps de terceiros devem obter o consentimento do usuário antes de acessar a câmera. No iOS e iPadOS, quando um usuário concede acesso à câmera a um app, esse app pode acessar imagens em tempo real das câmeras frontais e traseiras. Os apps não podem usar a câmera sem transparência de que ela está sendo usada.

As fotos e vídeos gravados com a câmera podem conter outras informações, como onde e quando foram gravados, a profundidade de campo e overcapture. Se os usuários não desejarem que as fotos e vídeos feitos com o app Câmera incluam localização, eles podem acessar Ajustes > Privacidade > Serviços de Localização > Câmera para controlar isso a qualquer momento. Se os usuários não desejarem que as fotos e vídeos incluam a localização ao compartilhá-los, eles podem desativar a localização no menu Opções da folha de compartilhamento.

Para oferecer uma posição melhor na experiência de RA do usuário, apps que usam ARKit podem usar informações do ambiente real ou de rastreamento de rosto da outra câmera. O rastreamento do ambiente real usa algoritmos no dispositivo do usuário para processar informações desses sensores e determinar sua posição em relação a um espaço físico. O rastreamento do ambiente real ativa recursos como a Direção Óptica no app Mapas.

Gerenciamento seguro de dispositivos

Visão geral do gerenciamento seguro de dispositivos

O iOS, iPadOS, macOS e tvOS oferecem suporte a políticas e configurações de segurança flexíveis de fácil aplicação e gerenciamento. Através delas, as organizações podem proteger informações corporativas e ajudar a garantir o cumprimento dos requisitos empresariais pelos funcionários, mesmo que eles usem dispositivos próprios (como parte de um programa “traga o seu próprio dispositivo” (BYOD), por exemplo).

As organizações podem usar recursos como proteção por senha, perfis de configuração, apagamento remoto e soluções de gerenciamento de dispositivos móveis (MDM) de terceiros para gerenciar uma gama de dispositivos, ajudando a manter os dados corporativos em segurança, mesmo quando esses dados são acessados pelos funcionários em seus dispositivos pessoais.

No iOS 13 ou posterior, iPadOS 13.1 ou posterior e macOS 10.15 ou posterior, os dispositivos Apple oferecem uma nova opção de registro de usuários elaborada especificamente para programas BYOD. O registro de usuários dá mais autonomia para os usuários em seus próprios dispositivos, ao mesmo tempo que aumenta a segurança dos dados corporativos ao armazená-los em um volume APFS (Apple File System) separado e protegido por criptografia. Isso oferece um melhor equilíbrio de segurança, privacidade e experiência do usuário nos programas BYOD.

Segurança de modelo de emparelhamento para iPhone e iPad

O iOS e iPadOS usam um modelo de emparelhamento para controlar o acesso a um dispositivo a partir de um computador host. O emparelhamento estabelece um relacionamento de confiança entre o dispositivo e o host conectado, simbolizado pela troca de chaves públicas. O iOS e iPadOS também usam essa demonstração de confiança para ativar funcionalidades adicionais com o host conectado, como a sincronização de dados. No iOS 9 ou posterior, os serviços:

- Que exigem emparelhamento não podem ser iniciados até que o dispositivo seja desbloqueado pelo usuário
- Não são iniciados a não ser que o dispositivo tenha sido desbloqueado recentemente
- Podem (como no caso da sincronização de fotos) exigir que o dispositivo seja desbloqueado para iniciar

O processo de emparelhamento requer que o usuário desbloqueie o dispositivo e aceite o pedido de emparelhamento do host. No iOS 9 ou posterior, o usuário também é solicitado a digitar sua senha e, depois disso, o host e o dispositivo trocam e salvam chaves públicas RSA de 2048 bits. Em seguida o host recebe uma chave de 256 bits capaz de desbloquear uma keybag de guarda armazenada no dispositivo. As chaves trocadas são usadas para iniciar uma sessão SSL criptografada, que é exigida pelo dispositivo antes que ele envie dados protegidos ao host ou inicie um serviço (sincronização via iTunes ou Finder, transferência de arquivos, desenvolvimento com Xcode, etc.). Para usar essa sessão criptografada em todas as comunicações, o dispositivo exige conexões de um host via Wi-Fi, devendo, portanto, ter sido emparelhado anteriormente via USB. O emparelhamento também ativa diversos recursos de diagnóstico. No iOS 9, os registros de emparelhamento expiram se não forem usados por mais de 6 meses. No iOS 11 ou posterior, esse intervalo é encurtado para 30 dias.

Certos serviços de diagnóstico, incluindo com.apple.mobile.pcapd, são restritos ao uso somente via USB. Além disso, o serviço com.apple.file_relay requer que um perfil de configuração assinado pela Apple esteja instalado. No iOS 11 ou posterior, a Apple TV pode usar o protocolo Secure Remote Password para estabelecer um relacionamento de emparelhamento via conexão sem fio.

O usuário pode usar as opções “Redefinir Ajustes de Rede” ou “Redefinir Localização e Privacidade” para limpar a lista de hosts confiáveis.

Gerenciamento de dispositivos móveis

Visão geral da segurança do gerenciamento de dispositivos móveis

Os sistemas operacionais da Apple oferecem suporte ao gerenciamento de dispositivos móveis (MDM), o qual permite a organizações configurar e gerenciar de forma segura implantações de dispositivos Apple em larga escala.

Como o MDM funciona em segurança

Os recursos de MDM têm como base tecnologias existentes dos sistemas operacionais, como perfis de configuração, registro via conexão sem fio e o serviço de Notificações Push da Apple (APNs). Por exemplo, o APNs é usado para despertar o dispositivo para que ele se comunique diretamente com sua solução MDM através de uma conexão segura. Com os APNs, nenhuma informação confidencial ou proprietária é transmitida.

Por meio do uso do MDM, os departamentos podem registrar dispositivos Apple em ambientes empresariais, configurar e atualizar ajustes via conexão sem fio, monitorar a conformidade com as políticas corporativas, gerenciar as políticas de atualização de software e até mesmo apagar ou bloquear remotamente dispositivos gerenciados.

Além dos registros tradicionais de dispositivos aos quais o iOS, iPadOS, macOS e tvOS oferecem suporte, um tipo de registro foi adicionado ao iOS 13 ou posterior, iPadOS 13.1 ou posterior e macOS 10.15 ou posterior — o Registro do Usuário. Os registros de usuários são registros de MDM que visam especificamente implantações do tipo “traga o seu próprio dispositivo” (BYOD), nas quais o dispositivo é de propriedade pessoal, embora seja usado em um ambiente gerenciado. Os registros de usuários concedem à solução MDM privilégios mais limitados do que aqueles de registros de dispositivos não supervisionados, além de proporcionarem a separação criptográfica entre os dados do usuário e os da empresa.

