Keamanan Platform Apple

Mei 2022

Konten

Keamanan Platform Apple

Pengantar keamanan platform Apple

Apple merancang keamanan ke inti platform-nya. Berdasarkan pengalaman membuat sistem operasi bergerak paling canggih di dunia, Apple telah membuat arsitektur keamanan yang mengatasi persyaratan unik ponsel, jam, desktop, dan rumah.

Setiap perangkat Apple menggabungkan *perangkat keras*, *perangkat lunak*, dan *layanan* yang dirancang untuk bekerja sama untuk keamanan maksimal serta pengalaman pengguna yang transparan demi menjaga informasi pribadi tetap aman. Misalnya, silicon dan perangkat keras keamanan rancangan Apple menyediakan fitur keamanan penting. Selain itu, perlindungan perangkat lunak bekerja untuk menjaga sistem operasi dan app pihak ketiga tetap terlindungi. Terakhir, layanan menyediakan mekanisme untuk pembaruan perangkat lunak yang aman dan tepat waktu, memperkuat ekosistem app yang terlindungi, dan memfasilitasi komunikasi serta pembayaran yang aman. Hasilnya, perangkat Apple tidak hanya melindungi perangkat dan datanya, tapi seluruh ekosistem, termasuk semua hal yang pengguna lakukan secara lokal, di jaringan, dan dengan layanan internet utama.

Kami tidak hanya merancang produk yang sederhana, intuitif, dan andal, tapi juga aman. Fitur keamanan utama, seperti enkripsi perangkat berbasis perangkat keras, tidak dapat dinonaktifkan secara tidak sengaja. Fitur lainnya, seperti Face ID dan Touch ID, meningkatkan pengalaman pengguna dengan pengamanan perangkat lebih mudah dan intuitif. Karena banyak dari fitur ini yang diaktifkan secara default, pengguna atau bagian TI tidak perlu melakukan konfigurasi ekstensif.

Dokumentasi ini menyediakan detail mengenai bagaimana teknologi dan fitur keamanan diterapkan di dalam platform Apple. Hal ini juga membantu organisasi menggabungkan fitur dan teknologi keamanan platform Apple dengan kebijakan dan prosedur mereka sendiri untuk memenuhi kebutuhan keamanan khusus mereka.

Konten dokumentasi dibagi ke dalam topik pembahasan berikut:

- **Keamanan dan biometrik perangkat keras:** Silicon dan perangkat keras yang membangun landasan untuk keamanan di perangkat Apple, termasuk Apple silicon, Secure Enclave, mesin kriptografis, Face ID, dan Touch ID
- **Keamanan sistem:** Fungsi perangkat keras dan perangkat lunak terpadu yang menyediakan boot aman, pembaruan, dan proses pengoperasian sistem operasi Apple
- **Enkripsi dan Perlindungan Data:** Arsitektur dan rancangan yang melindungi data pengguna jika perangkat hilang atau dicuri, atau jika orang atau proses yang tidak berwenang mencoba menggunakan atau memodifikasinya
- **Keamanan app:** Perangkat lunak dan layanan yang menyediakan ekosistem app yang aman dan memungkinkan app berjalan dengan aman dan tanpa mengganggu integritas platform

- **Keamanan layanan:** Layanan Apple untuk identifikasi, pengelolaan kata sandi, pembayaran, komunikasi, dan menemukan perangkat yang hilang
- **Keamanan jaringan:** Protokol jaringan standar industri yang menyediakan pengesahan dan enkripsi data yang aman pada saat transmisi
- **Keamanan kit pengembang:** Kerangka "kit" untuk pengelolaan rumah dan kesehatan yang aman serta pribadi, serta ekstensi perangkat dan kemampuan layanan Apple terhadap app pihak ketiga
- **Manajemen perangkat aman:** Metode yang memungkinkan pengelolaan perangkat Apple, membantu mencegah penggunaan yang tidak sah, dan mengaktifkan penghapusan jarak jauh jika perangkat hilang atau dicuri

Komitmen terhadap keamanan

Apple berkomitmen untuk membantu melindungi pelanggan dengan teknologi privasi dan keamanan terkemuka—dirancang untuk menjaga informasi pribadi—serta metode yang menyeluruh untuk membantu melindungi data perusahaan di lingkungan perusahaan. Apple memberikan imbalan kepada peneliti untuk menemukan kerentanan dengan menawarkan Apple Security Bounty. Detail program dan kategori hadiah tersedia di https://developer.apple.com/security-bounty/.

Kami mempekerjakan tim keamanan khusus untuk mendukung semua produk Apple. Tim menyediakan pengauditan dan pengujian keamanan untuk produk yang dalam pengembangan dan telah dirilis. Tim Apple juga menyediakan alat dan pelatihan keamanan, dan secara aktif mengawasi ancaman serta laporan masalah keamanan baru. Apple adalah anggota Forum of Incident Response and Security Teams (FIRST).

Apple terus menembus batas dari hal yang memungkinkan pada keamanan dan privasi. Apple menggunakan silikon khusus di berbagai produk—dari Apple Watch ke iPhone dan iPad, ke Keping Keamanan T2 dan Apple silicon di Mac—yang meningkatkan bukan hanya efisiensi komputasi tapi juga keamanan. Misalnya, Apple silicon membentuk landasan boot aman, Face ID dan Touch ID, serta Perlindungan Data. Selain itu, fitur keamanan di perangkat yang ditenagai oleh Apple silicon—seperti Perlindungan Integritas Kernel, Kode Pengesahan Penunjuk, dan Pembatasan Izin Cepat—membantu menangani jenis serangan siber yang umum. Maka, meskipun kode penyerang dieksekusi, dampak serangannya berkurang secara drastis.

Untuk mengoptimalkan fitur keamanan ekstensif yang tersedia secara internal di platform kami, organisasi dianjurkan untuk meninjau kebijakan TI dan keamanan mereka untuk memastikan bahwa mereka telah benar-benar memanfaatkan lapisan teknologi keamanan yang ditawarkan oleh platform ini.

Untuk mempelajari lebih lanjut tentang cara melaporkan masalah ke Apple dan berlangganan pemberitahuan keamanan, lihat Melaporkan kerentanan keamanan atau privasi.

Apple percaya privasi adalah hak dasar setiap manusia dan memiliki berbagai kontrol dan pilihan internal yang memungkinkan pengguna menentukan bagaimana dan kapan app menggunakan informasi mereka, serta informasi apa yang digunakan. Untuk mempelajari lebih lanjut mengenai pendekatan Apple terhadap privasi, kontrol privasi di perangkat Apple, dan kebijakan privasi Apple, lihat https://www.apple.com/id/privacy**.**

Catatan: Kecuali dinyatakan berbeda, dokumentasi ini mencakup versi sistem operasi berikut: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4, dan watchOS 8.5.

Keamanan dan biometrik perangkat keras

Tinjauan keamanan perangkat keras

Agar aman, perangkat lunak harus berada di perangkat keras yang memiliki keamanan internal. Oleh karena itu, perangkat Apple—yang menjalankan iOS, iPadOS, macOS, tvOS, dan watchOS—memiliki kemampuan keamanan yang dirancang ke dalam silikon. Kemampuan ini termasuk CPU yang menenagai fitur keamanan sistem, serta silicon tambahan yang didedikasikan untuk fungsi keamanan. Perangkat keras khusus keamanan mengikuti prinsip dukungan fungsi yang didefinisikan secara terbatas dan rahasia agar dapat meminimalisasi area serangan. Salah satu komponennya adalah ROM boot, yang membuat akar kepercayaan perangkat keras untuk boot aman, mesin AES khusus untuk enkripsi serta dekripsi yang efisien dan aman, serta Secure Enclave. *Secure Enclave* adalah sistem pada keping (SoC) yang terdapat di semua perangkat iPhone, iPad, Apple Watch, Apple TV serta HomePod baru, dan di Mac dengan Apple silicon serta Mac dengan Keping Keamanan T2 Apple. Secure Enclave sendiri mengikuti prinsip rancangan yang sama dengan SoC, berisi ROM boot dan mesin AES diskretnya sendiri. Secure Enclave juga menyediakan landasan untuk pembuatan aman dan penyimpanan kunci yang penting untuk mengenkripsi data saat disimpan, dan melindungi serta mengevaluasi data biometrik untuk Face ID dan Touch ID.

Enkripsi penyimpanan harus bersifat cepat dan efisien. Pada saat yang bersamaan, enkripsi tidak dapat mengekspos data (atau *materi kunci*) yang digunakan untuk membuat hubungan kunci kriptografis. Mesin perangkat keras AES menyelesaikan masalah ini dengan melakukan enkripsi dan dekripsi sebaris yang cepat *saat file ditulis atau dibaca*. Saluran khusus dari Secure Enclave menyediakan materi kunci penting ke mesin AES tanpa mengekspos informasi ini ke Prosesor Aplikasi (atau CPU) atau keseluruhan sistem operasi. Ini membantu memastikan bahwa teknologi Perlindungan Data dan FileVault Apple melindungi file pengguna tanpa memaparkan kunci enkripsi jangka panjang.

Apple telah merancang boot aman untuk melindungi level terendah dari perangkat lunak agar tidak diubah dan untuk mengizinkan hanya perangkat lunak sistem operasi tepercaya dari Apple yang dimuat saat proses mulai. Boot aman dimulai di kode tetap yang disebut ROM Boot, yang dipasang pada saat SoC Apple dibuat dan disebut sebagai *dasar kepercayaan perangkat keras*. Di komputer Mac dengan keping T2, kepercayaan untuk boot aman macOS dimulai dengan keping T2. (Keping T2 dan Secure Enclave juga mengeksekusi proses boot amannya sendiri menggunakan ROM boot terpisah—ini adalah analog pasti mengenai bagaimana keping seri A dan kumpulan M1 melakukan boot dengan aman.)

Secure Enclave juga memproses data wajah dan sidik jari dari sensor Face ID serta Touch ID di perangkat Apple. Hal ini memberikan pengesahan aman sambil menjaga data biometrik tetap pribadi dan aman. Ini juga memungkinkan pengguna untuk mendapatkan manfaat dari keamanan kode sandi dan kata sandi yang lebih panjang dan rumit dengan kenyamanan pengesahan cepat untuk akses atau pembelian di berbagai situasi.

Keamanan SoC Apple

Silicon rancangan Apple membangun arsitektur umum di semua produk Apple dan kini menenagai Mac, serta iPhone, iPad, Apple TV, dan Apple Watch. Selama lebih dari satu dekade, tim perancang silikon Apple berkelas dunia telah membuat dan meningkatkan sistem pada keping (SoC) Apple. Hasilnya adalah arsitektur yang dapat diskalakan yang dirancang khusus untuk semua perangkat yang memimpin industri dalam kemampuan keamanan. Landasan umum untuk fitur keamanan ini hanya mungkin dilakukan dari perusahaan yang merancang silicon-nya sendiri untuk berfungsi dengan perangkat lunaknya.

Apple silicon telah dirancang dan dibuat untuk mengaktifkan secara spesifik fitur keamanan sistem yang dijelaskan di bawah.

Fitur	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Kelompok M1
Perlindungan Integritas Kernel	✓	✓	✓	✓	✓	✓
Pembatasan Izin Cepat		✓	✓	✓	✓	✓
Perlindungan Integritas Koprosesor Sistem			✓	✓	✓	✓
Kode Pengesahan Penunjuk			✓	✓	✓	✓
Lapisan Perlindungan Halaman		✓	✓	✓	✓	Lihat Catatan di bawah.

Catatan: Lapisan Perlindungan Halaman (PPL) mengharuskan platform untuk *hanya* mengeksekusi kode yang ditandatangani dan tepercaya; ini adalah model keamanan yang tidak berlaku bagi macOS.

Silicon rancangan Apple juga mengaktifkan secara spesifik kemampuan Perlindungan Data yang dijelaskan di bawah.

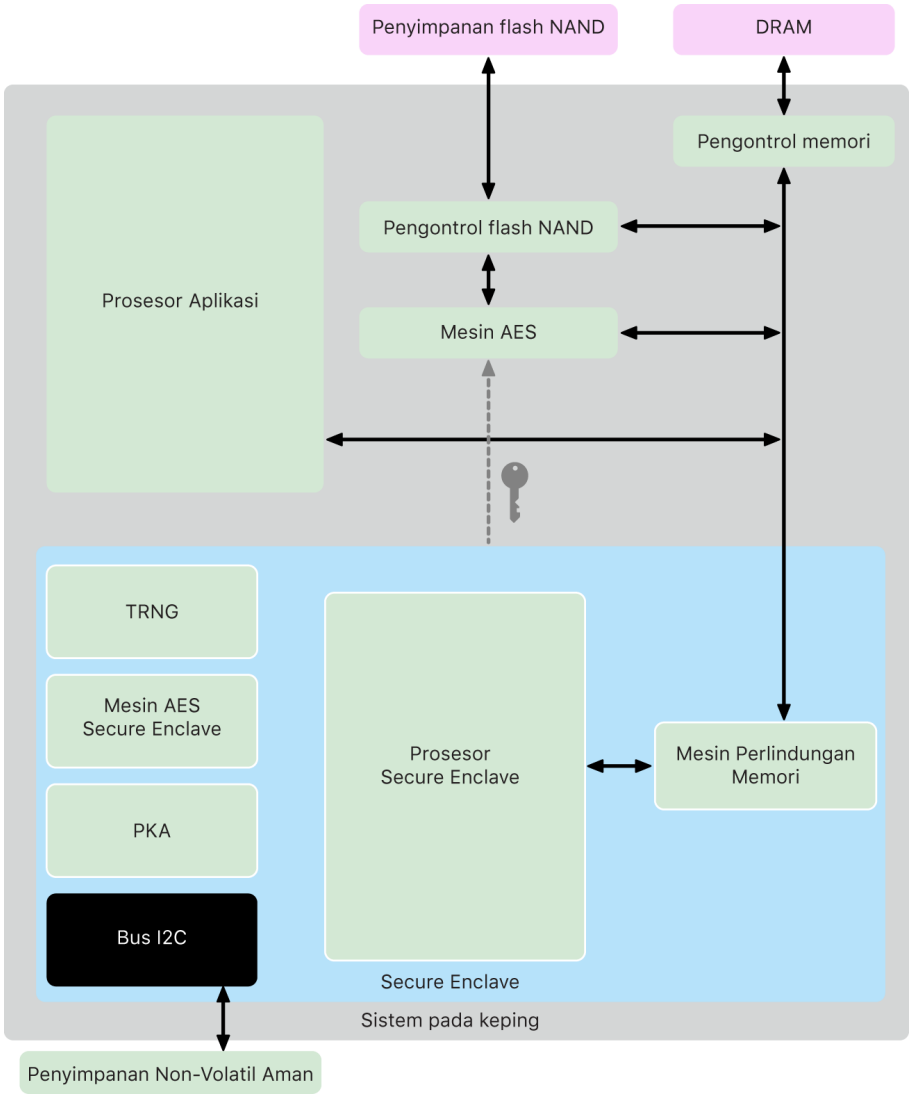
Fitur	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, Kelompok M1
Perlindungan Kunci yang Disegel (SKP)	✓	✓	✓	✓	✓
recoveryOS - Semua Kelas Perlindungan Data yang dilindungi	✓	✓	✓	✓	✓
Boot DFU, Diagnostik, dan Pembaruan alternatif - Data kelas A, B, dan C yang dilindungi			✓	✓	✓

Secure Enclave

Secure Enclave adalah subsistem aman khusus di versi terbaru dari iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch, dan HomePod.

Tinjauan

Secure Enclave adalah subsistem aman terdedikasi yang terintegrasi ke sistem pada keping (SoC) Apple. Secure Enclave terisolasi dari prosesor utama untuk menyediakan lapisan keamanan tambahan dan dirancang untuk terus menjaga data pengguna yang sensitif bahkan saat kernel Prosesor Aplikasi diretas. Secure Enclave mengikuti prinsip rancangan yang sama dengan SoC—ROM boot untuk membuat dasar kepercayaan perangkat keras, mesin AES untuk operasi kriptografis yang efisien dan aman, serta memori yang dilindungi. Meskipun tidak disertai dengan penyimpanan, Secure Enclave memiliki mekanisme untuk menyimpan informasi secara aman di penyimpanan terpasang yang terpisah dari penyimpanan kilat NAND yang digunakan oleh Prosesor Aplikasi dan sistem operasi.



Secure Enclave adalah fitur perangkat keras dari sebagian besar versi iPhone, iPad, Mac, Apple TV, Apple Watch, dan HomePod—yaitu:

- iPhone 5s atau lebih baru
- iPad Air atau lebih baru
- Komputer MacBook Pro dengan Touch Bar (2016 dan 2017) yang berisi Keping T1 Apple
- Komputer Mac berbasis Intel yang berisi Keping Keamanan T2 Apple
- Komputer Mac dengan Apple silicon
- Apple TV HD atau lebih baru
- Apple Watch Series 1 atau lebih baru
- HomePod dan HomePod mini

Prosesor Secure Enclave

Prosesor Secure Enclave menyediakan daya komputasi utama untuk Secure Enclave. Untuk menyediakan isolasi terkuat, Prosesor Secure Enclave hanya didedikasikan untuk penggunaan Secure Enclave. Ini membantu untuk mencegah serangan saluran samping yang bergantung pada perangkat lunak jahat yang berbagi inti eksekusi yang sama dengan perangkat lunak target yang diserang.

Prosesor Secure Enclave menjalankan versi mikrokernel L4 khusus Apple. Prosesor Secure Enclave dirancang untuk beroperasi secara efisien pada kecepatan clock yang lebih rendah, yang membantu untuk melindunginya terhadap serangan clock dan daya. Prosesor Secure Enclave, dimulai dengan A11 dan S4, disertai dengan mesin perlindungan memori dan memori yang dienkripsi dengan kemampuan anti-pemutaran ulang, boot aman, pembuat nomor acak khusus, dan mesin AES-nya sendiri.

Mesin Perlindungan Memori

Secure Enclave beroperasi dari area memori DRAM perangkat yang terdedikasi. Beberapa lapisan perlindungan mengisolasi memori yang dilindungi Secure Enclave dari Prosesor Aplikasi.

Saat perangkat dimulai, ROM Boot Secure Enclave membuat kunci perlindungan memori sementara acak untuk Mesin Perlindungan Memori. Kapan pun Secure Enclave menulisi area memori terdedikasinya, Mesin Perlindungan Memori mengenkripsi blok memori menggunakan AES dalam mode XEX (xor-encrypt-xor) Mac, dan mengkalkulasikan tag pengesahan Kode Pengesahan Pesan Berbasis Cipher (CMAC) untuk memori. Mesin Perlindungan Memori menyimpan tag pengesahan bersamaan dengan memori yang dienkripsi. Saat Secure Enclave membaca memori, Mesin Perlindungan Memori memverifikasi tag pengesahan. Jika tag pengesahan sesuai, Mesin Perlindungan Memori mendekripsi blok memori. Jika tag tidak sesuai, Mesin Perlindungan Memori memberikan sinyal kesalahan ke Secure Enclave. Setelah kesalahan pengesahan memori, Secure Enclave berhenti menerima permintaan hingga sistem di-boot ulang.

Dimulai dengan SoC A11 dan S4 Apple, Mesin Perlindungan Memori menambahkan perlindungan pemutaran ulang untuk memori Secure Enclave. Untuk membantu mencegah pemutaran ulang data keamanan yang sangat penting, Mesin Perlindungan Memori menyimpan nomor unik sekali pakai yang disebut *nonce* untuk blok memori bersamaan dengan tag pengesahan. Nonce digunakan sebagai tweak tambahan untuk tag pengesahan CMAC. Nonce untuk semua blok memori dilindungi menggunakan hierarki integritas yang berdasar di SRAM terdedikasi dalam Secure Enclave. Untuk penulisan, Mesin Perlindungan Memori *memperbarui* nonce dan setiap level hierarki integritas hingga SRAM. Untuk pembacaan, Mesin Perlindungan Memori *memverifikasi* nonce dan setiap level hierarki integritas hingga SRAM. Ketidaksesuaian nonce ditangani secara serupa dengan ketidaksesuaian tag pengesahan.

Di SoC Apple A14, A15, kelompok M1, dan versi lebih baru, Mesin Perlindungan Memori mendukung dua kunci perlindungan memori sementara. Kunci pertama digunakan untuk data khusus Secure Enclave, dan kunci kedua digunakan untuk data yang dibagikan dengan Neural Engine Aman.

Mesin Perlindungan Memori beroperasi sejajar dan secara transparan dengan Secure Enclave. Secure Enclave membaca dan menulisi memori layaknya DRAM reguler yang tidak dienkripsi, sedangkan pengamat di luar Secure Enclave hanya melihat versi memori yang dienkripsi dan disahkan. Hasilnya adalah perlindungan memori yang kuat tanpa mengorbankan kinerja dan kompleksitas perangkat lunak.

ROM Boot Secure Enclave

Secure Enclave disertai dengan ROM Boot Secure Enclave terdedikasi. Seperti ROM Boot Prosesor Aplikasi, ROM Boot Secure Enclave merupakan kode tetap yang membangun dasar kepercayaan pada perangkat keras untuk Secure Enclave.

Di proses mulai sistem, iBoot menetapkan area memori terdedikasi ke Secure Enclave. Sebelum menggunakan memori, ROM Boot Secure Enclave memulai Mesin Perlindungan Memori untuk menyediakan perlindungan kriptografis bagi memori yang dilindungi Secure Enclave.

Prosesor Aplikasi lalu mengirimkan image sepOS ke ROM Boot Secure Enclave. Setelah menyalin image sepOS ke memori yang dilindungi Secure Enclave, ROM Boot Secure Enclave memeriksa hash kriptografis dan tanda tangan image untuk memverifikasi bahwa sepOS telah disahkan untuk dijalankan di perangkat. Jika image sepOS ditandatangani dengan benar untuk dijalankan di perangkat, ROM Boot Secure Enclave akan mentransfer kontrol ke sepOS. Jika tanda tangan tidak sah, ROM Boot Secure Enclave dirancang untuk mencegah penggunaan Secure Enclave lebih lanjut hingga pengaturan ulang keping berikutnya.

Di A10 Apple dan SoC yang lebih baru, ROM Boot Secure Enclave mengunci hash sepOS ke register yang didedikasikan untuk tujuan ini. Akselerator Kunci Publik menggunakan hash ini untuk kunci yang terikat sistem operasi (terikat OS).

Monitor Boot Secure Enclave

Di A13 Apple dan SoC yang lebih baru, Secure Enclave menyertakan Monitor Boot yang dirancang untuk memastikan integritas yang lebih kuat di hash sepOS yang di-boot.

Di proses mulai sistem, konfigurasi Perlindungan Integritas Koprosesor Sistem (SCIP) Prosesor Secure Enclave membantu mencegah Prosesor Secure Enclave agar tidak mengeksekusi kode apa pun selain ROM Boot Secure Enclave. Monitor Boot membantu mencegah Secure Enclave agar tidak memodifikasi konfigurasi SCIP secara langsung. Untuk membuat sepOS yang dimuat menjadi dapat dieksekusi, ROM Boot Secure Enclave mengirimkan permintaan berisi alamat dan ukuran sepOS yang dimuat kepada Monitor Boot. Saat permintaan diterima, Monitor Boot mengatur ulang Prosesor Secure Enclave, membuat hash sepOS yang dimuat, memperbarui pengaturan SCIP untuk mengizinkan eksekusi sepOS yang dimuat, dan memulai eksekusi dalam kode yang baru dimuat. Saat sistem melanjutkan boot, proses yang sama digunakan kapan pun kode dibuat menjadi dapat dieksekusi. Setiap kali, Monitor Boot memperbarui hash proses boot yang berjalan. Monitor Boot juga menyertakan parameter keamanan kritis di hash yang berjalan.

Saat boot selesai, Monitor Boot menyelesaikan hash yang berjalan dan mengirimkannya ke Akselerator Kunci Publik agar dapat digunakan untuk kunci yang terikat OS. Proses ini dirancang agar pengikatan kunci sistem operasi tidak dapat dilewati bahkan dengan kerentanan di ROM Boot Secure Enclave.

Pembuat Angka Acak Sejati

Pembuat Angka Acak Sejati (TRNG) digunakan untuk membuat data acak yang aman. Secure Enclave menggunakan TRNG kapan pun Secure Enclave membuat kunci kriptografis acak, seeding kunci acak, atau entropi lainnya. TRNG didasarkan pada beberapa osilator cincin yang kemudian diproses dengan CTR_DRBG (algoritme berdasarkan cipher blok dalam Mode Penghitung).

Kunci Kriptografis Dasar

Secure Enclave menyertakan kunci kriptografis dasar ID unik (UID). UID unik bagi setiap perangkat terpisah dan tidak terkait ke pengenal lain di perangkat.

UID yang dibuat secara acak digabungkan ke dalam SoC pada saat produksi. Dimulai dari SoC A9, UID dibuat oleh TRNG Secure Enclave selama produksi dan ditulis ke gabungan menggunakan proses perangkat lunak yang dijalankan sepenuhnya di Secure Enclave. Proses ini melindungi UID agar tidak terlihat di luar perangkat selama produksi sehingga tidak tersedia untuk akses atau penyimpanan oleh Apple atau pemasoknya.

sepOS menggunakan UID untuk melindungi rahasia spesifik perangkat. UID memungkinkan data untuk dikaitkan secara kriptografis ke perangkat tertentu. Misalnya, hierarki kunci yang melindungi sistem file meliputi UID, sehingga jika penyimpanan SSD internal dipindahkan dari satu perangkat ke perangkat lain, file tidak akan dapat diakses. Rahasia khusus perangkat lainnya yang terlindungi meliputi data Face ID atau Touch ID. Di Mac, hanya penyimpanan yang internal sepenuhnya yang ditautkan ke mesin AES yang menerima level enkripsi ini. Misalnya, perangkat penyimpanan eksternal yang tersambung melalui USB maupun penyimpanan berbasis PCIe yang ditambahkan ke Mac Pro 2019 tidak dienkripsi dengan cara ini.

Secure Enclave juga memiliki ID grup (GID) perangkat, yang umum bagi semua perangkat yang menggunakan SoC tertentu (misalnya, semua perangkat yang menggunakan SoC A15 Apple berbagi GID yang sama).

UID dan GID tidak tersedia melalui Joint Test Action Group (JTAG) atau antarmuka debug lainnya.

Mesin AES Secure Enclave

Mesin AES Secure Enclave adalah blok perangkat keras yang digunakan untuk melakukan kriptografi simetris berdasarkan cipher AES. Mesin AES dirancang untuk menahan bocornya informasi dengan menggunakan waktu dan Analisis Daya Statis (SPA). Dimulai dengan SoC A9, Mesin AES juga menyertakan tindakan balasan Analisis Daya Dinamis (DPA).

Mesin AES mendukung kunci perangkat keras dan perangkat lunak. Kunci perangkat keras diturunkan dari UID atau GID Secure Enclave. Kunci ini tetap berada di Mesin AES dan tidak terlihat bahkan bagi perangkat lunak sepOS. Meskipun dapat meminta operasi enkripsi dan dekripsi dengan kunci perangkat keras, perangkat lunak tidak dapat mengekstrak kunci.

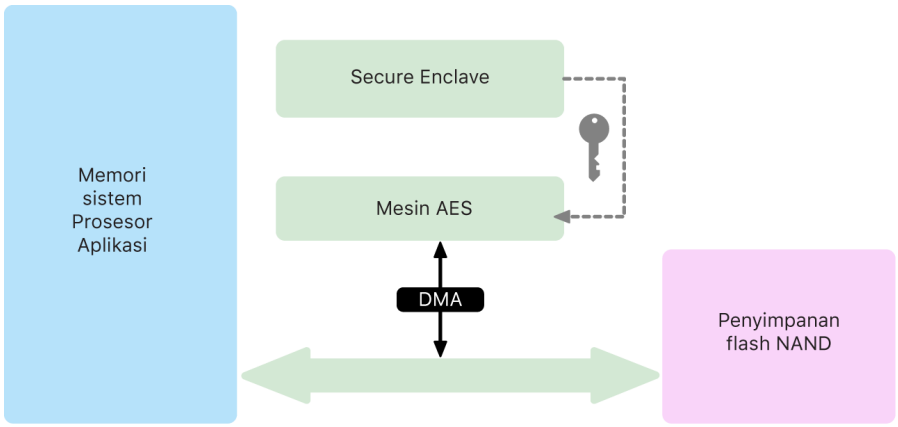
Di A10 Apple dan SoC yang lebih baru, Mesin AES menyertakan bit seeding yang dapat dikunci yang membedakan kunci yang diturunkan dari UID atau GID. Hal ini memungkinkan akses data agar dikondisikan di mode operasi perangkat. Misalnya, bit seeding yang dapat dikunci digunakan untuk menolak akses ke data yang dilindungi kata sandi saat melakukan boot dari mode Peningkatan Firmware Perangkat (DFU). Untuk informasi lainnya, lihat Kode sandi dan kata sandi.

Mesin AES

Setiap perangkat Apple dengan Secure Enclave juga memiliki mesin kripto AES256 khusus (“Mesin AES”) yang terdapat di jalur akses memori langsung (DMA) antara penyimpanan kilat NAND (nonvolatil) dan memori sistem utama, sehingga membuat enkripsi file menjadi sangat efisien. Di prosesor A9 atau seri A yang lebih baru, subsistem penyimpanan kilat berada di bus terisolasi yang hanya diberi akses ke memori yang berisi data pengguna melalui mesin kripto DMA.

Di waktu boot, sepOS membuat kunci pembungkusan sementara menggunakan TRNG. Secure Enclave mengirimkan kunci ini ke Mesin AES menggunakan kabel terdedikasi, yang dirancang untuk mencegahnya diakses oleh perangkat lunak di luar Secure Enclave. Kemudian, sepOS dapat menggunakan kunci pembungkusan sementara untuk membungkus kunci file agar dapat digunakan oleh driver sistem file Prosesor Aplikasi. Saat drive sistem file membaca atau menulisi file, driver mengirimkan kunci yang dibungkus ke Mesin AES, yang akan membuka kunci. Mesin AES tidak pernah mengekspos kunci yang tidak dibungkus ke perangkat lunak.

Catatan: Mesin AES adalah komponen terpisah dari Secure Enclave dan Mesin AES Secure Enclave, tapi operasinya terkait erat ke Secure Enclave seperti yang ditampilkan di bawah.



Akselerator Kunci Publik

Akselerator Kunci Publik (PKA) adalah blok perangkat keras yang digunakan untuk melakukan operasi kriptografi asimetris. PKA mendukung algoritme penandatanganan dan enkripsi RSA dan ECC (Kriptografi Kurva Eliptis). PKA dirancang untuk menahan bocornya informasi menggunakan waktu dan serangan saluran samping seperti SPA dan DPA.

PKA mendukung kunci perangkat lunak dan perangkat keras. Kunci perangkat keras diturunkan dari UID atau GID Secure Enclave. Kunci ini tetap berada di PKA dan tidak terlihat bahkan bagi perangkat lunak sepOS.

Dimulai dari SoC A13, implementasi enkripsi PKA telah teruji sebagai benar secara matematis menggunakan teknik verifikasi formal.

Di SoC A10 Apple dan lebih baru, PKA mendukung kunci terikat OS, yang juga disebut sebagai Perlindungan Kunci yang Disegel (SKP). Kunci ini dibuat menggunakan gabungan UID perangkat dan hash sepOS yang dijalankan di perangkat. Hash disediakan oleh ROM Boot Secure Enclave, atau oleh Monitor Boot Secure Enclave di A13 Apple atau SoC yang lebih baru. Kunci ini juga digunakan untuk memverifikasi versi sepOS saat membuat permintaan ke layanan Apple tertentu dan juga digunakan untuk meningkatkan keamanan data yang dilindungi kode sandi dengan membantu mencegah akses ke materi kunci jika perubahan penting dibuat ke sistem tanpa pengesahan pengguna.

Penyimpanan non-volatil aman

Secure Enclave dilengkapi dengan perangkat penyimpanan non-volatil aman terdedikasi. Penyimpanan non-volatil aman terhubung ke Secure Enclave menggunakan bus I2C terdedikasi, sehingga penyimpanan hanya dapat diakses oleh Secure Enclave. Semua kunci enkripsi data pengguna berakar di entropi yang disimpan di penyimpanan non-volatil Secure Enclave.

Di perangkat dengan A12, S4, dan SoC yang lebih baru, Secure Enclave dipasangkan dengan Komponen Penyimpanan Aman untuk penyimpanan entropi. Komponen Penyimpanan Aman dirancang dengan kode ROM tetap, pembuat nomor acak perangkat keras, kunci kriptografi unik per perangkat, mesin kriptografis, dan deteksi kerusakan fisik. Secure Enclave dan Komponen Penyimpanan Aman berkomunikasi menggunakan protokol yang dienkripsi dan disahkan yang menyediakan akses eksklusif ke entropi.

Perangkat yang pertama kali dirilis pada Musim Gugur 2020 atau lebih baru dilengkapi dengan Komponen Penyimpanan Aman generasi ke-2. Komponen Penyimpanan Aman generasi ke-2 menambahkan kotak kunci penghitung. Setiap kotak kunci penghitung menyimpan salt 128 bit, pemverifikasi kode sandi 128 bit, penghitung 8 bit, dan nilai percobaan maksimum 8 bit. Akses ke kotak kunci penghitung dilakukan melalui protokol yang dienkripsi dan disahkan.

Kotak kunci penghitung menyimpan entropi yang dibutuhkan untuk membuka data pengguna yang dilindungi kode sandi. Untuk mengakses data pengguna, Secure Enclave yang dipasangkan harus menurunkan nilai entropi kode sandi yang benar dari kode sandi pengguna dan UID Secure Enclave. Kode sandi pengguna tidak dapat dipelajari menggunakan percobaan membuka yang dikirim dari sumber selain Secure Enclave yang dipasangkan. Jika batas percobaan kode sandi terlampaui (misalnya, 10 percobaan di iPhone), data yang dilindungi kode sandi akan dihapus sepenuhnya oleh Komponen Penyimpanan Aman.

Untuk membuat kotak kunci penghitung, Secure Enclave mengirimi Komponen Penyimpanan Aman nilai entropi kode sandi dan nilai percobaan maksimum. Komponen Penyimpanan Aman membuat nilai salt menggunakan pembuat angka acaknya. Komponen lalu menurunkan nilai pemverifikasi kode sandi dan nilai entropi kotak kunci dari entropi kode sandi yang disediakan, kunci kriptografis unik Komponen Penyimpanan Aman, dan nilai salt. Komponen Penyimpanan Aman memulai kotak kunci penghitung dengan jumlah 0, nilai percobaan maksimum yang disediakan, nilai pemverifikasi kode sandi yang diturunkan, dan nilai salt. Komponen Penyimpanan Aman lalu mengembalikan nilai entropi kotak kunci yang dibuat ke Secure Enclave.

Untuk menerima nilai entropi kotak kunci dari kotak kunci penghitung nanti, Secure Enclave mengirimkan entropi kode sandi ke Komponen Penyimpanan Aman. Komponen Penyimpanan Aman terlebih dahulu menambahkan penghitung untuk kotak kunci. Jika penghitung yang ditambahkan melampaui nilai percobaan maksimum, Komponen Penyimpanan Aman menghapus kotak kunci penghitung sepenuhnya. Jika jumlah percobaan maksimum belum tercapai, Komponen Penyimpanan Aman mencoba untuk menurunkan nilai pemverifikasi kode sandi dan nilai entropi kotak kunci dengan algoritme yang sama dengan yang digunakan untuk membuat kotak kunci penghitung. Jika nilai pemverifikasi kode sandi turunan sesuai dengan nilai pemverifikasi kode sandi yang disimpan, Komponen Penyimpanan Aman mengembalikan nilai entropi kotak kunci ke Secure Enclave dan mengatur ulang penghitung ke 0.

Kunci yang digunakan untuk mengakses data yang dilindungi kata sandi berakar di entropi yang disimpan di kotak kunci penghitung. Untuk informasi lainnya, lihat Tinjauan Perlindungan Data.

Penyimpanan non-volatil aman digunakan untuk semua layanan anti-pemutaran ulang di Secure Enclave. Layanan anti-pemutaran ulang di Secure Enclave digunakan untuk pembatalan data pada saat kejadian yang menandai batasan anti-pemutaran ulang meliputi, tapi tidak terbatas pada, hal berikut ini:

- Perubahan kode sandi
- Mengaktifkan atau menonaktifkan Face ID atau Touch ID
- Menambah atau menghapus wajah Face ID atau sidik jari Touch ID
- Pengaturan ulang Face ID atau Touch ID
- Menambahkan atau menghapus kartu Apple Pay
- Menghapus Semua Konten dan Pengaturan

Di arsitektur yang tidak disertai dengan Komponen Penyimpanan aman, EEPROM (memori hanya baca yang dapat dihapus dan diprogram secara elektris) digunakan untuk menyediakan layanan penyimpanan aman untuk Secure Enclave. Seperti Komponen Penyimpanan Aman, EEPROM dipasang dan hanya dapat diakses dari Secure Enclave, tapi tidak berisi fitur keamanan perangkat keras khusus dan tidak menjamin akses eksklusif ke entropi (terlepas dari karakteristik pemasangan fisiknya) serta fungsi kotak kunci penghitung.

Neural Engine Aman

Di perangkat dengan Face ID, Neural Engine Aman mengonversi gambar 2D dan peta kedalaman ke representasi matematis wajah pengguna.

Di SoC A11 hingga A13, Neural Engine Aman diintegrasikan ke Secure Enclave. Neural Engine Aman menggunakan akses memori langsung (DMA) untuk kinerja tinggi. Unit manajemen memori input-output (IOMMU) di bawah kontrol kernel sepOS membatasi akses langsung ini ke bidang memori yang disahkan.

Dimulai dari A14 dan kelompok M1, Neural Engine Aman diimplementasikan sebagai mode aman di Neural Engine Prosesor Aplikasi. Pengontrol keamanan perangkat keras terdedikasi beralih di antara tugas Prosesor Aplikasi dan Secure Enclave, yang mengatur ulang status Neural Engine di setiap transisi untuk menjaga data Face ID tetap aman. Mesin terdedikasi menerapkan enkripsi memori, pengesahan, dan kontrol akses. Pada saat yang bersamaan, mesin menggunakan kunci kriptografis terpisah dan cakupan memori untuk membatasi Neural Engine Aman ke bidang memori yang disahkan.

Monitor daya dan clock

Semua elektronik dirancang untuk beroperasi dalam batas voltase dan gelombang frekuensi. Saat dioperasikan di luar gelombang ini, elektronik tidak dapat berfungsi dengan benar lalu kontrol keamanan dapat dilewati. Untuk membantu memastikan bahwa voltase dan frekuensi tetap berada dalam cakupan yang aman, Secure Enclave dirancang dengan sirkuit pengawasan. Sirkuit pengawasan ini dirancang untuk memiliki gelombang pengoperasian yang lebih besar dibandingkan sisa Secure Enclave. Jika monitor mendeteksi titik operasi ilegal, clock di Secure Enclave secara otomatis berhenti dan tidak dimulai ulang hingga pengaturan ulang SoC berikutnya.

Ringkasan fitur Secure Enclave

Catatan: Produk A12, A13, S4, dan S5 yang pertama kali dirilis pada Musim Gugur 2020 memiliki Komponen Penyimpanan Aman generasi ke-2, sedangkan produk yang lebih lama berdasarkan SoC ini memiliki Komponen Penyimpanan Aman generasi ke-1.