Tipos de registro

- *Registro Automático do Dispositivo:* o Registro Automático do Dispositivo permite que organizações configurem e gerenciem dispositivos a partir do momento que os dispositivos são tirados da caixa (em um processo conhecido como *implantação Avançada Automática*). Esses dispositivos são conhecidos como *supervisionados* e os usuários têm a opção de impedir que o perfil do MDM seja removido pelo usuário. O Registro Automático do Dispositivo foi projetado para dispositivos de propriedade da organização.
- *Registro do Dispositivo:* o Registro do Dispositivo permite que organizações façam com que usuários registrem dispositivos manualmente e gerenciem vários aspectos do uso do dispositivo, incluindo a capacidade de apagá-los. O Registro do Dispositivo também possui um conjunto maior de payloads e restrições que podem ser aplicados ao dispositivo. Quando um usuário remove um perfil de registro, todos os perfis de configuração, seus respectivos ajustes e apps gerenciados baseados nesse perfil de registro são removidos juntos com ele.

- *Registro do Usuário:* o Registro do Usuário é projetado para dispositivos de propriedade do usuário e é integrado a IDs Apple Gerenciados para estabelecer a identidade do usuário no dispositivo. IDs Apple Gerenciados fazem parte do perfil de Registro do Usuário, e o usuário deve autenticar com sucesso para que o registro seja concluído. IDs Apple Gerenciados podem ser usados ao mesmo tempo que o ID Apple pessoal com o qual o usuário já iniciou a sessão. Apps e contas gerenciados usam um ID Apple Gerenciado, enquanto apps e contas pessoais usam um ID Apple pessoal.

Restrições de dispositivos

As restrições podem ser ativadas — ou em alguns casos, desativadas — por administradores para ajudar a impedir que usuários acessem um certo app, serviço ou função de um iPhone, iPad, Mac ou Apple TV que esteja inscrito em uma solução MDM. As restrições são enviadas para os dispositivos em um payload de restrições, o qual faz parte de um perfil de configuração. Certas restrições em um iPhone podem ser espelhadas em um Apple Watch emparelhado.

Gerenciamento de ajustes de código e senha

Por padrão, o código do usuário pode ser definido por um PIN numérico. Nos dispositivos iOS e iPadOS com Face ID ou Touch ID, o tamanho mínimo do código é de quatro dígitos. Códigos maiores e mais complexos são recomendados, já que são mais difíceis de adivinhar ou atacar.

Administradores podem exigir códigos complexos e outras políticas através do MDM, Microsoft Exchange ActiveSync ou ao requisitar que usuários instalem perfis de configuração manualmente. Uma senha de administrador é necessária para a instalação do payload da política de código no macOS. Algumas políticas de código podem exigir certos tamanhos, composição ou outros atributos de código.

Exigência de perfis de configuração

Perfis de configuração são a principal forma usada por uma solução MDM para entregar e gerenciar políticas e restrições em dispositivos gerenciados. Caso organizações precisem configurar um grande número de dispositivos ou fornecer muitos ajustes de e-mail, ajustes de redes ou certificados personalizados a um grande número de dispositivos, os perfis de configuração são uma maneira segura de se fazer isso.

Perfis de configuração

Um *perfil de configuração* é um arquivo XML (com a extensão .mobileconfig) que consiste em payloads que carregam ajustes e informações de autorização em dispositivos Apple. Os perfis de configuração automatizam a configuração de ajustes, contas, restrições e credenciais. Esses arquivos podem ser criados por uma solução MDM ou pelo Apple Configurator para Mac, ou serem criados manualmente. Antes de enviar um perfil de configuração a um dispositivo Apple, organizações devem usar um perfil de registro para registrar o dispositivo na solução MDM.

Perfis de registro

Um *perfil de registro* é um perfil de configuração com um payload do MDM que registra o dispositivo na solução MDM especificada para esse dispositivo. Isso permite que a solução MDM envie comandos e perfis de configuração para o dispositivo e consulte certos aspectos do dispositivo. Quando um usuário remove um perfil de registro, todos os perfis de configuração, seus respectivos ajustes e apps gerenciados baseados nesse perfil de registro são removidos juntos com ele. Só pode haver um perfil de registro em um dispositivo por vez.

Ajustes de perfis de configuração

Um perfil de configuração contém uma série de ajustes em payloads específicos que podem ser especificados, incluindo, entre outros:

- Políticas de código e senha
- Restrição de recursos do dispositivo (por exemplo, desativar a câmera)
- Ajustes de rede e VPN
- Ajustes do Microsoft Exchange
- Ajustes do Mail
- Ajustes da conta
- Ajustes do serviço de diretório LDAP
- Ajustes do serviço de calendário CalDAV
- Credenciais e chaves
- Atualizações de software

Assinatura e criptografia do perfil

Um perfil de configuração pode ser assinado para validar sua origem e criptografado para ajudar a garantir sua integridade e proteger o conteúdo. Os perfis de configuração do iOS e iPadOS são criptografados por meio do Cryptographic Message Syntax (CMS) especificado no RFC 5652, com compatibilidade com 3DES e AES128.

Instalação de perfis

Os usuários podem instalar perfis de configuração diretamente nos dispositivos com o Apple Configurator para Mac. Os perfis também podem ser baixados pelo Safari, enviados como anexos em um e-mail, transferidos via AirDrop ou pelo app Arquivos no iOS e iPadOS, ou enviados por uma conexão sem fio com uma solução de gerenciamento de dispositivos móveis (MDM). Quando um usuário configura um dispositivo no Apple School Manager ou Apple Business Manager, o dispositivo baixa e instala um perfil para o registro no MDM. Para obter informações sobre como remover perfis, consulte Introdução a perfis de gerenciamento de dispositivos móveis em Implementação da Plataforma Apple.

Nota: em dispositivos supervisionados, perfis de configuração também pode ser bloqueados em um dispositivo. Isso é projetado para impedir sua remoção ou para permitir a remoção apenas com um código. Já que várias organizações usam seus próprios dispositivos iOS e iPadOS, os perfis de configuração que vinculam um dispositivo a uma solução MDM podem ser removidos, embora tal ação também remova todas as informações de configuração gerenciada, dados e apps.

Registro Automático do Dispositivo

As organizações podem registrar automaticamente dispositivos iOS, iPadOS, macOS e tvOS no gerenciamento de dispositivos móveis (MDM) sem que seja preciso tocá-los fisicamente ou prepará-los antes que os usuários os obtenham. Depois de se registrar em um dos serviços, o administrador inicia a sessão no site do serviço e vincula o programa à sua solução MDM. Os dispositivos comprados podem então ser atribuídos a usuários por meio do MDM. Durante o processo de configuração do dispositivo, a segurança de dados sigilosos pode ser aumentada por meio da aplicação de medidas de segurança apropriadas. Por exemplo:

- Fazer com que os usuários autentiquem como parte do fluxo de configuração inicial no Assistente de Configuração do dispositivo Apple durante a ativação.
- Fornecer uma configuração preliminar com acesso limitado e exigir configuração adicional do dispositivo para acessar dados sensíveis.

Depois da atribuição do usuário, quaisquer configurações, restrições ou controles específicos do MDM são instalados automaticamente. Todas as comunicações entre os dispositivos e os servidores Apple são criptografadas em trânsito por meio de HTTPS (TLS).

O processo de configuração para os usuários pode ser simplificado ainda mais por meio da remoção de etapas específicas do Assistente de Configuração dos dispositivos, para que os usuários possam começar a usá-los rapidamente. Os administradores também podem controlar se usuários podem remover o perfil de MDM do dispositivo e ajudarem a garantir a implementação de restrições ao longo do ciclo de vida do dispositivo. Depois que o dispositivo foi retirado da caixa e ativado, ele pode ser registrado na solução MDM da organização — e todos os ajustes de gerenciamento, apps e livros são instalados conforme definido pelo administrador do MDM.

Apple School Manager, Apple Business Manager e Apple Business Essentials

O Apple School Manager, o Apple Business Manager e o Apple Business Essentials são serviços oferecidos para que os administradores de TI possam implantar dispositivos Apple que uma organização tenha comprado diretamente da Apple ou através de Revendedores Autorizados Apple e operadoras participantes.

Quando usados com uma solução MDM, administradores podem simplificar o processo de configuração para usuários, configurar ajustes do dispositivo e distribuir apps e livros comprados nesses três serviços. O Apple School Manager também se integra a Sistemas de Informações de Alunos (SISs) diretamente ou via SFTP, e todos os três serviços podem usar o SCIM (Sistema para o Gerenciamento de Identidades entre Domínios) ou a autenticação federada com o Microsoft Azure Active Directory (Azure AD) para que administradores possam criar contas rapidamente.

A Apple mantém certificações em conformidade com os padrões ISO/IEC 27001 e 27018 para permitir que clientes da Apple analisem obrigações contratuais e de regulamentação. Essas certificações fornecem a nossos clientes uma declaração independente sobre as práticas de Privacidade e Segurança de Informações da Apple nos sistemas analisados. Para obter mais informações, consulte Certificações de segurança dos serviços de internet da Apple (em inglês) em Apple Platform Certifications.

Nota: para saber se um programa da Apple está disponível em um país ou região específica, consulte o artigo do Suporte da Apple: Disponibilidade de programas da Apple e métodos de pagamento para educação e negócios.

Supervisão de dispositivos

A *supervisão* normalmente evidencia que o dispositivo é de propriedade da organização, oferecendo a ela controle adicional sobre a configuração e restrições do dispositivo. Para obter mais informações, consulte Sobre a supervisão de dispositivos Apple em Implementação da Plataforma Apple.

Segurança do Bloqueio de Ativação

A maneira como a Apple exige o Bloqueio de Ativação depende do dispositivo ser um iPhone ou iPad, um Mac com Apple Silicon ou um Mac baseado em Intel com o chip Apple T2 Security.

Comportamento no iPhone e iPad

Em dispositivos iPhone e iPad, o Bloqueio de Ativação é aplicado através do processo de ativação depois da tela de seleção de Wi-Fi no Assistente de Configuração do iOS e iPadOS. Quando um dispositivo indica que está sendo ativado, ele envia um pedido a um servidor da Apple para obter um certificado de ativação. Nesse momento, dispositivos com Bloqueio de Ativação solicitam ao usuário que digite as credenciais do iCloud do usuário que ativou o Bloqueio de Ativação. O Assistente de Configuração do iOS e iPadOS progredirá apenas se um certificado válido puder ser obtido.

Comportamento em um Mac com Apple Silicon

Em um Mac com Apple Silicon, o LLB verifica a existência de uma LocalPolicy válida e se os valores do nonce da política LocalPolicy coincidem com os valores armazenados no Componente de Armazenamento Seguro. O LLB inicializa no recoveryOS se:

- Não houver uma LocalPolicy para o macOS atual
- Se a LocalPolicy não for válida para o macOS em questão
- Se os valores do hash do nonce da política LocalPolicy não coincidirem com os valores dos hashes armazenados no Componente de Armazenamento Seguro

O recoveryOS detecta que o computador Mac não está ativado e contata o servidor de ativação para obter um certificado de ativação. Nesse momento, se o dispositivo estiver com o Bloqueio de Ativação, o recoveryOS solicita ao usuário que digite as credenciais do iCloud do usuário que ativou o Bloqueio de Ativação. Depois de obter um certificado de ativação válido, a chave do certificado de ativação é usada para obter um certificado de RemotePolicy. O computador Mac usa a chave da LocalPolicy e o certificado da RemotePolicy para produzir uma LocalPolicy válida. O LLB não permitirá a inicialização do macOS se uma LocalPolicy válida não estiver presente.

Comportamento em computadores Mac baseados em Intel

Em um Mac baseado em Intel com um chip T2, o firmware do chip T2 verifica se um certificado de ativação válido está presente antes de permitir que o computador inicialize no macOS. O firmware da UEFI carregado pelo chip T2 é responsável por consultar o estado de ativação do dispositivo a partir do chip T2 e inicializar no recoveryOS em vez de inicializar no macOS se um certificado de ativação válido não estiver presente. O recoveryOS detecta que o Mac não está ativado e contata o servidor de ativação para obter um certificado de ativação. Nesse momento, se o dispositivo estiver com o Bloqueio de Ativação, o recoveryOS solicita ao usuário que digite as credenciais do iCloud do usuário que ativou o Bloqueio de Ativação. O firmware da UEFI não permitirá a inicialização do macOS se um certificado de ativação válido não estiver presente.

Modo Perdido Gerenciado e apagamento remoto

O Modo Perdido é usado para localizar dispositivos supervisionados quando eles são roubados. Depois de localizados, eles podem ser bloqueados ou apagados remotamente.

Modo Perdido Gerenciado

Se um dispositivo iOS ou iPadOS supervisionado com iOS 9 ou posterior for perdido ou roubado, o administrador de um gerenciamento de dispositivos móveis (MDM) pode ativar remotamente o Modo Perdido (chamado de Modo Perdido Gerenciado) nesse dispositivo. Quando o Modo Perdido Gerenciado está ativado, o usuário atual tem sua sessão encerrada e o dispositivo não pode ser desbloqueado. A tela mostra uma mensagem que pode ser personalizada pelo administrador, como por exemplo o número de telefone para o qual ligar caso o dispositivo seja encontrado. O administrador também pode solicitar que o dispositivo envie sua localização atual (mesmo se os Serviços de Localização estiverem desativados) e, opcionalmente, reproduza um som. Quando um administrador desativa o Modo Perdido Gerenciado, que é a única maneira de sair do modo, o usuário é informado dessa ação por meio de uma mensagem na Tela Bloqueada ou um alerta na tela de Início.

Apagamento remoto

Os dispositivos iOS, iPadOS e macOS podem ser apagados remotamente por um administrador ou usuário (o apagamento remoto imediato está disponível apenas se o FileVault do Mac estiver ativado). O apagamento remoto imediato é executado através do descarte seguro da chave de mídia do Armazenamento Apagável, o que torna todos os dados ilegíveis. No caso de apagamento remoto por meio do Microsoft Exchange ActiveSync, o dispositivo verifica com o Microsoft Exchange Server antes de realizar o apagamento.

Quando um comando de apagamento remoto é acionado via MDM ou iCloud, o dispositivo iPhone, iPad, iPod touch ou Mac atesta seu recebimento e realiza o apagamento.