SoC	Mesin Perlindungan Memori	Penyimpanan Aman	Mesin AES	PKA
A8	Enkripsi dan pengesahan	EEPROM	Ya	Tidak
A9	Enkripsi dan pengesahan	EEPROM	Perlindungan DPA	Ya
A10	Enkripsi dan pengesahan	EEPROM	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
A11	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	EEPROM	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS

SoC	Mesin Perlindungan Memori	Penyimpanan Aman	Mesin AES	PKA
A12 (perangkat Apple yang dirilis sebelum Musim Gugur 2020)	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 1	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
A12 (perangkat Apple yang dirilis setelah Musim Gugur 2020)	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 2	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
A13 (perangkat Apple yang dirilis sebelum Musim Gugur 2020)	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 1	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS dan Monitor Boot
A13 (perangkat Apple yang dirilis setelah Musim Gugur 2020)	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 2	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS dan Monitor Boot
A14, A15	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 2	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS dan Monitor Boot
S3	Enkripsi dan pengesahan	EEPROM	Perlindungan DPA dan bit seeding yang dapat dikunci	Ya
S4	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 1	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
S5 (perangkat Apple yang dirilis sebelum Musim Gugur 2020)	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 1	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
S5 (perangkat Apple yang dirilis setelah Musim Gugur 2020)	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 2	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
S6, S7	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 2	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
T2	Enkripsi dan pengesahan	EEPROM	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS
Kelompok M1	Enkripsi, pengesahan, dan pencegahan pemutaran ulang	Komponen Penyimpanan Aman gen 2	Perlindungan DPA dan bit seeding yang dapat dikunci	Kunci yang terikat OS dan Monitor Boot

Face ID dan Touch ID

Keamanan Face ID dan Touch ID

Kode sandi dan kata sandi penting bagi keamanan perangkat Apple. Pada saat yang bersamaan, pengguna memerlukan akses mudah ke perangkatnya, sering kali lebih dari seratus kali per hari. Pengesahan biometrik menyediakan cara untuk mempertahankan keamanan kode sandi kuat—atau bahkan untuk memperkuat kode sandi atau kata sandi karena tidak perlu dimasukkan secara manual—sembari menyediakan kemudahan membuka perangkat dengan cepat menggunakan jari atau pandangan selintas. Face ID dan Touch ID tidak menggantikan kode sandi atau kata sandi, tapi dalam sebagian besar situasi fitur tersebut membuat akses menjadi lebih cepat dan mudah.

Arsitektur keamanan biometrik Apple mengandalkan pemisahan tanggung jawab yang ketat di antara sensor biometrik dan Secure Enclave, serta koneksi aman di antara keduanya. Sensor menangkap gambar biometrik dan mengirimkannya dengan aman ke Secure Enclave. Selama pendaftaran, Secure Enclave memproses, mengenkripsi, dan menyimpan data template Face ID serta Touch ID yang sesuai. Selama pencocokan, Secure Enclave membandingkan data masuk dari sensor biometrik dengan template yang disimpan untuk menentukan apakah perangkat dibuka atau merespons bahwa kecocokan sah (untuk penggunaan Apple Pay, in-app, dan lainnya dari Face ID serta Touch ID). Arsitektur mendukung perangkat yang menyertakan sensor dan Secure Enclave (seperti iPhone, iPad, dan banyak sistem Mac), serta kemampuan untuk memisahkan sensor secara fisik ke periferal yang nantinya dipasangkan dengan aman ke Secure Enclave di Mac dengan Apple silicon.

Keamanan Face ID

Hanya dengan pandangan selintas, Face ID dengan aman membuka perangkat Apple. Fitur ini menyediakan pengesahan yang intuitif dan aman, yang dimungkinkan oleh sistem kamera TrueDepth, yang menggunakan teknologi mutakhir untuk memetakan geometri wajah pengguna dengan akurat. Face ID menggunakan jaringan neural untuk menentukan perhatian, mencocokkan, dan mencegah penipuan, sehingga pengguna dapat membuka telepon pengguna dengan melihat selintas, bahkan dengan memakai masker saat menggunakan perangkat yang didukung. Face ID secara otomatis beradaptasi terhadap perubahan penampilan pengguna, dan dengan cermat melindungi privasi serta keamanan data biometrik pengguna.

Face ID dirancang untuk mengonfirmasi perhatian pengguna, menyediakan pengesahan yang andal dengan tingkat kecocokan salah yang rendah, serta mencegah penipuan digital dan fisik.

Kamera TrueDepth akan mencari wajah pengguna secara otomatis saat pengguna membangunkan perangkat Apple yang dilengkapi Face ID (dengan mengangkatnya atau mengetuk layar), serta saat perangkat tersebut mencoba untuk mengesahkan pengguna untuk menampilkan pemberitahuan masuk atau saat app yang didukung meminta pengesahan Face ID. Saat wajah terdeteksi, Face ID akan mengonfirmasi perhatian dan niat untuk membuka dengan mendeteksi bahwa mata pengguna terbuka dan perhatian pengguna tertuju pada perangkat; untuk aksesibilitas, pemeriksaan perhatian Face ID dinonaktifkan saat VoiceOver diaktifkan dan, jika perlu, dapat dinonaktifkan secara terpisah. Deteksi perhatian selalu diperlukan saat menggunakan Face ID dengan masker.

Setelah adanya wajah yang atentif dikonfirmasi, kamera TrueDepth akan memproyeksikan dan membaca ribuan titik inframerah untuk membentuk peta kedalaman wajah, bersama dengan gambar inframerah 2D. Data ini digunakan untuk membuat rangkaian gambar 2D dan peta kedalaman, yang ditandatangani secara digital dan dikirimkan ke Secure Enclave. Untuk mencegah penipuan digital dan fisik, kamera TrueDepth mengacak rangkaian gambar 2D dan pengambilan peta kedalaman, serta memproyeksikan pola acak khusus perangkat. Bagian dari Neural Engine Aman—dilindungi di dalam Secure Enclave—mengubah data ini ke representasi matematis dan membandingkan representasi tersebut dengan data wajah yang terdaftar. Data wajah yang terdaftar ini sendiri merupakan representasi matematis dari wajah pengguna yang diambil dalam berbagai pose.

Keamanan Touch ID

Touch ID adalah sistem sensor sidik jari yang membuat akses aman ke perangkat Apple yang didukung menjadi lebih cepat dan lebih mudah. Teknologi ini membaca data sidik jari dari semua sudut dan mempelajari sidik jari pengguna lebih lanjut seiring waktu, sementara sensor terus memperluas peta sidik jari dengan bertambahnya node tumpang tindih tambahan yang teridentifikasi dengan setiap penggunaan.

Perangkat Apple dengan sensor Touch ID dapat dibuka menggunakan sidik jari. Touch ID tidak menggantikan kebutuhan untuk kode sandi perangkat atau kata sandi pengguna, yang masih diperlukan setelah proses mulai, mulai ulang, atau keluar (di Mac) perangkat. Di beberapa app, Touch ID juga dapat digunakan sebagai ganti kode sandi perangkat atau kata sandi pengguna—misalnya untuk membuka catatan yang dilindungi kata sandi di app Catatan, untuk membuka situs web yang dilindungi rantai kunci, dan untuk membuka kata sandi app yang didukung. Namun, kode sandi perangkat atau kata sandi pengguna selalu diperlukan dalam beberapa skenario (misalnya, untuk mengubah kode sandi perangkat atau kata sandi pengguna yang ada atau untuk menghapus pendaftaran sidik jari yang ada atau membuat sidik jari baru).

Saat sensor sidik jari mendeteksi sentuhan jari, fitur tersebut akan memicu larik pencitraan mutakhir untuk memindai jari dan mengirimkan pindaian ke Secure Enclave. Saluran yang digunakan untuk mengamankan koneksi ini beragam, tergantung apakah sensor Touch ID terpasang ke perangkat dengan Secure Enclave atau terletak di periferal terpisah.

Saat pemindaian sidik jari dibuatkan vektor untuk dianalisis, pindaian raster disimpan untuk sementara di memori terenkripsi di dalam Secure Enclave, lalu dihapus. Analisis menggunakan pemetaan sudut alur kerutan sub-dermal, proses tidak sempurna yang menghapus "data jari terperinci" yang diperlukan bagi rekonstruksi sidik jari sebenarnya milik pengguna. Selama pendaftaran, peta node yang dihasilkan disimpan dalam format terenkripsi yang hanya dapat dibaca oleh Secure Enclave sebagai template untuk dibandingkan dengan kecocokan di masa mendatang, tapi tanpa informasi identitas apa pun. Data ini tidak pernah dikirim ke luar perangkat. Data tidak dikirimkan ke Apple dan tidak disertakan di cadangan perangkat.

Keamanan saluran Touch ID internal

Komunikasi antara Secure Enclave dan sensor Touch ID internal berlangsung di bus antarmuka periferal serial. Prosesor meneruskan data ke Secure Enclave tapi tidak dapat membacanya. Data dienkripsi dan disahkan dengan kunci sesi yang dinegosiasikan menggunakan kunci bersama yang disediakan untuk setiap sensor Touch ID dan Secure Enclave terkaitnya di pabrik. Karena semua sensor Touch ID, kunci bersama bersifat kuat, acak, dan berbeda. Pertukaran kunci sesi menggunakan pembungkusan kunci AES, yang kedua sisinya menyediakan kunci acak yang membuat kunci sesi dan menggunakan enkripsi transpor yang menyediakan pengesahan dan kerahasiaan (menggunakan AES-CCM).

Magic Keyboard dengan Touch ID

Magic Keyboard dengan Touch ID (dan Magic Keyboard dengan Touch ID dan Keypad Numerik) menyediakan sensor Touch ID di papan ketik eksternal yang dapat digunakan dengan Mac dengan Apple silicon mana pun. Magic Keyboard dengan Touch ID melakukan tugas sensor biometrik; Magic Keyboard tidak menyimpan template biometrik, melakukan pencocokan biometrik, atau memberlakukan kebijakan keamanan (misalnya, harus memasukkan kata sandi setelah 48 jam tanpa dibuka). Sensor Touch ID di Magic Keyboard dengan Touch ID harus dipasangkan dengan aman ke Secure Enclave di Mac sebelum dapat digunakan, lalu Secure Enclave melakukan operasi pendaftaran dan pencocokan serta memberlakukan kebijakan keamanan dalam cara yang sama seperti untuk sensor Touch ID internal. Apple melakukan proses pemasangan di pabrik untuk Magic Keyboard dengan Touch ID yang dikirimkan dengan Mac. Pemasangan juga dapat dilakukan oleh pengguna jika perlu. Magic Keyboard dengan Touch ID dapat dipasangkan dengan aman hanya dengan satu Mac pada satu waktu, tapi Mac dapat mempertahankan pemasangan aman dengan maksimum lima papan ketik Magic Keyboard dengan Touch ID lain.

Magic Keyboard dengan sensor Touch ID dan Touch ID internal bersifat kompatibel. Jika jari yang terdaftar di sensor Touch ID Mac internal disediakan di Magic Keyboard dengan Touch ID, Secure Enclave di Mac berhasil memproses kecocokan—dan sebaliknya.

Untuk mendukung pemasangan aman dan komunikasi di antara Secure Enclave Mac dan Magic Keyboard dengan Touch ID, papan ketik dilengkapi dengan blok Akselerator Kunci Publik (PKA) perangkat keras, untuk menyediakan bukti, dan dengan kunci berbasis perangkat keras, untuk melakukan proses kriptografis yang diperlukan.

Pemasangan aman

Magic Keyboard dengan Touch ID harus dipasangkan ke Mac dengan aman sebelum dapat digunakan untuk operasi Touch ID. Untuk memasangkan, Secure Enclave di Mac dan blok PKA di Magic Keyboard dengan Touch ID bertukar kunci publik, yang terletak di CA Apple, dan menggunakan kunci jaminan yang disimpan di perangkat keras dan ECDH sementara untuk menjamin identitasnya dengan aman. Di Mac, data ini dilindungi oleh Secure Enclave; di Magic Keyboard dengan Touch ID, data ini dilindungi oleh blok PKA. Setelah pemasangan aman, semua data Touch ID yang dikomunikasikan di antara Mac dan Magic Keyboard dengan Touch ID dienkripsi oleh AES-GCM dengan panjang kunci 256 bit, dengan kunci ECDH sementara menggunakan kurva NIST P-256 berdasarkan identitas yang disimpan. (Ketukan tombol normal ditukar menggunakan keamanan Bluetooth menggunakan cara yang sama dengan papan ketik Bluetooth.)

Tujuan aman untuk memasangkan

Untuk melakukan beberapa operasi Touch ID untuk pertama kalinya, seperti mendaftarkan sidik jari baru, pengguna harus mengonfirmasi tujuannya secara fisik untuk menggunakan Magic Keyboard dengan Touch ID dengan Mac. Tujuan fisik dikonfirmasi dengan menekan tombol daya Mac dua kali saat diindikasikan oleh antarmuka pengguna, atau dengan berhasil mencocokkan sidik jari yang sebelumnya telah terdaftar dengan Mac. Untuk informasi lainnya, lihat Tujuan dan koneksi aman ke Secure Enclave.

Transaksi Apple Pay dapat disahkan dengan mencocokkan Touch ID atau dengan memasukkan kata sandi pengguna macOS dan menekan tombol Touch ID dia kali di Magic Keyboard dengan Touch ID. Cara terakhir memungkinkan pengguna mengonfirmasi tujuan fisik bahkan tanpa kecocokan Touch ID.

Magic Keyboard dengan keamanan saluran Touch ID

Untuk membantu memastikan saluran komunikasi aman di antara sensor Touch ID di Magic Keyboard dengan Touch ID dan Secure Enclave di Mac yang dipasangkan, hal berikut diperlukan:

- Pemasangan aman di antara Magic Keyboard dengan blok PKA Touch ID dan Secure Enclave sebagaimana dijelaskan di atas
- Saluran aman di antara Magic Keyboard dengan sensor Touch ID dan blok PKA-nya

Saluran aman di antara sensor Magic Keyboard dengan Touch ID dan blok PKA-nya dibuat di pabrik dengan menggunakan kunci unik yang dibagikan di antara keduanya. (Teknik ini sama dengan yang digunakan untuk membuat saluran aman di antara Secure Enclave di Mac dan sensor internalnya, untuk komputer Mac dengan Touch ID internal.)

Face ID, Touch ID, kode sandi, dan kata sandi

Untuk menggunakan Face ID atau Touch ID, pengguna harus mengatur perangkat sehingga kode sandi atau kata sandi diperlukan untuk membukanya. Saat Face ID atau Touch ID berhasil mendeteksi kecocokan, perangkat pengguna akan membuka tanpa meminta kode sandi atau kata sandi perangkat. Ini membuat penggunaan kode sandi atau kata sandi yang lebih kompleks dan panjang menjadi lebih praktis karena pengguna tidak harus memasukkannya sesering biasanya. Face ID dan Touch ID tidak menggantikan kode sandi atau kata sandi pengguna; sebagai gantinya, fitur tersebut menyediakan akses mudah ke perangkat dengan cepat dan praktis. Ini penting karena kode sandi atau kata sandi yang kuat membentuk landasan untuk bagaimana iPhone, iPad, Mac, atau Apple Watch pengguna melindungi data pengguna tersebut secara kriptografis.

Saat kode sandi atau kata sandi perangkat diperlukan

Pengguna dapat menggunakan kode sandi atau kata sandinya kapan pun alih-alih Face ID atau Touch ID, tapi terdapat situasi yang tidak mengizinkan biometrik. Operasi yang sensitif terhadap keamanan berikut selalu memerlukan pemasukan kode sandi atau kata sandi:

- Memperbarui perangkat lunak
- Menghapus perangkat
- Melihat atau mengubah pengaturan kode sandi
- Menginstal profil konfigurasi

- Membuka panel Keamanan & Privasi di Preferensi Sistem di Mac
- Membuka panel Pengguna & Grup di Preferensi Sistem di Mac (jika FileVault dinyalakan)

Kode sandi atau kata sandi juga diperlukan jika perangkat berada dalam salah satu kondisi berikut:

- Perangkat baru dinyalakan atau dimulai ulang.
- Pengguna telah keluar dari akun Mac mereka (atau belum masuk).
- Pengguna belum membuka perangkat selama lebih dari 48 jam.
- Pengguna belum menggunakan kode sandi atau kata sandi untuk membuka perangkat selama 156 jam (enam setengah hari), dan pengguna belum menggunakan biometrik untuk membuka perangkat selama 4 jam.
- Perangkat telah menerima perintah penguncian jarak jauh.
- Pengguna keluar dari daya mati/Darurat SOS dengan menekan dan menahan tombol volume dan tombol Tidur/Bangun secara bersamaan selama 2 detik, lalu menekan Batalkan.
- Terdapat lima kali gagal mencocokkan biometrik (untuk kegunaan, perangkat mungkin menawarkan untuk memasukkan kode sandi atau kata sandi alih-alih menggunakan biometrik setelah kurang dari lima kali gagal mencocokkan biometrik).

Saat Face ID dengan masker diaktifkan di iPhone, fitur tersedia selama 6,5 jam ke depan setelah salah satu tindakan pengguna berikut:

- Percobaan pencocokan Face ID berhasil (dengan atau tanpa masker)
- Validasi kode sandi perangkat
- Membuka perangkat dengan Apple Watch

Salah satu tindakan ini memperpanjang periode sebesar 6,5 jam saat dilakukan.

Saat Face ID atau Touch ID diaktifkan di iPhone atau iPad, perangkat akan segera terkunci ketika Tombol Tidur/Bangun ditekan, dan perangkat akan terkunci setiap kali masuk ke mode tidur. Face ID dan Touch ID memerlukan kecocokan—atau penggunaan kode sandi sebagai gantinya—setiap kali perangkat bangun.

Kemungkinan bagi orang lain di dunia untuk dapat membuka iPhone atau iPad pengguna kurang dari 1 banding 1.000.000 dengan Face ID—termasuk saat Face ID dengan masker dinyalakan. Untuk model iPhone, iPad, Mac pengguna dengan Touch ID dan yang dipasangkan dengan Magic Keyboard, kemungkinannya kurang dari 1 banding 50.000. Kemungkinan ini bertambah jika terdapat beberapa sidik jari (hingga 1 banding 10.000 dengan lima sidik jari) atau penampilan yang terdaftar (hingga 1 banding 500.000 dengan dua penampilan). Untuk perlindungan tambahan, Face ID dan Touch ID hanya mengizinkan lima percobaan pencocokan yang tidak berhasil sebelum kode sandi atau kata sandi diperlukan untuk mendapatkan akses ke perangkat atau akun pengguna. Dengan Face ID, kemungkinan tidak cocok lebih tinggi untuk:

- Saudara kembar atau saudara yang mirip dengan pengguna
- Anak berumur 13 ke bawah (karena fitur wajah khasnya belum sepenuhnya terbentuk)

Kemungkinan meningkat lebih jauh pada kedua kasus ini saat Face ID dengan masker digunakan. Jika pengguna khawatir mengenai kecocokan yang salah, pengguna dianjurkan oleh Apple untuk menggunakan kode sandi untuk mengesahkan.

Keamanan pencocokan wajah

Pencocokan wajah dilakukan di dalam Secure Enclave menggunakan jaringan neural yang dilatih secara khusus untuk tujuan tersebut. Apple mengembangkan jaringan neural pencocokan wajah menggunakan lebih dari satu miliar gambar termasuk gambar inframerah (IR) dan kedalaman yang dikumpulkan dalam kajian yang dilakukan dengan persetujuan dan sepengetahuan peserta. Kemudian, Apple bekerja dengan peserta dari seluruh dunia untuk mengikutsertakan representatif yang terdiri dari sekelompok orang dengan mempertimbangkan gender, umur, etnik, dan faktor lainnya. Kajian tersebut diperluas sesuai keperluan untuk menyediakan tingkat keakuratan tinggi untuk cakupan pengguna yang beragam. Face ID dirancang untuk dapat digunakan dengan topi, syal, kacamata, lensa kontak, dan berbagai jenis kacamata hitam. Face ID juga mendukung membuka dengan masker di perangkat iPhone mulai dari iPhone 12 dan iOS 15.4 atau lebih baru. Selain itu, fitur ini dirancang untuk dapat digunakan di dalam ruangan, luar ruangan, dan bahkan dalam kegelapan total. Jaringan neural tambahan—yang dirancang untuk mengenali dan menghalangi penipuan—berfungsi sebagai pertahanan terhadap upaya untuk membuka perangkat dengan foto atau topeng. Data Face ID, meliputi representasi matematis dari wajah pengguna, dienkripsi dan hanya tersedia bagi Secure Enclave. Data ini tidak pernah dikirim ke luar perangkat. Data tidak dikirimkan ke Apple dan tidak disertakan di cadangan perangkat. Data Face ID berikut hanya disimpan dan dienkripsi untuk digunakan oleh Secure Enclave, selama pengoperasian normal:

- Representasi matematis dari wajah pengguna dikalkulasikan selama pendaftaran
- Representasi matematis dari wajah pengguna dikalkulasikan di beberapa percobaan untuk membuka perangkat jika Face ID menganggapnya perlu untuk meningkatkan pencocokan di masa mendatang

Gambar wajah yang diambil selama pengoperasian normal tidak disimpan, tapi alih-alih segera dihapus setelah representasi matematis dikalkulasikan untuk pendaftaran atau perbandingan dengan data Face ID yang terdaftar.

Meningkatkan kecocokan Face ID

Untuk meningkatkan kinerja pencocokan dan agar dapat beradaptasi dengan perubahan alami dari wajah dan penampilan pengguna, Face ID meningkatkan simpanan representasi matematis seiring dengan berjalannya waktu. Setelah perangkat berhasil dibuka, Face ID dapat menggunakan representasi matematis yang baru dikalkulasikan—jika data tersebut memadai—untuk beberapa pencocokan sebelum data tersebut dihapus. Sebaliknya, jika Face ID gagal mengenali wajah tapi kualitas kecocokan lebih tinggi dari ambang tertentu, lalu pengguna memasukkan kode sandinya setelahnya, Face ID akan melakukan pengambilan gambar sekali lagi dan meningkatkan data Face ID yang terdaftar dengan representasi matematis yang baru dikalkulasikan. Data Face ID baru ini akan dihapus jika pengguna berhenti mencocokkan atau setelah digunakan beberapa kali untuk pencocokan; data baru juga dibuang saat opsi untuk mengatur ulang Face ID dipilih. Proses peningkatan ini memungkinkan Face ID untuk beradaptasi dengan perubahan drastis pada bulu wajah atau penggunaan tata rias pengguna sambil meminimalisasi kesalahan.

Penggunaan Face ID dan Touch ID

Membuka perangkat atau akun pengguna

Jika Face ID atau Touch ID dimatikan, saat perangkat atau kunci dikunci, kunci untuk kelas tertinggi Perlindungan Data—yang disimpan di Secure Enclave—akan dihapus. File dan item rantai kunci di kelas tersebut tidak dapat diakses hingga pengguna membuka perangkat atau akun dengan memasukkan kode sandi atau kata sandi mereka.

Jika Face ID atau Touch ID dinyalakan, kunci tidak akan dihapus saat perangkat atau akun terkunci; sebagai gantinya, kunci dibungkus dengan sebuah kunci yang diberikan ke subsistem Face ID atau Touch ID di dalam Secure Enclave. Saat pengguna mencoba membuka perangkat atau akun, jika perangkat mendeteksi kecocokan yang berhasil, perangkat akan menyediakan kunci untuk membuka bungkusan kunci Perlindungan Data, dan perangkat atau akun akan dibuka. Proses ini menyediakan perlindungan tambahan dengan mengharuskan kerja sama antara subsistem Perlindungan Data dan Face ID atau Touch ID untuk membuka perangkat.

Jika perangkat dimulai uang, kunci yang diperlukan untuk Face ID atau Touch ID untuk membuka perangkat atau akun akan hilang; kunci dibuang oleh Secure Enclave setelah semua kondisi dipenuhi yang memerlukan kode sandi atau kata sandi untuk dimasukkan.

Mengamankan pembelian dengan Apple Pay

Pengguna juga dapat menggunakan Face ID dan Touch ID dengan Apple Pay untuk memudahkan dan mengamankan pembelian di toko, app, dan web:

- *Menggunakan Face ID di toko:* Untuk mengesahkan pembayaran dalam toko dengan Face ID, pengguna harus terlebih dahulu mengonfirmasi niat untuk membayar dengan mengeklik tombol samping dua kali. Klik dua kali ini menangkap tujuan pengguna menggunakan gerakan fisik yang secara langsung tertaut ke Secure Enclave dan tahan terhadap pemalsuan oleh proses yang berbahaya. Lalu pengguna mengesahkan menggunakan Face ID sebelum meletakkan perangkat di dekat pembaca pembayaran nirkontak. Metode pembayaran Apple Pay yang berbeda dapat dipilih setelah pengesahan Face ID, yang memerlukan pengesahan ulang, tapi pengguna tidak harus mengeklik dua kali tombol samping lagi.
- *Menggunakan Face ID di app dan web:* Untuk melakukan pembayaran di dalam app dan web, pengguna mengonfirmasi niat mereka untuk membayar dengan mengeklik tombol samping dua kali, lalu mengesahkan menggunakan Face ID untuk mengesahkan pembayaran. Jika transaksi Apple Pay tidak diselesaikan dalam waktu 60 detik sejak tombol samping diklik dua kali, pengguna harus mengonfirmasi ulang niat untuk membayar dengan mengeklik dua kali lagi.
- *Menggunakan Touch ID:* Untuk Touch ID, tujuan pembayaran dikonfirmasi menggunakan gerakan pengaktifan sensor Touch ID yang digabungkan dengan sidik jari pengguna yang berhasil dicocokkan.

Menggunakan API yang disediakan oleh sistem

App pihak ketiga dapat menggunakan API yang disediakan sistem untuk meminta pengguna mengesahkan menggunakan Face ID atau Touch ID atau kode sandi atau kata sandi, dan app yang mendukung Touch ID akan mendukung Face ID secara otomatis tanpa perubahan apa pun. Saat menggunakan Face ID atau Touch ID, app hanya akan diberi tahu mengenai apakah pengesahan berhasil; app tidak dapat mengakses Face ID, Touch ID, atau data yang dikaitkan dengan pengguna terdaftar.

Melindungi item rantai kunci

Item rantai kunci juga dapat dilindungi dengan Face ID atau Touch ID, sehingga hanya dapat dirilis oleh Secure Enclave dengan keberhasilan pencocokan atau dengan kode sandi perangkat atau kata sandi akun. Pengembang app memiliki API untuk memverifikasi bahwa kode sandi atau kata sandi telah diatur oleh pengguna sebelum memerlukan Face ID atau Touch ID atau kode sandi atau kata sandi untuk membuka item rantai kunci. Pengembang app dapat melakukan salah satu hal berikut:

- Mewajibkan operasi API pengesahan tidak kembali ke kata sandi app atau kode sandi perangkat. Pengembang dapat menanyakan apakah pengguna terdaftar, sehingga memungkinkan Face ID atau Touch ID untuk digunakan sebagai faktor kedua di app yang sensitif terhadap keamanan.
- Membuat dan menggunakan kunci Kriptografi Kurva Eliptis (ECC) di dalam Secure Enclave yang dapat dilindungi oleh Face ID atau Touch ID. Operasi dengan kunci ini selalu dilakukan di dalam Secure Enclave setelah penggunaannya disahkan.

Melakukan dan menyetujui pembelian

Anda juga dapat mengonfigurasi Face ID atau Touch ID untuk menyetujui pembelian dari iTunes Store, App Store, Apple Books, dan lainnya sehingga Anda tidak harus memasukkan kata sandi ID Apple. Saat pembelian dilakukan, Secure Enclave memverifikasi bahwa pengesahan biometrik terjadi, lalu merilis kunci ECC yang digunakan untuk menandatangani permintaan toko.

Tujuan dan koneksi aman ke Secure Enclave

Tujuan aman menyediakan cara untuk mengonfirmasi tujuan pengguna tanpa berinteraksi dengan sistem operasi atau Prosesor Aplikasi. Koneksinya adalah tautan fisik—dari tombol fisik hingga Secure Enclave—yang tersedia pada perangkat berikut:

- iPhone X atau lebih baru
- Apple Watch Series 1 atau lebih baru
- iPad Pro (semua model)
- iPad Air (2020)
- Komputer Mac dengan Apple silicon

Dengan tautan ini, pengguna dapat mengonfirmasi tujuannya untuk menyelesaikan operasi dalam cara yang dirancang sedemikian rupa yang tidak dapat diakali oleh perangkat lunak yang dijalankan dengan hak root atau di kernel.

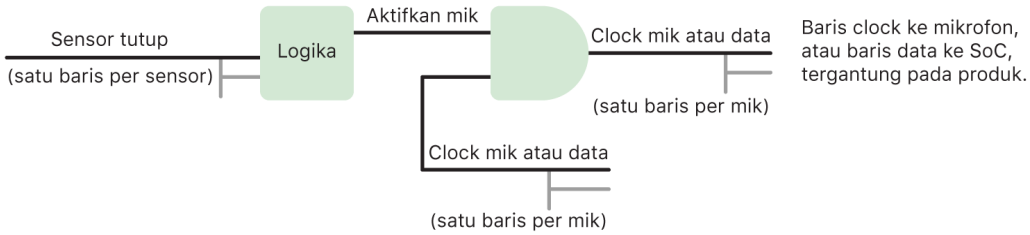
Fitur ini digunakan untuk mengonfirmasi tujuan pengguna selama transaksi Apple Pay dan saat menyelesaikan pemasangan Magic Keyboard dengan Touch ID ke Mac dengan Apple silicon. Penekanan dua kali pada tombol yang sesuai (untuk Face ID) atau pemindaian sidik jari (untuk Touch ID) saat diminta oleh antarmuka pengguna menandakan konfirmasi dari tujuan pengguna. Untuk informasi lainnya, lihat Mengamankan pembelian dengan Apple Pay. Mekanisme serupa—berdasarkan Secure Enclave dan firmware T2—didukung di model MacBook dengan Keping Keamanan T2 Apple tanpa Touch Bar.

Pemutusan mikrofon perangkat keras

Semua notebook Mac berbasis Apple silicon dan notebook Mac berbasis Intel dengan fitur Keping Keamanan T2 Apple dilengkapi dengan pemutusan perangkat keras yang menonaktifkan mikrofon selama layar ditutup. Di semua notebook MacBook Pro dan MacBook Air 13 inci dengan keping T2, semua notebook MacBook dengan keping T2 dari tahun 2019 atau lebih baru, dan notebook Mac dengan Apple silicon, pemutusan ini hanya diimplementasikan di perangkat keras. Pemutusan ini dirancang untuk mencegah perangkat lunak—bahkan dengan hak root atau kernel di macOS, dan bahkan perangkat lunak pada keping T2 atau firmware lainnya—mengakses mikrofon saat layar ditutup. (Kamera tidak terputus di perangkat keras karena area visualnya terhalangi sepenuhnya saat layar ditutup.)

Model iPad mulai pada tahun 2020 juga disertai dengan pemutusan mikrofon perangkat keras. Saat casing yang sesuai dengan MFi (termasuk yang dijual oleh Apple) dipasang ke iPad dan tertutup, mikrofon terputus di perangkat keras. Ini dirancang untuk mencegah data audio mikrofon agar tidak tersedia ke perangkat lunak apa pun—bahkan dengan hak root atau kernel di iPadOS, atau firmware perangkat lainnya.

Perlindungan di bagian ini diimplementasikan secara langsung dengan logika perangkat keras, sesuai dengan diagram sirkuit berikut:



Di setiap produk dengan pemutusan mikrofon perangkat keras, satu atau beberapa sensor tutup mendeteksi penutupan fisik tutup atau casing menggunakan beberapa properti fisik (misalnya, sensor efek Hall atau sensor sudut engsel) interaksi. Untuk sensor yang memerlukan kalibrasi, parameter diatur selama produksi perangkat dan proses kalibrasi menyertakan penguncian perangkat keras yang tidak dapat dibalikkan pada perubahan berikutnya terhadap parameter sensitif di sensor. Sensor ini memancarkan sinyal perangkat keras langsung yang melewati sekumpulan logika perangkat keras sederhana yang tidak dapat diprogram ulang. Logika ini menyediakan debounce, histeresis, dan/atau penundaan hingga 500 milidetik sebelum menonaktifkan mikrofon. Tergantung produk, sinyal ini dapat diimplementasikan dengan menonaktifkan jalur yang mengirimkan data di antara mikrofon dan Sistem pada Keping (SoC) atau dengan menonaktifkan salah satu jalur input ke modul mikrofon yang memungkinkannya untuk aktif—misalnya, jalur clock atau kontrol efektif yang sama.

Kartu Kilat dengan cadangan daya

Jika iOS tidak dapat dijalankan karena daya iPhone perlu diisi, mungkin masih terdapat cukup daya pada baterai untuk mendukung transaksi Kartu Kilat. Perangkat iPhone yang didukung dapat menggunakan fitur ini secara otomatis dengan:

- Kartu pembayaran atau transit yang ditetapkan sebagai kartu Transit Kilat
- Kartu ID pelajar dengan Mode Kilat yang dinyalakan
- Kunci Mobil dengan Mode Kilat yang dinyalakan
- Kunci Rumah dengan Mode Kilat yang dinyalakan
- Kartu akses Perhotelan atau Perusahaan dengan Mode Kilat yang dinyalakan

Jika tombol samping ditekan (atau di iPhone SE generasi ke-2, tombol Utama) layar akan menampilkan ikon baterai lemah serta teks yang menunjukkan bahwa Kartu Kilat tersedia untuk digunakan. Pengontrol NFC menjalankan transaksi Kartu Kilat dalam kondisi yang sama seperti ketika iOS dijalankan, bedanya transaksi hanya ditunjukkan dengan pemberitahuan haptik (tanpa ada pemberitahuan yang terlihat). Di iPhone SE generasi ke-2, transaksi yang telah selesai akan muncul di layar setelah beberapa detik. Fitur ini tidak tersedia ketika proses standar untuk mematikan perangkat yang dimulai pengguna dijalankan.

Keamanan sistem

Tinjauan keamanan sistem

Dengan berlandaskan pada kemampuan yang unik dari perangkat keras Apple, keamanan sistem bertanggung jawab untuk mengontrol akses ke sumber daya sistem di perangkat Apple tanpa mengganggu kegunaan. Keamanan sistem meliputi proses mulai, pembaruan perangkat lunak, dan perlindungan sumber daya sistem komputer seperti CPU, memori, disk, program perangkat lunak, serta data yang disimpan.

Versi terbaru sistem operasi Apple adalah yang paling aman. Bagian penting dari keamanan Apple adalah *boot aman*, yang melindungi sistem dari infeksi malware saat boot. Boot aman dimulai di perangkat keras dan membangun rantai kepercayaan melalui perangkat lunak, yang setiap langkahnya dirancang untuk memastikan bahwa langkah berikutnya berfungsi dengan benar sebelum menyerahkan kontrol. Model keamanan ini tidak hanya mendukung boot default perangkat Apple, tapi juga berbagai mode untuk pemulihan dan pembaruan terbaru di perangkat Apple. Subkomponen seperti Keping T2 dan Secure Enclave juga melakukan boot amannya sendiri untuk membantu memastikan komponen hanya melakukan boot kode yang berkualitas dari Apple. Sistem pembaruan dirancang untuk mencegah serangan penurunan versi, sehingga perangkat tidak dapat dikembalikan ke versi sistem operasi yang lama (yang kelemahannya diketahui penyerang) sebagai cara untuk mencuri data pengguna.

Perangkat Apple juga dilengkapi dengan perlindungan boot dan runtime sehingga dapat mempertahankan integritasnya selama proses pengoperasian. Silicon rancangan Apple di iPhone, iPad, Apple Watch, Apple TV, HomePod, dan Mac dengan Apple silicon menyediakan arsitektur umum untuk melindungi integritas sistem operasi. macOS juga disertai dengan kumpulan kemampuan perlindungan yang diperluas dan dapat dikonfigurasi agar dapat mendukung model komputasi berbeda, serta kemampuan yang didukung di semua platform perangkat keras Mac.

Boot aman

Proses boot untuk perangkat iOS dan iPadOS

Setiap langkah dari proses mulai berisi komponen yang ditandatangani oleh Apple secara kriptografis untuk memungkinkan pemeriksaan integritas sehingga boot hanya dilanjutkan setelah rantai kepercayaan terverifikasi. Komponen ini meliputi bootloader, kernel, ekstensi kernel, dan firmware pita dasar seluler. Rantai boot aman ini dirancang untuk memverifikasi bahwa level perangkat lunak terendah tidak dirusak.

Saat perangkat iOS atau iPadOS dinyalakan, Prosesor Aplikasinya akan langsung menjalankan kode dari memori hanya baca yang dikenal sebagai ROM Boot. Kode tetap ini, yang dikenal sebagai *dasar kepercayaan pada perangkat keras*, diterapkan pada saat pembuatan keping, dan tepercaya secara implisit. Kode ROM Boot berisi kunci publik otoritas sertifikat (CA) Dasar Apple—yang digunakan untuk memverifikasi bahwa bootloader iBoot ditandatangani oleh Apple sebelum mengizinkannya dimuat. Ini adalah langkah pertama dalam rantai kepercayaan yang setiap langkahnya memeriksa bahwa langkah berikutnya ditandatangani oleh Apple. Setelah menyelesaikan tugasnya, iBoot akan memverifikasi dan menjalankan kernel iOS atau iPadOS. Untuk perangkat dengan prosesor A9 atau seri A yang lebih lama, fase Bootloader Level Rendah (LLB) tambahan akan dimuat dan diverifikasi oleh ROM Boot dan kemudian akan memuat dan memverifikasi iBoot.

Kegagalan untuk memuat atau memverifikasi fase berikut ditangani dengan cara yang berbeda tergantung perangkat kerasnya:

- *ROM Boot tidak dapat memuat LLB (perangkat yang lebih lama):* Mode Peningkatan Firmware Perangkat (DFU)
- *LLB atau iBoot:* Mode Pemulihan

Di kedua kasus, perangkat harus terhubung ke Finder (di macOS 10.15 atau lebih baru) atau iTunes (macOS 10.14 atau lebih lama) melalui USB dan dipulihkan ke pengaturan default pabrik.

Register Kemajuan Boot (BPR) digunakan oleh Secure Enclave untuk membatasi akses ke data pengguna dalam berbagai mode dan diperbarui sebelum masuk ke mode berikut:

- *Mode DFU:* Diatur oleh ROM Boot pada perangkat dengan Apple A12 atau SoC yang lebih baru
- *Mode Pemulihan:* Diatur oleh iBoot pada perangkat dengan Apple A10, S2, atau SoC yang lebih baru

Di perangkat dengan akses seluler, subsistem pita dasar seluler melakukan boot aman tambahan menggunakan perangkat lunak dan kunci bertanda tangan yang diverifikasi oleh prosesor pita dasar.

Secure Enclave juga melakukan boot aman yang memeriksa bahwa perangkat lunaknya (sepOS) diverifikasi dan ditandatangani oleh Apple.

Implementasi iBoot yang aman bagi memori

Di iOS 14 dan iPadOS 14, Apple memodifikasi rantai alat kompilator C yang digunakan untuk membuat bootloader iBoot untuk meningkatkan keamanannya. Rantai alat yang dimodifikasi mengimplementasikan kode yang dirancang untuk mencegah masalah memori dan jenis keamanan yang biasanya ditemukan dalam program C. Misalnya, rantai alat membantu mencegah sebagian besar kerentanan di kelas berikut:

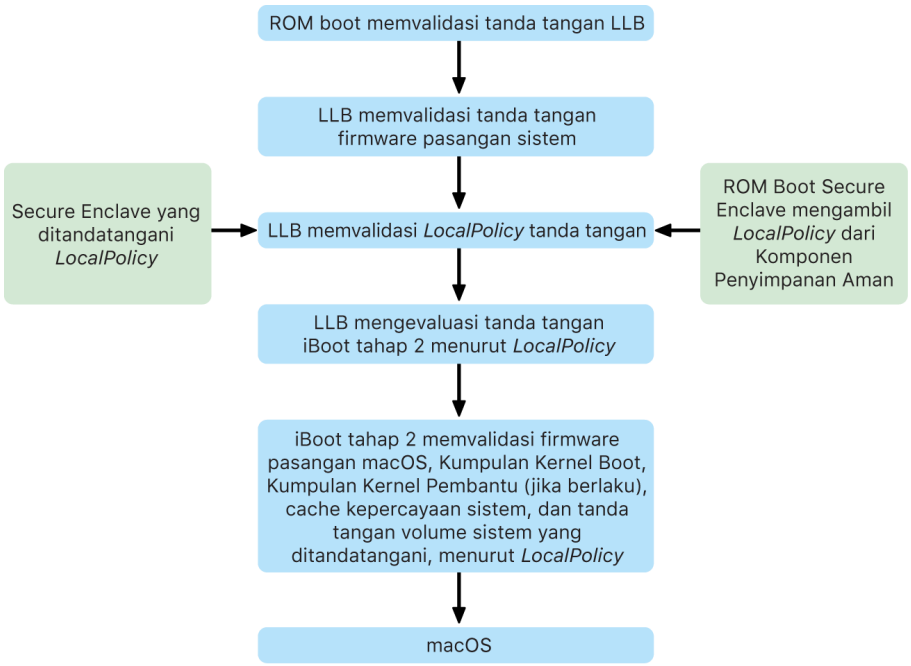
- Luapan buffer, dengan memastikan semua penunjuk membawa informasi batas yang diverifikasi saat mengakses memori
- Eksploitasi heap, dengan memisahkan data heap dari metadatanya dan secara akurat mendeteksi kondisi kesalahan seperti double free
- Kekeliruan jenis, dengan memastikan bahwa semua penunjuk membawa informasi jenis runtime yang diverifikasi selama operasi pemanggilan penunjuk
- Kekeliruan jenis yang disebabkan oleh kesalahan use after free (penggunaan setelah bebas), dengan memisahkan semua alokasi memori dinamis menurut jenis statis

Teknologi ini tersedia di iPhone dengan A13 Bionic Apple atau lebih baru, serta iPad dengan keping A14 Bionic.