O apagamento remoto não é possível nas seguintes situações:

- Com Registro do Usuário
- Com o uso do Microsoft Exchange ActiveSync quando a conta foi instalada com Registro do Usuário
- Com o uso do Microsoft Exchange ActiveSync se o dispositivo for supervisionado

Os usuários também podem usar o app Ajustes para apagar dispositivos iOS e iPadOS que estiverem em sua posse. E, conforme já mencionado, dispositivos iOS e iPadOS podem ser configurados para serem apagados automaticamente após uma série de tentativas malsucedidas de digitação do código.

Segurança do iPad Compartilhado no iPadOS

O iPad Compartilhado é um modo multiusuário para uso em implantações do iPad. Ele permite que usuários compartilhem um iPad ao mesmo tempo que mantém uma separação de documentos e dados para cada usuário. Cada usuário obtém sua própria localização de armazenamento reservada e privada, que é implementada como um volume APFS (Apple File System) protegido pelas credenciais do usuário. O iPad Compartilhado exige o uso de um ID Apple Gerenciado emitido e de propriedade da organização.

Com o iPad Compartilhado, um usuário pode iniciar sessão em um dispositivo de propriedade da organização configurado para ser utilizado por vários usuários. Os dados dos usuários são particionados em diretórios separados, cada um em seu próprio domínio de proteção de dados e protegido por permissões UNIX e sandbox. No iPadOS 13.4 ou posterior, usuários também podem iniciar a sessão em uma sessão temporária. Quando o usuário finaliza a sessão em uma sessão temporária, seu volume APFS é apagado e o espaço reservado para o volume retorna ao sistema.

Início de Sessão no iPad Compartilhado

Os IDs Apple Gerenciados tanto nativos quanto federados são aceitos ao iniciar uma sessão no iPad Compartilhado. Ao usar uma conta federada pela primeira vez, o usuário é redirecionado para o portal de início de sessão do provedor de identidade. Depois de autenticar, um token de acesso de curta duração é emitido para os IDs Apple Gerenciados armazenados e o processo de início de sessão continua de forma semelhante ao processo de início de sessão nativo de IDs Apple Gerenciados. Após o início de sessão, o Assistente de Configuração do iPad Compartilhado solicita ao usuário que defina um código (credencial) usado para proteger os dados locais no dispositivo e para autenticação na tela de início de sessão no futuro. Como em um dispositivo de usuário único, no qual o usuário iniciaria a sessão uma única vez no seu ID Apple Gerenciado com a conta federada e desbloquearia o dispositivo com o código, no iPad Compartilhado, o usuário inicia a sessão uma única vez com a conta federada e, a partir de então, usa o código estabelecido.

Quando um usuário inicia a sessão sem a autenticação federada, o ID Apple Gerenciado é autenticado com o Serviço de Identidade da Apple (IDS) pelo protocolo SRP. Se a autenticação for bem-sucedida, um token de acesso de curta duração específico do dispositivo é concedido. Se o usuário já tiver usado o dispositivo antes, ele já terá uma conta de usuário local, que é desbloqueada com a mesma credencial.

Se o usuário não tiver usado o dispositivo antes ou estiver usando o recurso de sessão temporária, o iPad Compartilhado fornece um novo ID de usuário UNIX, um volume APFS para armazenar os dados pessoais do usuário e chaves locais. Pelo fato de o armazenamento ser alocado (reservado) para o usuário quando da criação do volume APFS, pode não haver espaço suficiente para criar um volume novo. Nesse caso, o sistema identifica um usuário existente cujos dados tenham sido completamente sincronizados com a nuvem e o despeja do dispositivo para que o novo usuário possa iniciar a sessão. Na improvável eventualidade de que nenhum usuário existente tenha terminado de enviar seus dados à nuvem, o início de sessão do usuário novo falha. Para iniciar a sessão, o novo usuário precisará aguardar o término da sincronização dos dados de um usuário ou fazer com que um administrador apague à força uma conta de usuário existente, o que implica risco de perda de dados.

Se o dispositivo não estiver conectado à internet (se o usuário não tiver um ponto de acesso Wi-Fi, por exemplo), a autenticação pode usar a conta local como base durante um número limitado de dias. Nesse caso, apenas os usuários com contas locais previamente existentes ou uma sessão temporária podem iniciar a sessão. Depois que esse tempo limite expira, os usuários são obrigados a autenticar online, mesmo que uma conta local exista.

Depois que a conta local de um usuário for desbloqueada ou criada, caso tenha sido autenticada remotamente, o token de curta duração emitido pelos servidores da Apple é convertido em um token do iCloud que permite iniciar a sessão no iCloud. Em seguida, os ajustes do usuário são restaurados, e seus documentos e dados são sincronizados do iCloud.

Enquanto a sessão do usuário estiver ativa e o dispositivo permanecer on-line, os documentos e dados são armazenados no iCloud conforme forem criados ou modificados. Além disso, um mecanismo de sincronização em segundo plano ajuda a garantir que as alterações sejam enviadas ao iCloud ou a outros serviços da web através de sessões NSURLSession em segundo plano, após o usuário finalizar a sessão. Depois que a sincronização em segundo plano desse usuário for concluída, o volume APFS do usuário é desmontado e não pode ser montado novamente sem que o usuário inicie a sessão novamente.

Sessões temporárias não sincronizam dados com o iCloud e, embora uma sessão temporária possa iniciar a sessão em um serviço de sincronização de terceiros, como Box ou Google Drive, não há nenhuma possibilidade de continuar sincronizando os dados quando a sessão temporária termina.

Término de sessão no iPad Compartilhado

Quando um usuário finaliza a sessão no iPad Compartilhado, sua keybag é bloqueada imediatamente e todos os apps são encerrados. Para acelerar o caso de um usuário novo que inicia a sessão, o iPadOS posterga temporariamente algumas ações ordinárias de finalização de sessão e apresenta uma janela de início de sessão ao usuário novo. Se um usuário inicia a sessão durante esse tempo (aproximadamente 30 segundos), o iPad Compartilhado realiza a limpeza postergada como parte do início de sessão na conta do usuário novo. Porém, se o iPad Compartilhado permanecer ocioso, ele acionará a limpeza postergada. Durante a fase de limpeza, a Janela de Início de Sessão é reiniciada como se outra finalização de sessão tivesse ocorrido.

Quando uma sessão temporária termina, o iPad Compartilhado realiza a sequência completa de finalização de sessão e apaga imediatamente o volume APFS da sessão temporária.

Segurança do Apple Configurator

O Apple Configurator para Mac possui um design flexível, seguro e focado no dispositivo, permitindo que o administrador configure de forma fácil e rápida um ou dezenas de dispositivos iOS, iPadOS e tvOS conectados ao Mac via USB (ou dispositivos tvOS emparelhados através do Bonjour) antes de entregá-los aos usuários. Com o Apple Configurator para Mac, o administrador pode atualizar softwares, instalar apps e perfis de configuração, renomear e alterar a imagem da mesa de dispositivos, exportar informações sobre o dispositivo e documentos e muito mais.

O Apple Configurator para Mac também pode reviver ou restaurar computadores Mac com Apple Silicon e aqueles com o chip Apple T2 Security. Quando um Mac é revivido ou restaurado dessa maneira, o arquivo que contém as atualizações secundárias mais recentes dos sistemas operacionais (macOS, recoveryOS para Apple Silicon, ou sepOS para T2) é baixado de forma segura dos servidores da Apple e instalado diretamente no Mac. Depois do Mac ser revivido ou restaurado com sucesso, o arquivo é apagado do Mac que executa o Apple Configurator. Em momento algum o usuário pode inspecionar ou usar esse arquivo fora do Apple Configurator.