Komputer Mac dengan Apple silicon

Proses boot untuk Mac dengan Apple silicon

Saat Mac dengan Apple silicon dinyalakan, Mac melakukan proses boot yang sangat mirip dengan iPhone dan iPad.



Keping mengeksekusi kode dari ROM Boot pada langkah pertama di rantai kepercayaan. Boot aman macOS di Mac dengan Apple silicon bukan hanya memverifikasi kode sistem operasinya, tetapi juga kebijakan keamanan dan bahkan kext (didukung, walau tidak dianjurkan) yang dikonfigurasi oleh pengguna yang disahkan.

Saat diluncurkan, LLB (singkatan dari Bootstrap Level Rendah) lalu memverifikasi tanda tangan dan memuat firmware pasangan sistem untuk inti intra-SoC seperti penyimpanan, layar, manajemen sistem, dan pengontrol Thunderbolt. LLB juga bertanggung jawab untuk memuat LocalPolicy, yang merupakan file yang ditandatangani oleh Prosesor Secure Enclave. File LocalPolicy menjelaskan konfigurasi yang telah pengguna pilih untuk boot sistem dan kebijakan keamanan runtime. LocalPolicy memiliki format struktur data yang sama dengan semua objek boot lainnya, tapi ditandatangani secara lokal oleh kunci pribadi yang hanya tersedia dalam Secure Enclave komputer tertentu, dan bukan ditandatangani oleh server Apple pusat (seperti pembaruan perangkat lunak).

Untuk membantu mencegah pemutaran ulang LocalPolicy sebelumnya, LLB harus mencari nonce dari Komponen Penyimpanan Aman yang terpasang di Secure Enclave. Agar dapat dilakukan, LLB menggunakan ROM Boot Secure Enclave dan memastikan bahwa nonce di LocalPolicy sesuai dengan nonce di Komponen Penyimpanan Aman. Ini membantu mencegah LocalPolicy lama—yang mungkin telah dikonfigurasi untuk keamanan yang lebih rendah—agar tidak diterapkan ulang ke sistem setelah keamanan ditingkatkan. Hasilnya adalah boot aman di Mac dengan Apple silicon membantu melindungi terhadap bukan hanya pembalikan versi sistem operasi, tetapi juga terhadap penurunan kebijakan keamanan.

File LocalPolicy memeriksa apakah sistem operasi dikonfigurasi ke keamanan Penuh, Dikurangi, atau Permisif.

- *Keamanan Penuh:* Sistem berperilaku seperti iOS dan iPadOS, dan hanya mengizinkan boot perangkat lunak yang diketahui sebagai yang terbaru dan tersedia saat penginstalan.
- *Keamanan Dikurangi:* LLB diteruskan untuk memercayai tanda tangan “global” yang dibundel dengan sistem operasi. Ini memungkinkan sistem untuk menjalankan versi macOS yang lebih lama. Karena versi macOS yang lebih lama memiliki kerentanan yang belum diperbaiki, mode keamanan ini disebut *Dikurangi*. Ini juga level kebijakan yang diperlukan untuk mendukung ekstensi kernel boot (kext).
- *Keamanan Permisif:* Sistem berperilaku seperti Keamanan Dikurangi, yang menggunakan verifikasi tanda tangan global untuk iBoot dan lebih tinggi, tapi juga memberi tahu bahwa iBoot harus menerima beberapa objek boot yang ditandatangani oleh Secure Enclave dengan kunci yang sama dengan yang digunakan untuk menandatangani LocalPolicy. Level kebijakan ini mendukung pengguna yang membuat, menandatangani, dan melakukan boot kernel XNU khususnya sendiri.

Jika LocalPolicy menandakan ke LLB bahwa sistem operasi yang dipilih dijalankan di Keamanan Penuh, LLB akan mengevaluasi tanda tangan yang disesuaikan untuk iBoot. Jika Keamanan Dikurangi atau Keamanan Permisif dijalankan, iBoot mengevaluasi tanda tangan global. Kesalahan verifikasi tanda tangan apa pun menyebabkan sistem di-boot ke recoveryOS untuk memberikan pilihan perbaikan.

Setelah LLB meneruskan ke iBoot, iBoot memuat firmware yang dipasangkan dengan macOS seperti firmware untuk Neural Engine Aman, Prosesor Selalu Nyala, dan firmware lainnya. iBoot juga melihat informasi mengenai LocalPolicy yang diteruskan dari LLB. Jika LocalPolicy menandakan bahwa harus terdapat Kumpulan Kernel Pembantu (AuxKC), iBoot akan mencarinya di sistem file, memverifikasi bahwa AuxKC ditandatangani oleh Secure Enclave dengan kunci yang sama dengan LocalPolicy, dan memverifikasi bahwa hash-nya sesuai dengan hash yang disimpan di LocalPolicy. Jika AuxKC diverifikasi, iBoot meletakkannya ke memori dengan Kumpulan Kernel Boot sebelum mengunci bidang memori penuh yang mencakup Kumpulan Kernel Boot dan AuxKC dengan Perlindungan Integritas Koprosesor Sistem (SCIP). Jika kebijakan menandakan bahwa AuxKC harus ada tetapi tidak ditemukan, sistem melanjutkan boot ke macOS tanpa AuxKC. iBoot juga bertanggung jawab untuk memverifikasi hash root untuk volume sistem yang ditandatangani (SSV), untuk memeriksa bahwa sistem file yang akan dipasang kernel diverifikasi integritasnya secara penuh.

Mode boot untuk Mac dengan Apple silicon

Mac dengan Apple silicon memiliki mode boot yang dijelaskan di bawah.

Mode	Kombinasi tombol	Deskripsi
macOS	Dari status mati, tekan dan **lepas** tombol daya.	1. ROM Boot meneruskan ke LLB. 2. LLB memuat firmware yang dipasangkan dengan sistem dan LocalPolicy untuk macOS yang dipilih. 3. LLB mengunci indikasi ke Register Kemajuan Boot (BPR), melakukan boot ke macOS, dan diteruskan ke iBoot. 4. iBoot memuat firmware yang dipasangkan dengan macOS, cache kepercayaan statis, hierarki perangkat, dan Kumpulan Kernel Boot. 5. Jika LocalPolicy mengizinkannya, iBoot memuat Kumpulan Kernel Pembantu (AuxKC) dari kext pihak ketiga. 6. Jika LocalPolicy tidak menonaktifkannya, iBoot memverifikasi hash tanda tangan root untuk volume sistem yang ditandatangani (SSV).
recoveryOS yang dipasangkan	Dari status mati, tekan dan **tahan** tombol daya.	1. ROM Boot meneruskan ke LLB. 2. LLB memuat firmware yang dipasangkan dengan sistem dan LocalPolicy untuk recoveryOS. 3. LLB mengunci indikasi ke Register Kemajuan Boot, melakukan boot ke recoveryOS yang dipasangkan, dan diteruskan ke iBoot untuk recoveryOS yang dipasangkan. 4. iBoot memuat firmware yang dipasangkan dengan macOS, cache kepercayaan, hierarki perangkat, dan Kumpulan Kernel Boot. 5. Jika boot recoveryOS yang dipasangkan gagal, boot ke recoveryOS balik akan dicoba. *Catatan:* Penurunan keamanan tidak diizinkan di Local Policy recoveryOS yang dipasangkan.
recoveryOS balik	Dari status mati, **tekan dua kali dan tahan** tombol daya.	1. ROM Boot meneruskan ke LLB. 2. LLB memuat firmware yang dipasangkan dengan sistem dan LocalPolicy untuk recoveryOS. 3. LLB mengunci indikasi ke Register Kemajuan Boot, melakukan boot ke recoveryOS yang dipasangkan, dan diteruskan ke iBoot untuk recoveryOS. 4. iBoot memuat firmware yang dipasangkan dengan macOS, cache kepercayaan, hierarki perangkat, dan Kumpulan Kernel Boot. *Catatan:* Penurunan keamanan tidak diizinkan di Local Policy recoveryOS yang dipasangkan.
Mode aman	Boot ke recoveryOS seperti langkah di atas, lalu tahan **Shift** saat memilih volume mulai.	1. Melakukan boot ke recoveryOS seperti langkah di atas. 2. Menahan tombol Shift saat memilih volume menyebabkan app BootPicker untuk menyetujui macOS tersebut untuk melakukan boot, seperti normal, ini juga mengatur variabel `nvram` yang memberi tahu iBoot untuk tidak memuat AuxKC di boot berikutnya. 3. Sistem melakukan boot ulang dan melakukan boot ke volume yang ditargetkan, tetapi iBoot tidak memuat AuxKC.

Pembatasan recoveryOS yang dipasangkan

Di macOS 12.0.1 atau lebih baru, setiap penginstalan macOS baru juga menginstal versi recoveryOS yang dipasangkan ke grup volume APFS. Rancangan ini biasa ditemukan pengguna komputer Mac berbasis Intel, tapi di Mac dengan Apple silicon, ini menyediakan keamanan tambahan dan jaminan kompatibilitas. Karena setiap penginstalan macOS kini memiliki recoveryOS terdedikasi yang dipasangkan, ini membantu memastikan bahwa hanya recoveryOS terdedikasi yang dipasangkan yang dapat melakukan operasi penurunan keamanan. Ini membantu melindungi penginstalan versi macOS yang lebih baru dari perubahan yang dimulai dari versi macOS yang lebih lama, dan sebaliknya.

Pembatasan pemasangan diberlakukan sebagai berikut:

- Semua penginstalan macOS 11 dipasangkan ke recoveryOS. Jika penginstalan macOS 11 dipilih untuk melakukan boot secara default, recoveryOS di-boot dengan menahan tombol daya saat boot di Mac dengan Apple silicon. recoveryOS dapat menurunkan pengaturan keamanan penginstalan macOS 11, tapi tidak dapat menurunkan penginstalan macOS 12.0.1.
- Jika penginstalan macOS 12.0.1 atau lebih baru dipilih untuk melakukan boot secara default, recoveryOS-nya yang dipasangkan di-boot dengan menahan tombol daya saat Mac memulai. recoveryOS yang dipasangkan dapat menurunkan pengaturan keamanan untuk penginstalan macOS yang dipasangkan, tapi tidak dapat menurunkan penginstalan macOS lain.

Untuk melakukan boot ke recoveryOS yang dipasangkan untuk semua penginstalan macOS, penginstalan tersebut harus dipilih sebagai default, yang dilakukan menggunakan Disk Mulai di Preferensi Sistem atau dengan memulai recoveryOS mana pun dan menahan Option saat memilih volume.

Catatan: recoveryOS balik tidak dapat melakukan penurunan untuk semua penginstalan macOS.

Kontrol kebijakan keamanan Disk Mulai untuk Mac dengan Apple silicon

Tinjauan

Tidak seperti kebijakan keamanan di Mac berbasis Intel, kebijakan keamanan di Mac dengan Apple silicon ditujukan untuk setiap sistem operasi yang terinstal. Ini berarti beberapa sistem operasi macOS yang terinstal dengan versi dan kebijakan keamanan berbeda didukung di Mac yang sama. Demi alasan ini, *pemilih sistem operasi* telah ditambahkan ke Utilitas Keamanan Mulai.

Di Mac dengan Apple silicon, Utilitas Keamanan Sistem menandakan keseluruhan status keamanan macOS yang dikonfigurasi pengguna seperti boot kext atau konfigurasi Perlindungan Integritas Sistem (SIP). Jika perubahan pada pengaturan keamanan akan menurunkan keamanan secara signifikan atau membuat sistem lebih mudah diretas, pengguna harus masuk ke recoveryOS dengan menahan tombol daya (sehingga malware tidak dapat memicu sinyal, hanya seseorang dengan akses fisik yang dapat melakukannya), untuk melakukan perubahan. Karena ini, Mac berbasis Apple silicon juga tidak akan memerlukan (atau mendukung) kata sandi firmware—semua perubahan penting telah dibatasi oleh pengesahan pengguna. Untuk informasi lainnya tentang SIP, lihat Perlindungan Integritas Sistem.

Keamanan Penuh dan Keamanan Dikurangi dapat diatur menggunakan Utilitas Keamanan Mulai dari recoveryOS. Namun, Keamanan Permisif hanya dapat diakses dari alat baris perintah untuk pengguna yang menerima risiko penurunan keamanan Mac mereka.

Kebijakan Keamanan Penuh

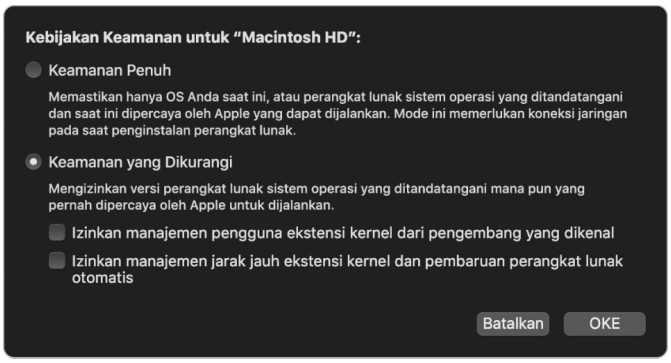
Keamanan Penuh adalah default-nya dan berperilaku seperti iOS dan iPadOS. Pada saat perangkat lunak diunduh dan dipersiapkan untuk penginstalan, alih-alih menggunakan tanda tangan global yang disertakan dengan perangkat lunak, macOS berkomunikasi dengan server penandatanganan Apple yang sama dengan yang digunakan untuk iOS dan iPadOS dan meminta tanda tangan "personal" yang baru. Tanda tangan dipersonalisasi jika menyertakan Identifikasi Keping Eksklusif (ECID)—ID unik yang dikhususkan bagi CPU Apple dalam kasus ini—sebagai bagian dari permintaan penandatanganan. Tanda tangan yang dikembalikan oleh server penandatanganan akan menjadi unik dan dapat digunakan hanya oleh CPU Apple tersebut. Saat kebijakan Keamanan Penuh diaktifkan, ROM Boot dan LLB membantu memastikan bahwa tanda tangan yang diberikan tidak hanya ditandatangani oleh Apple tapi juga spesifik untuk Mac, khususnya mengikat versi macOS tersebut ke Mac tersebut.

Penggunaan server penanda tangan juga menyediakan perlindungan terhadap serangan penurunan versi daripada pendekatan tanda tangan global biasa. Dalam sistem penandatanganan global, jangka waktu keamanan mungkin telah banyak diturunkan, tapi sistem yang tidak pernah melihat firmware terbaru tidak akan mengetahuinya. Misalnya, komputer yang saat ini percaya bahwa jangka waktu keamanan 1 sedang diaktifkan akan menerima perangkat lunak dari jangka waktu keamanan 2, meskipun jangka waktu keamanan saat ini yang sebenarnya adalah 5. Dengan sistem penandatanganan online Apple silicon, server penandatanganan dapat menolak pembuatan tanda tangan untuk perangkat lunak yang bukan merupakan jangka waktu keamanan terbaru.

Selain itu, jika penyerang menemukan kerentanan setelah jangka waktu keamanan berubah, mereka tidak dapat begitu saja mengambil perangkat lunak yang rentan dari jangka waktu sebelumnya dari sistem A dan menerapkannya ke sistem B agar dapat menyerangnya. Fakta bahwa kerentanan perangkat lunak dari jangka waktu yang lebih lama dipersonalisasi ke sistem A akan membantu mencegahnya untuk ditransfer dan, dengan demikian, tidak digunakan untuk menyerang sistem B. Semua mekanisme ini bekerja sama untuk menyediakan jaminan yang lebih kuat bahwa penyerang tidak dapat dengan sengaja menempatkan perangkat lunak yang rentan di suatu Mac agar dapat membobol perlindungan yang disediakan oleh perangkat lunak terbaru. Namun, pengguna yang memiliki nama pengguna dan kata sandi administrator untuk Mac selalu dapat memilih kebijakan keamanan yang paling baik untuk kasus penggunaan mereka.

Kebijakan Keamanan Dikurangi

Keamanan Dikurangi mirip dengan perilaku Keamanan Sedang di Mac berbasis Intel dengan keping T2, vendor (dalam hal ini, Apple) membuat tanda tangan digital untuk kode yang menegaskan bahwa kode berasal dari vendor. Rancangan ini membantu menghalangi agar tidak memasukkan kode yang tidak ditandatangani. Apple menyebut tanda tangan ini sebagai tanda tangan "global" karena tanda tangan tersebut dapat digunakan di Mac mana pun, selama jangka waktu yang tidak terbatas, untuk Mac yang saat ini memiliki kumpulan kebijakan Keamanan Dikurangi. Keamanan Dikurangi tidak menyediakan perlindungan terhadap serangan pembalikan versi (meskipun perubahan sistem operasi yang tidak sah dapat mengakibatkan terblokirnya data pengguna). Untuk informasi lainnya, lihat Ekstensi kernel di Mac dengan Apple silicon.

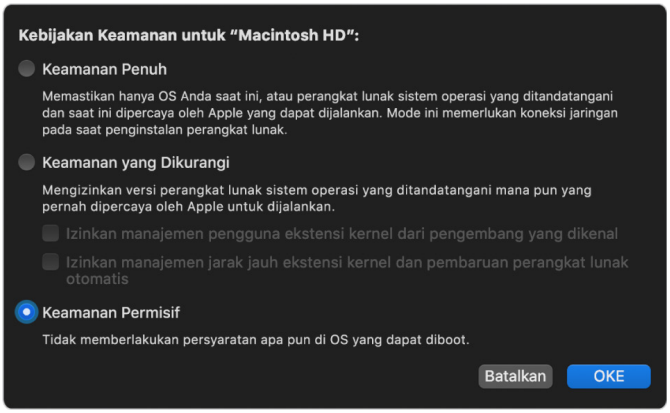


Selain memungkinkan pengguna untuk menjalankan versi macOS yang lebih lama, Keamanan Dikurangi diperlukan untuk tindakan lain yang dapat membahayakan keamanan sistem pengguna, seperti memperkenalkan ekstensi kernel pihak ketiga (kext). Kext memiliki hak yang sama dengan kernel, oleh sebab itu kerentanan di kext pihak ketiga dapat menyebabkan peretasan menyeluruh terhadap sistem operasi. Oleh karena itu pengembang sangat dianjurkan untuk mengadopsi ekstensi sistem sebelum dukungan kext dihapus dari macOS untuk komputer Mac dengan Apple silicon mendatang. Bahkan saat diaktifkan, kext pihak ketiga tidak dapat dimuat ke kernel sesuai permintaan. Sebagai gantinya, kext digabung ke Kumpulan Kernel Pembantu (AuxKC)—yang hash-nya disimpan di LocalPolicy—dan olah karenanya memerlukan boot ulang. Untuk informasi lainnya mengenai pembuatan AuxKC, lihat Ekstensi kernel di macOS.

Kebijakan Keamanan Permisif

Keamanan Permisif diperuntukkan bagi pengguna yang menerima risiko akibat menurunkan status keamanan Mac mereka ke status yang lebih tidak aman. Mode ini berbeda dari mode Tidak Ada Keamanan di Mac berbasis Intel dengan keping T2. Dengan Keamanan Permisif, verifikasi tanda tangan masih dilakukan bersamaan dengan seluruh rantai boot aman, tapi mengatur kebijakan ke Permisif memberi tahu iBoot untuk menerima objek boot yang ditandatangani oleh Secure Enclave secara lokal, seperti Kumpulan Kernel Boot buatan pengguna yang dibuat dari kernel XNU khusus. Dalam cara ini, Keamanan Permisif juga menyediakan kemampuan arsitektural untuk menjalankan kernel "sistem operasi yang sepenuhnya tidak tepercaya" arbitrer. Saat Kumpulan Kernel Boot khusus atau sistem operasi yang sepenuhnya tidak tepercaya dimuat di sistem, beberapa kunci dekripsi menjadi tidak tersedia. Ini dirancang untuk mencegah sistem operasi yang sepenuhnya tidak tepercaya mengakses data dari sistem operasi yang tepercaya.

Penting: Apple tidak menyediakan atau mendukung kernel XNU khusus.



Terdapat cara lain yang membedakan Keamanan Permisif dengan Tidak Ada Keamanan di Mac berbasis Intel dengan keping T2: Ini adalah prasyarat untuk beberapa penurunan keamanan yang sebelumnya dapat dikontrol secara independen. Yang paling jelas, untuk menonaktifkan Perlindungan Integritas Sistem (SIP) di Mac dengan Apple silicon, pengguna harus mengakui bahwa pengguna mengubah sistem ke Keamanan Permisif. Hal ini diperlukan karena menonaktifkan SIP selalu mengakibatkan sistem masuk ke kondisi yang membuat kernel lebih mudah diretas. Khususnya, menonaktifkan SIP di Mac dengan Apple silicon akan menonaktifkan pemberlakuan tanda tangan kext selama waktu pembuatan AuxKC, yang oleh karena itu mengizinkan kext arbitrer dimuat ke memori kernel. Peningkatan lain terhadap SIP yang telah dibuat di Mac dengan Apple silicon adalah bahwa tempat penyimpanan kebijakan telah dipindahkan ke luar NVRAM dan masuk ke LocalPolicy. Maka dari itu, menonaktifkan SIP kini memerlukan pengesahan oleh pengguna yang memiliki akses ke kunci penandatanganan LocalPolicy dari recoveryOS (dilakukan dengan menekan dan menahan tombol daya). Ini makin mempersulit penyerang yang hanya memanfaatkan perangkat lunak, atau bahkan penyerang yang memiliki akses langsung secara fisik, untuk menonaktifkan SIP.

Menurunkan ke Keamanan Permisif tidak dapat dilakukan dari app Utilitas Keamanan Mulai. Pengguna hanya dapat menurunkan versi dengan menjalankan alat baris perintah dari Terminal di recoveryOS, seperti `csrutil` (untuk menonaktifkan SIP). Setelah kebijakan diturunkan oleh pengguna, hasilnya akan terlihat di Utilitas Keamanan Mulai, sehingga pengguna dapat mengatur keamanan ke mode yang lebih aman dengan mudah.

Catatan: Mac dengan Apple silicon tidak memerlukan atau mendukung kebijakan boot media tertentu karena semua boot dilakukan secara lokal. Jika pengguna memilih untuk melakukan boot dari media eksternal, versi sistem operasi tersebut harus terlebih dahulu disesuaikan menggunakan boot ulang yang disahkan dari recoveryOS. Boot ulang ini membuat file LocalPolicy di drive internal yang digunakan untuk melakukan boot tepercaya dari sistem operasi yang disimpan di media eksternal. Ini berarti konfigurasi boot dari media eksternal selalu dinyalakan secara eksplisit di basis per sistem operasi, dan sudah memerlukan pengesahan pengguna, sehingga tidak memerlukan konfigurasi aman tambahan.

Pembuatan dan manajemen kunci penandatanganan LocalPolicy

Pembuatan

Saat macOS pertama kali diinstal di pabrik, atau saat hapus-instal tertambat dilakukan, Mac menjalankan kode dari disk RAM pemulihan sementara untuk memulai status default. Selama proses ini, lingkungan pemulihan membuat pasangan kunci publik dan pribadi baru yang disimpan di Secure Enclave. Kunci pribadi disebut sebagai *Kunci Identitas Pemilik (OIK)*. Jika OIK sudah ada, OIK akan dihapus sebagai bagian dari proses ini. Lingkungan pemulihan juga memulai kunci yang digunakan untuk Kunci Aktivasi; *Kunci Identitas Pengguna (UIK)*. Bagian proses tersebut yang unik bagi Mac dengan Apple silicon adalah saat sertifikasi UIK diminta untuk Kunci Aktivasi, sekumpulan batasan yang diminta untuk diberlakukan saat waktu validasi di LocalPolicy disertakan. Jika perangkat tidak dapat memperoleh UIK yang disertifikasi untuk Kunci Aktivasi (misalnya, karena perangkat saat ini diasosiasikan dengan akun Cari Mac Saya dan dilaporkan sebagai hilang), perangkat tidak dapat lanjut membuat Kebijakan Lokal. Jika perangkat diberikan *Sertifikat Identitas Pengguna (ucrt)*, ucrt tersebut berisi batasan kebijakan yang diterapkan server dan batasan kebijakan yang diminta pengguna di ekstensi X.509 v3.

Saat berhasil didapatkan, Kunci Aktivasi/`ucrt` disimpan di database di server dan juga dikembalikan ke perangkat. Setelah perangkat memiliki ucrt, permintaan sertifikasi untuk kunci publik yang terkait dengan OIK dikirim ke server *Otoritas Pengesahan Dasar (BAA)*. BAA memverifikasi permintaan sertifikasi OIK menggunakan kunci publik dari ucrt yang disimpan di database yang dapat diakses oleh BAA. Jika BAA dapat memverifikasi sertifikasi, BAA menyertifikasi kunci publik, menghasilkan *Sertifikat Identitas Pemilik (OIC)* yang ditandatangani oleh BAA dan berisi batasan yang disimpan di ucrt. OIC dikirim kembali ke Secure Enclave. Dari saat itu, kapan pun Secure Enclave menandatangani LocalPolicy baru, Secure Enclave melampirkan OIC ke Image4. LLB memiliki kepercayaan internal di sertifikat dasar BAA, yang membuatnya memercayai OIC, yang lalu membuatnya memercayai tanda tangan LocalPolicy secara keseluruhan.

Batasan RemotePolicy

Semua file Image4, bukan hanya Kebijakan Lokal, berisi batasan di evaluasi manifes Image4. Batasan ini dikodekan menggunakan pengidentifikasi objek khusus (OID) di sertifikat ujung. Perpustakaan verifikasi Image4 mencari OID batasan sertifikat khusus dari sertifikat selama evaluasi tanda tangan, lalu secara mekanis mengevaluasi batasan yang ditetapkan di dalamnya. Batasan berupa:

- X harus ada
- X tidak boleh ada
- X harus memiliki nilai tertentu

Misalnya, untuk tanda tangan yang "disesuaikan", batasan sertifikat akan berisi "ECID harus ada", dan untuk tanda tangan "global", batasan akan berisi "ECID tidak boleh ada". Batasan ini dirancang untuk memastikan bahwa semua file Image4 yang ditandatangani oleh kunci yang sesuai harus memenuhi persyaratan tertentu untuk menghindari kesalahan pembuatan manifes Image4 yang ditandatangani.

Pada konteks setiap LocalPolicy, batasan sertifikat Image4 ini dirujuk sebagai *RemotePolicy*. RemotePolicy yang berbeda dapat ada untuk LocalPolicies lingkungan boot yang berbeda. RemotePolicy digunakan untuk membatasi LocalPolicy recoveryOS sehingga saat di-boot, hanya dapat berperilaku layaknya di-boot dengan Keamanan Penuh. Ini meningkatkan kepercayaan pada integritas lingkungan boot recoveryOS sebagai tempat yang memungkinkan kebijakan diubah. RemotePolicy membatasi LocalPolicy agar tidak berisi ECID Mac tempat LocalPolicy dibuat, dan Hash Nonce Kebijakan Jarak Jauh (`rpnh`) spesifik yang disimpan di Komponen Penyimpanan Aman di Mac tersebut. `rpnh`, dan maka dari itu RemotePolicy, hanya diubah saat tindakan diambil untuk Cari Mac Saya dan Kunci Aktivasi—seperti pendaftaran, pembatalan pendaftaran, penguncian jarak jauh, dan penghapusan jarak jauh. Batasan Kebijakan Jarak Jauh ditetapkan dan ditentukan pada saat sertifikasi Kunci Identitas Pengguna (UIK) dan ditandatangani ke Sertifikat Identitas Pengguna (ucrt) yang diterbitkan. Beberapa batasan Kebijakan Jarak Jauh ditetapkan oleh server seperti ECID, ChipID, dan BoardID. Ini dirancang untuk mencegah suatu perangkat agar tidak menandatangani file LocalPolicy untuk perangkat lain. Batasan Kebijakan Jarak Jauh lain dapat ditentukan oleh perangkat untuk membantu mencegah penurunan Keamanan Kebijakan Lokal tanpa memberikan pengesahan lokal yang diperlukan untuk mengakses OIK saat ini dan pengesahan jarak jauh dari akun yang Dikunci Aktivasi oleh perangkat.

Konten file LocalPolicy untuk Mac dengan Apple silicon

LocalPolicy adalah file Image4 yang ditandatangani oleh Secure Enclave. Image4 adalah format struktur data yang dikodekan dengan ASN.1 (Abstract Syntax Notation One) DER yang digunakan untuk menjelaskan informasi mengenai objek rantai boot aman di platform Apple. Di model boot aman berbasis Image4, kebijakan keamanan diminta pada waktu penginstalan perangkat lunak yang dimulai oleh permintaan penandatanganan ke server penandatanganan Apple pusat. Jika kebijakan dapat diterima, server penandatanganan mengembalikan file Image4 yang ditandatangani, yang berisi berbagai rangkaian kode empat karakter (4CC). File Image4 yang ditandatangani dan 4CC ini dievaluasi saat proses mulai oleh perangkat lunak seperti ROM Boot atau LLB.

Penyerahan kepemilikan di antara sistem operasi

Akses ke Kunci Identitas Pemilik (OIK) disebut sebagai “Kepemilikan”. Kepemilikan diperlukan untuk memungkinkan pengguna untuk menandatangani kembali LocalPolicy setelah membuat perubahan kebijakan atau perangkat lunak. OIK dilindungi dengan hierarki kunci yang sama seperti yang dijelaskan di Perlindungan Kunci yang Disegel (SKP), dengan OIK dilindungi oleh Kunci enkripsi kunci (KEK) yang sama dengan Kunci enkripsi volume (VEK). Ini berarti OIK biasanya dilindungi oleh kata sandi pengguna dan pengukuran sistem operasi serta kebijakan. Hanya terdapat satu OIK untuk semua sistem operasi di Mac. Maka, saat menginstal sistem operasi kedua, persetujuan eksplisit diperlukan dari pengguna di sistem operasi pertama untuk menyerahkan Kepemilikan ke pengguna di sistem operasi kedua. Namun, pengguna belum ada untuk sistem operasi kedua, saat penginstal dijalankan dari sistem operasi pertama. Pengguna di sistem operasi biasanya tidak dibuat hingga sistem operasi di-boot dan Asisten Pengaturan dijalankan. Maka, dua tindakan baru diperlukan saat menginstal sistem operasi kedua di Mac dengan Apple silicon:

- Membuat LocalPolicy untuk sistem operasi kedua
- Menyiapkan “Instal Pengguna” untuk menyerahkan Kepemilikan

Saat menjalankan Asisten Penginstalan dan menargetkan penginstalan untuk volume kosong kedua, pengguna akan ditanyai apakah ingin menyalin pengguna dari volume saat ini untuk dijadikan pengguna pertama pada volume kedua. Jika pengguna memilih ya, “Instal Pengguna” yang dibuat adalah, sebenarnya, KEK yang diturunkan dari kata sandi pengguna dan kunci perangkat keras yang dipilih, yang kemudian digunakan untuk mengenkripsi OIK saat diserahkan ke sistem operasi kedua. Lalu, dari dalam Asisten Penginstalan sistem operasi kedua, kata sandi pengguna akan diminta untuk mengizinkannya mengakses OIK di Secure Enclave untuk sistem operasi baru. Jika pengguna memilih untuk tidak menyalin pengguna, Instal Pengguna masih dibuat dengan cara yang sama, namun kata sandi kosong digunakan alih-alih kata sandi pengguna. Alur kedua ini ada untuk skenario administrasi sistem tertentu. Namun, pengguna yang ingin melakukan penginstalan multi-volume dan ingin melakukan penyerahan Kepemilikan dalam cara yang paling aman harus selalu memilih untuk menyalin pengguna dari sistem operasi pertama ke sistem operasi kedua.

LocalPolicy di Mac dengan Apple silicon

Untuk Mac dengan Apple silicon, kontrol kebijakan keamanan lokal telah didelegasikan ke aplikasi yang dijalankan di Secure Enclave. Perangkat lunak dapat menggunakan info pengesahan pengguna dan mode boot CPU utama untuk menentukan siapa yang dapat mengubah kebijakan keamanan dan dari lingkungan boot mana. Ini membantu pencegahan perangkat lunak berbahaya agar tidak menggunakan kontrol kebijakan keamanan terhadap pengguna dengan menurunkannya untuk memperoleh lebih banyak hak.

Properti manifes LocalPolicy

File LocalPolicy berisi beberapa 4CC arsitektural yang ditemukan di sebagian besar file Image4—seperti ID papan atau model (BORD), menandakan keping Apple tertentu (CHIP), atau Identifikasi Keping Eksklusif (ECID). Tetapi 4CC hanya fokus di kebijakan keamanan yang dapat dikonfigurasi pengguna.

Catatan: Apple menggunakan istilah *One True recoveryOS (1TR) yang Dipasangkan* untuk menandakan boot ke recoveryOS yang dipasangkan menggunakan satu kali tekan dan tahan tombol daya fisik. Ini berbeda dari boot recoveryOS normal, yang dilakukan menggunakan NVRAM atau dua kali tekan dan tahan atau yang dapat terjadi saat ada kesalahan selama proses mulai. Penekanan tombol fisik jenis khusus meningkatkan kepercayaan bahwa lingkungan boot tidak dapat dijangkau oleh penyerang yang hanya memanfaatkan perangkat lunak yang telah masuk ke macOS.

Hash Nonce LocalPolicy (lpnh)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* `lpnh` digunakan untuk anti-pemutaran ulang LocalPolicy. Ini adalah hash SHA384 Nonce LocalPolicy (LPN) yang disimpan di Komponen Penyimpanan Aman dan dapat diakses menggunakan ROM Boot Secure Enclave atau Secure Enclave. Nonce raw tidak pernah terlihat bagi Prosesor Aplikasi, hanya ke sepOS. Penyerang yang ingin meyakinkan LLB bahwa LocalPolicy sebelumnya yang telah mereka dapatkan bersifat valid harus menempatkan nilai ke Komponen Penyimpanan Aman yang membuat hash ke nilai `lpnh` yang sama pada di LocalPolicy yang mereka ingin putar ulang. Biasanya, terdapat satu LPN yang valid di sistem—kecuali selama pembaruan perangkat lunak, saat terdapat dua yang valid—untuk mengizinkan kemungkinan kembali melakukan boot perangkat lunak lama saat terjadi kesalahan pembaruan. Saat LocalPolicy mana pun untuk sistem operasi mana pun diubah, semua kebijakan ditandatangani kembali dengan nilai *lpnh* baru sesuai dengan LPN baru yang ditemukan di Komponen Penyimpanan Aman. Perubahan ini terjadi saat pengguna mengubah pengaturan keamanan atau membuat sistem operasi baru dengan LocalPolicy baru untuk masing-masing.

Hash Nonce Kebijakan Jarak Jauh (rpnh)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* `rpnh` berperilaku sama dengan `lpnh` tapi hanya diperbarui saat kebijakan jarak jauh diperbarui, seperti saat mengubah status pendaftaran Lacak. Perubahan ini terjadi saat pengguna mengubah status Lacak di Mac mereka.

Hash Nonce recoveryOS (ronh)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* `ronh` berperilaku sama dengan lpnh, tapi ditemukan secara eksklusif di LocalPolicy untuk recoveryOS sistem. ronh diperbarui saat recoveryOS sistem diperbarui, seperti di pembaruan perangkat lunak. Nonce terpisah dari `lpnh` dan `rpnh` digunakan sehingga saat perangkat dinonaktifkan oleh Lacak, sistem operasi yang ada tersebut dapat dinonaktifkan (dengan menghapus LPN serta RPN dari Keping Penyimpanan Aman), dan tetap mempertahankan boot ke recoveryOS sistem. Dengan acara ini, sistem operasi dapat diaktifkan ulang saat pemilik sistem membuktikan kontrolnya terhadap sistem dengan memasukkan kata sandi iCloud mereka yang digunakan untuk akun Lacak. Perubahan ini terjadi saat pengguna memperbarui recoveryOS sistem atau membuat sistem operasi baru.

Hash Manifes Image4 Tahap Berikutnya (nsih)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* Bidang *nsih* mewakili hash SHA384 pada struktur data manifes Image4 yang menjelaskan macOS yang di-boot. Manifes Image4 macOS berisi pengukuran untuk semua objek boot—seperti iBoot, cache kepercayaan statis, hierarki perangkat, Kumpulan Kernel Boot, dan hash root volume yang merupakan volume sistem yang ditandatangani (SSV). Saat LLB diteruskan untuk melakukan boot macOS yang ditentukan, iBoot dirancang untuk memastikan bahwa hash manifes Image4 macOS yang dilampirkan ke iBoot sesuai dengan yang ditangkap di bidang `nsih` LocalPolicy. Dengan cara ini, `nsih` menangkap tujuan pengguna terkait jenis sistem operasi yang diinginkan pengguna saat ia membuat LocalPolicy. Pengguna mengubah nilai `nsih` secara implisit saat melakukan pembaruan perangkat lunak.

Hash Kebijakan Kumpulan Kernel Pembantu (AuxKC) (auxp)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* macOS
- *Deskripsi:* `auxp` adalah hash SHA384 kebijakan daftar kext yang disahkan oleh pengguna (UAKL). Ini digunakan pada waktu pembuatan AuxKC untuk membantu memastikan bahwa hanya kext yang disahkan oleh pengguna yang disertakan di AuxKC. `smb2` adalah prasyarat untuk mengatur bidang ini. Pengguna mengubah nilai `auxp` secara implisit saat mereka mengubah UAKL dengan menyetujui kext dari panel Keamanan & Privasi di Preferensi Sistem.

Hash Manifes Image4 Kumpulan Kernel Pembantu (AuxKC) (auxi)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* macOS
- *Deskripsi:* Setelah sistem memverifikasi bahwa hash UAKL sesuai dengan yang ditemukan di bidang `auxp` LocalPolicy, sistem meminta AuxKC untuk ditandatangani oleh aplikasi prosesor Secure Enclave yang bertanggung jawab atas penandatanganan LocalPolicy. Berikutnya, hash SHA384 pada tanda tangan manifes Image4 AuxKC ditempatkan ke LocalPolicy untuk menghindari kemungkinan pencampuran dan pencocokan AuxKC yang ditanda tangan sebelumnya ke sistem operasi pada waktu boot. Jika bidang `auxi` ditemukan di LocalPolicy, iBoot akan mencoba untuk memuat AuxKC dari penyimpanan dan memvalidasi tanda tangannya. iBoot juga memverifikasi bahwa hash manifes Image4 yang dilampirkan ke AuxKC sesuai dengan nilai yang ditemukan di bidang `auxi`. Jika AuxKC gagal dimuat untuk alasan apa pun, sistem melanjutkan boot tanpa objek boot ini, dan (maka) tanpa ada kext pihak ketiga yang dimuat. Bidang `auxp` adalah prasyarat untuk mengatur bidang auxi di LocalPolicy. Pengguna mengubah nilai `auxi` secara implisit saat mereka mengubah UAKL dengan menyetujui kext dari panel Keamanan & Privasi di Preferensi Sistem.