Os administradores também têm a opção de adicionar dispositivos ao Apple School Manager, Apple Business Manager ou Apple Business Essentials por meio do Apple Configurator para Mac ou Apple Configurator para iPhone, mesmo que os dispositivos não tenham sido comprados diretamente na Apple, em Revendedores Autorizados Apple ou em uma operadora de celular autorizada. Quando o administrador configura um dispositivo que foi registrado manualmente, ele se comporta como qualquer outro dispositivo em um daqueles serviços, com supervisão obrigatória e registro no gerenciamento de dispositivos móveis (MDM). No caso de dispositivos que não foram comprados diretamente, o usuário possui um período de 30 dias para liberar o dispositivo de um desses serviços, supervisão e MDM.

Para ativar dispositivos iOS, iPadOS e tvOS que não têm nenhuma conexão à internet, as organizações também podem usar o Apple Configurator para Mac e conectar esses dispositivos a um Mac host com uma conexão à internet enquanto eles estão sendo configurados. Administradores podem restaurar, ativar e preparar dispositivos com as configurações necessárias, incluindo apps, perfis e documentos, sem nunca precisar conectá-los a redes Wi-Fi ou celulares. Esse recurso não permite que um administrador contorne nenhum requisito existente do Bloqueio de Ativação exigido normalmente durante a ativação não conectada.

Segurança do Tempo de Uso

O Tempo de Uso é um recurso integrado para ver e gerenciar quanto tempo os adultos e as crianças passam usando apps, sites e outros. Existem dois tipos de usuários: adultos e crianças (gerenciadas).

Embora o Tempo de Uso não seja um recurso de segurança novo, é importante entender como ele protege a privacidade e a segurança dos dados coletados e compartilhados entre dispositivos. O Tempo de Uso está disponível no iOS 12 ou posterior, iPadOS 13.1 ou posterior, macOS 10.15 ou posterior, e alguns recursos no watchOS 6 ou posterior.

A tabela abaixo descreve os recursos principais do Tempo de Uso.

Recurso	Sistema operacional compatível
Visualizar dados sobre uso	iOS iPadOS macOS
Aplicar restrições adicionais	iOS iPadOS macOS watchOS
Definir limites de uso da web	iOS iPadOS macOS
Definir limites de uso de apps	iOS iPadOS macOS watchOS
Configurar o Repouso	iOS iPadOS macOS watchOS

Para usuários que gerenciam o uso de seus próprios dispositivos, os controles e dados de uso do Tempo de Uso podem ser sincronizados entre dispositivos associados à mesma conta do iCloud com a criptografia de ponta a ponta do CloudKit. Isso requer que a conta do usuário tenha a autenticação de dois fatores ativada (a sincronização fica ativada por padrão). O Tempo de Uso substitui o recurso de Restrições encontrado em versões anteriores do iOS e iPadOS, e o recurso de Controles Parentais encontrado em versões anteriores do macOS.

No iOS 13 ou posterior, iPadOS 13.1 ou posterior e macOS 10.15 ou posterior, os usuários do Tempo de Uso e as crianças gerenciadas compartilham automaticamente os dados de uso entre dispositivos se a autenticação de dois fatores estiver ativada em suas contas do iCloud. Quando um usuário limpa o histórico do Safari ou apaga um app, os dados de uso correspondentes são removidos do dispositivo e de todos os dispositivos sincronizados.

Pais e Tempo de Uso

Responsáveis também podem usar o Tempo de Uso em dispositivos iOS, iPadOS e macOS para entender e controlar o uso que as crianças fazem dos dispositivos. Se o pai ou mãe é organizador da família (no Compartilhamento Familiar do iCloud), pode visualizar os dados e gerenciar os ajustes do Tempo de Uso para seus filhos. As crianças são informadas quando seus responsáveis ativam o Tempo de Uso e elas também podem monitorar seu próprio uso. Quando os pais ativam o Tempo de Uso para seus filhos, definem um código de modo que os filhos não possam fazer alterações. Ao atingir a maioridade (a idade varia de acordo com o país ou região), a criança pode desativar essa monitoração.

Os dados de uso e ajustes de configuração são transferidos entre os dispositivos dos pais e dos filhos por meio do protocolo Serviço de Identidade da Apple (IDS), criptografado de ponta a ponta. Os dados criptografados podem ser armazenados brevemente em servidores IDS até serem lidos pelo dispositivo receptor (por exemplo, assim que o iPhone, iPad ou iPod touch for ligado, caso estivesse desligado). Tais dados não podem ser lidos pela Apple.

Análise do Tempo de Uso

Se o usuário ativar a opção Compartilhar Análise, somente os dados anonimizados a seguir serão coletados, para que a Apple possa entender melhor como o Tempo de Uso está sendo usado:

- Se o Tempo de Uso foi ativado durante o Assistente de Configuração ou posteriormente nos Ajustes
- Alteração no uso de uma Categoria após a criação de um limite para ela (em até 90 dias)
- Se o Tempo de Uso está ativado
- Se o Repouso está ativado
- Quantas vezes a consulta “Pedir Mais Tempo” foi usada
- Número de limites de apps
- Número de vezes que os usuários visualizaram o uso nos ajustes do Tempo de Uso, por tipo de usuário e por tipo de visualização (local, remota, widget)
- Número de vezes que os usuários ignoram um limite, por tipo de usuário
- Número de vezes que os usuários apagam um limite, por tipo de usuário

Nenhum dado específico de uso de apps ou da web é coletado pela Apple. Quando um usuário vê uma lista de apps nas informações de uso do Tempo de Uso, os ícones dos apps são obtidos diretamente da App Store, que não retém quaisquer dados dessas solicitações.

Glossário

acesso direto à memória (DMA) Um recurso que permite que subsistemas de hardware acessem a memória principal diretamente, contornando a CPU.

AES (Padrão de Criptografia Avançada) Um padrão de criptografia global popular, usado para criptografar dados para mantê-los privados.

AES-XTS Um modo do AES definido no IEEE 1619-2007 para a criptografia de mídias de armazenamento.

Aleatorização do Layout de Espaço de Endereço (ASLR) Uma técnica empregada pelos sistemas operacionais para dificultar o êxito da exploração de erros de software. A garantia de imprevisibilidade de endereços e offsets da memória impossibilita o hardcode desses valores pelo código de aproveitamento.

Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA) Um algoritmo de assinatura digital baseado em criptografia de curvas elípticas.

APFS (Apple File System) O sistema de arquivos padrão do iOS, iPadOS, tvOS, watchOS e computadores Mac com o macOS 10.13 ou posterior. O APFS oferece criptografia forte, compartilhamento de espaço, capturas, dimensionamento rápido de diretórios e fundamentos de sistema de arquivos melhorados.