Hash Penerimaan Kumpulan Kernel Pembantu (AuxKC) (auxr)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* macOS
- *Deskripsi:* `auxr` adalah hash SHA384 penerimaan AuxKC, yang menandakan kumpulan kext persis yang disertakan ke AuxKC. Penerimaan AuxKC dapat berupa subset UAKL, karena kext dapat dikecualikan dari AuxKC bahkan jika kext disahkan pengguna, jika diketahui dapat digunakan untuk serangan. Selain itu, beberapa kext yang dapat digunakan untuk merusak batas kernel pengguna dapat menyebabkan berkurangnya fungsionalitas seperti ketidakmampuan dalam menggunakan Apple Pay atau memutar konten 4K dan HDR. Pengguna yang menginginkan kemampuan ini harus memilih penyertaan AuxKC yang lebih dibatasi. Bidang `auxp` adalah prasyarat untuk mengatur bidang `auxr` di LocalPolicy. Pengguna mengubah nilai `auxr` secara implisit saat mereka membuat AuxKC baru dari panel Keamanan & Privasi di Preferensi Sistem.

Hash Manifes Image4 CustomOS (coih)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* `coih` adalah hash SHA384 dari manifes Image4 CustomOS. Muatan untuk manifes tersebut digunakan oleh iBoot (bukan kernel XNU) untuk mentransfer kontrol. Pengguna mengubah nilai `coih` secara implisit saat menggunakan alat baris perintah `kmutil configure-boot` pada 1TR.

UUID grup volume APFS (vuid)

- *Jenis:* OctetString (16)
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* `vuid` menandakan grup volume yang harus digunakan kernel sebagai root. Bidang ini sebagian besar digunakan untuk informasi dan tidak digunakan untuk pembatasan keamanan. `vuid` ini diatur oleh pengguna secara implisit saat membuat penginstalan sistem operasi baru.

UUID Grup kunci enkripsi kunci (KEK) (kuid)

- *Jenis:* OctetString (16)
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* `kuid` menandakan volume yang di-boot. Kunci enkripsi kunci biasanya telah digunakan untuk Perlindungan Data. Untuk setiap LocalPolicy, KEK digunakan untuk melindungi kunci penandatanganan LocalPolicy. `kuid` diatur oleh pengguna secara implisit saat membuat penginstalan sistem operasi baru.

Pengukuran Kebijakan Boot Tepercaya recoveryOS yang dipasangkan (prot)

- *Jenis:* OctetString (48)
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* Pengukuran Kebijakan Boot Tepercaya recoveryOS yang dipasangkan (TBPM) adalah kalkulasi hash SHA384 iteratif khusus melalui manifes Image4 LocalPolicy, kecuali nonce, untuk memberikan pengukuran yang konsisten sepanjang waktu (karena nonce seperti `lpnh` sering diperbarui). Bidang `prot`, yang hanya ditemukan di setiap LocalPolicy macOS, menyediakan pasangan untuk menandakan LocalPolicy recoveryOS yang sesuai dengan LocalPolicy macOS.

Memiliki Kebijakan Lokal recoveryOS yang Ditandatangani Secure Enclave (hrlp)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* `hrlp` menandakan apakah nilai `prot` (di atas) adalah pengukuran LocalPolicy recoveryOS yang ditandatangani oleh Secure Enclave atau tidak. Jika tidak, LocalPolicy recoveryOS ditandatangani oleh server penandatanganan online Apple, yang menandatangani item seperti file Image4 macOS.

Versi Sistem Operasi Lokal (love)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS, macOS
- *Deskripsi:* `love` menandakan versi OS tujuan pembuatan LocalPolicy. Versi diperoleh dari manifes status berikutnya selama pembuatan LocalPolicy dan digunakan untuk memberlakukan pembatasan pemasangan recoveryOS.

Multi-Boot Aman (smb0)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR, recoveryOS
- *Deskripsi:* Jika `smb0` ada dan benar, LLB memungkinkan manifes Image4 tahap berikutnya untuk ditandatangani secara global, alih-alih memerlukan tanda tangan yang disesuaikan. Pengguna dapat mengubah bidang ini dengan Utilitas Keamanan Mulai atau `bputil` untuk menurunkan ke Keamanan Dikurangi.

Multi-Boot Aman (smb1)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* Jika `smb1` ada dan benar, iBoot memungkinkan objek seperti kumpulan kernel khusus untuk ditandatangani oleh Secure Enclave dengan kunci yang sama seperti LocalPolicy. Keberadaan `smb0` adalah prasyarat untuk adanya `smb1`. Pengguna dapat mengubah bidang ini menggunakan alat baris perintah seperti `csrutil` atau `bputil` untuk menurunkan ke Keamanan Permisif.

Multi-Boot Aman (smb2)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* Jika `smb2` ada dan benar, iBoot memungkinkan Kumpulan Kernel Pembantu untuk ditandatangani oleh Secure Enclave dengan kunci yang sama seperti LocalPolicy. Keberadaan `smb0` adalah prasyarat untuk adanya `smb2`. Pengguna dapat mengubah bidang ini menggunakan Utilitas Keamanan Mulai atau `bputil` untuk menurunkan ke Keamanan Dikurangi dan mengaktifkan kext pihak ketiga.

Multi-Boot Aman (smb3)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* Jika `smb3` ada dan benar, pengguna di perangkat telah memilih kontrol mobile device management (MDM) pada perangkatnya. Keberadaan bidang ini membuat aplikasi prosesor Secure Enclave yang mengontrol LocalPolicy menerima pengesahan MDM alih-alih memerlukan pengesahan pengguna lokal. Pengguna dapat mengubah bidang ini menggunakan Utilitas Keamanan Mulai atau `bputil` untuk mengaktifkan kontrol yang dikelola pada kext pihak ketiga dan pembaruan perangkat lunak. (Di macOS 11.2 atau lebih baru, MDM juga dapat memulai pembaruan ke versi macOS terbaru jika mode keamanan saat ini adalah Keamanan Penuh.)

Multi-Boot Aman (smb4)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* macOS
- *Deskripsi:* Jika `smb4` ada dan benar, perangkat telah memilih kontrol MDM pada sistem operasi menggunakan Apple School Manager, Apple Business Manager, atau Apple Business Essentials. Keberadaan bidang ini membuat aplikasi Secure Enclave yang mengontrol LocalPolicy menerima pengesahan MDM alih-alih memerlukan pengesahan pengguna lokal. Bidang ini diubah oleh solusi MDM saat perangkat lunak mendeteksi bahwa nomor seri perangkat muncul di salah satu dari ketiga layanan tersebut.

Perlindungan Integritas Sistem (sip0)

- *Jenis:* Integer 64 bit yang tidak ditandatangani
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* `sip0` menyimpan bit kebijakan Perlindungan Integritas Sistem (SIP) yang sebelumnya disimpan di NVRAM. Bit kebijakan SIP baru ditambahkan di sini (alih-alih menggunakan bidang LocalPolicy seperti di bawah), jika bit hanya digunakan di macOS, dan tidak digunakan oleh LLB. Pengguna dapat mengubah bidang ini menggunakan `csrutil` dari 1TR untuk menonaktifkan SIP dan menurunkan ke Keamanan Permisif.

Perlindungan Integritas Sistem (sip1)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* Jika `sip1` ada dan benar, iBoot akan mengizinkan kegagalan untuk memverifikasi hash root volume SSV. Pengguna dapat mengubah bidang ini menggunakan `csrutil` atau `bputil` dari 1TR.

Perlindungan Integritas Sistem (sip2)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* Jika sip2 ada dan benar, iBoot tidak akan mengunci register perangkat keras *Area Hanya Baca Teks yang Dapat Dikonfigurasi (CTRR)* yang menandai memori kernel sebagai tidak dapat ditulisi. Pengguna dapat mengubah bidang ini menggunakan `csrutil` atau `bputil` dari 1TR.

Perlindungan Integritas Sistem (sip3)

- *Jenis:* Boolean
- *Lingkungan yang dapat berubah:* 1TR
- *Deskripsi:* Jika `sip3` ada dan benar, iBoot tidak akan memberlakukan daftar izin internalnya untuk variabel NVRAM boot-args, yang sebaliknya akan memfilter pilihan yang diteruskan ke kernel. Pengguna dapat mengubah bidang ini menggunakan `csrutil` atau `bputil` dari 1TR.

Sertifikat dan RemotePolicy

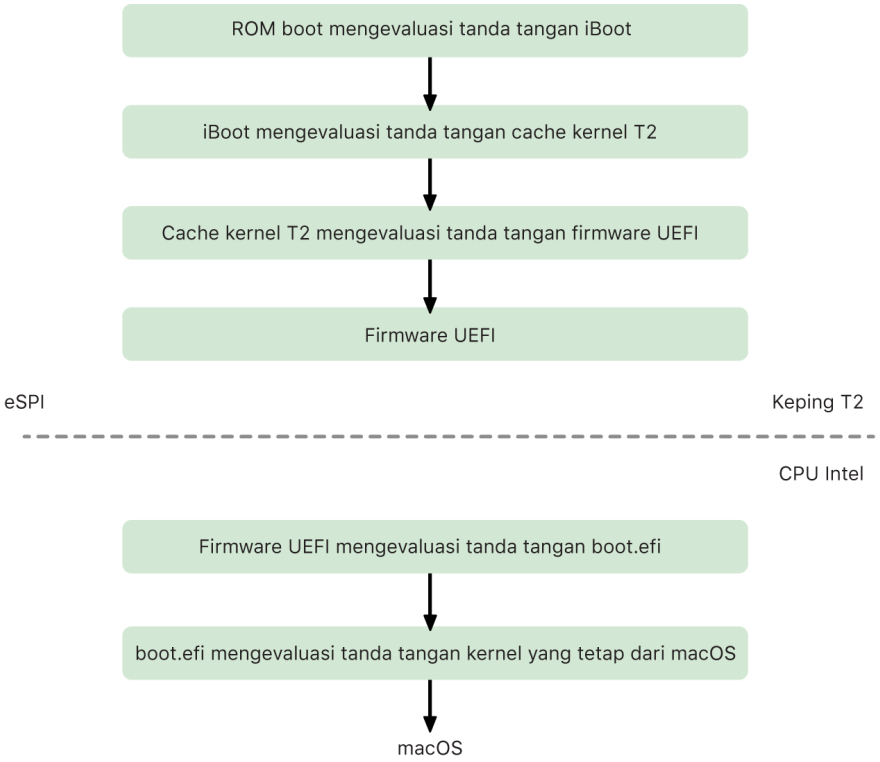
Seperti yang dijelaskan di Pembuatan dan manajemen kunci penandatanganan LocalPolicy, Image4 LocalPolicy juga berisi Sertifikat Identitas Pemilik (OIC) dan RemotePolicy yang disematkan.

Komputer Mac berbasis Intel

Proses boot untuk Mac berbasis Intel

Mac berbasis Intel dengan Keping Keamanan T2 Apple

Saat komputer Mac berbasis Intel dengan Keping Keamanan T2 Apple dinyalakan, keping melakukan boot aman dari ROM Boot-nya dengan cara yang sama seperti di iPhone, iPad, dan Mac dengan Apple silicon. Ini memverifikasi bootloader iBoot dan merupakan langkah pertama dalam rantai kepercayaan, iBoot memeriksa kode kernel dan ekstensi kernel pada keping T2, yang kemudian memeriksa firmware UEFI Intel. Firmware UEFI dan tanda tangan terkait awalnya hanya tersedia bagi keping T2.



Setelah verifikasi, image firmware UEFI dipetakan ke bagian memori keping T2. Memori ini dibuat tersedia bagi CPU Intel melalui Antarmuka Periferal Serial yang ditingkatkan (eSPI). Saat melakukan boot untuk pertama kalinya, CPU Intel mengambil firmware UEFI melalui eSPI dari salinan firmware yang telah diperiksa integritasnya dan dipetakan ke memori, yang terdapat di keping T2.

Evaluasi rantai kepercayaan dilanjutkan di CPU Intel, dengan firmware UEFI yang mengevaluasi tanda tangan untuk boot.efi, yang merupakan bootloader macOS. Tanda tangan boot aman macOS yang terdapat pada prosesor Intel disimpan dalam format Image4 yang sama dengan yang digunakan di iOS, iPadOS, dan boot aman keping T2, dan kode yang mengurai file Image4 merupakan kode diperkuat yang sama dari penerapan boot aman iOS dan iPadOS saat ini. Boot.efi pada gilirannya memverifikasi tanda tangan file baru, yang bernama immutablekernel. Jika boot aman diaktifkan, file immutablekernel merepresentasikan kumpulan lengkap ekstensi kernel Apple yang diperlukan untuk booting macOS. Kebijakan boot aman dihentikan pada saat diserahkan ke immutablekernel, lalu kebijakan keamanan macOS (seperti Perlindungan Integritas Sistem dan ekstensi kernel yang ditandatangani) akan diterapkan.

Jika terjadi kesalahan atau kegagalan dalam proses ini, Mac akan masuk ke dalam mode Pemulihan, mode Pemulihan Keping Keamanan T2 Apple, atau mode Peningkatan Firmware Perangkat (DFU) Keping Keamanan T2 Apple.

Microsoft Windows di Mac berbasis Intel dengan keping T2

Secara default, Mac berbasis Intel yang mendukung boot aman hanya memercayai konten yang ditandatangani oleh Apple. Namun, untuk meningkatkan keamanan penginstalan Boot Camp, Apple juga mendukung boot aman untuk Windows. Firmware Antarmuka Firmware Terpadu yang Dapat Diperluas (UEFi) menyertakan salinan sertifikat Microsoft Windows Production CA 2011 yang digunakan untuk mengesahkan bootloader Microsoft.

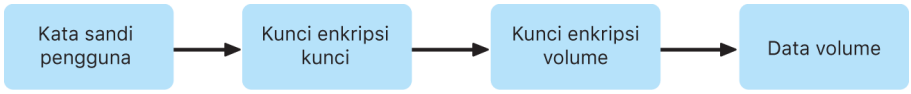
Catatan: Pada saat ini tidak ada kepercayaan yang disediakan untuk Microsoft Corporation UEFI CA 2011, yang akan mengizinkan verifikasi kode yang ditandatangani oleh mitra Microsoft. CA UEFI ini biasa digunakan untuk memverifikasi keabsahan bootloader untuk sistem operasi lainnya, seperti varian Linux.

Dukungan untuk boot aman Windows tidak diaktifkan secara default. Sebagai gantinya, dukungan tersebut diaktifkan menggunakan Asisten Boot Camp (BCA). Saat pengguna menjalankan BCA, macOS dikonfigurasi ulang untuk memercayai kode yang ditandatangani pihak pertama Microsoft selama boot. Setelah BCA selesai, jika macOS gagal dalam evaluasi kepercayaan pihak pertama Apple selama boot aman, firmware UEFI akan mencoba untuk mengevaluasi kepercayaan objek menurut format boot aman UEFI. Jika evaluasi kepercayaan berhasil, Mac akan melanjutkan dan melakukan boot Windows. Jika tidak, Mac memasuki recoveryOS dan pengguna akan diberi tahu mengenai kegagalan evaluasi kepercayaan.

Komputer Mac berbasis Intel tanpa keping T2

Mac berbasis Intel tanpa keping T2 tidak mendukung boot aman. Oleh karena itu, firmware Antarmuka Firmware Terpadu yang Dapat Diperluas (UEFi) memuat booter macOS (boot.efi) dari sistem file tanpa verifikasi, dan booter memuat kernel (prelinkedkernel) dari sistem file tanpa verifikasi. Untuk melindungi integritas rantai kunci, pengguna harus mengaktifkan mekanisme keamanan berikut:

- *Perlindungan Integritas Sistem (SIP):* Diaktifkan secara default, ini melindungi booter dan kernel dari penulisan berbahaya dari dalam macOS yang sedang dijalankan.
- *FileVault:* Ini dapat diaktifkan dengan dua cara: oleh pengguna atau oleh administrator mobile device management (MDM). Ini melindungi dari penyerang yang memiliki akses langsung secara fisik menggunakan Mode Disk Target untuk menimpa booter.
- *Kata Sandi Firmware:* Ini dapat diaktifkan dengan dua cara: oleh pengguna atau oleh administrator MDM. Ini membantu menghalangi penyerang yang memiliki akses langsung secara fisik yang meluncurkan mode boot alternatif seperti recoveryOS, Mode Satu Pengguna, atau Mode Disk Target, tempat booter dapat ditimpa. Ini juga membantu mencegah booting dari media alternatif, yang dapat digunakan oleh penyerang untuk menjalankan kode untuk menimpa booter.



Mode boot Mac berbasis Intel dengan Keping Keamanan T2 Apple

Mac berbasis Intel dengan Keping Keamanan T2 Apple memiliki berbagai mode boot yang dapat diaktifkan pada saat booting dengan menekan kombinasi tombol, yang dikenali oleh firmware atau booter UEFI. Beberapa mode boot, seperti Mode Pengguna Tunggal, tidak akan berfungsi kecuali kebijakan keamanan diubah ke Tidak Ada Keamanan di Utilitas Keamanan Mulai.

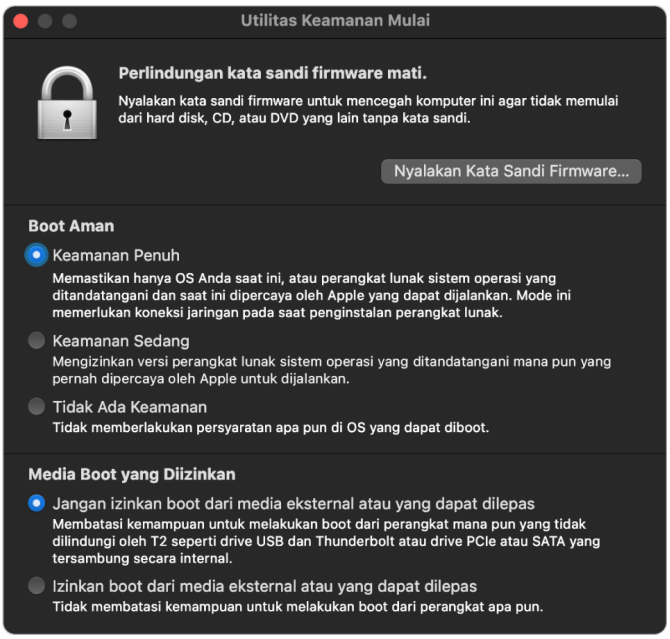
Mode	Kombinasi tombol	Deskripsi
Boot macOS	Tidak Ada	Firmware UEFI menyerahkan ke booter macOS (aplikasi UEFI), yang menyerahkan ke kernel macOS. Dalam proses booting standar Mac dengan FileVault yang diaktifkan, booter macOS memunculkan antarmuka Jendela Masuk, yang mengambil kata sandi untuk mendekripsi penyimpanan.
Manajer Mulai	Option (⌥)	Firmware UEFI meluncurkan aplikasi UEFI internal yang menghadirkan antarmuka pemilihan perangkat boot kepada pengguna.
Mode Disk Target (TDM)	T	Firmware UEFI meluncurkan aplikasi UEFI internal yang mengekspos perangkat penyimpanan internal sebagai perangkat penyimpanan mentah berbasis blok melalui FireWire, Thunderbolt, USB, atau gabungan ketiganya (tergantung model Mac-nya).
Mode Satu Pengguna	Command (⌘)-S	Kernel macOS meneruskan bendera –s di vektor argumen launchd, yang kemudian membuat shell satu pengguna di tty app Konsol. *Catatan:* Jika pengguna keluar dari shell, macOS melanjutkan boot ke Jendela Masuk.

Mode	Kombinasi tombol	Deskripsi
recoveryOS	Command (⌘)-R	Firmware UEFI memuat macOS minimum dari file image disk (.dmg) yang ditandatangani di perangkat penyimpanan internal.
recoveryOS Internet	Option (⌥)-Command (⌘)-R	Image disk yang ditandatangani diunduh dari internet menggunakan HTTP.
Diagnostik	D	Firmware UEFI memuat lingkungan diagnostik UEFI minimum dari file image disk yang ditandatangani di perangkat penyimpanan internal.
Diagnostik Internet	Option (⌥)-D	Image disk yang ditandatangani diunduh dari internet menggunakan HTTP.
Boot Windows	Tidak Ada	Jika Windows telah diinstal menggunakan Boot Camp, firmware UEFI meneruskan ke booter Windows, yang meneruskan ke kernel Windows.

Utilitas Keamanan Mulai di Mac dengan Keping Keamanan T2 Apple

Tinjauan

Di Mac berbasis Intel dengan Keping Keamanan T2 Apple, Utilitas Keamanan Mulai menangani sejumlah pengaturan kebijakan keamanan. Utilitas dapat diakses dengan melakukan boot ke recoveryOS dan memilih Utilitas Keamanan Mulai dari menu Utilitas serta melindungi pengaturan keamanan yang didukung dari manipulasi mudah oleh penyerang.



Perubahan kebijakan penting memerlukan pengesahan, bahkan dalam mode Pemulihan. Jika dibuka untuk pertama kalinya, Utilitas Keamanan Mulai akan meminta pengguna untuk memasukkan kata sandi administrator dari penginstalan macOS utama yang terkait dengan recoveryOS yang sedang di-boot. Jika tidak ada, administrator harus dibuat sebelum kebijakan dapat diubah. Keping T2 mengharuskan agar komputer Mac yang sedang diboot ke recoveryOS dan pengesahan dengan info pengesahan yang didukung Secure Enclave telah berlangsung sebelum perubahan kebijakan dapat dilakukan. Perubahan kebijakan keamanan memiliki dua persyaratan implisit. recoveryOS harus:

- Diboot dari perangkat penyimpanan dan secara langsung terhubung ke keping T2 karena partisi atau perangkat lainnya tidak memiliki info pengesahan yang didukung Secure Enclave yang terikat pada perangkat penyimpanan internal.
- Berada di volume berbasis APFS karena hanya terdapat dukungan untuk menyimpan Pengesahan dalam info pengesahan Pemulihan yang dikirimkan Secure Enclave di volume APFS “Praboot” drive. Volume berformat HFS plus tidak dapat menggunakan boot aman.

Kebijakan ini hanya ditampilkan di Utilitas Keamanan Mulai di Mac berbasis Intel dengan keping T2. Meskipun sebagian besar kasus penggunaan tidak memerlukan perubahan terhadap kebijakan boot aman, pengguna utamanya memiliki kontrol atas pengaturan perangkat mereka dan dapat memilih tergantung kebutuhannya, untuk menonaktifkan atau menurunkan fungsionalitas boot aman di Mac.

Perubahan kebijakan boot aman yang dilakukan dari dalam app ini hanya berlaku untuk evaluasi rantai kepercayaan yang sedang diverifikasi di prosesor Intel. Pilihan “Keping T2 boot aman” selalu berlaku.

Kebijakan boot aman dapat dikonfigurasi ke salah satu dari tiga pengaturan ini: Keamanan Penuh, Keamanan Sedang, dan Tidak Ada Keamanan. Tidak Ada Keamanan yang sepenuhnya menonaktifkan evaluasi boot aman di prosesor Intel dan memungkinkan pengguna untuk melakukan boot apa pun yang mereka inginkan.

Kebijakan boot Keamanan Penuh

Keamanan Penuh adalah kebijakan boot default, dan berperilaku mirip dengan iOS serta iPadOS atau Keamanan Penuh di Mac dengan Apple silicon. Pada saat perangkat lunak diunduh dan disiapkan untuk penginstalan, perangkat lunak disesuaikan dengan tanda tangan yang menyertakan Identifikasi Keping Eksklusif (ECID)—ID unik yang dikhususkan bagi keping T2 dalam kasus ini—sebagai bagian dari permintaan penandatanganan. Tanda tangan yang dikembalikan oleh server penandatanganan akan menjadi unik dan dapat digunakan hanya oleh keping T2 tersebut. Firmware Antarmuka Firmware Terpadu yang Dapat Diperluas (UEFi) dirancang untuk memastikan bahwa tanda tangan yang diberikan tidak hanya ditandatangani oleh Apple tapi juga spesifik untuk Mac, khususnya mengikat versi macOS tersebut ke Mac tersebut. Ini membantu mencegah serangan pembalikan versi seperti yang dijelaskan untuk Keamanan Penuh di Mac dengan Apple silicon.

Kebijakan boot Keamanan Sedang

Kebijakan boot Keamanan Sedang dapat dikatakan sama dengan boot aman UEFI tradisional, vendor (dalam kasus ini, Apple) membuat tanda tangan digital untuk kode agar dapat menegaskan bahwa kode tersebut berasal dari vendor. Dengan cara ini, penyerang terhalangi untuk memasukkan kode yang tidak ditandatangani. Kami menyebut tanda tangan ini sebagai tanda tangan "global" karena tanda tangan tersebut dapat digunakan di Mac mana pun, selama jangka waktu yang tidak terbatas, untuk Mac yang saat ini memiliki kumpulan kebijakan Keamanan Sedang. iOS, iPadOS, atau keping T2 tidak mendukung tanda tangan global. Pengaturan ini tidak berupaya untuk mencegah serangan pembalikan versi.

Kebijakan boot media

Kebijakan boot media hanya ada di Mac berbasis Intel dengan keping T2 dan tidak bergantung pada kebijakan boot aman. Sehingga meskipun pengguna menonaktifkan boot aman, ini tidak mengubah perilaku default pencegahan apa pun kecuali perangkat penyimpanan yang terhubung secara langsung ke keping T2 untuk melakukan boot Mac. (Kebijakan boot media tidak diperlukan di Mac dengan Apple silicon. Untuk Informasi lainnya, lihat Kontrol kebijakan keamanan Disk Mulai.)

Perlindungan kata sandi firmware di Mac berbasis Intel

macOS di komputer Mac berbasis Intel dengan Keping Keamanan T2 Apple mendukung penggunaan Kata Sandi Firmware untuk membantu mencegah modifikasi pengaturan firmware yang tidak disengaja di Mac tertentu. Kata Sandi Firmware dirancang untuk mencegah pemilihan mode boot alternatif seperti boot ke recoveryOS atau Mode Pengguna Tunggal, boot dari volume yang tidak disahkan, atau boot ke Mode Disk Target.

Catatan: Kata sandi firmware tidak diperlukan di Mac dengan Apple silicon, karena fungsi firmware penting yang dibatasi telah dipindahkan ke recoveryOS dan (saat FileVault diaktifkan) recoveryOS memerlukan pengesahan pengguna sebelum fungsi pentingnya dapat dijangkau.

Mode paling mendasar dari kata sandi firmware dapat dicapai dari Utilitas Kata Sandi Firmware recoveryOS di Mac berbasis Intel *tanpa* keping T2, dan dari Utilitas Keamanan Mulai di Mac berbasis Intel *dengan* keping T2. Pilihan lanjutan (seperti kemampuan untuk meminta kata sandi di setiap boot) tersedia dari alat baris perintah `firmwarepasswd` di macOS.

Pengaturan Kata Sandi Firmware secara khusus penting untuk mengurangi risiko serangan di komputer Mac berbasis Intel tanpa keping T2 dari penyerang yang memiliki akses langsung secara fisik. Kata Sandi Firmware dapat membantu mencegah penyerang untuk melakukan booting ke recoveryOS, tempat mereka dapat menonaktifkan Perlindungan Integritas Sistem (SIP). Dan dengan membatasi booting dari media alternatif, penyerang tidak dapat mengeksekusi kode yang memiliki hak dari sistem operasi lain agar dapat menyerang firmware periferal.

Mekanisme pengaturan ulang kata sandi firmware ada untuk membantu pengguna yang lupa kata sandinya. Pengguna menekan kombinasi tombol saat mulai dan diberikan string khusus model untuk disediakan ke AppleCare. AppleCare menandatangani secara digital sumber yang diperiksa tanda tangannya oleh Pengenal Sumber Seragam (URI). Jika tanda tangan disahkan dan kontennya dikhususkan bagi suatu Mac, firmware UEFI menghapus kata sandi firmware.

Untuk pengguna yang tidak ingin orang lain menghapus kata sandi firmware melalui metode perangkat lunak, pilihan `–disable–reset–capability` telah ditambahkan ke alat baris perintah `firmwarepasswd` di macOS 10.15. Sebelum mengatur pilihan ini, pengguna diharuskan untuk memahami bahwa jika kata sandi terlupakan dan harus dihapus, pengguna bertanggung jawab untuk membayar biaya penggantian logic board yang diperlukan untuk menjalankan ini. Organisasi yang ingin melindungi komputer Mac mereka dari penyerang eksternal dan dari pegawai harus mengatur kata sandi firmware di sistem yang dimiliki oleh organisasi. Ini dapat dilakukan di perangkat pada salah satu cara berikut:

- Pada waktu penyediaan, secara manual menggunakan alat baris perintah `firmwarepasswd`
- Dengan alat manajemen pihak ketiga yang menggunakan alat baris perintah `firmwarepasswd`
- Menggunakan mobile device management (MDM)

Lingkungan recoveryOS dan diagnostik untuk Mac berbasis Intel

recoveryOS

recoveryOS sepenuhnya terpisah dari macOS utama, dan seluruh kontennya disimpan di file image disk bernama BaseSystem.dmg. Terdapat juga BaseSystem.chunklist terkait, yang digunakan untuk memverifikasi integritas BaseSystem.dmg. Chunklist merupakan rangkaian hash untuk potongan BaseSystem.dmg sebesar 10 MB. Firmware Antarmuka Firmware Terpadu yang Dapat Diperluas (UEFi) mengevaluasi tanda tangan file chunklist, lalu mengevaluasi hash satu potongan, satu per satu, dari BaseSystem.dmg. Ini membantu memastikan bahwa hash cocok dengan konten bertanda tangan di chunklist. Jika terdapat hash yang tidak cocok, boot dari recoveryOS lokal akan dibatalkan dan firmware UEFI akan mencoba untuk booting dari recoveryOS Internet sebagai gantinya.

Jika verifikasi berhasil diselesaikan, firmware UEFI akan memasang BaseSystem.dmg sebagai disk RAM dan meluncurkan boot.efi yang terdapat di dalamnya. Firmware UEFI tidak perlu melakukan pemeriksaan spesifik terhadap boot.efi dan boot.efi pun tidak perlu memeriksa kernel karena seluruh konten dari sistem operasi (bagian yang utuh dari elemen ini) telah diperiksa integritasnya.

Diagnostik Apple

Sebagian besar prosedur untuk booting lingkungan diagnostik lokal sama dengan peluncuran recoveryOS. File AppleDiagnostics.dmg dan AppleDiagnostics.chunklist yang terpisah akan digunakan, tapi diverifikasi dengan cara yang sama dengan file BaseSystem. Alih-alih meluncurkan boot.efi, firmware UEFI meluncurkan file di dalam image disk (file .dmg) bernama diags.efi, yang berfungsi untuk mengaktifkan berbagai driver UEFI lainnya yang dapat berinteraksi dengan dan memeriksa kesalahan di perangkat keras.

recoveryOS internet dan lingkungan diagnostik

Jika terjadi kesalahan pada peluncuran lingkungan pemulihan atau diagnostik lokal, firmware UEFI mencoba untuk mengunduh image dari internet sebagai gantinya. (Pengguna juga dapat meminta image secara spesifik untuk diambil dari internet menggunakan rangkaian kunci spesial yang disimpan pada saat boot.) Validasi integritas image disk dan chunklist yang diunduh dari Server Pemulihan OS dijalankan dengan cara yang sama dengan image yang diambil dari perangkat penyimpanan.

Meskipun koneksi ke Server Pemulihan OS menggunakan HTTP, konten utuh yang telah diunduh akan tetap diperiksa integritasnya sebagaimana yang dijelaskan sebelumnya, dan dengan demikian terlindungi dari manipulasi oleh penyerang yang memiliki kontrol atas jaringan. Jika verifikasi integritas potongan individual gagal, potongan tersebut akan diminta ulang dari Server Pemulihan OS sebanyak 11 kali, sebelum berhenti mengupayakan dan menampilkan kesalahan.

Saat mode pemulihan internet dan diagnostik ditambahkan ke komputer Mac pada tahun 2011, kami memutuskan bahwa lebih baik untuk menggunakan transpor HTTP yang lebih sederhana, dan menangani pengesahan konten menggunakan mekanisme chunklist, alih-alih mengimplementasikan fungsionalitas HTTPS yang lebih rumit di firmware UEFI, dan akibatnya meningkatkan permukaan serangan firmware.

Keamanan volume sistem yang ditandatangani di iOS, iPadOS, dan macOS

Di macOS 10.15, Apple memperkenalkan volume sistem hanya baca, volume terdedikasi dan terisolasi untuk konten sistem. macOS 11 atau lebih baru menambahkan perlindungan kriptografi kuat ke konten sistem dengan *volume sistem yang ditandatangani (SSV)*. SSV menyediakan mekanisme kernel yang memverifikasi integritas konten sistem pada runtime dan menolak data apa pun—kode dan non-kode—tanpa tanda tangan kriptografi yang valid dari Apple. Dimulai di iOS 15 dan iPadOS 15, volume sistem di perangkat iOS dan iPadOS juga mendapatkan perlindungan kriptografi pada volume sistem yang ditandatangani.

Tidak hanya membantu mencegah perusakan perangkat lunak Apple apa pun yang merupakan bagian dari sistem operasi, SSV juga membuat pembaruan perangkat lunak macOS menjadi lebih andal dan aman. Selain itu, karena SSV menggunakan snapshot Apple File System (APFS), jika pembaruan tidak dapat dilakukan, versi sistem lama dapat dipulihkan tanpa penginstalan ulang.

Sejak diperkenalkan, APFS telah menyediakan integritas metadata sistem file menggunakan ceksum non-kriptografi di perangkat penyimpanan internal. SSV memperkuat mekanisme integritas dengan menambahkan hash kriptografis, sehingga memperluas mekanisme untuk mencakup semua bita data file. Data dari perangkat penyimpanan internal (termasuk metadata sistem file) di-hash secara kriptografi di jalur baca, dan hash lalu dibandingkan dengan nilai yang diharapkan di metadata sistem file. Saat terjadi ketidaksesuaian, sistem menganggap data telah dirusak dan tidak akan mengembalikannya ke perangkat lunak yang meminta.

Setiap hash SHA256 SSV disimpan di hierarki metadata sistem file utama, yang di-hash sendiri. Selain itu, karena setiap node hierarki secara rekursif memverifikasi integritas hash turunannya—mirip dengan hierarki hash biner (Merkle)—maka nilai hash node dasar, disebut *segel*, mencakup semua bita data di SSV, yang berarti tanda tangan kriptografis meliputi seluruh volume sistem.

Selama penginstalan dan pembaruan macOS, segel dikomputasi ulang dari sistem file di perangkat dan pengukuran tersebut diverifikasi dengan pengukuran yang ditandatangani oleh Apple. Di Mac dengan Apple silicon, bootloader memverifikasi segel sebelum mentransfer kontrol ke kernel. Di Mac berbasis Intel dengan Keping Keamanan T2 Apple, bootloader meneruskan pengukuran dan tanda tangan ke kernel, yang nantinya memverifikasi segel secara langsung sebelum memasang sistem file root. Di kedua kasus, jika verifikasi gagal, proses mulai akan dihentikan, dan pengguna akan diminta untuk menginstal ulang macOS. Prosedur ini diulang pada setiap boot kecuali pengguna telah memilih untuk memasuki mode keamanan yang lebih rendah dan telah memilih secara terpisah untuk menonaktifkan volume sistem yang ditandatangani.

Selama pembaruan perangkat lunak iOS dan iPadOS, volume sistem disiapkan dan dikomputasi ulang dengan cara yang sama. Bootloader iOS dan iPadOS memverifikasi bahwa segel aman dan cocok dengan nilai yang ditandatangani oleh Apple sebelum mengizinkan perangkat untuk memulai kernel. Ketidakcocokan saat boot akan meminta pengguna untuk memperbarui perangkat lunak sistem di perangkat. Pengguna tidak diizinkan untuk menonaktifkan perlindungan volume sistem yang ditandatangani di iOS dan iPadOS.

SSV dan penandatanganan kode

Penandatanganan kode masih ada dan diberlakukan oleh kernel. Volume sistem yang ditandatangani menyediakan perlindungan saat bita mana pun dibaca dari perangkat penyimpanan internal. Sebaliknya, penandatanganan kode menyediakan perlindungan saat objek Mach dipetakan secara memori sebagai dapat dieksekusi. SSV dan penandatanganan kode melindungi kode yang dapat dieksekusi di semua jalur baca dan eksekusi.

SSV dan FileVault

Di macOS 11, perlindungan saat penyimpanan yang sama untuk konten sistem disediakan oleh SSV, oleh karena itu volume sistem tidak perlu dienkripsi lagi. Modifikasi apa pun yang dibuat ke sistem file saat penyimpanan akan terdeteksi oleh sistem file saat dibaca. Jika pengguna telah mengaktifkan FileVault, konten pengguna di volume data masih dienkripsi dengan rahasia yang disediakan oleh pengguna.

Jika pengguna memilih untuk menonaktifkan SSV, sistem yang disimpan menjadi rentan terhadap perusakan, dan perusakan ini dapat memungkinkan penyerang untuk mengekstrak data pengguna yang dienkripsi saat berikutnya sistem dimulai. Oleh karena itu, sistem tidak akan mengizinkan pengguna untuk menonaktifkan SSV jika FileVault diaktifkan. Perlindungan saat penyimpanan harus diaktifkan atau dinonaktifkan untuk kedua volume dalam cara yang konsisten.

Di macOS 10.15 atau lebih lama, FileVault melindungi perangkat lunak sistem operasi saat penyimpanan dengan mengenkripsi pengguna dan konten sistem dengan kunci yang dilindungi oleh rahasia yang disediakan oleh pengguna. Hal ini melindungi dari penyerang dengan akses secara fisik ke perangkat agar tidak mengakses atau secara efektif memodifikasi sistem file yang berisi perangkat lunak sistem.

SSV dan Mac dengan Keping Keamanan T2 Apple

Di Mac dengan keping Keamanan T2 Apple, hanya macOS yang dilindungi oleh SSV. Perangkat lunak yang dijalankan di keping T2 dan memverifikasi macOS dilindungi oleh boot aman.

Pembaruan perangkat lunak aman

Keamanan adalah proses; tidak cukup untuk hanya mengandalkan boot versi sistem operasi yang terinstal di pabrik—harus terdapat mekanisme untuk memperoleh pembaruan keamanan terbaru dengan cepat dan aman. Apple secara berkala merilis pembaruan perangkat lunak untuk menyelesaikan masalah keamanan yang muncul. Pengguna perangkat iOS dan iPadOS menerima pemberitahuan pembaruan di perangkat. Pengguna Mac menemukan pembaruan yang tersedia di Preferensi Sistem. Pembaruan dikirimkan secara nirkabel, untuk pengadopsian perbaikan keamanan terbaru dengan cepat.

Proses pembaruan

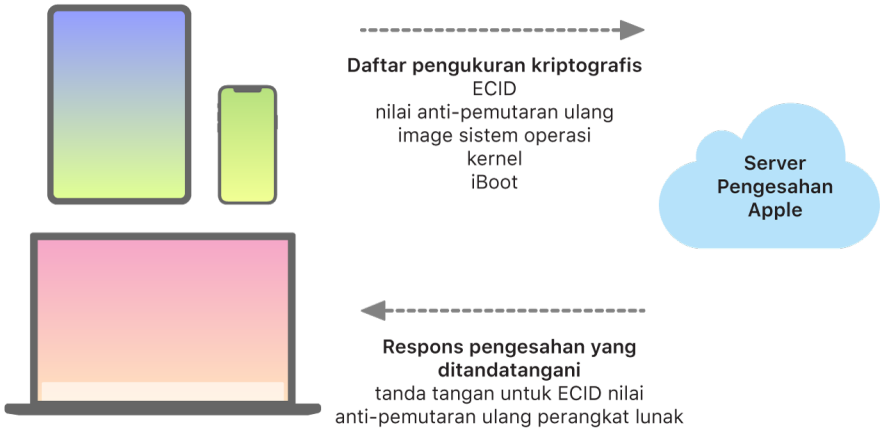
Proses pembaruan menggunakan dasar kepercayaan berbasis perangkat keras yang sama dengan yang digunakan oleh boot aman yang dirancang untuk hanya menginstal kode yang ditandatangani oleh Apple. Proses pembaruan juga menggunakan pengesahan perangkat lunak sistem untuk memeriksa bahwa hanya versi salinan perangkat lunak yang ditandatangani secara aktif oleh Apple yang dapat diinstal di perangkat iOS dan iPadOS, atau di komputer Mac dengan pengaturan Keamanan Penuh yang dikonfigurasi sebagai kebijakan boot aman di Utilitas Keamanan Mulai. Dengan proses aman ini, Apple dapat menghentikan penandatanganan versi sistem operasi lama yang memiliki kerentanan yang diketahui dan membantu mencegah serangan penurunan.