Apple Business Manager Um portal web simples para administradores de TI que oferece uma maneira rápida e eficiente para que organizações implantem dispositivos Apple comprados diretamente da Apple ou de um Revendedor Autorizado Apple ou operadora participante. Elas podem registrar dispositivos automaticamente em suas soluções de gerenciamento de dispositivos móveis (MDM) sem que seja preciso tocá-los fisicamente ou prepará-los antes que os usuários os obtenham.

Apple School Manager Um portal web simples para administradores de TI que oferece uma maneira rápida e eficiente para que organizações implantem dispositivos Apple comprados diretamente da Apple ou de um Revendedor Autorizado Apple ou operadora participante. Elas podem registrar dispositivos automaticamente em suas soluções de gerenciamento de dispositivos móveis (MDM) sem que seja preciso tocá-los fisicamente ou prepará-los antes que os usuários os obtenham.

Armazenamento Apagável Área dedicada do armazenamento NAND, usada para armazenar chaves criptográficas, que pode ser endereçada diretamente e apagada com segurança. Mesmo não fornecendo proteção caso um ataque físico ao dispositivo ocorra, as chaves armazenadas no Armazenamento Apagável podem ser usadas como parte de uma hierarquia de chaves para facilitar o apagamento rápido e invocar segurança.

autorização do software do sistema Um processo que combina chaves criptográficas integradas ao hardware com um serviço on-line para verificar que apenas softwares legítimos da Apple, adequados a dispositivos compatíveis, sejam fornecidos e instalados durante a atualização.

bits de núcleo de software Bits dedicados no Mecanismo AES do Secure Enclave que são afixados ao UID ao gerar chaves a partir do UID. Cada bit de núcleo de software tem um bit de bloqueio correspondente. A ROM de Inicialização do Secure Enclave e o sistema operacional podem alterar independentemente o valor de cada bit de núcleo de software, contanto que o bit de bloqueio correspondente não tenha sido definido. Depois que o bit de bloqueio é definido, não é possível modificar o bit de núcleo de software nem o bit de bloqueio. Os bits de núcleo de software e seus bloqueadores são redefinidos quando o Secure Enclave é reinicializado.

Boot Camp Um utilitário do Mac que permite a instalação do Microsoft Windows em computadores Mac compatíveis.

chave de mídia Parte da hierarquia de chave de criptografia que ajuda a fornecer um apagamento seguro e instantâneo. No iOS, iPadOS, tvOS e watchOS, a chave de mídia embala os metadados no volume de dados (sendo assim, sem ela, o acesso a todas as chaves únicas por arquivo não é possível, deixando inacessíveis os arquivos protegidos pela Proteção de Dados). No macOS, a chave de mídia embala o material das chaves, todos os metadados e dados no volume protegido pelo FileVault. Em ambos os casos, o apagamento da chave de mídia deixa os dados criptografados inacessíveis.

chave derivada do código (PDK) A chave de criptografia derivada do trançamento da senha do usuário com a chave SKP de longo prazo e o UID do Secure Enclave.

chave do sistema de arquivos Chave que criptografa os metadados de cada arquivo, incluindo sua chave de classe. Mantida no Armazenamento Apagável, priorizando facilitar o apagamento rápido em detrimento da confidencialidade.

chave única por arquivo A chave usada pela Proteção de Dados para criptografar um arquivo no sistema de arquivos. A chave única por arquivo é embalada por uma chave de classe e armazenada nos metadados do arquivo.

chaves Infraestrutura e conjunto de APIs usadas pelos sistemas operacionais da Apple e apps de terceiros para armazenar e obter senhas, chaves e outras credenciais sigilosas.

circuito integrado (CI) Também conhecido como *microchip*.

CKRecord Um dicionário de pares chave-valor que contêm dados salvos ou transferidos do CloudKit.

Cofre de Dados Um mecanismo — aplicado pelo kernel — para proteger contra o acesso não autorizado a dados, independentemente de o app que os solicita usar sandbox.

Componente de Armazenamento Seguro Um chip projetado com um código ROM imutável, um gerador de números aleatórios de hardware, mecanismos criptográficos e detecção de adulteração física. Em dispositivos compatíveis, o Secure Enclave é emparelhado com um Componente de Armazenamento Seguro para armazenamento do nonce antirreprodução. Para ler e atualizar os nonces, o Secure Enclave e o chip de armazenamento empregam um protocolo seguro que ajuda a garantir acesso exclusivo aos nonces. Há diversas gerações dessa tecnologia com garantias de segurança diferentes.

controlador de memória O subsistema em um sistema no chip que controla a interface entre o sistema no chip e sua memória principal.

Controlador do SSD Um subsistema de hardware que gerencia a mídia de armazenamento (unidade de estado sólido).

Elliptic Curve Diffie-Hellman Exchange Ephemeral (ECDHE) Um mecanismo de troca de chaves baseado em curvas elípticas. A ECDHE permite que duas partes concordem com uma chave secreta de modo que impeça que a chave seja descoberta por um interceptador observando as mensagens entre as duas partes.

embalagem de chaves Criptografia de uma chave com outra. O iOS e iPadOS usam a embalagem de chaves NIST AES, conforme o RFC 3394.

Firmware da Interface de Firmware Extensível Unificada (UEFi) Uma tecnologia de substituição da BIOS para conectar um firmware ao sistema operacional de um computador.

Gatekeeper No macOS, uma tecnologia projetada para ajudar a garantir que apenas softwares confiáveis sejam executados no Mac de um usuário.

Gerenciador de Inicialização de Baixo Nível (LLB) Em computadores Mac com arquitetura de inicialização de dois estágios, o LLB contém o código chamado pela ROM de Inicialização que, por sua vez, carrega o iBoot como parte da cadeia de inicialização segura.

gerenciamento de dispositivos móveis (MDM) Um serviço que permite que um administrador gerencie remotamente os dispositivos registrados. Depois do registro de um dispositivo, o administrador pode usar o serviço de MDM através da rede para configurar ajustes e realizar outras tarefas no dispositivo sem a interação do usuário.

HMAC Um código de autenticação de mensagem que usa hash e baseia-se em uma função de hash criptográfico.

iBoot O gerenciador de inicialização de segundo estágio para todos os dispositivos Apple. Código que carrega o XNU, como parte da cadeia de inicialização segura. Dependendo da geração do sistema no chip (SoC), o iBoot pode ser carregado pelo Gerenciador de Inicialização de Baixo Nível ou diretamente pela ROM de Inicialização.

ID de grupo (GID) Semelhante ao UID, mas comum a cada processador de uma classe.

ID exclusivo (UID) Chave AES de 256 bits gravada em cada processador durante o processo de manufatura. Não pode ser lida por firmware ou software e é usada apenas pelo Mecanismo AES de hardware do processador. Para obter a chave em si, seria preciso montar um ataque físico altamente sofisticado e caro contra o silício do processador. O UID não está relacionado a nenhum outro identificador do dispositivo, incluindo, entre outros, o UDID.

Identificação Exclusiva de Chip (ECID) Um identificador de 64 bits exclusivo ao processador de cada dispositivo iOS e iPadOS. Quando uma ligação é atendida em um dispositivo, o toque de dispositivos próximos emparelhados com o iCloud é interrompido com um breve anúncio por meio de Bluetooth Low Energy (BLE) 4.0. Os bytes do anúncio são criptografados pelo mesmo método dos anúncios do Handoff. Usado como parte do processo de personalização, ele não é considerado um segredo.

Identificador Uniforme de Recursos (URI) String de caracteres que identifica um recurso baseado na web.

Interface de Periférico Serial Aprimorada (eSPI) Um barramento completo projetado para comunicação serial síncrona.

Joint Test Action Group (JTAG) Uma ferramenta padrão de depuração de hardware usada por programadores e desenvolvedores de circuitos.

keybag Estrutura de dados usada para armazenar uma coleção de chaves de classe. Cada tipo (usuário, dispositivo, sistema, backup, guarda ou Backup do iCloud) possui o mesmo formato.

Um cabeçalho contendo: Versão (definida como quatro no iOS 12 ou posterior), Tipo (sistema, backup, guarda ou Backup do iCloud), UUID da Keybag, um HMAC caso a keybag esteja assinada e o método usado para embalar as chaves de classe — trançamento com o UID ou PBKDF2, juntamente com o sal e a contagem da iteração.

Uma lista de chaves de classe: UUID da chave, Classe (qual arquivo ou classe da Proteção de Dados das Chaves), tipo de embalagem (apenas chave derivada do UID; chave derivada do UID e chave derivada do código), chave de classe embalada e uma chave pública para classes assimétricas.

mapeamento do ângulo de fluxo dos sulcos Representação matemática da direção e largura dos sulcos extraídos de parte de uma impressão digital.

mecanismo criptográfico AES Um componente de hardware dedicado que implementa o AES.

Modo de Atualização do Firmware do Dispositivo (DFU) Modo no qual o código ROM de Inicialização aguarda por recuperação via USB. A tela fica preta quando no modo DFU, mas ao conectar-se a um computador com o iTunes ou o Finder aberto, o seguinte diálogo é apresentado: "O iTunes (ou o Finder) detectou um (iPad, iPhone ou iPod touch) em modo de recuperação. O usuário precisa restaurar esse (iPad, iPhone ou iPod touch) antes de usá-lo com o iTunes (ou o Finder)."

modo de recuperação Um modo usado para restaurar vários dispositivos Apple se ele não reconhecer o dispositivo do usuário para que o usuário possa reinstalar o sistema operacional.

módulo de segurança de hardware (HSM) Computador especializado inviolável que resguarda e gerencia chaves digitais.

NAND Memória flash não volátil.

nonce Um número exclusivo, de utilização única, empregado em vários protocolos de segurança.

perfil de provisão Um arquivo de lista de propriedades (arquivo .plist) assinado pela Apple que contém um conjunto de entidades e direitos que permitem a instalação e o teste de apps em um dispositivo iOS ou iPadOS. Um perfil de provisão de desenvolvimento lista os dispositivos escolhidos por um desenvolvedor para distribuição ad hoc. Um perfil de provisão de distribuição contém o ID do app de apps desenvolvidos por empresas.

Proteção da Integridade do Coprocessador do Sistema (SCIP) Um mecanismo usado pela Apple projetado para impedir modificações ao firmware do coprocessador.

Proteção de Chave Selada (SKP) Uma tecnologia na Proteção de Dados que protege (ou *sela*) as chaves de criptografia com medidas do software do sistema e chaves disponíveis apenas no hardware (como o UID do Secure Enclave).

Proteção de Dados Um mecanismo de proteção de arquivos e chaves para dispositivos Apple compatíveis. Também pode referir-se às APIs que os apps usam para proteger arquivos e itens das chaves.

Recompensa de Segurança da Apple Uma recompensa oferecida pela Apple a pesquisadores que relatem uma vulnerabilidade que afete os sistemas operacionais mais recentes disponíveis e, nos casos relevantes, o hardware mais recente.

Registro de Progresso de Inicialização (BPR) Um conjunto de sinalizações de hardware do sistema no chip (SoC) que o software pode usar para rastrear os modos de inicialização nos quais o dispositivo entrou, como o modo de Atualização do Firmware do Dispositivo (DFU) e o modo de Recuperação. Depois que uma sinalização de Registro de Progresso de Inicialização é definida, ela não pode ser limpa. Isso permite que um software posterior obtenha um indicador confiável do estado do sistema.

ROM de Inicialização Primeiro código executado pelo processador de um dispositivo ao ser inicializado. Por ser parte integral do processador, não pode ser alterado pela Apple ou por um atacante.

sepOS O firmware do Secure Enclave, baseado na versão do microkernel L4 personalizado pela Apple.

Serviço de Identidade da Apple (IDS) Diretório da Apple de chaves públicas do iMessage, endereços APNs, números de telefone e endereços de e-mail usados para buscar chaves e endereços de dispositivos.

serviço de Notificações Push da Apple (APNs) Serviço mundial fornecido pela Apple que entrega notificações push para dispositivos Apple.

sistema no chip (SoC) Circuito integrado (CI) que incorpora vários componentes em um único chip. O Processador de Aplicativos, o Secure Enclave e outros coprocessadores são componentes do SoC.

trançamento Processo pelo qual o código de um usuário é transformado em uma chave criptográfica e fortificado com o UID do dispositivo. Esse processo ajuda a garantir que ataques de força bruta tenham que ser realizados em um dispositivo específico, diminuindo assim a probabilidade da ocorrência (que não pode ser feita em paralelo). O algoritmo do trançamento (PBKDF2) usa AES chaveado com o UID do dispositivo como função pseudoaleatória (PRF) em cada iteração.

Unidade de Gerenciamento de Memória de Entrada/Saída (IOMMU) Uma unidade de gerenciamento de memória de entrada/saída. Um subsistema em um chip integrado que controla o acesso ao espaço de endereço de outros dispositivos e periféricos de entrada/saída.

xART Uma abreviação de Tecnologia Antirreprodução Ampliada (em inglês). Um conjunto de serviços que fornecem armazenamento criptografado, autenticado e persistente ao Secure Enclave com capacidades antirreprodução baseadas na arquitetura do armazenamento físico. Consulte Componente de Armazenamento Seguro.

XNU Núcleo dos sistemas operacionais da Apple. É considerado confiável e exige medidas de segurança como assinatura de código, sandbox, verificação de direitos e Aleatorização de Espaço de Endereço (ASLR).

XProtect No macOS, uma tecnologia antivírus, com base em assinaturas, para detecção e remoção de malware.