Demi keamanan pembaruan perangkat lunak yang lebih andal, jika perangkat yang akan ditingkatkan tersambung secara fisik ke Mac, salinan lengkap iOS atau iPadOS akan diunduh dan diinstal. Namun, untuk pembaruan perangkat lunak secara nirkabel (OTA), *hanya komponen yang diperlukan untuk menyelesaikan pembaruan yang diunduh,* yang meningkatkan efisiensi jaringan dengan tidak mengunduh keseluruhan sistem operasi. Terlebih lagi, pembaruan perangkat lunak dapat disimpan dalam cache pada Mac yang menjalankan macOS 10.13 atau lebih baru dengan Cache Konten yang dinyalakan, sehingga perangkat iOS dan iPadOS tidak perlu mengunduh ulang pembaruan yang diperlukan melalui internet. (Perangkat masih perlu menghubungi server Apple untuk menyelesaikan proses pembaruan.)

Proses pembaruan yang disesuaikan

Selama peningkatan dan pembaruan, koneksi dibuat ke server pengesahan penginstalan Apple, yang menyertakan daftar pengamanan kriptografis untuk setiap bagian bundel penginstalan yang akan diinstal (misalnya, iBoot, kernel, dan image sistem operasi), nilai anti-pemutaran ulang acak (nonce), dan Identifikasi Keping Eksklusif (ECID) unik milik perangkat.

Server pengesahan membandingkan daftar tindakan pengamanan yang disediakan dengan versi yang diizinkan untuk penginstalan dan, jika menemukan kecocokan, akan menambahkan ECID ke tindakan pengamanan dan menandatangani hasilnya. Server meneruskan kumpulan lengkap data yang ditandatangani ke perangkat sebagai bagian dari proses peningkatan. Dengan menambahkan ECID, pengesahan untuk perangkat yang diminta menjadi bersifat "khusus". Dengan hanya mengesahkan dan menandatangani tindakan pengamanan yang diketahui, server membantu memastikan bahwa pembaruan dilakukan sebagaimana mestinya seperti disediakan oleh Apple.



Evaluasi rantai kepercayaan waktu boot memverifikasi bahwa tanda tangan berasal dari Apple dan bahwa pengukuran item dimuat dari perangkat penyimpanan, bersama dengan ECID perangkat, cocok dengan yang tercakup oleh tanda tangan. Langkah ini dirancang untuk memastikan bahwa, di perangkat yang mendukung personalisasi, pengesahan ditujukan bagi perangkat tertentu dan bahwa sistem operasi atau versi firmware yang lebih lama dari perangkat tidak dapat disalin ke perangkat lain. Nonce membantu mencegah penyerang untuk menyimpan respons server dan menggunakannya untuk merusak perangkat atau mengubah perangkat lunak sistem.

Proses penyesuaian adalah alasan koneksi jaringan ke Apple selalu diperlukan untuk memperbarui perangkat apa pun dengan silicon rancangan Apple, termasuk Mac berbasis Intel dengan Keping Keamanan T2 Apple.

Terakhir, volume data pengguna tidak pernah dipasang selama pembaruan perangkat lunak, untuk membantu mencegah apa pun dibaca atau ditulis ke volume tersebut selama pembaruan.

Di perangkat dengan Secure Enclave, perangkat keras tersebut juga menggunakan pengesahan perangkat lunak sistem untuk memeriksa integritas perangkat lunaknya dan dirancang untuk mencegah penginstalan penurunan versi.

Integritas sistem operasi

Apple merancang sistem operasinya dengan keamanan di dalamnya. Rancangan ini disertai dengan dasar kepercayaan perangkat keras—untuk memungkinkan boot aman—serta proses pembaruan perangkat lunak aman yang cepat dan aman. Sistem operasi Apple juga menggunakan kemampuan perangkat keras berbasis silicon dengan fungsi khususnya untuk membantu mencegah eksploitasi saat sistem berjalan. Fitur runtime ini melindungi integritas kode tepercaya saat sedang dieksekusi. Dengan kata lain, perangkat lunak sistem operasi Apple membantu memitigasi serangan dan teknik eksploitasi yang berasal dari app berbahaya, web, atau melalui saluran lainnya. Perlindungan yang tercantum di sini tersedia di perangkat dengan SoC rancangan Apple yang didukung, termasuk iOS, iPadOS, tvOS, watchOS, dan kini macOS di Mac dengan Apple silicon.

Fitur	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Kelompok M1
Perlindungan Integritas Kernel	✓	✓	✓	✓	✓	✓
Pembatasan Izin Cepat		✓	✓	✓	✓	✓
Perlindungan Integritas Koprosesor Sistem			✓	✓	✓	✓
Kode Pengesahan Penunjuk			✓	✓	✓	✓
Lapisan Perlindungan Halaman		✓	✓	✓	✓	Lihat Catatan di bawah.

Catatan: Lapisan Perlindungan Halaman (PPL) mengharuskan platform untuk *hanya* mengeksekusi kode yang ditandatangani dan tepercaya; ini adalah model keamanan yang tidak berlaku bagi macOS.

Perlindungan Integritas Kernel

Setelah kernel sistem operasi menyelesaikan inisialisasi, Perlindungan Integritas Kernel (KIP) diaktifkan untuk membantu mencegah modifikasi kernel dan kode driver. Pengontrol memori menyediakan bidang memori fisik terlindungi yang digunakan iBoot untuk memutar kernel dan ekstensi kernel. Setelah proses mulai selesai, pengontrol memori akan menolak penulisan pada bidang memori fisik terlindungi. Unit Manajemen Memori (MMU) Prosesor Aplikasi dikonfigurasi untuk membantu mencegah pemetaan kode istimewa dari memori fisik di luar bidang memori terlindungi dan untuk membantu mencegah pemetaan yang dapat ditulisi terhadap memori fisik di dalam bidang memori kernel.

Untuk mencegah konfigurasi ulang, perangkat keras yang digunakan untuk mengaktifkan KIP akan dikunci setelah proses boot selesai.

Pembatasan Izin Cepat

Dimulai dari SoC A11 Bionic dan S3 Apple, primitif perangkat keras baru diperkenalkan. Primitif ini, Pembatasan Izin Cepat, menyertakan register CPU untuk membatasi izin dengan cepat per ulir. Dengan Pembatasan Izin Cepat (juga dikenal sebagai register APRR), sistem operasi yang didukung dapat menghapus izin eksekusi dengan cepat dari memori tanpa dibebankan dengan panggilan sistem dan proses walk atau flush tabel halaman. Register ini menyediakan satu level mitigasi tambahan untuk serangan dari web, khususnya untuk kode yang disusun saat runtime (disusun secara langsung)—karena memori tidak dapat dieksekusi dengan efektif saat sedang dibaca dan ditulisi.

Perlindungan Integritas Koprosesor Sistem

Firmware koprosesor menangani sebagian besar tugas sistem penting—misalnya, Secure Enclave, prosesor sensor gambar, dan koprosesor motion. Maka dari itu, keamanannya adalah bagian utama dari keamanan keseluruhan sistem. Untuk mencegah modifikasi firmware koprosesor, Apple menggunakan mekanisme yang disebut *Perlindungan Integritas Koprosesor Sistem (SCIP)*.

SCIP berfungsi seperti Perlindungan Integritas Kernel (KIP): Pada saat boot, iBoot memuat firmware setiap koprosesor ke bidang memori terlindungi, salah satunya yang disimpan dan dipisahkan dari bidang KIP. iBoot mengonfigurasi setiap unit memori koprosesor untuk membantu mencegah:

- Pemetaan yang dapat dieksekusi di luar bagian bidang memori terlindunginya
- Pemetaan yang dapat ditulisi di dalam bagian bidang memori terlindunginya

Pada saat boot, untuk mengonfigurasi SCIP Secure Enclave, sistem Operasi Secure Enclave digunakan. Setelah proses boot selesai, perangkat keras yang digunakan untuk mengaktifkan SCIP dikunci. Ini dirancang untuk mencegah konfigurasi ulang.

Kode Pengesahan Penunjuk

Kode Pengesahan Penunjuk (PAC) digunakan sebagai perlindungan terhadap eksploitasi bug kerusakan memori. Perangkat lunak sistem dan app internal menggunakan PAC untuk membantu mencegah modifikasi penunjuk fungsi dan alamat balik (penunjuk kode). PAC menggunakan lima nilai rahasia 128 bit untuk menandatangani instruksi dan data kernel, serta setiap proses ruang pengguna memiliki kunci B-nya sendiri. Item diberi salt dan ditandatangani sebagaimana yang ditunjukkan di bawah.

Item	Kunci	Salt
Alamat Balik Fungsi	IB	Alamat penyimpanan
Penunjuk Fungsi	IA	0
Fungsi Pengaktifan Blok	IA	Alamat penyimpanan
Cache Metode Objective-C	IB	Alamat penyimpanan + Kelas + Pemilih
Entri Tabel V C++	IA	Alamat penyimpanan + Hash (nama metode yang rusak)
Label Goto yang Dihitung	IA	Hash (nama fungsi)
Status Ulir Kernel	GA	•
Register Status Ulir Pengguna	IA	Alamat penyimpanan
Penunjuk Tabel V C++	DA	0

Nilai tanda tangan disimpan di bit penambalan yang tidak digunakan di bagian atas penunjuk 64 bit. Tanda tangan diverifikasi sebelum digunakan, dan penambalan dipulihkan untuk membantu memastikan bahwa alamat penunjuk berfungsi. Kegagalan verifikasi akan mengakibatkan pembatalan. Verifikasi ini meningkatkan kesulitan banyak serangan, seperti serangan pemrograman berorientasi balik (ROP), yang mencoba untuk menipu perangkat agar dengan berbahaya menjalankan kode yang ada dengan memanipulasi alamat balik fungsi yang tersimpan di tumpukan.

Lapisan Perlindungan Halaman

Lapisan Perlindungan Halaman (PPL) di iOS, iPadOS, dan watchOS dirancang untuk mencegah kode ruang pengguna agar tidak dimodifikasi setelah verifikasi tanda tangan kode selesai. Berdasarkan di Perlindungan Integritas Kernel dan Pembatasan Izin Cepat, PPL mengelola penimpaan izin tabel halaman untuk memastikan bahwa hanya PPL yang dapat mengubah halaman terlindungi yang berisi kode pengguna dan tabel halaman. Sistem menyediakan pengurangan permukaan serangan dalam jumlah besar dengan mendukung penguatan integritas kode di seluruh sistem, meskipun dengan kernel yang telah disusupi. Perlindungan ini tidak ditawarkan di macOS karena PPL hanya berlaku di sistem tempat semua kode yang dieksekusi harus ditandatangani.

Kemampuan keamanan sistem macOS tambahan

Kemampuan keamanan sistem macOS tambahan

macOS beroperasi dalam kumpulan perangkat keras yang lebih luas (misalnya, CPU berbasis Intel, CPU berbasis Intel yang digabungkan dengan Keping Keamanan T2 Apple, dan SoC berbasis Apple silicon) dan mendukung serangkaian kasus penggunaan komputasi untuk tujuan umum. Saat beberapa pengguna hanya menggunakan app dasar terinstal atau app yang tersedia dari App Store, pengguna lain adalah peretas kernel yang ingin menonaktifkan semua perlindungan platform penting sehingga mereka dapat menjalankan dan mengetes kodenya saat dieksekusi dengan level kepercayaan tertinggi. Sebagian besar berada di antaranya, dan banyak pengguna yang memiliki periferal serta perangkat lunak yang memerlukan level akses yang beragam. Apple merancang platform macOS dengan pendekatan terintegrasi terhadap perangkat keras, perangkat lunak, dan layanan—platform yang menyediakan keamanan secara default dan memudahkan konfigurasi, penerapan, dan pengelolaan tetapi mempertahankan konfigurabilitas yang diharapkan pengguna. macOS juga disertai dengan teknologi keamanan kunci yang diperlukan tenaga IT profesional untuk membantu melindungi data perusahaan dan melakukan integrasi di dalam lingkungan jaringan perusahaan yang aman.

Kemampuan berikut mendukung dan membantu mengamankan kebutuhan pengguna macOS yang beragam. Kemampuan termasuk:

- Keamanan volume sistem yang ditandatangani
- Perlindungan Integritas Sistem
- Cache kepercayaan
- Perlindungan untuk periferal
- Dukungan Rosetta 2 (penerjemahan otomatis) dan keamanan untuk Mac dengan Apple silicon
- Dukungan dan perlindungan DMA
- Dukungan dan keamanan ekstensi kernel (kext)
- Dukungan dan keamanan ROM Pilihan
- Keamanan firmware UEFI untuk komputer Mac berbasis Intel

Perlindungan Integritas Sistem

macOS menggunakan izin kernel untuk membatasi kemampuan menulis file sistem penting dengan fitur yang disebut *Perlindungan Integritas Sistem (SIP)*. Fitur ini terpisah dan merupakan tambahan dari Perlindungan Integritas Kernel (KIP) berbasis perangkat keras yang tersedia di Mac dengan Apple silicon, yang melindungi modifikasi kernel di memori. Teknologi kontrol akses wajib dimanfaatkan untuk menyediakan ini dan sejumlah perlindungan level kernel lainnya, termasuk sandbox dan Vault Data.

Kontrol akses wajib

macOS menggunakan kontrol akses wajib—kebijakan yang mengatur pembatasan keamanan yang dibuat oleh pengembang, yang tidak dapat ditimpa. Pendekatan ini berbeda dari kontrol akses diskresioner, yang mengizinkan pengguna untuk menimpa kebijakan keamanan menurut preferensi mereka.

Kontrol akses wajib tidak dapat dilihat oleh pengguna, tapi merupakan teknologi mendasar yang membantu memungkinkan beberapa fitur penting, termasuk sandbox, pengawasan orang tua, preferensi yang dikelola, ekstensi, dan Perlindungan Integritas Sistem.

Perlindungan Integritas Sistem

Perlindungan Integritas Sistem membatasi komponen ke hanya baca pada lokasi sistem file penting khusus untuk membantu mencegah kode berbahaya agar tidak memodifikasinya. Perlindungan Integritas Sistem adalah pengaturan khusus komputer yang menyala secara default saat pengguna meningkatkan ke OS X 10.11 atau lebih baru. Di Mac berbasis Intel, menonaktifkan fitur ini akan menghapus perlindungan untuk semua partisi di perangkat penyimpanan fisik. macOS menerapkan kebijakan keamanan ini ke setiap proses yang dijalankan di sistem, baik kebijakan dijalankan dalam sandbox maupun dengan hak administratif.

Cache kepercayaan

Salah satu objek yang disertakan di rantai Boot Aman adalah cache kepercayaan statis, catatan tepercaya semua biner Mach-O yang dikontrol ke volume sistem yang ditandatangani. Setiap Mach-O diwakili oleh hash direktori kode. Untuk pencarian yang efisien, hash ini diurutkan sebelum disisipkan ke cache kepercayaan. Direktori kode adalah hasil operasi penandatanganan yang dilakukan oleh `codesign(1)`. Untuk memberlakukan cache kepercayaan, SIP harus tetap diaktifkan. Untuk menonaktifkan pemberlakuan cache kepercayaan di Mac dengan Apple silicon, boot aman harus dikonfigurasi ke Keamanan Permisif.

Saat biner dieksekusi (baik sebagai bagian dari pemunculan proses baru atau pemetaan kode yang dapat dieksekusi ke proses yang ada), direktori kodenya diekstrak dan di-hash. Jika hash hasil ditemukan di cache kepercayaan, pemetaan yang dapat dieksekusi yang dibuat untuk biner akan diberi izin hak platform—yaitu, pemetaan dapat memiliki hak dan mengeksekusi tanpa verifikasi lebih lanjut untuk pengesahan tanda tangannya. Ini berbanding terbalik dengan Mac berbasis Intel, di mana hak platform diteruskan ke konten sistem operasi oleh sertifikat Apple yang menandatangani biner. (Sertifikat ini tidak membatasi hak apa yang dapat dimiliki oleh biner.)

Biner non-platform (misalnya, kode pihak ketiga yang disahkan) harus memiliki rantai sertifikat yang sah agar dapat mengeksekusi, dan hak yang mungkin dimiliki dibatasi oleh profil yang menandatangani yang diterbitkan ke pengembang oleh Apple Developer Program.

Semua biner yang dikirim dalam macOS ditandatangani dengan *pengenal platform*. Di Mac dengan Apple silicon, pengenal ini digunakan untuk menandakan bahwa meskipun biner ditandatangani oleh Apple, hash direktori kodenya harus ada di cache kepercayaan agar dapat dieksekusi. Di Mac berbasis Intel, pengenal platform digunakan untuk melakukan pencabutan biner yang ditargetkan dari perilisan macOS yang lebih lama; pencabutan yang ditargetkan ini membantu mencegah biner tersebut agar tidak dieksekusi di versi yang lebih baru.

Cache kepercayaan statis sepenuhnya mengunci kumpulan biner ke versi macOS yang diberikan. Perilaku ini membantu mencegah biner yang ditandatangani Apple dengan sah dari sistem operasi yang lebih lama agar tidak diperkenalkan ke sistem operasi yang lebih baru agar penyerang dapat memperoleh keuntungan.

Kode platform yang dikirim ke luar sistem operasi

Apple mengirimkan beberapa biner—misalnya, Xcode dan tumpukan alat pengembangan—yang tidak ditandatangani dengan pengenal platform. Meski begitu, biner masih diizinkan untuk dieksekusi dengan hak platform di Mac dengan Apple silicon dan Mac dengan keping T2. Karena perangkat lunak platform ini dikirim secara terpisah dari macOS, perangkat lunak tidak tunduk pada perilaku pencabutan yang diberlakukan oleh cache kepercayaan statis.

Cache kepercayaan yang dapat dimuat

Apple mengirimkan paket perangkat lunak tertentu dengan *cache kepercayaan yang dapat dimuat*. Cache ini memiliki struktur data yang sama dengan cache kepercayaan statis. Meskipun hanya terdapat satu cache kepercayaan statis—dan kontennya dijamin selalu terkunci ke cakupan hanya baca setelah inisialisasi awal kernel selesai—cache kepercayaan yang dapat dimuat ditambahkan ke sistem pada runtime.

Cache kepercayaan ini disahkan melalui mekanisme yang sama dengan yang mengesahkan firmware boot (penyesuaian menggunakan layanan penandatanganan tepercaya Apple) atau sebagai objek yang ditandatangani secara global (yang tanda tangannya tidak mengikat objek ke perangkat tertentu).

Contoh dari cache kepercayaan yang disesuaikan adalah cache yang dikirim dengan image disk yang digunakan untuk melakukan diagnostik bidang di Mac dengan Apple silicon. Cache kepercayaan ini disesuaikan, bersamaan dengan image disk, dan dimuat ke kernel komputer Mac subjek saat di-boot ke mode diagnostik. Cache kepercayaan memungkinkan perangkat lunak dalam image disk untuk dijalankan dengan hak platform.

Contoh dari cache kepercayaan yang ditandatangani secara global yang dikirim dengan pembaruan perangkat lunak macOS. Cache kepercayaan ini mengizinkan potongan kode dalam pembaruan perangkat lunak—*otak pembaruan*—untuk dijalankan dengan hak platform. Otak pembaruan melakukan pekerjaan apa pun untuk menyiapkan pembaruan perangkat lunak yang tidak dapat dilakukan sistem host dalam cara yang konsisten di semua versi.

Keamanan prosesor periferal di komputer Mac

Semua sistem komputasi modern memiliki banyak prosesor periferal internal yang didedikasikan untuk tugas seperti jaringan, grafik, manajemen daya, dan lainnya. Prosesor periferal ini umumnya memiliki satu fungsi dan jauh lebih lemah dari CPU utama. Periferal internal yang tidak menerapkan keamanan yang memadai menjadi target yang lebih mudah dieksploitasi oleh penyerang, sehingga sistem operasi dapat terus diserang. Dengan menginfeksi firmware prosesor periferal, penyerang dapat menargeti perangkat lunak di CPU utama atau secara langsung mengambil data sensitif (misalnya, perangkat Ethernet dapat melihat konten paket yang tidak terenkripsi).

Jika memungkinkan, Apple berupaya untuk mengurangi jumlah prosesor periferal yang diperlukan dan untuk menghindari desain yang memerlukan firmware. Namun jika proses terpisah dengan firmware-nya sendiri diperlukan, akan dilakukan upaya untuk membantu memastikan bahwa penyerang tidak dapat membobol prosesor tersebut. Ini dapat dilakukan dengan memverifikasi proses dalam salah satu cara:

- Menjalankan prosesor sehingga membuatnya mengunduh firmware terverifikasi dari CPU utama saat proses mulai
- Membuat prosesor periferal menerapkan rantai boot amannya sendiri, untuk memverifikasi firmware prosesor periferal setiap kali Mac dimulai

Apple bekerja sama dengan vendor untuk mengaudit penerapannya dan meningkatkan desain mereka agar menyertakan properti yang diinginkan seperti:

- Memastikan kekuatan kriptografis minimum
- Memastikan pembatalan yang andal atas firmware yang diketahui buruk
- Menonaktifkan antarmuka debug
- Menandatangani firmware dengan kunci kriptografi yang disimpan di modul keamanan perangkat keras yang dikontrol Apple (HSM)

Dalam beberapa tahun terakhir, Apple telah bekerja sama dengan beberapa vendor eksternal untuk mengadopsi struktur data “Image4”, kode verifikasi, dan infrastruktur penandatanganan yang sama dengan yang digunakan oleh Apple silicon.

Ketika operasi bebas penyimpanan atau penyimpanan plus boot aman bukan merupakan pilihan, desain mengharuskan pembaruan firmware untuk ditandatangani secara kriptografis dan diverifikasi sebelum penyimpanan tetap dapat diperbarui.

Rosetta 2 di Mac dengan Apple silicon

Mac dengan Apple silicon mampu menjalankan kode yang disusun untuk kumpulan instruksi x86_64 menggunakan mekanisme penerjemahan yang disebut *Rosetta 2*. Terdapat dua jenis penerjemahan yang ditawarkan: langsung dan di awal.

Penerjemahan langsung

Di pipeline penerjemahan langsung (JIT), objek Mach x86_64 teridentifikasi lebih awal di jalur eksekusi image. Saat image ini ditemui, kernel mentransfer kontrol ke bagian penerjemahan Rosetta khusus alih-alih ke editor tautan dinamis, `dyld(1)`. Bagian penerjemahan lalu menerjemahkan halaman x86_64 selama eksekusi image. Penerjemahan ini terjadi sepenuhnya di dalam proses. Kernel masih memverifikasi hash kode setiap halaman x86_64 terhadap tanda tangan kode yang dilampirkan ke biner saat halaman salah dimasukkan. Jika hash tidak cocok, kernel memberlakukan kebijakan pemulihan yang sesuai untuk proses tersebut.

Penerjemahan di awal

Pada jalur penerjemahan di awal (AOT), biner x86_64 dibaca dari penyimpanan saat sistem menganggap respons kode tersebut optimal. Artefak yang diterjemahkan ditulis ke penyimpanan sebagai jenis file objek Mach khusus. File tersebut serupa dengan image yang dapat dieksekusi, tapi ditandai untuk mengindikasikan bahwa artefak adalah produk terjemahan image lain.

Di model ini, artefak AOT menurunkan semua informasi identitasnya dari image yang dapat dieksekusi x86_64 asli. Untuk memberlakukan pengikatan ini, entitas userspace yang berhak menandatangani artefak terjemahan menggunakan kunci khusus perangkat yang dikelola oleh Secure Enclave. Kunci ini hanya dirilis ke entitas userspace yang berhak, yang teridentifikasi seperti menggunakan hak yang dibatasi. Direktori kode yang dibuat untuk artefak terjemahan menyertakan hash direktori kode image yang dapat dieksekusi x86_64 asli. Tanda tangan pada artefak terjemahan sendiri dikenal sebagai *tanda tangan tambahan*.

Pipeline AOT dimulai serupa dengan pipeline JIT, dengan kernel mentransfer kontrol ke runtime Rosetta alih-alih ke editor tautan dinamis, `dyld(1)`. Namun runtime Rosetta kemudian mengirimkan permintaan komunikasi antarproses (IPC) ke layanan sistem Rosetta, yang bertanya apakah ada terjemahan AOT yang tersedia untuk image yang dapat dieksekusi saat ini. Jika ditemukan, layanan Rosetta menyediakan pengendali ke terjemahan tersebut, dan dipetakan ke proses serta dieksekusi. Selama eksekusi, kernel memberlakukan hash direktori kode dari artefak terjemahan yang disahkan oleh tanda tangan yang berdasar di kunci penandatanganan khusus perangkat. Hash direktori kode image x86_64 asli tidak terlibat di proses ini.

Artefak terjemahan disimpan di Vault Data yang tidak dapat diakses saat runtime oleh entitas apa pun kecuali layanan Rosetta. Layanan Rosetta mengelola akses ke cache-nya dengan mendistribusikan deskriptor file hanya baca ke masing-masing artefak terjemahan; hal ini membatasi akses ke cache artefak AOT. Komunikasi antarproses layanan ini dan jejak dependen layanan ini sengaja disimpan dengan sangat sempit untuk membatasi permukaan serangannya.

Jika hash direktori kode image x86_64 asli tidak sesuai dengan hash yang dikodekan ke tanda tangan artefak terjemahan AOT, hasil ini akan dianggap serupa dengan tanda tangan kode yang tidak sah, dan tindakan pemberlakuan yang sesuai akan diambil.

Jika proses jarak jauh meminta kernel memberikan hak atau properti identitas kode lainnya milik file yang diterjemahkan oleh AOT, properti identitas image x86_64 asli akan dikembalikan ke proses.

Konten cache kepercayaan statis

macOS 11 mengirimkan biner "besar" Mach yang berisi potongan kode komputer x86_64 dan arm64. Di Mac dengan Apple silicon, pengguna dapat menentukan untuk mengeksekusi potongan x86_64 pada biner sistem melalui pipeline Rosetta—misalnya untuk memuat plug-in yang tidak memiliki varian arm64 asli. Untuk mendukung pendekatan ini, cache kepercayaan statis yang dikirimkan dengan macOS, umumnya, berisi tiga hash direktori kode per file objek Mach:

- Hash direktori kode potongan arm64
- Hash direktori kode potongan x86_64
- Hash direktori kode terjemahan AOT pada potongan x86_64

Prosedur penerjemahan AOT Rosetta bersifat telah ditentukan sebelumnya dan menghasilkan output serupa untuk input apa pun, terlepas dari kapan penerjemahan dilakukan atau di perangkat apa penerjemahan dilakukan.

Selama pembuatan macOS, semua file objek Mac dijalankan melalui pipeline penerjemahan AOT Rosetta yang terkait dengan versi macOS yang sedang dibuat, dan hasil dari hash direktori kode dicatat ke cache kepercayaan. Demi alasan efisiensi, produk terjemahan sebenarnya tidak dikirim dengan sistem operasi dan dikonstitusi ulang sesuai permintaan saat pengguna memintanya.

Saat image x86_64 sedang dieksekusi di Mac dengan Apple silicon, jika hash direktori kode image tersebut berada dalam cache kepercayaan statis, hash direktori kode artefak AOT yang dihasilkan *juga* diharapkan berada dalam cache kepercayaan statis. Produk seperti itu tidak ditandatangani oleh kunci khusus perangkat, karena otoritas penandatanganan berdasar di rantai boot aman Apple.

Kode x86_64 yang tidak ditandatangani

Mac dengan Apple silicon tidak mengizinkan kode arm64 asli untuk dieksekusi kecuali tanda tangan yang sah dilampirkan. Tanda tangan ini dapat sesederhana tanda tangan kode ad hoc (msl. `codesign(1)`) yang tidak memiliki identitas asli dari salah satu pasangan rahasia kunci asimetris (ini hanyalah pengukuran biner yang tidak disahkan).

Untuk kompatibilitas biner, kode x86_64 yang diterjemahkan diizinkan untuk dieksekusi melalui Rosetta tanpa informasi tanda tangan sama sekali. Tidak ada identitas khusus yang diteruskan ke kode ini melalui prosedur penandatanganan Secure Enclave khusus perangkat, dan identitas dieksekusi dengan batasan yang sama seperti mengeksekusi kode yang tidak ditandatangani di Mac berbasis Intel.

Perlindungan akses memori langsung untuk komputer Mac

Untuk mendapatkan hasil tinggi pada antarmuka berkecepatan tinggi PCIe, FireWire, Thunderbolt, dan USB, komputer harus mendukung akses memori langsung (DMA) dari periferal. Dengan kata lain, komputer harus dapat membaca dan menulisi RAM tanpa keterlibatan CPU secara terus-menerus. Sejak 2012, komputer Mac telah menerapkan berbagai teknologi untuk melindungi dari serangan DMA, sehingga menyediakan kumpulan perlindungan DMA yang terbaik dan paling lengkap di semua PC.

Perlindungan akses memori langsung untuk Mac dengan Apple silicon

Sistem pada keping Apple berisi Unit Manajemen Memori Input/Output (IOMMU) untuk setiap agen DMA di sistem, termasuk port PCIe dan Thunderbolt. Karena setiap IOMMU memiliki kumpulan tabel penerjemahan alamatnya sendiri untuk menerjemahkan permintaan DMA, periferal yang tersambung melalui PCIe atau Thunderbolt hanya dapat mengakses memori yang telah dipetakan secara eksplisit untuk penggunaannya. Periferal tidak dapat mengakses memori milik bagian lain pada sistem—seperti kernel atau firmware—memori yang ditetapkan ke periferal lain. Jika IOMMU mendeteksi percobaan oleh periferal untuk mengakses memori yang tidak dipetakan untuk penggunaan periferal tersebut, panik kernel akan dipicu.

Perlindungan akses memori langsung untuk Mac berbasis Intel

Komputer Mac berbasis Intel dengan Intel Virtualization Technology for Directed I/O (Teknologi Virtualisasi Intel untuk I/O yang Diarahkan atau VT-d) memulai IOMMU, yang mengaktifkan pemetaan ulang DMA dan mengganggu pemetaan ulang pada awal proses boot untuk memitigasi berbagai kelas kerentanan keamanan. Perangkat keras IOMMU Apple memulai operasi dengan kebijakan penolakan default, sehingga segera saat sistem dinyalakan, sistem secara otomatis memulai pemblokiran permintaan DMA dari periferal. Setelah dimulai oleh perangkat lunak, IOMMU mulai mengizinkan permintaan DMA dari periferal ke area memori yang telah dipetakan secara eksplisit untuk penggunaannya.

Catatan: Pemetaan ulang gangguan untuk PCIe tidak diperlukan di Mac dengan Apple silicon karena setiap IOMMU menangani MSI untuk periferalnya sendiri.

Mulai dari macOS 11, semua komputer Mac dengan Keping Keamanan T2 Apple menjalankan driver UEFI yang memfasilitasi DMA di lingkungan ring 3 yang dibatasi saat driver ini dipasangkan dengan perangkat eksternal. Properti ini membantu memitigasi kerentanan keamanan yang dapat terjadi saat perangkat berbahaya berinteraksi dengan driver UEFI dalam cara yang tidak terduga pada saat boot. Khususnya, hal ini mengurangi dampak kerentanan di driver yang menangani buffer DMA.

Ekstensi kernel di macOS

Dimulai dari macOS 11, jika diaktifkan, ekstensi kernel (kext) pihak ketiga tidak dapat dimuat ke kernel sesuai permintaan. Sebaliknya, ekstensi digabungkan ke *Kumpulan Kernel Pembantu (AuxKC)* yang dimuat selama proses boot. Untuk Mac dengan Apple silicon, pengukuran AuxKC ditandatangani ke LocalPolicy (untuk perangkat keras sebelumnya, AuxKC berada di volume data). Membuat ulang AuxKC memerlukan persetujuan pengguna dan pemulaian ulang macOS untuk memuat perubahan ke kernel, dan boot aman perlu dikonfigurasikan ke Keamanan Dikurangi.

Penting: Kext tidak lagi dianjurkan untuk macOS. Kext membahayakan integritas dan keterandalan sistem operasi, dan Apple menganjurkan pengguna untuk memilih solusi yang tidak memerlukan perluasan kernel.

Ekstensi kernel di Mac dengan Apple silicon

Kext harus diaktifkan secara eksplisit untuk Mac dengan Apple silicon dengan menahan tombol daya saat mulai untuk masuk ke mode One True Recovery (1TR), lalu menurunkan ke Keamanan Dikurangi dan mencentang kotak untuk mengaktifkan ekstensi kernel. Tindakan ini juga memerlukan kata sandi administrator untuk mengesahkan penurunan. Gabungan 1TR dan persyaratan kata sandi mempersulit penyerang yang hanya memanfaatkan perangkat lunak yang memulai dari dalam macOS untuk memasukkan kext ke macOS, yang nantinya dapat mereka eksploitasi untuk memperoleh hak kernel.

Setelah pengguna mengesahkan kext untuk dimuat, alur Pemuatan Ekstensi Kernel yang Disetujui Pengguna digunakan untuk mengesahkan penginstalan kext. Pengesahan yang digunakan untuk alur di atas juga digunakan untuk menangkap hash SHA384 dari daftar kext yang disahkan pengguna (UAKL) di LocalPolicy. Daemon manajemen kernel (`kmd`) lalu bertanggung jawab untuk memvalidasi hanya kext tersebut yang ditemukan di UAKL untuk penyertaan ke AuxKC.

- Jika Perlindungan Integritas Sistem (SIP) diaktifkan, tanda tangan setiap kext diverifikasi sebelum disertakan di AuxKC.
- Jika SIP dinonaktifkan, tanda tangan kext tidak akan diberlakukan.

Pendekatan ini memungkinkan alur Keamanan Permisif untuk pengembang atau pelanggan yang bukan bagian dari Apple Developer Program untuk menguji kext sebelum ditandatangani.

Setelah AuxKC dibuat, pengukurannya dikirimkan ke Secure Enclave untuk ditandatangani dan disertakan di struktur data Image4 yang dapat dievaluasi oleh iBoot saat mulai. Sebagai bagian dari konstruksi AuxKC, tanda terima kext juga dibuat. Tanda terima ini berisi daftar kext yang benar-benar disertakan di AuxKC, karena kumpulan dapat berupa subset UAKL jika kext yang dilarang ditemui. Hash SHA384 dari struktur data Image4 AuxKC dan tanda terima kext disertakan di LocalPolicy. Hash Image4 AuxKC digunakan untuk verifikasi tambahan oleh iBoot saat mulai untuk membantu memastikan bahwa file Image4 AuxKC yang ditandatangani oleh Secure Enclave versi lama tidak dapat dimulai dengan LocalPolicy yang lebih baru. Tanda terima kext digunakan oleh subsistem seperti Apple Pay untuk menentukan apakah terdapat kext yang saat ini dimuat yang dapat mengganggu kepercayaan macOS. Jika ada, kemampuan Apple Pay dapat dinonaktifkan.

Alternatif kext (macOS 10.15 atau lebih baru)

macOS 10.15 memungkinkan pengembang untuk memperluas kemampuan macOS dengan menginstal dan mengelola ekstensi sistem yang dijalankan di ruang pengguna alih-alih di level kernel. Dengan menjalankan di ruang pengguna, ekstensi sistem meningkatkan stabilitas dan keamanan macOS. Meskipun kext telah dilengkapi dengan akses penuh terhadap seluruh sistem operasi, ekstensi yang dijalankan di ruang pengguna hanya diberi hak yang diperlukan untuk menjalankan fungsi yang ditetapkannya.

Pengembang dapat menggunakan kerangka yang meliputi DriverKit, EndpointSecurity, dan NetworkExtension untuk menulisi driver USB dan antarmuka manusia, alat keamanan titik ujung (seperti pencegahan data hilang atau agen titik ujung lain), dan alat VPN serta jaringan, semuanya tanpa perlu menulisi kext. Agen keamanan pihak ketiga hanya boleh digunakan jika memanfaatkan API ini atau memiliki langkah-langkah yang lengkap untuk bertransisi ke dan dari ekstensi kernel.

Pemuatan Ekstensi Kernel yang Disetujui Pengguna

Untuk meningkatkan keamanan, persetujuan pengguna diperlukan untuk memuat ekstensi kernel yang diinstal dengan atau setelah menginstal macOS 10.13. Proses ini disebut sebagai *Pemuatan Ekstensi Kernel yang Disetujui Pengguna*. Pengesahan administrator diperlukan untuk menyetujui ekstensi kernel. Ekstensi kernel tidak memerlukan pengesahan jika:

- Diinstal di Mac saat menjalankan macOS 10.12 atau lebih lama
- Mengganti ekstensi yang disetujui sebelumnya
- Diizinkan untuk memuat tanpa persetujuan pengguna dengan menggunakan alat baris perintah `spctl` yang tersedia saat Mac di-boot dari recoveryOS
- Diizinkan untuk memuat menggunakan konfigurasi mobile device management (MDM)

  Mulai dari macOS 10.13.2, pengguna dapat menggunakan MDM untuk menetapkan daftar ekstensi kernel yang memuat tanpa persetujuan pengguna. Pilihan ini memerlukan Mac yang menjalankan macOS 10.13.2 yang terdaftar di MDM—melalui Apple School Manager, Apple Business Manager, atau pendaftaran MDM yang dilakukan oleh pengguna.

Keamanan ROM Pilihan di macOS

Catatan: ROM Pilihan saat ini tidak didukung di Mac dengan Apple silicon.

Keamanan ROM Pilihan di Mac dengan Keping Keamanan T2 Apple

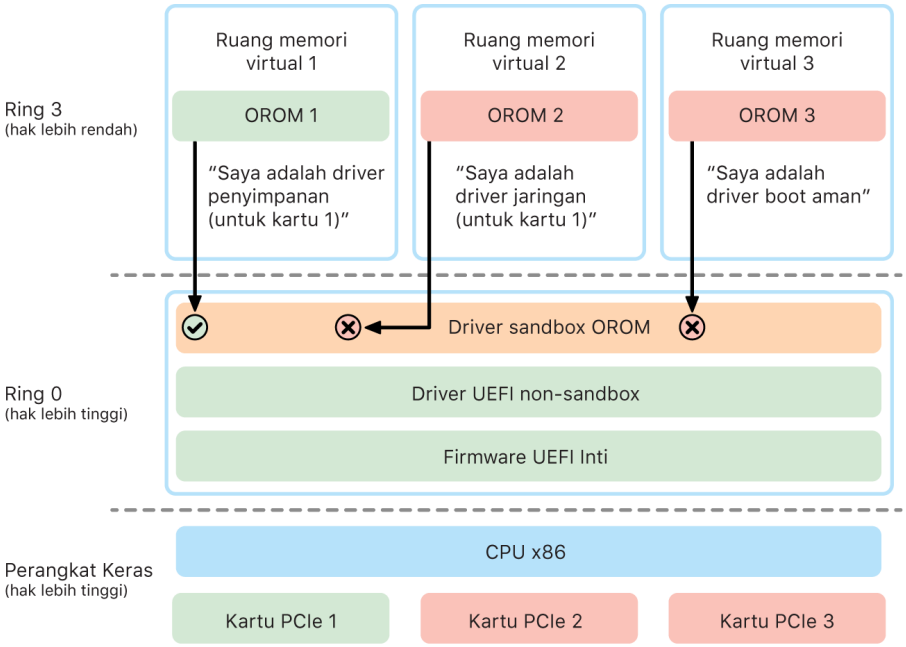
Perangkat Thunderbolt dan PCIe dapat memiliki “ROM Pilihan (OROM)” yang dipasang secara fisik ke perangkat. (Ini biasanya bukan merupakan ROM yang sebenarnya, tapi keping yang dapat ditulisi ulang yang menyimpan firmware.) Di sistem berbasis UEFI, firmware tersebut biasanya merupakan driver UEFI, yang dibaca oleh firmware UEFI dan dieksekusi. Kode yang dieksekusi harus menginisialisasi dan mengonfigurasi perangkat keras tempat kode diambil, sehingga perangkat keras menjadi dapat digunakan oleh seluruh bagian lainnya dari firmware. Kemampuan ini diperlukan agar perangkat pihak ketiga yang bersifat khusus dapat dimuat dan dioperasikan pada fase mulai paling awal—misalnya untuk memulai dari larik RAID eksternal.

Namun, karena OROM biasanya dapat ditulisi kembali, jika penyerang menimpa OROM dari periferal yang sah, kode penyerang dieksekusi di awal proses boot, dan akan dapat mengubah lingkungan eksekusi dan merusak integritas perangkat lunak yang dimuat setelahnya. Sama halnya, jika penyerang memperkenalkan perangkat berbahayanya ke sistem, mereka juga akan dapat mengeksekusi kode berbahaya.

Di macOS 10.12.3, perilaku komputer Mac yang dijual setelah 2011 diubah menjadi tidak mengeksekusi OROM secara default pada saat Mac di-boot, kecuali jika kombinasi tombol ditekan. Kombinasi kunci ini melindungi dari OROM berbahaya yang diperkenalkan secara tidak sengaja ke rangkaian boot macOS. Perilaku default dari Utilitas Kata Sandi Firmware juga diubah sehingga ketika pengguna mengatur kata sandi firmware, OROM tidak dapat dieksekusi bahkan jika kombinasi tombol ditekan. Ini melindungi dari penyerang yang memiliki akses langsung secara fisik untuk memperkenalkan OROM berbahaya dengan sengaja. Untuk pengguna yang masih harus menjalankan OROM dan telah mengatur kata sandi firmware, pilihan non-default dapat dikonfigurasi menggunakan alat baris perintah `firmwarepasswd` di macOS.

Keamanan sandbox OROM

Di macOS 10.15, firmware UEFI diperbarui agar berisi mekanisme untuk sandbox OROM dan untuk membatalkan hak dari OROM. Firmware UEFI biasanya mengeksekusi semua kode, termasuk OROM, pada level hak CPU maksimum, yang disebut ring 0, dan memiliki satu ruang memori virtual bersama untuk semua kode dan data. Ring 0 merupakan tingkat hak tempat kernel macOS dijalankan, sementara level hak yang lebih bawah, ring 3, adalah tempat app dijalankan. Sandbox OROM membatalkan hak OROM dengan menggunakan pemisahan memori virtual seperti yang dilakukan oleh kernel, lalu membuat OROM dijalankan di ring 3.



Sandbox secara drastis membatasi lebih jauh antarmuka yang dapat dipanggil OROM (seperti filter panggilan sistem di kernel) dan jenis perangkat yang dapat diregister OROM (seperti persetujuan app.) Keuntungan desain ini adalah bahwa OROM berbahaya tidak lagi dapat menulis secara langsung di mana pun dalam memori ring 0. Sebagai gantinya, OROM dibatasi ke antarmuka sandbox yang sangat sempit dan didefinisi dengan baik. Antarmuka terbatas ini secara drastis mengurangi permukaan serangan dan memaksa penyerang untuk pertama-tama keluar dari sandbox dan meningkatkan hak.

Keamanan firmware UEFI di Mac berbasis Intel

Mac berbasis Intel dengan Keping Keamanan T2 Apple menawarkan keamanan menggunakan firmware UEFI (Intel).

Tinjauan

Sejak 2006, komputer Mac dengan CPU berbasis Intel menggunakan firmware Intel berbasis Kit Pengembangan (EDK) Antarmuka Firmware yang Dapat Diperluas (EFI) versi 1 atau versi 2. Kode berbasis EDK2 sesuai dengan spesifikasi Antarmuka Firmware Terpadu yang Dapat Diperluas (UEFI). Bagian ini merujuk ke firmware Intel sebagai *firmware UEFI*. Firmware UEFI adalah kode pertama yang dieksekusi pada keping Intel.

Untuk Mac berbasis Intel tanpa Keping Keamanan T2 Apple, dasar kepercayaan firmware UEFI adalah keping tempat firmware tersimpan. Pembaruan firmware UEFI ditandatangani secara digital oleh Apple dan diverifikasi oleh firmware sebelum memperbarui penyimpanan. Untuk membantu mencegah serangan penurunan versi, pembaruan harus selalu memiliki versi yang lebih baru dari versi yang ada. Namun, penyerang dengan akses fisik ke Mac mungkin dapat menggunakan perangkat keras untuk memasangkan ke keping penyimpanan firmware dan memperbarui keping tersebut agar berisi konten berbahaya. Sama halnya, jika kerentanan terdapat di awal proses boot firmware UEFI (sebelum membatasi penulisan terhadap keping penyimpanan), ini juga dapat mengakibatkan infeksi firmware UEFI secara terus-menerus. Ini adalah pembatasan arsitektur perangkat keras yang umum di sebagian besar PC berbasis Intel dan ada di semua komputer Mac berbasis Intel tanpa keping T2.

Untuk membantu mencegah serangan fisik yang merusak firmware UEFI, komputer Mac dirancang ulang untuk mendasari kepercayaan di firmware UEFI di keping T2. Di komputer Mac ini, dasar kepercayaan firmware UEFI secara khusus adalah firmware T2, sebagaimana yang dijelaskan di Proses boot untuk Mac berbasis Intel.

Subkomponen Intel Management Engine (ME)

Satu subkomponen yang disimpan di firmware UEFI adalah firmware *Intel Management Engine (ME)*. ME—prosesor dan subsistem terpisah di dalam keping Intel—sebagian besar digunakan untuk perlindungan hak cipta audio dan video di Mac yang hanya memiliki grafik berbasis Intel. Untuk melindungi permukaan serangan subkomponen, Mac berbasis Intel menjalankan firmware ME khusus yang sebagian besar komponennya telah dihapus. Karena hasil firmware ME Mac menjadi lebih kecil dari build minimum default yang disediakan Intel, banyak komponen yang telah menjadi subjek serangan publik oleh peneliti keamanan di masa lampau tidak lagi ada.

Mode Manajemen Sistem (SMM)

Prosesor Intel memiliki mode eksekusi khusus yang berbeda dari pengoperasian normal. Mode yang disebut *Mode Manajemen Sistem (SMM)* ini pada awalnya diperkenalkan untuk menangani operasi peka waktu seperti manajemen daya. Namun, untuk menjalankan tindakan seperti itu, komputer Mac harus pernah menggunakan pengontrol mikro diskret yang disebut *Pengontrol Manajemen Sistem (SMC)*. SMC telah diintegrasikan ke keping T2 sehingga tidak lagi memiliki pengontrol mikro terpisah.

Keamanan sistem untuk watchOS

Apple Watch menggunakan banyak kemampuan keamanan platform berbasis perangkat keras yang sama dengan yang digunakan oleh iOS dan iPadOS. Misalnya, Apple Watch:

- Melakukan boot aman dan pembaruan perangkat lunak aman
- Memelihara Integritas sistem operasi
- Membantu melindungi data—baik di perangkat dan saat berkomunikasi dengan iPhone yang dipasangkan atau internet

Teknologi yang didukung mencakup teknologi yang tercantum di Keamanan Sistem (misalnya, KIP, SKP, dan SCIP) serta teknologi Perlindungan Data, rantai kunci, dan jaringan.

Memperbarui watchOS

watchOS dapat dikonfigurasi untuk diperbarui pada malam hari. Untuk informasi lainnya mengenai bagaimana kode sandi Apple Watch disimpan dan digunakan selama pembaruan, lihat Kantong Kunci.

Deteksi tangan

Jika deteksi pergelangan tangan diaktifkan, perangkat akan dikunci secara otomatis segera setelah dilepaskan dari pergelangan tangan pengguna. Jika deteksi pergelangan tangan dinonaktifkan, Pusat Kontrol menyediakan pilihan untuk mengunci Apple Watch. Jika Apple Watch dikunci, Apple Pay hanya dapat digunakan dengan memasukkan kode sandi di Apple Watch. Deteksi pergelangan tangan dimatikan menggunakan app Apple Watch di iPhone. Pengaturan ini juga dapat diterapkan menggunakan solusi mobile device management (MDM).

Kunci Aktivasi

Saat Lacak dinyalakan di iPhone, Apple Watch pasangannya dapat menggunakan Kunci Aktivasi. Kunci Aktivasi menyulitkan orang untuk menggunakan atau menjual Apple Watch yang telah hilang atau dicuri. Kunci Aktivasi memerlukan ID Apple dan kata sandi pengguna untuk melepaskan, menghapus, atau mengaktifkan kembali Apple Watch.

Pemasangan aman dengan iPhone

Apple Watch hanya dapat dipasangkan dengan satu iPhone pada satu waktu. Saat Apple Watch dilepas, iPhone memerintahkan instruksi untuk menghapus semua konten dan data dari jam.

Pemasangan Apple Watch dengan iPhone diamankan menggunakan proses luar jalur untuk menukar kunci publik, diikuti oleh rahasia bersama tautan Bluetooth Rendah Energi (BLE). Apple Watch menampilkan pola animasi, yang diambil oleh kamera di iPhone. Pola berisi rahasia dikodekan yang digunakan untuk pemasangan luar jalur BLE 4.1. Entri Kunci Sandi BLE Standar digunakan sebagai metode pemasangan balik, jika perlu.

Setelah sesi BLE dibuat dan dienkripsi menggunakan protokol keamanan tertinggi yang tersedia di Spesifikasi Inti Bluetooth, iPhone dan Apple Watch bertukar kunci menggunakan:

- Proses yang diadaptasi dari Layanan Identitas Apple (IDS) sebagaimana dijelaskan di tinjauan keamanan iMessage.
- Pertukaran kunci menggunakan IKEv2/IPsec. Pertukaran kunci awal disahkan menggunakan kunci sesi Bluetooth (untuk skenario pemasangan) atau kunci IDS (untuk skenario pembaruan sistem operasi). Setiap perangkat membuat pemasangan kunci Ed25519 256 bit publik serta pribadi, dan kunci publik akan ditukar selama proses pertukaran kunci awal.

Catatan: Mekanisme yang digunakan untuk pertukaran kunci dan enkripsi berbeda-beda, bergantung pada versi sistem operasi yang ada di iPhone dan Apple Watch. Perangkat iPhone yang menjalankan iOS 13 atau lebih baru saat dipasangkan dengan Apple Watch yang menjalankan watchOS 6 atau lebih baru hanya menggunakan IKEv2/IPsec untuk pertukaran kunci dan enkripsi.

Setelah kunci ditukar:

- Kunci sesi Bluetooth dibuang dan semua komunikasi di antara iPhone dan Apple Watch dienkripsi menggunakan salah satu metode yang tercantum di atas—dengan Bluetooth, Wi-Fi, dan tautan seluler terenkripsi yang menyediakan lapisan enkripsi kedua.
- (Hanya IKEv2/IPsec) Kunci disimpan di rantai kunci Sistem dan digunakan untuk mengesahkan sesi IKEv2/IPsec mendatang di antara perangkat. Komunikasi lebih lanjut antarperangkat ini dienkripsi dan integritasnya dilindungi menggunakan AES-256-GCM atau ChaCha20-Poly1305 (kunci 256 bit) di perangkat iPhone yang menjalankan iOS 15 atau lebih baru yang dipasangkan dengan Apple Watch Series 4 atau lebih baru yang menjalankan watchOS 8 atau lebih baru.

Alamat perangkat Bluetooth Rendah Energi dirotasi dengan interval 15 menit untuk mengurangi risiko pelacakan lokal perangkat jika seseorang menyiarkan pengenal tetap.

Untuk mendukung app yang memerlukan streaming data, enkripsi disediakan dengan metode yang dijelaskan di keamanan FaceTime, menggunakan Layanan Identitas Apple (IDS) yang disediakan oleh iPhone yang dipasangkan atau koneksi internet langsung.

Apple Watch mengimplementasikan penyimpanan terenkripsi perangkat keras dan perlindungan file berbasis kelas serta item rantai kunci. Kantong kunci dengan akses terkontrol untuk item rantai kunci juga digunakan. Kunci yang digunakan untuk komunikasi antara Apple Watch dan iPhone juga diamankan menggunakan perlindungan berbasis kelas. Untuk informasi lainnya, lihat Kantong kunci untuk Perlindungan data.

Buka Otomatis dan Apple Watch

Demi kenyamanan lebih saat menggunakan beberapa perangkat Apple, sebagian perangkat dapat membuka perangkat lain secara otomatis dalam situasi tertentu. Buka Otomatis mendukung tiga penggunaan:

- Apple Watch dapat dibuka oleh iPhone.
- Mac dapat dibuka oleh Apple Watch.
- iPhone dapat dibuka oleh Apple Watch saat pengguna terdeteksi dengan hidung dan mulutnya yang tertutup.

Tiga kasus penggunaan ini dibangun pada landasan dasar yang sama: protokol Stasiun ke Stasiun (STS) yang saling mengesahkan, dengan Kunci Jangka Panjang yang ditukar saat pengaktifan fitur dan kunci sesi unik sementara yang dinegosiasikan untuk setiap permintaan. Terlepas dari saluran komunikasi yang mendasari, saluran STS dinegosiasikan secara langsung di antara Secure Enclave di kedua perangkat, dan semua material kriptografis disimpan dalam domain yang aman (dengan pengecualian komputer Mac tanpa Secure Enclave, yang menghapus saluran STS di kernel).

Membuka

Rangkaian pembukaan lengkap dapat dipecah ke dalam dua fase. Pertama, perangkat yang sedang dibuka (“target”) membuat rahasia pembukaan kriptografis dan mengirimkannya ke perangkat yang membuka (“inisiator”). Selanjutnya, inisiator membuka menggunakan rahasia yang sebelumnya dibuat.

Untuk mengaktifkan buka otomatis, perangkat harus terhubung satu sama lain menggunakan koneksi BLE. Lalu, rahasia pembukaan 32 bita yang dibuat secara acak oleh perangkat target dikirimkan ke inisiator melalui saluran STS. Selama biometrik atau pembukaan kode sandi berikutnya, perangkat target membungkus kunci turunan kode sandinya (PDK) dengan rahasia pembukaan dan membuang rahasia pembukaan dari memorinya.

Untuk membuka, perangkat memulai koneksi BLE baru, lalu menggunakan Wi-Fi rekan ke rekan untuk memperkirakan dengan aman jarak di antara keduanya. Jika perangkat berada dalam jangkauan tertentu dan kebijakan keamanan yang diperlukan terpenuhi, inisiator mengirimkan rahasia pembukaannya ke target melalui saluran STS. Lalu, target membuat rahasia pembukaan 32 bita baru dan mengembalikannya ke inisiator. Jika rahasia pembukaan saat ini yang dikirim oleh inisiator berhasil mendekripsi catatan pembukaan, perangkat target dibuka dan PDK dibungkus ulang dengan rahasia pembukaan baru. Terakhir, rahasia pembukaan dan PDK baru lalu dibuang dari memori target.

Kebijakan keamanan Buka Otomatis Apple Watch

Demi kenyamanan tambahan, Apple Watch dapat dibuka oleh iPhone secara langsung setelah pengaturan awal, tanpa mengharuskan pengguna memasukkan kode sandi di Apple Watch. Agar ini dapat dilakukan, rahasia pembukaan acak (dibuat selama rangkaian pembukaan pertama setelah pengaktifan fitur) digunakan untuk membuat catatan eskrow jangka panjang, yang disimpan di kantong kunci Apple Watch. Rahasia catatan eskrow disimpan di rantai kunci iPhone dan digunakan untuk melakukan bootstrap sesi baru setelah setiap memulai ulang Apple Watch.

Kebijakan keamanan Buka Otomatis iPhone

Kebijakan keamanan tambahan yang diterapkan ke Buka Otomatis iPhone dengan Apple Watch. Apple Watch tidak dapat digunakan sebagai pengganti Face ID di iPhone untuk operasi lainnya, seperti Apple Pay atau pengesahan app. Saat Apple Watch berhasil membuka iPhone yang dipasangkan, jam menampilkan pemberitahuan dan memutar haptik terkait. Jika pengguna mengetuk tombol Kunci iPhone di pemberitahuan, jam mengirimi iPhone perintah penguncian melalui BLE. Saat menerima perintah penguncian, iPhone mengunci dan menonaktifkan Face ID dan pembukaan menggunakan Apple Watch. Pembukaan iPhone berikutnya harus dilakukan dengan kode sandi iPhone.

Kriteria berikut harus terpenuhi untuk berhasil membuka iPhone yang dipasangkan dari Apple Watch (saat diaktifkan):

- iPhone harus telah dibuka menggunakan metode lain setidaknya sekali setelah Apple Watch yang dikaitkan dikenakan di tangan dan dibuka.
- Sensor harus dapat mendeteksi hidung dan mulut yang tertutup.
- Jarak yang diukur berkisar antara 2–3 meter atau kurang
- Apple Watch tidak boleh berada dalam mode waktu tidur.
- Apple Watch atau iPhone harus telah dibuka baru-baru ini, atau Apple Watch harus telah mengalami gerakan fisik yang menandakan bahwa pemakai aktif (misalnya, tidak tidur).
- iPhone harus telah dibuka setidaknya sekali selama 6,5 jam terakhir.
- iPhone harus mengizinkan Face ID untuk membuka perangkat. (Untuk informasi lainnya, lihat Face ID, Touch ID, kode sandi, dan kata sandi.)

Menyetujui di macOS dengan Apple Watch

Saat Buka Otomatis dengan Apple Watch diaktifkan, Apple Watch dapat digunakan sebagai ganti atau bersama Touch ID, untuk menyetujui pengesahan dan autentikasi perintah dari:

- App macOS dan Apple yang meminta pengesahan
- App pihak ketiga yang meminta autentikasi
- Kata sandi yang disimpan Safari
- Catatan Aman

Penggunaan Wi-Fi, seluler, iCloud, dan Gmail yang aman

Saat Apple Watch tidak dalam jangkauan Bluetooth, Wi-Fi atau seluler dapat digunakan sebagai gantinya. Apple Watch bergabung secara otomatis dengan jaringan Wi-Fi yang telah digunakan di iPhone yang dipasangkan dan yang info pengesahannya telah diselaraskan ke Apple Watch saat kedua perangkat dalam jangkauan. Perilaku Gabung Otomatis ini kemudian dapat dikonfigurasi secara terpisah per jaringan di bagian Wi-Fi di app Pengaturan Apple Watch. Jaringan Wi-Fi yang belum pernah digunakan sebelumnya di salah satu perangkat dapat digunakan secara otomatis di bagian Wi-Fi di app Pengaturan Apple Watch.

Saat Apple Watch dan iPhone berada di luar jangkauan, Apple Watch akan terhubung secara otomatis ke server iCloud dan Gmail untuk mengambil Mail, sebagai ganti penyelarasan data Mail dengan iPhone yang dipasangkan melalui internet. Untuk akun Gmail, pengguna harus mengesahkan ke Google di bagian Mail di app Apple Watch di iPhone. Token OAuth yang diterima dari Google akan dikirimkan ke Apple Watch dalam format yang terenkripsi melalui Layanan Identitas (IDS) Apple sehingga dapat digunakan untuk mengambil Mail. Token OAuth ini tidak pernah digunakan untuk konektivitas dengan server Gmail dari iPhone yang dipasangkan.

Pembuatan angka acak

Pembuat angka semu acak kriptografis (CPRNG) merupakan komponen pembangun penting untuk perangkat lunak yang aman. Pada tahap ini, Apple menyediakan CPRNG perangkat lunak tepercaya yang dijalankan di kernel iOS, iPadOS, macOS, tvOS, dan watchOS. CPRNG tersebut berfungsi untuk mengagregatkan entropi mentah dari sistem dan menyediakan angka acak aman kepada konsumen di kernel dan ruang pengguna.

Sumber entropi

CPRNG kernel diseeding dari beberapa sumber entropi selama boot dan sepanjang masa pakai perangkat. Ini meliputi (dapat berubah tergantung ketersediaan):

- TRNG perangkat keras Secure Enclave
- Jitter berbasis waktu yang dikumpulkan selama boot
- Entropi yang dikumpulkan dari gangguan perangkat keras
- File seed yang digunakan untuk mempertahankan entropi selama boot
- Instruksi acak Intel—misalnya, RDSEED dan RDRAND (hanya di Mac berbasis Intel)

CPRNG kernel

CPRNG Kernel adalah desain yang berasal dari Fortuna yang menargetkan level keamanan 256 bit. CPRNG kernel ini menyediakan angka acak berkualitas tinggi bagi konsumen ruang pengguna menggunakan API berikut:

- Panggilan sistem `getentropy`(2)
- Perangkat acak (/dev/random)

CPRNG kernel menerima entropi yang disediakan pengguna melalui penulisan ke perangkat acak.

Perangkat Riset Keamanan Apple

Perangkat Riset Keamanan Apple adalah iPhone yang secara khusus digabungkan yang mengizinkan peneliti keamanan agar dapat melakukan riset di iOS tanpa menghapus atau menonaktifkan fitur keamanan platform iPhone. Dengan perangkat ini, peneliti dapat memuat konten yang dijalankan dengan izin yang setara dengan platform, dan dengan demikian melakukan penelitian pada platform yang lebih mirip dengan model perangkat produksi.

Untuk membantu memastikan perangkat pengguna tidak terpengaruh oleh kebijakan eksekusi perangkat riset keamanan, perubahan kebijakan diimplementasikan dalam varian iBoot dan Kumpulan Kernel Boot. Ini gagal di-boot di perangkat keras pengguna. Riset iBoot memeriksa status penggabungan baru dan memasuki loop panik jika dijalankan pada perangkat keras gabungan non-riset.

Subsistem cryptex memungkinkan pengguna untuk memuat cache kepercayaan yang disesuaikan dan image disk yang berisi konten yang sesuai. Sejumlah tindakan pertahanan yang mendalam telah diterapkan yang dirancang untuk memastikan bahwa subsistem ini tidak mengizinkan eksekusi pada perangkat pengguna:

- `launchd` tidak memuat daftar properti `cryptexd` launchd jika perangkat pelanggan normal terdeteksi.
- `cryptexd` dibatalkan jika perangkat pelanggan normal terdeteksi.
- `AppleImage4` tidak menawarkan nonce yang digunakan untuk memverifikasi cryptex riset di perangkat pelanggan normal.
- Server penandatanganan menolak untuk menyesuaikan image disk cryptex untuk perangkat yang tidak ada di daftar izin eksplisit.

Untuk menghormati privasi peneliti keamanan, hanya pengukuran (misalnya, hash) yang dapat dieksekusi atau cache kernel dan pengenal perangkat riset keamanan yang dikirimkan ke Apple selama penyesuaian. Apple tidak menerima konten cryptex yang dimuat ke perangkat.

Untuk menghindari percobaan pihak yang jahat untuk menyamarkan perangkat riset sebagai perangkat pengguna untuk mengelabui target agar menggunakannya untuk penggunaan sehari-hari, perangkat riset keamanan memiliki perbedaan berikut:

- Perangkat riset keamanan hanya dimulai saat dayanya diisi. Ini dapat dilakukan menggunakan kabel Lightning atau pengisi daya yang kompatibel dengan Qi. Jika perangkat tidak diisi dayanya selama mulai, perangkat masuk ke mode Pemulihan. Jika pengguna mulai mengisi daya dan memulai ulang perangkat, perangkat dimulai dengan normal. Setelah XNU dimulai, perangkat tidak perlu diisi dayanya untuk melanjutkan operasi.
- Kata *Perangkat Riset Keamanan* ditampilkan di bawah logo Apple selama proses mulai iBoot.
- Kernel XNU di-boot dalam mode verbose.
- Perangkat diukir di sisi dengan pesan “Property of Apple. Confidential and Proprietary. Call +1 877 595 1125.”

Berikut adalah tindakan tambahan yang diimplementasikan di perangkat lunak yang muncul setelah boot:

- Kata *Perangkat Riset Keamanan* ditampilkan selama pengaturan perangkat.
- Kata *Perangkat Riset Keamanan* ditampilkan di Layar Terkunci dan di app Pengaturan.

Perangkat Riset Keamanan memberi peneliti kemampuan berikut yang tidak dimiliki oleh perangkat pengguna. Peneliti dapat:

- Mentransfer kode yang dapat dieksekusi ke perangkat dengan hak arbitrer pada tingkat izin yang sama seperti komponen sistem operasi Apple
- Memulai layanan pada saat mulai
- Mempertahankan konten di setiap mulai ulang
- Menggunakan hak `research.com.apple.license-to-operate` untuk mengizinkan proses untuk mendebug proses lainnya di sistem, termasuk proses sistem.

  Namespace `research.` hanya tunduk pada varian RESEARCH dari ekstensi kernel AppleMobileFileIntegrity; proses apa pun dengan hak ini dimatikan di perangkat pelanggan selama validasi tanda tangan.
- Menyesuaikan dan memulihkan cache kernel khusus

Enkripsi dan Perlindungan Data

Tinjauan Enkripsi dan Perlindungan Data

Kemampuan rantai boot aman, keamanan sistem, dan keamanan app membantu memverifikasi bahwa hanya kode dan app tepercaya yang dijalankan di perangkat. Perangkat Apple memiliki fitur enkripsi tambahan untuk menjaga data pengguna, bahkan ketika bagian lain dari infrastruktur keamanan telah terganggu (misalnya, jika perangkat hilang atau menjalankan kode tidak tepercaya). Semua fitur ini menguntungkan pengguna dan administrator TI, melindungi informasi pribadi dan perusahaan, dan menyediakan cara untuk menghapus perangkat secara instan dan menyeluruh jika dicuri atau hilang.

Perangkat iOS dan iPadOS menggunakan metodologi enkripsi yang disebut *Perlindungan Data*, sementara data di Mac berbasis Intel dilindungi dengan teknologi enkripsi volume yang disebut *FileVault*. Mac dengan Apple silicon menggunakan model hibrida yang mendukung Perlindungan Data, dengan dua kondisi: Kelas level perlindungan terendah (D) tidak didukung, dan level default (Kelas C) menggunakan kunci volume dan bertindak layaknya FileVault di Mac berbasis Intel. Di semua kasus, hierarki manajemen kunci berakar di silicon khusus Secure Enclave, dan Mesin AES khusus mendukung enkripsi berkecepatan saluran dan membantu memastikan kunci enkripsi jangka panjang tidak terpapar ke sistem operasi atau CPU kernel (tempat mereka dapat disusupi). (Mac berbasis Intel dengan T1 atau yang tidak memiliki Secure Enclave tidak menggunakan silicon tertanam untuk melindungi kunci enkripsi FileVault-nya.)

Selain menggunakan Perlindungan Data dan FileVault untuk membantu mencegah akses yang tidak disahkan ke data, Apple menggunakan *kernel sistem operasi* untuk memberlakukan perlindungan dan keamanan. Kernel menggunakan kontrol akses untuk memasukkan app ke sandbox (yang membatasi data apa yang dapat diakses oleh app) dan mekanisme yang disebut *Vault Data* (yang membatasi akses ke data app dari semua app lain yang meminta alih-alih membatasi panggilan yang dapat dilakukan oleh app).

Kode sandi dan kata sandi

Untuk melindungi data pengguna dari serangan berbahaya, Apple menggunakan kode sandi di iOS serta iPadOS dan kata sandi di macOS. Kode sandi atau kata sandi yang semakin panjang akan semakin kuat—dan lebih mudah untuk mencegah serangan brute force. Untuk mencegah serangan lebih jauh, Apple memberlakukan penundaan waktu (untuk iOS dan iPadOS) dan jumlah percobaan kata sandi yang dibatasi (untuk Mac).

Di iOS dan iPadOS, pengaturan kode sandi atau kata sandi perangkat, pengguna secara otomatis mengaktifkan Perlindungan Data. Perlindungan Data juga diaktifkan di perangkat lainnya yang menyertakan sistem pada keping (SoC) Apple—seperti Mac dengan Apple silicon, Apple TV, dan Apple Watch. Di macOS, Apple menggunakan program enkripsi volume internal *FileVault*.

Bagaimana kode sandi dan kata sandi kuat meningkatkan keamanan

iOS dan iPadOS mendukung kode sandi alfanumerik enam digit, empat digit dan dengan panjang arbitrer. Selain membuka perangkat, kode sandi atau kata sandi menyediakan entropi untuk kunci enkripsi tertentu. Ini berarti penyerang yang memegang perangkat tidak dapat mengakses data dalam kelas perlindungan tertentu tanpa kode sandi.

Kode sandi atau kata sandi dikaitkan dengan UID perangkat, sehingga upaya brute-force harus dilakukan pada perangkat yang diserang. Jumlah pengulangan yang besar digunakan untuk memperlambat tiap upaya. Jumlah pengulangan dikalibrasi sehingga satu upaya memerlukan waktu kira-kira 80 milidetik. Faktanya, ini memerlukan waktu lebih dari lima setengah tahun untuk mencoba semua kombinasi kode sandi alfanumerik enam digit dengan huruf kecil dan angka.

Semakin kuat kode sandi yang digunakan pengguna, semakin kuat kunci enkripsinya. Selain itu, dengan menggunakan Face ID dan Touch ID, pengguna dapat membuat kode sandi yang lebih kuat dibandingkan dengan yang lebih praktis. Kode sandi yang lebih kuat meningkatkan jumlah efektif entropi yang melindungi kunci enkripsi untuk Perlindungan Data, tanpa dampak negatif terhadap pengalaman pengguna saat membuka perangkat beberapa kali sepanjang hari.

Jika kata sandi panjang yang hanya berisi angka dimasukkan, keypad numerik akan ditampilkan di Layar Terkunci alih-alih papan ketik lengkap. Kode sandi numerik yang lebih panjang dapat lebih mudah dimasukkan daripada kode sandi alfanumerik yang lebih pendek, dan keduanya memiliki keamanan yang sama.

Pengguna dapat menetapkan kode sandi alfanumerik yang lebih panjang dengan memilih Kode Alfanumerik Khusus di Pilihan Kode Sandi di Pengaturan > Touch ID & Kode Sandi atau Face ID & Kode Sandi.

Cara penundaan waktu yang terus bertambah mengurangi serangan brute force (iOS, iPadOS)

Di iOS dan iPadOS, untuk melawan lebih jauh serangan brute force terhadap kode sandi, terdapat peningkatan penundaan waktu setelah kode sandi yang tidak sah dimasukkan di Layar Terkunci, seperti yang ditampilkan di tabel di bawah.

Upaya	Penundaan yang diberlakukan
1-4	Tidak Ada
5	1 menit
6	5 menit
7-8	15 menit
9	1 jam

Jika pilihan Hapus Data dinyalakan (di Pengaturan > Touch ID & Kode Sandi), semua konten dan pengaturan akan dihapus dari penyimpanan setelah 10 kali berturut-turut salah memasukkan kode sandi. Salah memasukkan kode yang sandi yang sama secara berturut-turut tidak dihitung. Pengaturan ini juga tersedia sebagai kebijakan administratif melalui solusi mobile device management (MDM) yang mendukung fitur ini dan melalui Microsoft Exchange ActiveSync, dan dapat diatur ke ambang yang lebih rendah.

Di perangkat dengan Secure Enclave, penundaan diberlakukan oleh Secure Enclave. Jika perangkat dimulai ulang selama penundaan berbatas waktu, penundaan masih akan diberlakukan, dengan timer yang dimulai dari awal untuk periode saat ini.

Cara penundaan waktu yang terus bertambah mengurangi serangan brute force (macOS)

Untuk membantu mencegah serangan brute-force, saat Mac dimulai, upaya untuk memasukkan kata sandi tidak boleh lebih dari 10 kali pada Jendela Masuk atau menggunakan Mode Disk Target, dan penundaan waktu yang terus bertambah akan diterapkan setelah sejumlah upaya gagal. Penundaan diberlakukan oleh Secure Enclave. Jika Mac dimulai ulang selama penundaan berbatas waktu, penundaan masih akan diberlakukan, dengan timer yang dimulai dari awal untuk periode saat ini.

Tabel di bawah menampilkan penundaan di antara upaya memasukkan kata sandi di Mac dengan Apple silicon dan Mac dengan keping T2.

Upaya	Penundaan yang diberlakukan
5	1 menit
6	5 menit
7	15 menit
8	15 menit
9	1 jam
10	Dinonaktifkan

Untuk membantu menghalangi agar malware tidak menyebabkan hilangnya data secara permanen dengan mencoba untuk menyerang kata sandi pengguna, batas ini tidak diberlakukan setelah pengguna berhasil masuk ke Mac, tapi diberlakukan kembali setelah boot ulang. Jika 10 upaya tersebut habis digunakan, tersedia 10 upaya lagi setelah boot ke recoveryOS. Dan jika upaya tambahan tersebut habis, akan terdapat 10 upaya tambahan lagi untuk setiap mekanisme pemulihan FileVault (pemulihan iCloud, kunci pemulihan FileVault, dan kunci institusi), dengan jumlah maksimum 30 upaya tambahan. Setelah upaya tambahan tersebut habis, Secure Enclave tidak lagi memproses permintaan apa pun untuk mendekripsi volume atau memverifikasi kata sandi, dan data di drive tidak akan dapat dipulihkan.

Untuk membantu melindungi data di pengaturan perusahaan, TI harus mendefinisikan dan menerapkan kebijakan konfigurasi FileVault menggunakan solusi MDM. Organisasi memiliki beberapa pilihan untuk mengelola volume terenkripsi, termasuk kunci pemulihan institusi, kunci pemulihan pribadi (yang dapat secara opsional disimpan dengan MDM untuk eskrow), atau kombinasi keduanya. Rotasi kunci juga dapat diatur sebagai kebijakan di MDM.

Di Mac dengan Keping Keamanan T2 Apple, kata sandi memiliki fungsi yang sama, kecuali bahwa kunci yang dibuat digunakan untuk enkripsi FileVault alih-alih Perlindungan Data. macOS juga menawarkan pilihan pemulihan kata sandi tambahan:

- Pemulihan iCloud
- Pemulihan FileVault
- Kunci institusional FileVault

Perlindungan Data

Tinjauan Perlindungan Data

Apple menggunakan teknologi yang disebut Perlindungan Data untuk melindungi data di penyimpanan kilat pada perangkat yang disertai dengan SoC Apple—seperti iPhone, iPad, Apple Watch, Apple TV, dan Mac dengan Apple silicon. Dengan Perlindungan Data, perangkat dapat merespons kejadian umum seperti panggilan telepon masuk saat sekaligus menyediakan enkripsi tingkat tinggi bagi data pengguna. Beberapa app sistem (seperti Pesan, Mail, Kalender, Kontak, Foto) dan nilai data Kesehatan menggunakan Perlindungan Data secara default. App pihak ketiga menerima perlindungan ini secara otomatis.

Penerapan

Perlindungan Data diterapkan dengan membangun dan mengelola hierarki kunci dan berbasis teknologi enkripsi perangkat keras pada setiap perangkat Apple. Perlindungan Data dikontrol pada basis per file dengan menetapkan tiap file ke suatu kelas; aksesibilitas ditetapkan berdasarkan dibuka atau tidaknya kunci kelas. APFS (Apple File System) memungkinkan sistem file untuk membuat subdivisi kunci lebih lanjut menjadi basis per area (tempat bagian dari file dapat memiliki kunci yang berbeda).

Setiap kali file di volume data dibuat, Perlindungan Data akan membuat kunci 256 bit baru (*kunci per file*) dan memberikannya ke Mesin AES perangkat keras, yang menggunakan kunci tersebut untuk mengenkripsi file pengguna dituliskan ke penyimpanan kilat. Di perangkat A14, A15, dan kelompok M1, enkripsi menggunakan AES-256 dalam mode XTS tempat kunci per file 256 bit melewati Fungsi Turunan Kunci (Publikasi Khusus NIST 800-108) untuk menurunkan kunci tweak 256 bit dan kunci cipher 256 bit. Perangkat keras generasi A9 hingga A13, S5, S6, dan S7 menggunakan AES-128 dalam mode XTS tempat 256 bit per kunci file dibagi untuk menyediakan kunci tweak 128 bit dan kunci cipher 128 bit.

Di Mac dengan Apple silicon, Perlindungan Data menjadi default ke Kelas C (lihat Kelas Perlindungan Data) tapi menggunakan kunci volume alih-alih kunci per area atau per file—secara efektif membuat ulang model keamanan FileVault untuk data pengguna. Pengguna masih harus memilih FileVault agar dapat menerima perlindungan penuh pengaitan hierarki kunci enkripsi dengan kata sandinya. Pengembang juga dapat memilih kelas perlindungan yang lebih tinggi yang menggunakan kunci per file atau per area.

Perlindungan Data di perangkat Apple

Di perangkat Apple dengan Perlindungan Data, setiap file dilindungi dengan kunci per file (atau per area) unik. Kunci, yang dibungkus menggunakan algoritme pembungkusan kunci NIST AED, dibungkus lebih jauh dengan salah satu kunci kelas, tergantung bagaimana file akan diakses. Kunci per file yang dibungkus lalu disimpan di metadata file.

Perangkat dengan format APFS dapat mendukung klon file (salinan bebas memori menggunakan teknologi penyalinan saat penulisan). Jika file diklon, setiap setengah klon mendapatkan kunci baru untuk menerima penulisan masuk sehingga data baru dituliskan ke media dengan kunci baru. Seiring berjalannya waktu, file dapat berisi berbagai area (atau potongan), masing-masing dipetakan ke kunci yang berbeda. Namun demikian, semua area yang terdiri dari file akan dilindungi oleh kunci dengan kelas yang sama.

Saat file dibuka, metadatanya akan didekripsi dengan kunci sistem file, mengungkapkan kunci per file yang dibungkus dan catatan mengenai kelas mana yang melindunginya. Pembungkusan kunci per file (atau per area) dibuka dengan kunci kelas, lalu dipasok ke Mesin AES perangkat keras, yang mendekripsi file saat file dibaca dari penyimpanan kilat. Semua penanganan kunci file yang dibungkus dilakukan di Secure Enclave; kunci file tidak pernah dipaparkan secara langsung ke Prosesor Aplikasi. Pada saat mulai, Secure Enclave menegosiasikan kunci jangka pendek dengan Mesin AES. Saat Secure Enclave membuka bungkus kunci file, kunci dibungkus kembali dengan kunci jangka pendek dan dikirimkan kembali ke Prosesor Aplikasi.

Metadata semua file di sistem file volume data dienkripsi dengan kunci volume acak, yang dibuat saat sistem operasi diinstal untuk pertama kalinya atau saat perangkat dihapus oleh pengguna. Kunci ini dienkripsi dan dibungkus oleh key wrapping key yang hanya diketahui oleh Secure Enclave untuk penyimpanan jangka panjang. Key wrapping key berubah setiap kali pengguna menghapus perangkat mereka. Pada SoC A9 (dan lebih baru), Secure Enclave mengandalkan entropi, dicadangkan oleh sistem anti pemutaran ulang, untuk mengaktifkan kemampuan untuk dihapus dan melindungi key wrapping key-nya, di antara aset lainnya. Untuk informasi lainnya, lihat Penyimpanan non-volatil aman.

Seperti kunci per file atau per area, kunci metadata volume data tidak pernah dipaparkan secara langsung ke Prosesor Aplikasi, sebagai gantinya, Secure Enclave menyediakan versi jangka pendek untuk setiap boot. Saat disimpan, kunci sistem file yang dienkripsi juga dibungkus oleh “kunci yang dapat dihapus” yang disimpan di Penyimpanan yang Dapat Dihapus atau oleh menggunakan key wrapping key media, yang dilindungi oleh mekanisme anti-pemutaran ulang Secure Enclave. Kunci ini tidak menyediakan kerahasiaan tambahan bagi data. Sebagai gantinya, kunci dirancang untuk dihapus dengan cepat saat diminta (oleh pengguna dengan pilihan Hapus Semua Konten & Pengaturan, atau oleh pengguna atau administrator yang menggunakan perintah penghapusan jarak jauh dari solusi mobile device management (MDM), Microsoft Exchange ActiveSync, atau iCloud). Jika kunci dihapus dengan cara ini, semua file akan menjadi tidak dapat diakses secara kriptografis.