Histórico de revisão do documento

Histórico de revisão do documento

Data	Resumo
Dezembro de 2022	Tópicos adicionados: • Proteção Avançada de Dados do iCloud Tópicos atualizados: • Visão geral da segurança do iCloud • Criptografia do iCloud • Segurança do Backup do iCloud • Segurança de contatos de recuperação de conta • Segurança de Contatos de Legado
Maio de 2022	Atualizado para: • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 Tópicos adicionados: • Restrições do recoveryOS emparelhado • Versão do Sistema Operacional Local (love) • Compartilhamento de dados de Saúde • Segurança de contatos de recuperação de conta • Segurança de Contatos de Legado • Segurança do Tap to Pay on iPhone • Acesso usando a Carteira da Apple • Tipos de credenciais de acesso • Documentos de identidade na Carteira da Apple • Acessórios do HomeKit compatíveis com a Siri

Data	Resumo
Maio de 2022	Tópicos atualizados: • Magic Keyboard com Touch ID • Face ID, Touch ID, códigos e senhas • Segurança da identificação facial • Cartões Expressos com reserva de energia • Modos de inicialização para um Mac com Apple Silicon • Conteúdo de um arquivo LocalPolicy para um Mac com Apple Silicon • Segurança do volume de sistema assinado no iOS, iPadOS e macOS • Segurança do sistema para o watchOS • Dispositivo de Pesquisa de Segurança da Apple • Função do Apple File System • Proteção do acesso de apps a dados de usuário • Introdução à segurança de apps para macOS • Proteção contra malware no macOS • Visão geral da segurança do iCloud • Sincronização segura das chaves • Recuperação segura das Chaves do iCloud • Uso do Apple Pay para pagamentos com cartões • Tíquetes por proximidade no Apple Pay • Inutilização de cartões com o Apple Pay • Solicitação do Apple Card • Segurança do Apple Cash • Adição de cartões de transporte público e eMoney à Carteira da Apple • Proteção do Apple Messages for Business • Segurança do FaceTime • Segurança das chaves de carro no iOS • Segurança do Apple Configurator Tópicos removidos: • Acessórios do HomeKit e iCloud

Data	Resumo
Maio de 2021	Atualizado para: • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 Tópicos adicionados: • Magic Keyboard com Touch ID. • Intenção de segurança e conexões ao Secure Enclave. • Desbloqueio Automático e Apple Watch. • Hash do Manifesto CustomOS Image4 (coih). Tópicos editados: • Duas novas transações de Modo Expresso adicionadas a Cartões Expressos com reserva de energia. • Edição em Resumo de recursos do Secure Enclave. • Conteúdo de atualização de software adicionado à Multi-inicialização Segura (smb3). • Conteúdo adicional para Proteção de Chave Selada (SKP).

Data	Resumo
Fevereiro de 2021	Atualizado para: • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 Tópicos adicionados: • Implementação do iBoot em memória segura • Processo de inicialização para um Mac com Apple Silicon • Modos de inicialização para um Mac com Apple Silicon • Controle da política de segurança do Disco de Inicialização para um Mac com Apple Silicon • Criação e gerenciamento da chave de assinatura da LocalPolicy • Conteúdo de um arquivo LocalPolicy para um Mac com Apple Silicon • Segurança do volume de sistema assinado no iOS, iPadOS e macOS • Dispositivo de Pesquisa de Segurança da Apple • Monitoração de Senhas • Segurança de IPv6 • Segurança das chaves de carro no iOS Tópicos atualizados: • Secure Enclave • Desconexão do microfone por hardware • recoveryOS e ambientes de diagnóstico para um computador Mac baseado em Intel • Proteções do acesso direto à memória em computadores Mac • Extensões do kernel no macOS • Proteção da Integridade do Sistema • Segurança do sistema para o watchOS • Gerenciamento do FileVault no macOS • Acesso de apps a senhas salvas • Recomendações de segurança de senha • Segurança do Apple Cash • Proteção do Apple Messages for Business • Privacidade de Wi-Fi • Segurança do Bloqueio de Ativação • Segurança do Apple Configurator

Data	Resumo
Abril de 2020	Atualizado para: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Atualizações: • Desconexão do microfone do iPad adicionado à Desconexão do microfone por hardware. • Cofres de dados adicionados à Proteção do acesso de apps a dados do usuário. • Atualizações ao Gerenciamento do FileVault no macOS e Ferramentas de linha de comando. • Adições à Ferramenta de Remoção de Malware em Proteção contra malware no macOS. • Atualizações à Segurança do iPad Compartilhado no iPadOS.
Dezembro de 2019	Os documentos Manual de Segurança do iOS, Visão Geral da Segurança no macOS e Visão Geral do Chip Apple T2 Security foram combinados Atualizado para: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Controles de Privacidade, Siri e Sugestões da Siri, e Prevenção de Rastreamento Inteligente do Safari foram removidos. Consulte https://www.apple.com/br/privacy/ para obter as informações mais recentes sobre esses recursos.
Maio de 2019	Atualizado para o iOS 12.3 • Compatível com TLS 1.3 • Descrição revisada da segurança do AirDrop • Modo DFU e modo de Recuperação • Requisitos de código para conexão de acessórios
Novembro de 2018	Atualizado para o iOS 12.1 • FaceTime em Grupo
Setembro de 2018	Atualizado para o iOS 12 Secure Enclave • Proteção da Integridade do Sistema Operacional • Express Card com reserva de energia • Modo DFU e modo de Recuperação • Acessórios do HomeKit TV Remote • Tíquetes por proximidade • Cartões de ID de estudante • Sugestões da Siri • Atalhos na Siri • App Atalhos • Gerenciamento de senha de usuário • Tempo de Uso • Certificações de Segurança e Programas

Data	Resumo
Julho de 2018	Atualizado para o iOS 11.4 • Políticas de biometria • HomeKit • Apple Pay • Bate-papo de Negócios • Mensagens no iCloud • Apple Business Manager
Dezembro de 2017	Atualizado para o iOS 11.2 • Apple Pay Cash
Outubro de 2017	Atualizado para o iOS 11.1 • Certificações de Segurança e Programas • Touch ID/Face ID • Notas Compartilhadas • Criptografia de ponta a ponta do CloudKit • Atualização de TLS • Apple Pay, Pagamento na web com o Apple Pay • Sugestões da Siri • iPad Compartilhado
Julho de 2017	Atualizado para o iOS 10.3 • Secure Enclave • Proteção de Dados de Arquivos • Keybags • Certificações de Segurança e Programas • SiriKit • HealthKit • Segurança de Rede • Bluetooth • iPad Compartilhado • Modo Perdido • Bloqueio de Ativação • Controles de Privacidade
Março de 2017	Atualizado para o iOS 10 Segurança do Sistema • Classes de Proteção de Dados • Certificações de Segurança e Programas • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Início de sessão único • Apple Pay, Pagamento na web com o Apple Pay • Provisão de cartões de crédito, débito e pré-pagos • Sugestões do Safari

Data	Resumo
Maio de 2016	Atualizado para o iOS 9.3 • IDs Apple Gerenciados • Autenticação de dois fatores para ID Apple • Keybags • Certificações de Segurança • Modo Perdido, Bloqueio de Ativação • Notas Seguras • Apple School Manager • iPad Compartilhado
Setembro de 2015	Atualizado para o iOS 9 Bloqueio de ativação do Apple Watch • Políticas de código • Suporte à API do Touch ID • A Proteção de dados no A8 usa AES-XTS • Keybags para atualização de software não supervisionada • Atualizações de certificação • Modelo de confiança de app empresarial • Proteção de Dados para favoritos do Safari • Segurança de Transporte em Apps • Especificações VPN • Acesso Remoto ao iCloud para o HomeKit • Cartões de Fidelidade no Apple Pay, app da administradora do cartão no Apple Pay • Indexação local do Spotlight • Modelo de Emparelhamento do iOS • Apple Configurator 2 • Restrições

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

BR028-00625