Konten file mungkin dienkripsi dengan satu atau beberapa kunci per file (atau per area), yang dibungkus dengan kunci kelas dan disimpan di metadata file, yang pada gilirannya dienkripsi dengan kunci sistem file. Kunci kelas dilindungi dengan UID perangkat keras dan, untuk beberapa kelas, dengan kode sandi pengguna. Hierarki ini memberikan fleksibilitas dan kinerja. Misalnya, pengubahan kelas file hanya memerlukan pembungkusan ulang kunci per file-nya, dan perubahan kode sandi hanya membungkus ulang kelas kunci.

Kelas Perlindungan Data

Saat file baru dibuat di perangkat yang mendukung Perlindungan Data, file akan diberi kelas oleh app yang membuatnya. Setiap kelas menggunakan kebijakan yang berbeda untuk menentukan kapan data dapat diakses. Kelas dan kebijakan dasar dijelaskan di bagian berikut. Komputer Mac berbasis Apple silicon tidak mendukung Kelas D: Tidak Ada Perlindungan, dan batas keamanan dibangun di sekitar masuk dan keluar (bukan mengunci atau membuka seperti di iPhone, iPad, dan iPod touch).

Kelas	Jenis perlindungan
Kelas A: Perlindungan Menyeluruh	NSFileProtectionComplete
Kelas B: Dilindungi Kecuali Terbuka	NSFileProtectionCompleteUnlessOpen
Kelas C: Dilindungi Hingga Pengesahan Pengguna Pertama *Catatan:* macOS menggunakan kunci volume untuk membuat ulang karakteristik perlindungan FileVault.	NSFileProtectionCompleteUntilFirstUser Authentication
Kelas D: Tidak Ada Perlindungan *Catatan:* Tidak didukung di macOS.	NSFileProtectionNone

Perlindungan Menyeluruh

NSFileProtectionComplete: Kunci kelas dilindungi dengan kunci turunan dari kode sandi atau kata sandi pengguna dan UID perangkat. Tidak lama setelah pengguna mengunci perangkat (10 detik, jika pengaturan Memerlukan Kata Sandi adalah Segera), kunci kelas yang didekripsi dihapus, membuat semua data di kelas ini tidak dapat diakses hingga pengguna memasukkan kode sandi lagi atau membuka (masuk ke) perangkat dengan Face ID atau Touch ID.

Di macOS, tidak lama setelah pengguna terakhir keluar, kunci kelas yang didekripsi dihapus, membuat semua data di kelas ini tidak dapat diakses hingga pengguna memasukkan kode sandi lagi atau masuk ke perangkat menggunakan Touch ID.

Dilindungi Kecuali Terbuka

NSFileProtectionCompleteUnlessOpen: Beberapa file mungkin harus dituliskan saat perangkat dikunci atau pengguna keluar. Contohnya, lampiran email yang sedang diunduh di latar belakang. Perilaku ini dicapai dengan menggunakan kriptografi kurva eliptis (ECDH alih-alih Curve25519). Kunci per file yang biasa dilindungi oleh kunci yang diturunkan menggunakan Persetujuan Kunci Diffie-Hellman Satu Pass sebagaimana yang dijelaskan di NIST SP 800-56A.

Kunci publik jangka pendek untuk Persetujuan disimpan bersama kunci per file yang dibungkus. KDF adalah Fungsi Derivasi Kunci Rangkaian (Alternatif yang Disetujui 1) sebagaimana yang dijelaskan di 5.8.1 pada NIST SP 800-56A. AlgorithmID dihilangkan. PartyUInfo dan PartyVInfo masing-masing adalah kunci jangka pendek dan kunci publik statis. SHA256 digunakan sebagai fungsi hash. Segera setelah file ditutup, kunci per file akan dihapus dari memori. Untuk membuka file lagi, rahasia bersama dibuat ulang menggunakan kunci pribadi kelas Dilindungi Kecuali Terbuka dan kunci publik jangka pendek milik file, yang digunakan untuk membuka kunci per file yang kemudian digunakan untuk mendekripsi file.

Di macOS, bagian pribadi NSFileProtectionCompleteUnlessOpen dapat diakses selama pengguna apa pun di sistem masuk atau disahkan.

Dilindungi Hingga Pengesahan Pengguna Pertama

NSFileProtectionCompleteUntilFirstUserAuthentication: Kelas ini berfungsi dengan cara yang sama dengan Perlindungan Menyeluruh, kecuali bahwa kunci kelas yang didekripsi tidak dihapus dari memori saat perangkat dikunci atau pengguna keluar. Perlindungan di kelas ini memiliki properti yang mirip dengan enkripsi volume penuh desktop, dan melindungi data dari serangan yang melibatkan boot ulang. Ini adalah kelas default untuk semua data app pihak ketiga yang tidak ditetapkan ke kelas Perlindungan Data.

Di macOS, kelas ini menggunakan kunci volume yang dapat diakses asalkan volume dipasang, dan bertindak seperti FileVault.

Tidak Ada Perlindungan

NSFileProtectionNone: Kunci kelas ini hanya dilindungi dengan UID, dan disimpan di Penyimpanan Dapat Dihapus. Karena semua kunci yang diperlukan untuk mendekripsi file di kelas ini disimpan di perangkat, enkripsi hanya dapat memanfaatkan fitur penghapusan jarak jauh cepat. Jika file tidak diberi kelas Perlindungan Data, file masih akan disimpan dalam format yang dienkripsi (sebagaimana semua data di perangkat iOS dan iPadOS).

Ini tidak didukung di macOS.

Catatan: Di macOS, untuk volume yang tidak terkait dengan sistem operasi yang di-boot, semua kelas perlindungan data dapat diakses selama volume dipasang. Kelas perlindungan data default adalah NSFileProtectionCompleteUntilFirstUserAuthentication. Fungsionalitas kunci per area tersedia di Rosetta 2 dan app asli.

Kantong kunci untuk Perlindungan data

Kunci untuk file dan kelas Perlindungan Data rantai kunci dikumpulkan serta dikelola di kantong kunci di iOS, iPadOS, watchOS, dan tvOS. Sistem operasi ini menggunakan kantong kunci berikut: pengguna, perangkat, cadangan, eskrow, dan Cadangan iCloud.

Kantong kunci pengguna

Kantong kunci pengguna adalah tempat kunci kelas terbungkus yang digunakan di operasi normal perangkat disimpan. Misalnya, saat kode sandi dimasukkan, *NSFileProtectionComplete* akan dimuat dari kantong kunci pengguna dan dibuka bungkusnya. Itu merupakan file daftar properti biner (.plist) yang disimpan di kelas Tanpa Perlindungan.

Untuk perangkat dengan SoCs yang lebih awal dari A9, konten file .plist dienkripsi dengan kunci yang disimpan di Penyimpanan Dapat Dihapus. Untuk meneruskan keamanan ke kantong kunci, kunci ini dihapus dan dibuat ulang setiap kali pengguna mengubah kode sandinya.

Untuk perangkat dengan SoC A9 atau lebih baru, file .plist berisi kunci yang menunjukkan bahwa kantong kunci disimpan di loker yang dilindungi oleh nonce anti pemutaran ulang yang dikontrol Secure Enclave.

Secure Enclave mengelola kantong kunci pengguna dan dapat ditanyai perihal status kunci perangkat. Ekstensi ini melaporkan bahwa perangkat dibuka hanya jika semua kunci kelas di kantong kunci pengguna dapat diakses dan telah berhasil dibuka bungkusnya.

Kantong kunci perangkat

Kantong kunci perangkat digunakan untuk menyimpan kunci kelas terbungkus yang digunakan untuk operasi yang melibatkan data khusus perangkat. Perangkat iPadOS yang dikonfigurasi untuk penggunaan bersama kadang memerlukan akses ke info pengesahan sebelum semua pengguna masuk; oleh karena itu, kantong kunci yang tidak dilindungi oleh kode sandi pengguna akan diperlukan.

iOS dan iPadOS tidak mendukung pemisahan kriptografis atas konten sistem file per pengguna, yang berarti bahwa sistem menggunakan kunci kelas dari kantong kunci perangkat untuk membungkus kunci per file. Namun, rantai kunci menggunakan kunci kelas dari kantong kunci pengguna untuk melindungi item di rantai kunci pengguna. Di perangkat iOS dan iPadOS yang dikonfigurasi untuk digunakan oleh satu pengguna (konfigurasi default), kantong kunci perangkat dan pengguna berjumlah satu dan sama, serta dilindungi oleh kode sandi pengguna.

Kantong kunci cadangan

Kantong kunci cadangan dibuat saat cadangan terenkripsi dibuat oleh Finder (macOS 10.15 atau lebih baru) atau iTunes (di macOS 10.14 atau lebih lama) dan disimpan di komputer tempat perangkat dicadangkan. Kantong kunci baru dibuat dengan kumpulan kunci baru, dan data cadangan dienkripsi ulang ke kunci baru ini. Sebagaimana dijelaskan sebelumnya, item rantai kunci non-migrasi tetap dibungkus dengan kunci turunan UID, sehingga memungkinkan item untuk dipulihkan ke perangkat tempat asal pencadangan, tapi membuatnya tidak dapat diakses di perangkat lain.

Kantong kunci—dilindungi dengan kata sandi yang diatur—dijalankan melalui 10 juta iterasi fungsi derivasi kunci PBKDF2. Meskipun pengulangan ini berjumlah besar, tidak ada keterikatan terhadap perangkat tertentu, dan oleh karena itu serangan brute-force yang paralel di banyak komputer secara teori dapat dicoba dilakukan di kantong kunci cadangan. Ancaman ini dapat dilawan dengan kata sandi yang cukup kuat.

Jika pengguna memilih untuk tidak mengenkripsi cadangan, file cadangan tidak akan dienkripsi terlepas dari kelas Perlindungan Datanya, tapi rantai kunci akan tetap dilindungi dengan kunci turunan dari UID. Ini alasan mengapa item rantai kunci dimigrasi ke perangkat baru hanya jika kata sandi cadangan diatur.

Kantong kunci eskrow

Kantong kunci eskrow digunakan untuk penyelarasan dengan Finder (di macOS 10.15 atau lebih baru) atau iTunes (macOS 10.14 atau lebih lama) melalui USB dan mobile device management (MDM). Kantong kunci ini memungkinkan Finder atau iTunes untuk mencadangkan dan menyelaraskan tanpa mengharuskan pengguna untuk memasukkan kode sandi, dan memungkinkan solusi MDM untuk menghilangkan kode sandi pengguna dari jauh. Kantong kunci disimpan di komputer yang digunakan untuk menyelaraskan dengan Finder atau iTunes, atau di solusi MDM yang mengelola perangkat dari jauh.

Kantong kunci eskrow meningkatkan pengalaman pengguna pada saat penyelarasan perangkat, yang berpotensi memerlukan akses ke semua kelas data. Saat perangkat yang dikunci kode sandi pertama kali terhubung ke Finder atau iTunes, pengguna akan diminta untuk memasukkan kode sandi. Perangkat kemudian membuat kantong kunci eskrow berisi kunci kelas yang sama dengan kunci kelas yang digunakan di perangkat, yang dilindungi oleh kunci yang baru dibuat. Kantong kunci eskrow dan kunci yang melindunginya dibagi antara perangkat dan host atau server, dengan data yang disimpan di perangkat dalam kelas Dilindungi Hingga Pengesahan Pengguna Pertama. Inilah alasan kode sandi perangkat harus dimasukkan sebelum pengguna mencadangkan dengan Finder atau iTunes untuk pertama kalinya setelah di-boot ulang.

Pada saat pembaruan perangkat lunak secara nirkabel (OTA), pengguna dimintai kode sandinya saat memulai pembaruan. Ini digunakan untuk membuat token buka sekali pakai dengan aman yang membuka kantong kunci pengguna setelah pembaruan. Token ini tidak dapat dibuat tanpa memasukkan kode sandi pengguna, dan token yang dibuat sebelumnya menjadi tidak sah jika kode sandi pengguna berubah.

Token buka sekali pakai dapat digunakan untuk penginstalan pembaruan perangkat lunak yang diawasi atau tidak diawasi. Token dienkripsi dengan kunci turunan dari nilai penghitung monoton saat ini di Secure Enclave, UUID kantong kunci, dan UID Secure Enclave.

Di SoC A9 (dan lebih baru), token Buka sekali pakai tidak lagi mengandalkan penghitung atau Penyimpanan Dapat Dihapus. Sebagai gantinya, token dilindungi oleh nonce anti pemutaran ulang yang dikontrol Secure Enclave.

Token buka sekali pakai untuk pembaruan perangkat lunak yang diawasi kedaluwarsa setelah 20 menit. Di iOS 13 dan iPadOS 13.1 atau lebih baru, token disimpan di loker yang dilindungi oleh Secure Enclave. Sebelum iOS 13, token ini diekspor dari Secure Enclave dan ditulis ke Penyimpanan Dapat Dihapus atau dilindungi oleh mekanisme anti-pemutaran ulang Secure Enclave. Timer kebijakan menambah penghitung jika perangkat belum di-boot ulang selama 20 menit.

Pembaruan perangkat lunak yang tidak diawasi terjadi ketika sistem mendeteksi bahwa pembaruan tersedia dan saat salah satu hal berikut benar:

- Pembaruan otomatis dikonfigurasi di iOS 12 atau lebih baru.
- Pengguna memilih Instal Nanti saat diberi tahu mengenai pemberitahuan tersebut.

Setelah pengguna memasukkan kode sandinya, token buka sekali pakai akan dibuat dan dapat tetap berlaku di Secure Enclave hingga 8 jam. Jika pembaruan belum dijalankan, token buka sekali pakai ini akan dihapus pada setiap proses penguncian dan dibuat kembali pada setiap proses pembukaan berikutnya. Setiap proses pembukaan memulai ulang rentang waktu 8 jam. Setelah 8 jam, timer kebijakan akan membuat token buka sekali pakai menjadi tidak sah.

Kantong kunci Cadangan iCloud

Kantong kunci Cadangan iCloud mirip dengan kantong kunci cadangan. Semua kunci kelas di kantong kunci ini bersifat asimetris (menggunakan Curve25519, seperti kelas Perlindungan Data Dilindungi Kecuali Terbuka). Kantong kunci asimetris juga digunakan untuk cadangan di aspek pemulihan rantai kunci dari Rantai Kunci iCloud.

Melindungi kunci dalam mode boot alternatif

Perlindungan Data dirancang untuk menyediakan akses ke data pengguna hanya setelah pengesahan yang berhasil, dan hanya ke pengguna yang disahkan. Kelas perlindungan data dirancang untuk mendukung berbagai kasus penggunaan, seperti kemampuan untuk membaca dan menulis beberapa data bahkan saat perangkat terkunci (tapi setelah pertama kali dibuka). Langkah tambahan diambil untuk melindungi akses ke data pengguna selama mode boot alternatif seperti langkah yang digunakan untuk mode Peningkatan Firmware Perangkat (DFU), mode Pemulihan, Diagnostik Apple, atau bahkan selama pembaruan perangkat lunak. Kemampuan ini didasarkan pada gabungan fitur perangkat keras dan perangkat lunak, serta telah diperluas karena silicon rancangan Apple telah berkembang.

Fitur	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, Kelompok M1
Pemulihan: Semua Kelas Perlindungan Data yang dilindungi	✓	✓	✓	✓	✓
Boot alternatif mode DFU, Pemulihan, dan pembaruan perangkat lunak: Data kelas A, B, dan C yang dilindungi		✓	✓	✓	✓

Mesin AES Secure Enclave dilengkapi dengan bit seeding perangkat lunak yang dapat dikunci. Jika kunci dibuat dari UID, bit seeding ini disertakan di fungsi derivasi kunci untuk membuat hierarki kunci tambahan. Penggunaan bit seeding bergantung pada sistem pada keping:

- Mulai dari SoC Apple A10 dan S3, bit seeding didedikasikan untuk membedakan kunci yang dilindungi oleh kode sandi pengguna. Bit seeding diatur untuk kunci yang memerlukan kode sandi pengguna (termasuk kunci Perlindungan Data Kelas A, Kelas B, dan Kelas C), dan dibersihkan untuk kunci yang tidak memerlukan kode sandi pengguna (termasuk kunci metadata sistem file dan kunci Kelas D).
- Di iOS 13 atau lebih baru dan iPadOS 13.1 atau lebih baru di perangkat dengan A10 atau lebih baru, semua data pengguna dibuat tidak dapat diakses secara kriptografis saat perangkat di-boot ke Mode Diagnostik. Ini dicapai dengan memperkenalkan bit seeding tambahan yang pengaturannya mengatur kemampuan untuk mengakses kunci media, yang diperlukan untuk mengakses metadata (dan oleh karenanya meliputi juga konten dari semua file) pada volume data terenkripsi dengan Perlindungan Data. Perlindungan ini meliputi file yang terlindungi di semua kelas (A, B, C, dan D), bukan hanya file yang memerlukan kode sandi pengguna.
- Pada SoC A12, ROM Boot Secure Enclave mengunci bit seeding kode sandi jika Prosesor Aplikasi telah memasuki mode Peningkatan Firmware Perangkat (DFU) atau Mode Pemulihan. Saat bit seeding kode sandi dikunci, operasi untuk mengubahnya tidak akan diizinkan. Ini dirancang untuk mencegah akses ke data yang dilindungi dengan kode sandi pengguna.

Jika dipulihkan setelah memasuki mode DFU, perangkat akan kembali ke kondisi baik yang diketahui sambil memastikan bahwa hanya ada kode bertanda tangan Apple yang tidak dimodifikasi. Mode DFU dapat diaktifkan secara manual.

Lihat artikel Dukungan Apple berikut mengenai cara mengaktifkan mode DFU di perangkat:

Perangkat	Artikel
iPhone, iPad, iPod touch	Jika Anda lupa kode sandi iPhone Anda
Apple TV	Jika Anda melihat simbol peringatan di Apple TV
Mac dengan Apple silicon	Memulihkan atau mengaktifkan kembali Mac dengan Apple silicon

Melindungi data pengguna saat diserang

Penyerang yang mencoba mengekstrak data pengguna sering kali mencoba sejumlah teknik: mengekstrak data yang dienkripsi ke medium lain untuk serangan brute-force, memanipulasi versi sistem operasi, atau mengubah atau melemahkan kebijakan keamanan perangkat untuk memudahkan serangan. Penyerangan data di perangkat sering kali memerlukan komunikasi dengan perangkat menggunakan antarmuka fisik seperti Lightning atau USB. Perangkat Apple disertai dengan fitur yang membantu mencegah serangan tersebut.

Perangkat Apple mendukung teknologi yang disebut *Perlindungan Kunci yang Disegel (SKP)* yang dirancang untuk memastikan materi kriptografis tidak tersedia di luar perangkat, atau yang digunakan jika manipulasi dibuat ke versi sistem operasi atau pengaturan keamanan tanpa pengesahan pengguna yang tepat. Fitur ini *tidak* disediakan oleh Secure Enclave, melainkan didukung oleh register perangkat keras yang ada di lapisan bawah agar dapat menyediakan lapisan perlindungan tambahan ke kunci yang penting untuk mendekripsi data pengguna yang independen dari Secure Enclave.

Catatan: SKP hanya tersedia di perangkat dengan SoC rancangan Apple.

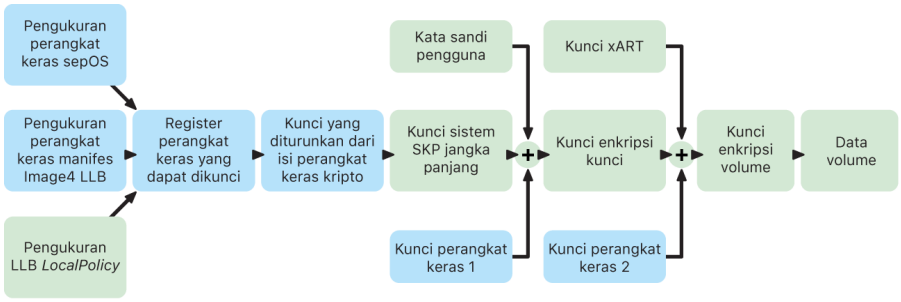
Fitur	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, Kelompok M1
Perlindungan Kunci yang Disegel	✓	✓	✓	✓	✓

iPhone dan iPad juga dapat dikonfigurasi untuk hanya mengaktifkan koneksi data dalam kondisi yang mengindikasikan perangkat masih dalam kontrol pengguna yang disahkan secara fisik.

Perlindungan Kunci yang Disegel (SKP)

Di perangkat Apple yang mendukung Perlindungan Data, kunci enkripsi kunci (KEK) dilindungi (atau disegel) dengan pengukuran perangkat lunak di sistem, serta terikat ke UID yang hanya tersedia dari Secure Enclave. Di Mac dengan Apple silicon, perlindungan KEK diperkuat lebih jauh dengan menggabungkan informasi mengenai kebijakan keamanan di sistem, karena macOS mendukung perubahan kebijakan keamanan penting (misalnya, menonaktifkan boot aman atau SIP) yang tidak didukung di platform lain. Di Mac dengan Apple silicon, perlindungan ini mencakup kunci FileVault, karena FileVault diimplementasikan menggunakan Perlindungan Data (Kelas C).

Kunci yang dihasilkan dari pengaitan kata sandi pengguna, kunci SKP jangka panjang, dan kunci Perangkat Keras 1 (UID dari Secure Enclave) disebut *kunci turunan kata sandi*. Kunci ini digunakan untuk melindungi kantong kunci pengguna (di semua platform yang didukung) dan KEK (hanya di macOS), lalu mengaktifkan buka biometrik atau buka otomatis dengan perangkat lainnya seperti Apple Watch.



Monitor Boot Secure Enclave menangkap pengukuran OS Secure Enclave yang dimuat. Saat ROM Boot Prosesor Aplikasi mengukur manifes Image4 yang terpasang ke LLB, manifes tersebut berisi pengukuran semua firmware yang dipasangkan dengan sistem lainnya yang juga dimuat. LocalPolicy berisi konfigurasi keamanan inti untuk macOS yang dimuat. LocalPolicy juga berisi bidang `nsih` yang merupakan hash manifes Image4 macOS. Manifes Image4 macOS berisi pengukuran semua firmware yang dipasangkan dengan macOS dan objek boot macOS inti seperti Kumpulan Kernel Boot atau hash root volume sistem yang ditandatangani (SSV).

Jika penyerang dapat dengan tidak terduga mengubah salah satu komponen konfigurasi firmware, perangkat lunak, atau keamanan terukur di atas, komponen akan memodifikasi pengukuran yang disimpan di register perangkat keras. Modifikasi pengukuran menyebabkan *kunci root pengukuran sistem (SMRK)* yang diturunkan dari perangkat keras kripto untuk diturunkan ke nilai berbeda, yang secara efektif membuka segel di hierarki kunci. Hal ini menyebabkan *kunci perangkat pengukuran sistem (SMDK)* tidak dapat diakses, yang pada gilirannya menyebabkan KEK, yang pada akibatnya data tidak dapat diakses.

Namun, saat diserang, sistem harus mengakomodasi pembaruan perangkat lunak asli yang mengubah pengukuran firmware dan bidang `nsih` di LocalPolicy untuk menunjuk ke pengukuran macOS baru. Di sistem lain yang berupaya untuk menggabungkan pengukuran firmware tapi tidak memiliki sumber kebenaran yang diketahui baik, pengguna diharuskan untuk menonaktifkan keamanan, memperbarui firmware, lalu mengaktifkan ulang sehingga garis dasar pengukuran baru dapat ditangkap. Hal ini meningkatkan risiko penyerang merusak firmware selama pembaruan perangkat lunak secara signifikan. Sistem dibantu oleh fakta bahwa manifes Image4 berisi semua pengukuran yang diperlukan. Perangkat keras yang mendekripsi SMDK dengan SMRK saat pengukuran cocok selama boot normal juga dapat mengenkripsi SMDK ke SMRK mendatang yang diajukan. Dengan menentukan pengukuran yang diharapkan setelah pembaruan perangkat lunak, perangkat keras dapat mengenkripsi SMDK yang dapat diakses di sistem operasi saat ini, sehingga tetap dapat diakses di sistem operasi mendatang. Serupa dengan hal sebelumnya, saat pelanggan secara sah mengubah pengaturan keamanannya di LocalPolicy, SMDK harus dienkripsi ke SMRK mendatang berdasarkan pengukuran untuk LocalPolicy yang dikomputasi oleh LLB pada mulai ulang berikutnya.

Mengaktifkan koneksi data dengan aman di iOS dan iPadOS

Di perangkat iOS atau iPadOS, jika tidak ada koneksi data yang dibuat baru-baru ini, pengguna harus menggunakan Face ID, Touch ID, atau kode sandi untuk mengaktifkan koneksi data melalui antarmuka Lightning, USB, atau Smart Connector. Ini membatasi serangan permukaan terhadap perangkat yang tersambung secara fisik seperti pengisi daya berbahaya selagi masih mengaktifkan penggunaan aksesori lainnya dalam jangka waktu yang wajar. Jika lebih dari satu jam telah berlalu sejak perangkat iOS atau iPadOS dikunci atau sejak koneksi data aksesori diputus, perangkat tidak akan mengizinkan koneksi data baru untuk dibuat hingga perangkat dibuka. Selama periode satu jam ini, hanya koneksi data dari aksesori yang sebelumnya telah disambungkan ke perangkat saat dalam status terbuka yang akan diizinkan. Aksesori ini diingat selama 30 hari setelah aksesori terakhir terhubung. Upaya oleh aksesori yang tidak diketahui untuk membuka koneksi data selama periode waktu ini akan menonaktifkan semua koneksi data aksesori melalui Lightning, USB, dan Smart Connector hingga perangkat dibuka lagi. Periode satu jam ini:

- Membantu memastikan bahwa pengguna yang sering menyambungkan perangkat ke Mac atau PC, aksesori, atau ke CarPlay tidak perlu memasukkan kode sandi setiap kali mereka memasangkan perangkat
- Penting karena ekosistem aksesori tidak menyediakan cara yang andal secara kriptografis untuk mengidentifikasi aksesori sebelum membuat koneksi data

Selain itu, jika telah lebih dari 3 hari sejak koneksi data dibuat dengan aksesori, perangkat tidak akan mengizinkan koneksi data baru segera setelah perangkat terkunci. Ini bertujuan untuk meningkatkan perlindungan bagi pengguna yang tidak sering menggunakan aksesori tersebut. Koneksi data melalui Lightning, USB, dan Smart Connector juga dinonaktifkan setiap kali perangkat berada dalam kondisi yang membuatnya memerlukan kode sandi untuk mengaktifkan ulang pengesahan biometrik.

Pengguna dapat memilih untuk mengaktifkan kembali koneksi data selalu nyala di Pengaturan (pengaturan sebagian perangkat asistif akan melakukan ini secara otomatis).

Peran Apple File System

Apple File System (APFS) merupakan sistem file khusus yang dirancang dengan mengutamakan enkripsi. APFS berfungsi di semua platform Apple—untuk iPhone, iPad, iPod touch, Mac, Apple TV, dan Apple Watch. Dioptimalkan untuk penyimpanan Kilat/SSD, APFS dilengkapi dengan enkripsi yang kuat, metadata salin saat tulis, berbagi ruang, klon file dan direktori, snapshot, pengubahan ukuran direktori dengan cepat, primitif penyimpanan aman atomik, dan fondasi sistem file yang lebih baik, serta desain salin saat tulis yang unik yang menggunakan paduan I/O untuk memberikan kinerja maksimum sekaligus memastikan keterandalan data.

Berbagi ruang

APFS mengalokasikan ruang penyimpanan sesuai permintaan. Jika satu wadah APFS memiliki beberapa volume, ruang kosong wadah tersebut dibagikan dan hanya dapat dialokasikan ke salah satu volume terpisah sebagaimana diperlukan. Setiap volume hanya menggunakan bagian dari seluruh wadah, sehingga ruang yang tersedia adalah ukuran total wadah, dikurangi ruang yang digunakan di semua volume di wadah.

Beberapa volume

Di macOS 10.15 atau lebih baru, wadah APFS yang digunakan untuk memulai Mac harus berisi setidaknya lima volume, tiga volume pertama disembunyikan dari pengguna:

- *Volume pra-boot:* Volume ini tidak dienkripsi dan berisi data yang diperlukan untuk melakukan boot setiap volume sistem di wadah.
- *Volume VM:* Volume ini tidak dienkripsi dan digunakan oleh macOS untuk menyimpan file pertukaran yang dienkripsi.
- *Volume pemulihan:* Volume ini tidak dienkripsi dan harus tersedia tanpa membuka volume sistem agar dapat dimulai di recoveryOS.
- *Volume sistem:* Berisi yang berikut:
  - Semua file yang diperlukan untuk memulai Mac
  - Semua app asli yang terinstal di macOS (app yang dulunya disimpan di folder /Aplikasi kini disimpan di /Sistem/Aplikasi)

  Catatan: Secara default, tidak ada proses yang dapat menulisi volume Sistem, bahkan proses sistem Apple.
- *Volume data:* Berisi data yang dapat berubah, seperti:
  - Semua data di dalam folder pengguna, termasuk foto, musik, video, dan dokumen
  - App yang diinstal pengguna, termasuk AppleScript dan aplikasi Automator
  - Kerangka dan daemon khusus yang diinstal oleh pengguna, organisasi, atau app pihak ketiga
  - Lokasi lainnya yang dimiliki dan ditulis oleh pengguna, seperti /Aplikasi, /Perpustakaan, /Pengguna, /Volume, /usr/local, /private, dan /tmp

Volume data dibuat untuk setiap volume sistem tambahan. Volume pra-boot, VM, dan pemulihan dibagikan dan tidak diduplikatkan.

Di macOS 11 atau lebih baru, volume sistem ditangkap dalam snapshot. Sistem operasi di-boot dari snapshot volume sistem, bukan hanya pemasangan hanya baca pada volume sistem yang dapat berubah.

Di iOS dan iPadOS, penyimpanan dibagi setidaknya ke dalam dua volume APFS:

- Volume sistem
- Volume data

Perlindungan data rantai kunci

Banyak app yang harus menangani kata sandi dan data pendek namun sensitif lainnya, seperti kunci dan token masuk. Rantai kunci menyediakan cara yang aman untuk menyimpan item ini. Berbagai sistem operasi Apple menggunakan mekanisme berbeda untuk memperkuat jaminan terkait dengan kelas perlindungan rantai kunci yang berbeda. Di macOS (termasuk Mac dengan Apple silicon), Perlindungan Data tidak digunakan secara langsung untuk memperkuat jaminan ini.

Tinjauan

Item rantai kunci dienkripsi menggunakan dua kunci AES-256-GCM yang berbeda, kunci tabel (metadata), dan kunci per baris (kunci rahasia). Metadata rantai kunci (semua atribut selain kSecValue) dienkripsi dengan kunci metadata untuk mempercepat pencarian, dan nilai rahasia (kSecValueData) dienkripsi dengan kunci rahasia. Kunci metadata dilindungi oleh Secure Enclave, tapi disimpan dalam cache di Prosesor Aplikasi untuk memungkinkan dijalankannya permintaan cepat rantai kunci. Kunci rahasia selalu memerlukan perpindahan bolak-balik melalui Secure Enclave.

Rantai kunci diterapkan sebagai database SQLite, yang disimpan di sistem file. Hanya ada satu database, dan daemon `securityd` menentukan item rantai kunci mana yang dapat diakses tiap proses atau app. API Akses Rantai Kunci membuat panggilan ke daemon, yang meminta hak “Keychain-access-groups”, “application-identifier”, dan “application-group” milik app. Alih-alih membatasi akses ke satu proses, grup akses mengizinkan item rantai kunci untuk dibagikan antar-app.

Item rantai kunci hanya dapat dibagikan antar-app dari pengembang yang sama. Untuk membagikan item rantai kunci, app pihak ketiga menggunakan grup akses dengan prefiks yang disediakan melalui Apple Developer Program di grup aplikasinya. Persyaratan prefiks dan keunikan grup aplikasi diberlakukan melalui penandatanganan kode, penyediaan profil, dan Apple Developer Program.

Data rantai kunci dilindungi menggunakan struktur kelas yang mirip dengan yang digunakan di Perlindungan Data file. Kelas ini memiliki perilaku yang sama dengan kelas Perlindungan Data file tapi menggunakan kunci dan fungsi yang khas.

Ketersediaan	Perlindungan data file	Perlindungan data rantai kunci
Saat terbuka	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Saat dikunci	NSFileProtectionCompleteUnlessOpen	-

Ketersediaan	Perlindungan data file	Perlindungan data rantai kunci
Setelah pertama kali dibuka	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Selalu	NSFileProtectionNone	kSecAttrAccessibleAlways
Kode sandi diaktifkan	-	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

App yang menggunakan layanan penyegaran latar belakang dapat menggunakan *kSecAttrAccessibleAfterFirstUnlock* untuk item rantai kunci yang harus diakses saat pembaruan latar belakang.

Kelas *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* berperilaku sama dengan *kSecAttrAccessibleWhenUnlocked*, namun hanya tersedia saat perangkat dikonfigurasi dengan kode sandi. Kelas ini hanya terdapat di kantong kunci sistem; kelas ini:

- Tidak diselaraskan ke Rantai Kunci iCloud
- Tidak dicadangkan
- Tidak disertakan di kantong kunci eskrow

Jika kode sandi dihapus atau diatur ulang, item menjadi tidak berguna dengan menghapus kunci kelas.

Kelas rantai kunci lainnya memiliki versi “Hanya perangkat ini”, yang selalu dilindungi dengan UID saat disalin dari perangkat selama pencadangan, membuatnya tidak berguna jika dipulihkan ke perangkat lain. Apple memiliki keamanan dan kegunaan yang berimbang dengan memilih kelas rantai kunci yang bergantung pada jenis informasi yang diamankan dan saat diperlukan oleh iOS dan iPadOS. Misalnya, sertifikat VPN harus selalu tersedia sehingga perangkat memiliki koneksi yang berkelanjutan, tapi diklasifikasikan sebagai “non-migrasi”, sehingga tidak dapat dipindahkan ke perangkat lain.

Perlindungan kelas data rantai kunci

Perlindungan kelas yang tercantum di bawah diberlakukan untuk item rantai kunci.

Item	Dapat Diakses
Kata sandi Wi-Fi	Setelah pertama kali dibuka
Akun Mail	Setelah pertama kali dibuka
Akun Microsoft Exchange ActiveSync	Setelah pertama kali dibuka
Kata sandi VPN	Setelah pertama kali dibuka
LDAP, CalDAV, CardDAV	Setelah pertama kali dibuka
Token akun jejaring sosial	Setelah pertama kali dibuka
Kunci enkripsi iklan Handoff	Setelah pertama kali dibuka
Token iCloud	Setelah pertama kali dibuka
Kunci iMessage	Setelah pertama kali dibuka

Item	Dapat Diakses
Kata sandi berbagi rumah	Saat terbuka
Kata sandi Safari	Saat terbuka
Penanda Safari	Saat terbuka
Cadangan Finder/iTunes	Saat dibuka, non-migrasi
Kunci pribadi yang diinstal oleh profil konfigurasi	Saat dibuka, non-migrasi
Sertifikat VPN	Selalu, non-migrasi
Kunci Bluetooth®	Selalu, non-migrasi
Token layanan Pemberitahuan Push Apple (APN)	Selalu, non-migrasi
Sertifikat iCloud dan kunci pribadi	Selalu, non-migrasi
PIN SIM	Selalu, non-migrasi
Sertifikat yang diinstal oleh profil konfigurasi	Selalu
Token Lacak	Selalu
Pesan Suara	Selalu

Kontrol akses rantai kunci

Rantai kunci dapat menggunakan daftar kontrol akses (ACL) untuk mengatur kebijakan aksesibilitas dan persyaratan pengesahan. Item dapat menciptakan situasi yang memerlukan keberadaan pengguna dengan menetapkan bahwa item tidak dapat diakses kecuali disahkan menggunakan Face ID, Touch ID, atau memasukkan kode sandi atau kata sandi perangkat. Akses ke item juga dapat dibatasi dengan menetapkan bahwa pendaftaran Face ID atau Touch ID belum berubah sejak item ditambahkan. Pembatasan ini membantu mencegah penyerang untuk menambahkan sidik jari mereka untuk mengakses item rantai kunci. ACL dievaluasi di dalam Secure Enclave dan dilepaskan ke kernel hanya jika batasannya yang ditetapkan dipenuhi.

Arsitektur rantai kunci di macOS

macOS juga menyediakan akses ke rantai kunci untuk menyimpan dengan mudah dan aman nama pengguna dan kata sandi, identitas digital, kunci enkripsi, serta catatan aman. Rantai kunci dapat diakses dengan membuka app Akses Rantai Kunci di /Aplikasi/Utilitas/. Dengan menggunakan rantai kunci, pengguna tidak perlu memasukkan—atau bahkan mengingat—info pengesahan untuk setiap sumber. Rantai kunci default awal dibuat untuk setiap pengguna Mac, meskipun pengguna dapat membuat rantai kunci lain untuk tujuan tertentu.

Selain bergantung pada rantai kunci pengguna, macOS mengandalkan sejumlah rantai kunci tingkat sistem yang memelihara aset pengesahan yang tidak bersifat khusus untuk pengguna, seperti info pengesahan jaringan dan identitas infrastruktur kunci publik (PKI). Salah satu rantai kunci ini, Dasar Sistem, bersifat tetap dan menyimpan sertifikat otoritas sertifikat dasar (CA) PKI internet untuk memfasilitasi tugas umum seperti perbankan online dan perdagangan elektronik. Sama halnya, pengguna dapat menyebarkan sertifikat CA yang disediakan secara internal ke komputer Mac untuk membantu validasi situs dan layanan internal.

FileVault

Enkripsi volume dengan FileVault di macOS

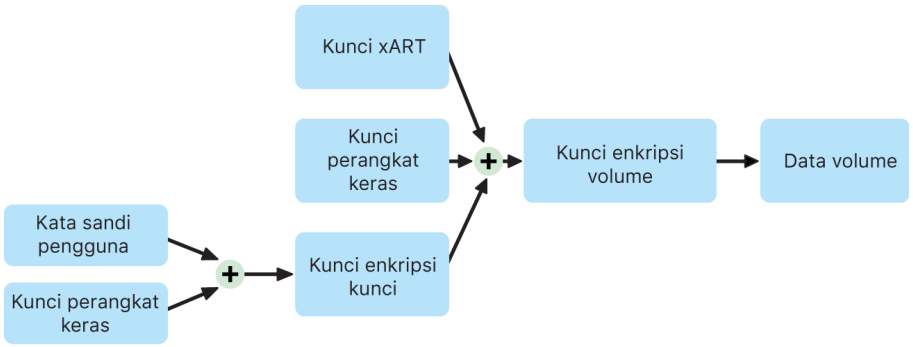
Komputer Mac menawarkan FileVault, kemampuan enkripsi internal untuk mengamankan semua data pada saat disimpan. FileVault menggunakan algoritme enkripsi data AES-XTS untuk melindungi volume lengkap di perangkat penyimpan internal dan eksternal.

FileVault di Mac dengan Apple silicon diimplementasikan menggunakan Perlindungan Data Kelas C dengan kunci volume. Di Mac dengan Keping Keamanan T2 Apple serta Mac dengan Apple silicon, perangkat penyimpanan internal terenkripsi yang tersambung secara langsung ke Secure Enclave memanfaatkan kemampuan keamanan perangkat kerasnya serta kemampuan mesin AES. Setelah pengguna menyalakan FileVault di Mac, info pengesahannya diperlukan selama proses boot.

Penyimpanan internal dengan FileVault dinyalakan

Tanpa info pengesahan masuk yang valid atau kunci pemulihan kriptografis, volume APFS internal tetap terenkripsi dan dilindungi dari akses yang tidak sah, bahkan jika perangkat penyimpanan fisik dilepas dan disambungkan ke komputer lain. Di macOS 10.15, ini termasuk volume sistem dan volume data. Dimulai dari macOS 11, volume sistem dilindungi oleh fitur volume sistem yang ditandatangani (SSV), tetapi volume data tetap dilindungi oleh enkripsi. Enkripsi volume internal di Mac dengan Apple silicon serta komputer Mac dengan keping T2 diterapkan dengan mengonstruksi dan mengelola hierarki kunci, dan memanfaatkan teknologi enkripsi perangkat keras yang terdapat dalam keping. Hierarki kunci ini dirancang untuk mencapai empat target secara bersamaan:

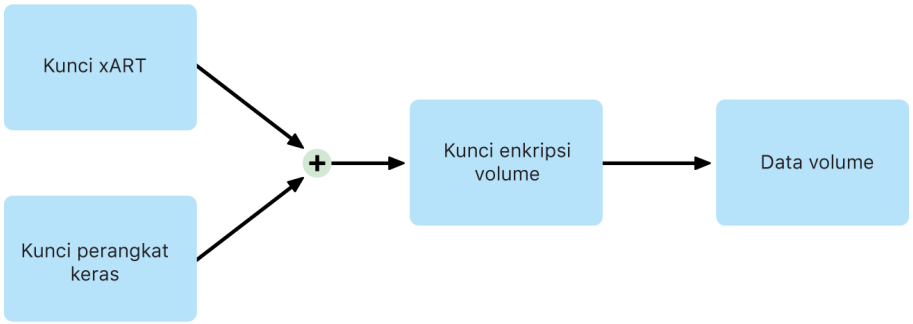
- Mengharuskan kata sandi pengguna untuk dekripsi
- Melindungi sistem dari serangan brute-force secara langsung terhadap media penyimpanan yang dilepas dari Mac
- Menyediakan metode yang cepat dan aman untuk menghapus konten dengan menghapus materi kriptografis yang diperlukan
- Memungkinkan pengguna untuk mengubah kata sandi mereka (dan pada gilirannya kunci kriptografis yang digunakan untuk melindungi file mereka) tanpa mengharuskan seluruh volume untuk dienkripsi ulang



Di Mac dengan Apple silicon dan Mac dengan keping T2, semua penanganan kunci FileVault berlangsung di Secure Enclave; kunci enkripsi tidak pernah terpapar secara langsung ke CPU Intel. Semua volume APFS dibuat dengan kunci enkripsi volume secara default. Konten volume dan metadata dienkripsi dengan kunci enkripsi volume ini, yang dibungkus dengan kunci kelas. Kunci kelas ini dilindungi oleh kombinasi kata sandi pengguna dan UID perangkat keras saat FileVault dinyalakan.

Penyimpanan internal dengan FileVault dimatikan

Jika FileVault tidak dinyalakan di Mac dengan Apple silicon atau Mac dengan keping T2 selama proses Asisten Pengaturan awal, volume tetap terenkripsi tapi kunci enkripsi volume hanya dilindungi oleh UID perangkat keras di Secure Enclave.



Jika FileVault dinyalakan di kesempatan berikutnya—proses yang berlangsung karena data telah dienkripsi—mekanisme anti-pemutaran ulang membantu menghalangi kunci lama (hanya berbasis UID perangkat keras) sehingga tidak dapat digunakan untuk mendekripsi volume. Volume kemudian dilindungi oleh kombinasi kata sandi pengguna dan UID perangkat keras sebagaimana dijelaskan berikutnya.

Menghapus volume FileVault

Saat menghapus volume, kunci enkripsi volumenya dihapus dengan aman oleh Secure Enclave. Ini membantu mencegah akses di masa mendatang dengan kunci ini bahkan oleh Secure Enclave. Selain itu, semua kunci enkripsi volume dibungkus dengan kunci media. Kunci media tidak menyediakan kerahasiaan tambahan untuk data; tapi sebagai gantinya, dirancang untuk memungkinkan penghapusan data dengan cepat dan aman karena tanpanya, dekripsi tidak akan memungkinkan.

Di Mac dengan Apple silicon dan Mac dengan keping T2, kunci media akan dihapus oleh teknologi dukungan Secure Enclave—misalnya oleh perintah MDM jarak jauh. Jika kunci media dihapus dengan cara ini, volume akan menjadi tidak dapat diakses secara kriptografis.

Perangkat penyimpanan yang dapat dilepas

Enkripsi perangkat penyimpanan yang dapat dilepas tidak menggunakan kemampuan keamanan Secure Enclave, dan enkripsinya dijalankan dengan cara yang sama dengan Mac berbasis Intel tanpa keping T2.

Mengelola FileVault di macOS

Di macOS, organisasi dapat mengelola FileVault menggunakan SecureToken atau Token Bootstrap.

Menggunakan Token Aman

Apple File System (APFS) di macOS 10.13 atau lebih baru mengubah bagaimana kunci enkripsi FileVault dibuat. Di versi macOS sebelumnya di volume CoreStorage, kunci yang digunakan di proses enkripsi FileVault dibuat saat pengguna atau organisasi menyalakan FileVault di Mac. Pada macOS di volume APFS, kunci dibuat selama pembuatan pengguna, pengaturan kata sandi pengguna pertama, atau selama proses masuk pertama oleh pengguna Mac. Penerapan kunci enkripsi ini, saat mereka dibuat, dan bagaimana mereka disimpan adalah bagian dari fitur yang disebut *Token Aman*. Secara spesifik, token aman adalah versi kunci enkripsi kunci (KEK) yang dibungkus dan dilindungi oleh kata sandi pengguna.

Saat menyebarkan FileVault di APFS, pengguna dapat terus:

- Menggunakan alat dan proses yang ada, seperti kunci pemulihan pribadi (PRK) yang dapat disimpan dengan solusi mobile device management (MDM) untuk eskrow
- Membuat dan menggunakan kunci pemulihan institusional (IRK)
- Menangguhkan pengaktifan FileVault hingga pengguna masuk atau keluar dari Mac

Di macOS 11, mengatur kata sandi awal untuk pengguna paling pertama di Mac akan membuat pengguna tersebut memiliki token aman. Dalam beberapa alur kerja, hal ini mungkin tidak diharapkan, karena sebelumnya, memberikan token aman pertama akan mengharuskan akun pengguna untuk masuk. Untuk mencegah hal ini terjadi, tambahkan `;DisabledTags;SecureToken` ke atribut `AuthenticationAuthority` pengguna yang dibuat dengan program sebelum mengatur kata sandi pengguna, seperti yang ditampilkan di bawah:

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

Menggunakan Token Bootstrap

macOS 10.15 memperkenalkan fitur baru—*Token Bootstrap*—untuk membantu pemberian token aman ke akun bergerak dan akun administrator yang dibuat pendaftaran perangkat opsional (“administrator terkelola”). Di macOS 11, token bootstrap dapat memberikan token aman ke pengguna mana pun yang masuk ke komputer Mac, termasuk akun pengguna lokal. Penggunaan fitur Token Bootstrap dari macOS 10.15 atau lebih baru memerlukan:

- Pendaftaran Mac di MDM menggunakan Apple School Manager atau Apple Business Manager, yang membuat Mac diawasi
- Dukungan vendor MDM

Di macOS 10.15.4 atau lebih baru, token bootstrap dibuat dan dieskrow ke MDM pada masuk pertama kali oleh pengguna mana pun dengan Token Aman yang diaktifkan jika solusi MDM mendukung fitur tersebut. Token bootstrap juga dapat dibuat dan dieskrow ke MDM menggunakan alat baris perintah `profiles`, jika perlu.

Di macOS 11, token bootstrap juga dapat digunakan untuk lebih dari sekadar memberikan token aman ke akun pengguna. Di Mac dengan Apple silicon, token bootstrap, jika tersedia, dapat digunakan untuk mengesahkan penginstalan ekstensi kernel dan pembaruan perangkat lunak saat dikelola menggunakan MDM.

Cara Apple melindungi data pribadi pengguna

Melindungi akses app ke data pengguna

Selain mengenkripsi data pada saat disimpan, Perangkat Apple membantu mencegah app untuk mengakses informasi pribadi milik pengguna tanpa izin menggunakan berbagai teknologi termasuk Vault Data. Di Pengaturan di iOS dan iPadOS, atau Preferensi Sistem di macOS, pengguna dapat melihat app mana yang mereka izinkan untuk mengakses informasi tertentu, serta memberikan atau membatalkan akses tertentu pada masa mendatang. Akses diberlakukan di app berikut:

- *iOS, iPadOS, dan macOS:* Kalender, Kamera, Kontak, Mikrofon, Foto, Pengingat, Pengenalan ucapan
- *iOS dan iPadOS:* Bluetooth, Rumah, Media, app Media dan Apple Music, Gerakan serta kebugaran
- *iOS dan watchOS:* Kesehatan
- *macOS:* Pengawasan input (misalnya, penekanan papan ketik), Perintah, Rekaman layar (misalnya, jepretan dan video layar diam), Preferensi Sistem

Di iOS 13.4 atau lebih baru dan iPadOS 13.4 atau lebih baru, semua app pihak ketiga secara otomatis melindungi datanya di Vault Data. Vault Data membantu melindungi dari akses tanpa izin ke data, bahkan dari proses yang tidak disandbox. Kelas tambahan di iOS 15 atau lebih baru menyertakan Jaringan Lokal, Interaksi Di Sekitar, Sensor Riset & Data Penggunaan, dan Fokus.

Jika pengguna masuk ke iCloud, app di iOS dan iPadOS diberi akses secara default ke iCloud Drive. Pengguna dapat mengontrol setiap akses app di iCloud di Pengaturan. iOS dan iPadOS juga menyediakan pembatasan yang dirancang untuk mencegah perpindahan data antara app dan akun yang diinstal oleh solusi mobile device management (MDM) dan yang diinstal oleh pengguna.

Melindungi akses ke data kesehatan pengguna

HealthKit menyediakan repositori pusat untuk data kesehatan dan kebugaran di iPhone serta Apple Watch. HealthKit juga dapat digunakan langsung dengan perangkat kesehatan dan kebugaran seperti monitor detak jantung Bluetooth Rendah Energi (BLE) yang kompatibel dan koprosesor gerakan yang terdapat di banyak perangkat iOS. Semua interaksi HealthKit dengan app kesehatan dan kebugaran, badan layanan kesehatan, serta perangkat kesehatan dan kebugaran memerlukan izin pengguna. Data ini disimpan di kelas Perlindungan Data Dilindungi Kecuali Terbuka. Akses ke data dinonaktifkan 10 menit setelah perangkat dikunci dan data akan dapat diakses lain kali pengguna memasukkan kode sandinya atau menggunakan Face ID atau Touch ID untuk membuka perangkat.

Mengumpulkan dan menyimpan data kesehatan serta kebugaran

HealthKit juga mengumpulkan dan menyimpan data pengelolaan, seperti izin akses untuk app, nama perangkat yang terhubung ke HealthKit, dan informasi jadwal yang digunakan untuk meluncurkan app saat data baru tersedia. Data ini disimpan di kelas Perlindungan Data Dilindungi Hingga Pengesahan Pengguna Pertama. File jurnal sementara menyimpan rekaman kesehatan yang dibuat saat perangkat terkunci, seperti saat pengguna berolahraga. Ini disimpan di kelas Perlindungan Data Dilindungi Kecuali Terbuka. Ketika perangkat dibuka, file jurnal sementara diimpor ke database kesehatan utama, lalu dihapus setelah penggabungan selesai.

Data Kesehatan dapat disimpan di iCloud. Enkripsi ujung ke ujung untuk data Kesehatan memerlukan iOS 12 atau lebih baru dan autentikasi dua faktor. Jika tidak, data pengguna masih terenkipsi saat disimpan dan ditransmisikan, tapi tidak dienkripsi dengan metode ujung ke ujung. Setelah pengguna menyalakan autentikasi dua faktor dan memperbarui ke iOS 12 atau lebih baru, data kesehatan pengguna dimigrasi ke enkripsi ujung ke ujung.

Jika pengguna mencadangkan perangkatnya menggunakan Finder (di macOS 10.15 atau lebih baru) atau iTunes (macOS 10.14 atau lebih lama), data kesehatan hanya disimpan jika cadangan dienkripsi.

Catatan kesehatan klinis

Pengguna dapat masuk ke sistem kesehatan yang didukung di dalam app Kesehatan untuk mendapatkan salinan catatan kesehatan klinis mereka. Saat menghubungkan pengguna ke sistem kesehatan, pengguna mengesahkan menggunakan info pengesahan klien OAuth 2. Setelah menghubungkan, data catatan kesehatan klinis akan diunduh secara langsung dari institusi kesehatan menggunakan koneksi yang dilindungi TLS 1.3. Setelah diunduh, catatan kesehatan klinis akan disimpan dengan aman bersama data kesehatan lainnya.

Integritas data Kesehatan

Data yang disimpan di database meliputi metadata untuk melacak sumber setiap rekaman data. Metadata ini berisi pengenal app yang mengidentifikasi app yang disimpan di rekaman. Selain itu, item metadata opsional dapat berisi salinan rekaman yang ditandatangani secara digital. Ini dimaksudkan untuk menyediakan integritas data untuk rekaman yang dibuat oleh perangkat tepercaya. Format yang digunakan untuk tanda tangan digital adalah Sintaksis Pesan Kriptografi (CMS) yang tercantum di RFC 5652.

Akses data Kesehatan oleh app pihak ketiga

Akses ke API HealthKit dikontrol dengan hak, dan app harus menaati pembatasan mengenai cara menggunakan data. Misalnya, app tidak diizinkan untuk menggunakan data kesehatan untuk pengiklanan. App juga diharuskan untuk menyediakan kebijakan privasi yang merinci penggunaan data kesehatan kepada pengguna.

Akses app ke data kesehatan dikontrol oleh pengaturan Privasi pengguna. Pengguna diminta untuk memberikan akses saat app meminta akses ke data kesehatan, sama dengan Kontak, Foto, dan sumber data iOS lainnya. Namun, dengan data kesehatan, app diberi akses terpisah untuk membaca dan menulis data, seperti akses terpisah untuk setiap jenis data kesehatan. Pengguna dapat melihat, dan membatalkan, izin yang telah mereka berikan untuk mengakses data kesehatan di Pengaturan > Kesehatan > Akses Data & Perangkat.

Jika diberi izin untuk menulis data, app juga dapat membaca data yang mereka tulis. Jika diberi izin untuk membaca data, app dapat membaca data yang ditulis oleh semua sumber. Namun, app tidak dapat menentukan akses yang diberikan ke app lainnya. Selain itu, app tidak dapat mengetahui secara pasti apakah app telah diberi akses baca ke data kesehatan. Jika app tidak memiliki akses baca, semua permintaan tidak menghasilkan data—respons yang sama dengan yang diberikan database kosong. Ini dirancang untuk mencegah app untuk menyimpulkan status kesehatan pengguna dengan mempelajari jenis data yang dilacak pengguna.

ID Medis untuk pengguna

App Kesehatan memberi pengguna pilihan untuk mengisi formulir ID Medis dengan informasi yang mungkin penting selama keadaan darurat medis. Informasi dimasukkan atau diperbarui secara manual dan tidak diselaraskan dengan informasi di database kesehatan.

Informasi ID Medis dapat dilihat dengan mengetuk tombol Darurat di Layar Terkunci. Informasi disimpan di perangkat menggunakan kelas Perlindungan Data Tidak Ada Perlindungan sehingga dapat diakses tanpa harus memasukkan kode sandi perangkat. ID Medis adalah fitur opsional yang memungkinkan pengguna menentukan cara menyeimbangkan masalah keselamatan dan privasi. Data ini dicadangkan di Cadangan iCloud di iOS 13 atau lebih lama. Di iOS 14, ID Medis diselaraskan di antara perangkat menggunakan CloudKit dan memiliki karakteristik enkripsi yang sama dengan sisa data kesehatan.

Berbagi kesehatan

Di iOS 15, app Kesehatan memberikan pengguna pilihan yang membagikan data Kesehatan mereka dengan pengguna lain. Data kesehatan dibagikan di antara dua pengguna menggunakan enkripsi iCloud ujung ke ujung, dan Apple tidak dapat mengakses data yang dikirim melalui berbagi Kesehatan. Untuk menggunakan fitur, pengguna yang mengirim dan menerima harus menjalankan iOS 15 atau lebih baru dan menyalakan autentikasi dua faktor.

Pengguna juga dapat memilih untuk membagikan data Kesehatan mereka dengan penyedia layanan kesehatan mereka menggunakan fitur Bagikan dengan Penyedia di app Kesehatan. Data yang dibagikan menggunakan fitur ini hanya tersedia bagi institusi kesehatan yang dipilih oleh pengguna menggunakan enkripsi ujung ke ujung, dan Apple tidak mempertahankan atau memiliki akses ke kunci enkripsi untuk mendekripsi, melihat, atau mengakses data Kesehatan yang dibagikan melalui fitur Bagikan dengan Penyedia. Detail lebih lanjut mengenai cara rancangan layanan ini melindungi data Kesehatan pengguna dapat ditemukan di bagian Keamanan dan Privasi pada Panduan Pendaftaran Apple untuk Organisasi Layanan Kesehatan.

Tanda tangan digital dan enkripsi

Daftar kontrol akses

Data rantai kunci dipartisi dan dilindungi dengan daftar kontrol akses (ACL). Oleh karena itu, info pengesahan yang disimpan oleh app pihak ketiga tidak dapat diakses oleh app dengan berbagai identitas kecuali jika pengguna menyetujuinya secara eksplisit. Perlindungan ini menyediakan mekanisme untuk mengamankan info pengesahan autentikasi di perangkat Apple di berbagai cakupan app dan layanan di dalam organisasi.

Mail

Di app Mail, pengguna dapat mengirim pesan yang ditandatangani secara digital dan dienkripsi. Mail secara otomatis menemukan subjek alamat email sensitif huruf besar RFC 5322 yang sesuai atau nama alternatif subjek di sertifikat penandatanganan digital dan enkripsi di token Verifikasi Identifikasi Pribadi (PIV) terlampir di kartu cerdas yang kompatibel. Jika akun email yang dikonfigurasi cocok dengan alamat email di sertifikat penandatanganan digital atau enkripsi pada token PIV terlampir, Mail akan secara otomatis menampilkan tombol penandatanganan di bar alat jendela pesan baru. Jika Mail memiliki sertifikat enkripsi email penerima atau dapat menemukannya di Microsoft Exchange global address list (GAL), ikon gembok terbuka akan muncul di bar alat pesan baru. Ikon gembok terkunci menunjukkan bahwa pesan akan dikirimkan terenkripsi dengan kunci publik penerima.

S/MIME per pesan

iOS, iPadOS, serta macOS mendukung S/MIME per pesan. Ini berarti bahwa pengguna S/MIME dapat memilih untuk selalu menandatangani dan mengenkripsi pesan secara default atau untuk menandatangani dan mengenkripsi pesan terpisah secara selektif.

Identitas yang digunakan dengan S/MIME dapat dikirimkan ke perangkat Apple menggunakan profil konfigurasi, solusi mobile device management (MDM), Protokol Pendaftaran Sertifikat Sederhana (SCEP), atau Microsoft Active Directory Certificate Authority.

Kartu cerdas

macOS 10.12 atau lebih baru disertai dengan dukungan asli untuk kartu PIV. Kartu ini digunakan secara luas di organisasi komersial dan pemerintah untuk autentikasi dua faktor, penandatanganan digital, dan enkripsi.

Kartu cerdas menyertakan satu identitas atau lebih yang memiliki sepasang kunci publik dan pribadi dan sertifikat terkait. Pembukaan kartu cerdas dengan nomor identifikasi pribadi (PIN) menyediakan akses ke kunci pribadi yang digunakan untuk pengesahan, enkripsi, dan operasi penandatanganan. Sertifikat tersebut menentukan tujuan penggunaan kunci, dan atribut yang diasosiasikan dengannya, dan apakah kunci tersebut divalidasi (ditandatangani) oleh otoritas sertifikat (CA).

Kartu cerdas dapat digunakan untuk autentikasi dua faktor. Dua faktor yang diperlukan untuk membuka kartu adalah “sesuatu yang dimiliki pengguna” (kartu) dan “sesuatu yang diketahui pengguna” (PIN). macOS 10.12 atau lebih baru juga memiliki dukungan asli untuk pengesahan Jendela Masuk kartu cerdas dan pengesahan sertifikat klien ke situs web di Safari. Sistem operasi tersebut juga mendukung pengesahan Kerberos menggunakan pasangan kunci (PKINIT) untuk masuk tunggal ke layanan yang didukung Kerberos. Untuk mempelajari lebih lanjut mengenai kartu cerdas dan macOS, lihat Pengantar integrasi kartu cerdas di *Penyebaran Platform Apple*.

Image disk terenkripsi

Di macOS, image disk terenkripsi berfungsi sebagai wadah aman tempat pengguna dapat menyimpan atau mentransfer dokumen sensitif dan file lainnya. Image disk terenkripsi dibuat menggunakan Utilitas Disk di /Aplikasi/Utilitas/. Image disk dapat dienkripsi menggunakan enkripsi AES 128 bit atau 256 bit. Karena image disk yang terpasang diperlakukan sebagai volume lokal yang tersambung ke Mac, pengguna dapat menyalin, memindahkan, dan membuka file serta folder yang tersimpan di dalamnya. Untuk FileVault, konten image disk dienkripsi dan didekripsi secara real time. Dengan image disk terenkripsi, pengguna dapat dengan aman bertukar dokumen, file, dan folder dengan menyimpan image disk terenkripsi ke media yang dapat dilepas, mengirimkannya sebagai lampiran pesan email, atau menyimpannya di server jarak jauh. Untuk informasi lainnya mengenai image disk terenkripsi, lihat Petunjuk Pengguna Utilitas Disk.

Keamanan app

Tinjauan keamanan app

Kini, app adalah salah satu elemen paling penting dari arsitektur keamanan. Meskipun sangat bermanfaat bagi produktivitas pengguna, app juga berpotensi untuk berdampak negatif bagi keamanan sistem, stabilitas, dan data pengguna jika tidak ditangani dengan benar.

Oleh karena itu, Apple menyediakan lapisan perlindungan untuk membantu memastikan bahwa app bebas dari malware dan belum diubah. Perlindungan tambahan memberlakukan perantaraan akses dari app ke data pengguna yang dilakukan secara hati-hati. Kontrol keamanan ini menyediakan platform yang aman dan stabil untuk app, sehingga memungkinkan ribuan pengembang untuk menghadirkan ratusan ribu app di iOS, iPadOS, dan macOS—tanpa memengaruhi integritas sistem. Dan pengguna dapat mengakses app ini di perangkat Apple mereka tanpa khawatir terhadap virus, malware, atau serangan yang tidak diinginkan.

Di iPhone, iPad, dan iPod touch, semua app diambil dari App Store—dan semua app di-sandbox—untuk menyediakan kontrol paling ketat.

Di Mac, banyak app yang diambil dari App Store, tapi pengguna Mac juga mengunduh dan menggunakan app dari internet. Untuk mendukung pengunduhan internet dengan aman, macOS dilapisi dengan kontrol tambahan. Pertama, secara default di macOS 10.15 atau lebih baru, semua app Mac harus dinotarisasi oleh Apple agar dapat diluncurkan. Persyaratan ini membantu memastikan bahwa app ini bebas dari malware yang diketahui tanpa harus menyediakan app melalui App Store. Selain itu, macOS menyertakan perlindungan antivirus canggih untuk memblokir—dan jika perlu menghapus—malware.

Sebagai kontrol tambahan di seluruh platform, sandboxing membantu melindungi data pengguna dari akses yang tidak sah oleh app. Dan di macOS, data di area kritis akan dilindungi—yang membantu memastikan bahwa pengguna tetap memegang kontrol atas akses ke file di Desktop, Dokumen, Unduhan, dan area lainnya dari semua app, apakah app yang mencoba akses di-sandbox atau tidak.

Kemampuan asli	**Ekuivalen pihak ketiga**
Daftar plug-in yang tidak disetujui, daftar ekstensi Safari yang tidak disetujui	Definisi Virus/Malware
Karantina File	Definisi Virus/Malware
Tanda tangan XProtect/YARA	Definisi Virus/Malware; perlindungan titik ujung

Kemampuan asli	Ekuivalen pihak ketiga
Gatekeeper	Perlindungan titik ujung; memberlakukan penandatanganan kode di app untuk membantu memastikan hanya perangkat lunak tepercaya yang berjalan
eficheck (Penting untuk Mac tanpa Keping Keamanan T2 Apple)	Perlindungan titik ujung; deteksi rootkit
Firewall aplikasi	Perlindungan titik ujung; firewall
Filter Paket (pf)	Solusi firewall
Perlindungan Integritas Sistem	Terdapat di macOS
Kontrol Akses Wajib	Terdapat di macOS
Daftar pengecualian kext	Terdapat di macOS
Penandatanganan kode app wajib	Terdapat di macOS
Notarisasi app	Terdapat di macOS

Keamanan app di iOS dan iPadOS

Pengantar keamanan app untuk iOS dan iPadOS

Tidak seperti platform bergerak lainnya, iOS dan iPadOS tidak mengizinkan pengguna untuk menginstal app tidak bertanda tangan yang berpotensi bahaya dari situs web atau untuk menjalankan app yang tidak tepercaya. Saat runtime, tanda tangan kode memastikan bahwa semua halaman memori yang dapat dieksekusi dibuat saat halaman dimuat guna membantu memastikan app belum dimodifikasi setelah diinstal atau terakhir diperbarui.

Setelah diverifikasi sebagai app yang berasal dari sumber tepercaya, iOS dan iPadOS memberlakukan tindakan pengamanan yang dirancang untuk mencegahnya menjadi berbahaya bagi app atau bagian sistem lainnya.

Proses penandatanganan kode app di iOS dan iPadOS

Di iOS dan iPadOS, Apple menawarkan keamanan app melalui hal seperti penandatanganan wajib untuk kode, proses masuk yang ketat bagi pengembang, dan lainnya.

Penandatanganan kode wajib

Setelah dimulai, kernel iOS dan iPadOS akan mengontrol proses dan app pengguna mana yang dapat dijalankan. Untuk membantu memastikan bahwa semua app berasal dari sumber yang diketahui dan disetujui dan belum dirusak, iOS dan iPadOS mengharuskan semua kode yang dapat dijalankan untuk ditandatangani menggunakan sertifikat dari Apple. App yang menyertai perangkat, seperti Mail dan Safari, ditandatangani oleh Apple. App pihak ketiga juga harus divalidasi dan ditandatangani menggunakan sertifikat dari Apple. Penandatanganan kode yang wajib memperluas konsep rantai kepercayaan dari sistem operasi ke app dan membantu mencegah app pihak ketiga untuk memuat sumber kode yang tidak bertanda tangan atau menggunakan kode yang berubah sendiri.

Cara pengembang menandatangani app mereka

Pengembang dapat menandatangani app mereka melalui validasi sertifikat (melalui Apple Developer Program). Pengembang juga dapat menanamkan kerangka di dalam app mereka dan membuat agar kode tersebut divalidasi dengan sertifikat yang diterbitkan oleh Apple (melalui string pengenal tim).

- *Validasi sertifikat:* Untuk mengembangkan dan menginstal app di perangkat iOS atau iPadOS, pengembang harus mendaftar di Apple dan bergabung dengan Apple Developer Program. Identitas sebenarnya dari setiap pengembang, baik perorangan maupun bisnis, diverifikasi oleh Apple sebelum sertifikatnya diterbitkan. Sertifikat ini memungkinkan pengembang untuk menandatangani app dan mengirimkannya ke App Store untuk diedarkan. Oleh karena itu, semua app di App Store telah dikirimkan oleh orang atau organisasi yang dapat dikenali, sehingga dapat mencegah pembuatan app yang berbahaya. App juga telah ditinjau oleh Apple untuk membantu memastikan bahwa app biasanya beroperasi sebagaimana dijelaskan dan tidak berisi bug yang kentara atau masalah penting lainnya. Selain teknologi yang telah dibahas, proses kurasi ini meyakinkan pengguna akan kualitas app yang mereka beli.
- *Validasi tanda tangan kode:* iOS dan iPadOS memungkinkan pengembang untuk menanamkan kerangka di dalam app mereka, yang dapat digunakan oleh app itu sendiri atau oleh ekstensi yang ditanamkan di dalam app. Untuk melindungi sistem dan app lainnya dari kode pihak ketiga yang dimuat di dalam ruang alamat mereka, sistem akan melakukan validasi tanda tangan kode pada semua perpustakaan dinamis yang ditautkan proses saat diluncurkan. Verifikasi ini diselesaikan melalui pengenal tim (ID Tim), yang diekstrak dari sertifikat yang diterbitkan Apple. Pengenal tim adalah string alfanumerik 10 karakter—misalnya, 1A2B3C4D5F. Program dapat menautkan perpustakaan platform yang disertakan pada sistem atau perpustakaan dengan pengenal tim yang sama di tanda tangan kodenya sebagai file utama yang dapat dieksekusi. Mengingat penyertaan file yang dapat dieksekusi sebagai bagian dari sistem tidak memiliki pengenal tim, file hanya dapat ditautkan dengan perpustakaan yang disertakan pada sistem itu sendiri.

Memverifikasi app in-house khusus

Bisnis yang memenuhi syarat juga memiliki kemampuan untuk menulis app in-house khusus untuk digunakan di dalam organisasi mereka dan mengedarkannya ke karyawan mereka. Bisnis dan organisasi dapat mengirimkan permohonan ke Apple Developer Enterprise Program (ADEP). Untuk informasi lainnya dan untuk meninjau persyaratan, lihat situs web Apple Developer Enterprise Program. Setelah menjadi anggota ADEP, organisasi dapat mendaftar untuk mendapatkan profil penyedia yang mengizinkan app in-house khusus untuk dijalankan di perangkat yang disahkan.

Pengguna harus menginstal profil penyedia untuk menjalankan app ini. Ini membantu memastikan bahwa hanya pengguna yang ditargetkan organisasi yang dapat memuat app ke perangkat iOS dan iPadOS mereka. App yang diinstal melalui mobile device management (MDM) dipercaya secara implisit karena hubungan antara organisasi dan perangkat telah terbangun. Jika tidak, pengguna harus menyetujui profil penyedia di Pengaturan. Organisasi juga dapat membatasi pengguna agar tidak menyetujui app dari pengembang yang tidak diketahui. Saat app in-house khusus pertama kali diluncurkan, perangkat harus menerima konfirmasi positif dari Apple bahwa app diizinkan untuk dijalankan.

Keamanan proses runtime di iOS dan iPadOS

iOS dan iPadOS membantu memastikan keamanan runtime dengan menggunakan “sandbox”, hak yang ditetapkan, serta Pengacakan Tata Letak Ruang Alamat (ASLR).

Sandboxing

Semua app pihak ketiga “berjalan dalam sandbox”, sehingga dilarang untuk mengakses file yang disimpan oleh app lainnya atau untuk melakukan perubahan ke perangkat. Sandbox dirancang untuk mencegah app untuk mengumpulkan atau memodifikasi informasi yang disimpan oleh app lainnya. Setiap app memiliki direktori utama unik untuk filenya, yang ditetapkan secara acak saat app diinstal. Jika app pihak ketiga memerlukan informasi yang bukan miliknya, app akan mengaksesnya hanya dengan menggunakan layanan yang disediakan secara eksplisit oleh iOS dan iPadOS.

File sistem dan sumber daya juga dilindungi dari app pengguna. Sebagian besar file sistem dan sumber daya iOS dan iPadOS dijalankan sebagai pengguna "bergerak" bukan istimewa, sebagaimana halnya dengan app pihak ketiga. Keseluruhan partisi sistem operasi dipasang sebagai hanya baca. Alat yang tidak diperlukan, seperti layanan masuk jarak jauh, tidak disertakan pada perangkat lunak sistem, dan API tidak mengizinkan app meningkatkan hak mereka untuk memodifikasi app lainnya atau iOS dan iPadOS itu sendiri.

Penggunaan hak

Akses oleh app pihak ketiga terhadap informasi pengguna, dan ke fitur seperti iCloud dan ekstensibilitas, dikontrol menggunakan hak yang ditetapkan. Hak adalah pasangan nilai utama yang masuk ke app dan mengizinkan pengesahan di luar faktor runtime seperti ID pengguna UNIX. Karena hak ditandatangani secara digital, hak tidak dapat diubah. Hak digunakan secara ekstensif oleh app sistem dan daemon untuk melakukan operasi istimewa tertentu yang sebaliknya mengharuskan agar proses dijalankan sebagai root. Ini sangat mengurangi potensi peningkatan hak oleh app sistem atau daemon yang sudah disusupi.

Selain itu, app hanya dapat menjalankan pemrosesan latar belakang melalui API yang disediakan sistem. Ini memungkinkan app untuk terus berfungsi tanpa mengurangi kinerja atau memengaruhi masa pakai baterai secara drastis.

Pengacakan Tata Letak Ruang Alamat

Pengacakan Tata Letak Ruang Alamat (ASLR) membantu melindungi dari eksploitasi bug kerusakan memori. App internal menggunakan ASLR untuk membantu mengacak semua wilayah memori saat diluncurkan. Selain berfungsi saat peluncuran, ASLR secara acak menyusun alamat memori dari kode yang dapat dieksekusi, perpustakaan sistem, dan konstruksi pemrograman terkait, sehingga kian mengurangi potensi dari banyak eksploitasi. Misalnya, serangan return-to-libc mencoba untuk menipu perangkat agar menjalankan kode berbahaya dengan memanipulasi alamat memori dari tumpukan dan perpustakaan sistem. Dengan membuat penempatan yang acak, serangan ini menjadi lebih sulit untuk dilakukan, khususnya di beberapa perangkat. Xcode dan lingkungan pengembangan iOS dan iPadOS, mengumpulkan program pihak ketiga secara otomatis dengan dukungan ASLR yang menyala.

Fitur Execute Never

Perlindungan lebih lanjut disediakan oleh iOS dan iPadOS menggunakan fitur Execute Never (XN) ARM, yang menandai halaman memori sebagai tidak dapat dieksekusi. Halaman memori yang ditandai sebagai dapat ditulisi dan dapat dieksekusi hanya dapat digunakan oleh app dengan kondisi yang dikontrol secara ketat: Kernel memeriksa keberadaan hak penandatanganan kode dinamis khusus Apple. Selain itu, hanya satu panggilan `mmap` yang dapat dilakukan untuk meminta halaman yang dapat dieksekusi dan ditulisi, yang diberi alamat acak. Safari menggunakan fungsi ini untuk kompilator Just-in-Time (JIT) JavaScript-nya.

Ekstensi pendukung di iOS, iPadOS, dan macOS

iOS, iPadOS, dan macOS memungkinkan app untuk menyediakan fungsinya bagi app lain dengan menyediakan ekstensi. Ekstensi adalah biner yang dapat dieksekusi bertanda tangan dengan tujuan khusus yang disertakan di dalam app. Selama penginstalan, sistem secara otomatis mendeteksi ekstensi dan membuatnya tersedia untuk app lain menggunakan sistem pencocokan.

Titik ekstensi

Area sistem yang mendukung ekstensi disebut dengan *titik ekstensi*. Setiap titik ekstensi menyediakan API dan memberlakukan kebijakan bagi area tersebut. Sistem menentukan ekstensi mana yang tersedia berdasarkan aturan pencocokan khusus titik ekstensi. Sistem akan meluncurkan proses ekstensi secara otomatis jika diperlukan dan mengelola masa berlakunya. Hak dapat digunakan untuk membatasi ketersediaan ekstensi bagi app sistem tertentu. Misalnya, widget tampilan Hari Ini hanya muncul di Pusat Pemberitahuan, dan ekstensi berbagi hanya tersedia dari panel Berbagi. Contoh dari titik ekstensi adalah widget Hari Ini, Bagikan, Tindakan, Pengeditan Foto, Penyedia File, dan Papan Ketik Khusus.

Cara ekstensi berkomunikasi

Ekstensi dijalankan di ruang alamatnya sendiri. Komunikasi antara ekstensi dan app tempat asal aktivasi ekstensi menggunakan komunikasi antarproses yang diperantarai oleh kerangka sistem. Ekstensi tidak dapat mengakses file atau ruang memori satu sama lain. Ekstensi dirancang agar terisolasi dari satu sama lain, dari app yang mewadahinya, dan app yang menggunakannya. Ekstensi berjalan dalam sandbox seperti app pihak ketiga lain dan memiliki wadah yang terpisah dari wadah app yang mewadahinya. Namun, ekstensi berbagi akses yang sama terhadap kontrol privasi dengan app wadah. Sehingga jika pengguna memberi akses Kontak ke app, pemberian akses ini dapat diperluas ke ekstensi yang ditanam di dalam app tapi tidak ke ekstensi yang diaktifkan oleh app.

Cara papan ketik khusus digunakan

Papan ketik khusus adalah ekstensi jenis khusus karena diaktifkan oleh pengguna untuk keseluruhan sistem. Setelah diaktifkan, ekstensi papan ketik digunakan untuk semua bidang teks kecuali input kode sandi dan semua tampilan teks aman. Untuk membatasi transfer data pengguna, papan ketik khusus dijalankan secara default di sandbox yang sangat terbatas yang memblokir akses ke jaringan, ke layanan yang menjalankan operasi jaringan atas nama proses tertentu, dan ke API yang akan mengizinkan ekstensi untuk mengambil data pengetikan. Pengembang papan ketik khusus dapat meminta agar ekstensi mereka memiliki Akses Terbuka, yang akan memungkinkan sistem untuk menjalankan ekstensi di sandbox default setelah mendapatkan persetujuan dari pengguna.

MDM dan ekstensi

Untuk perangkat yang terdaftar di solusi mobile device management (MDM), ekstensi dokumen dan papan ketik mematuhi aturan Buka Di Dikelola. Misalnya, solusi MDM dapat membantu mencegah pengguna untuk mengekspor dokumen dari app terkelola ke Penyedia Dokumen yang tidak dikelola, atau membantu mencegahnya agar tidak menggunakan papan ketik tidak dikelola dengan app terkelola. Selain itu, pengembang app dapat mencegah penggunaan ekstensi papan ketik pihak ketiga di dalam app mereka.

Perlindungan app dan grup app di iOS serta iPadOS

Di iOS dan iPadOS, organisasi dapat melindungi app secara aman dengan menggunakan SDK IOS dan dengan bergabung dengan Grup App di Portal Pengembang Apple.

Mengadopsi Perlindungan Data di app

Kit Pengembangan Perangkat Lunak (SDK) iOS untuk iOS dan iPadOS menawarkan rangkaian lengkap API yang memudahkan pengembang pihak ketiga dan in-house untuk mengadopsi Perlindungan Data dan membantu memastikan perlindungan level tertinggi di app mereka. Perlindungan Data tersedia untuk API file dan database, termasuk NSFileManager, CoreData, NSData, dan SQLite.

Database app Mail (termasuk lampiran), buku terkelola, penanda Safari, gambar peluncuran app, dan data lokasi juga disimpan melalui enkripsi dengan kunci yang dilindungi oleh kode sandi pengguna di perangkat mereka. Kalender (kecuali lampiran), Kontak, Pengingat, Catatan, Pesan, dan Foto menerapkan hak Perlindungan Data Dilindungi Hingga Pengesahan Pengguna Pertama.

App yang diinstal pengguna yang tidak mengaktifkan kelas Perlindungan Data tertentu menerima Dilindungi Hingga Pengesahan Pengguna Pertama secara default.

Menggabungkan Grup App

App dan ekstensi yang dimiliki oleh akun pengembang tertentu dapat berbagi konten saat dikonfigurasi agar menjadi bagian dari Grup App. Pengembang memiliki kebebasan untuk membuat grup yang sesuai di Portal Pengembang Apple dan menyertakan kumpulan app dan ekstensi yang diinginkan. Setelah dikonfigurasi agar menjadi bagian dari Grup App, app memiliki akses ke:

- Wadah bersama di volume untuk penyimpanan, yang tetap berada di perangkat selama setidaknya satu app dari grup diinstal
- Preferensi bersama
- Item rantai kunci bersama

Portal Pengembang Apple membantu memastikan bahwa ID grup (GID) bersifat unik di semua ekosistem app.

Memverifikasi aksesori di iOS dan iPadOS

Program pelisensian Made for iPhone, iPad, dan iPod touch (MFi) menyediakan akses produsen aksesori yang teruji terhadap Protokol Aksesori iPod (iAP) dan komponen perangkat keras pendukung yang diperlukan.

Saat aksesori MFi berkomunikasi dengan perangkat iOS atau iPadOS menggunakan konektor Lightning atau konektor USB-C atau melalui Bluetooth, perangkat meminta aksesori untuk membuktikan bahwa aksesori telah disahkan oleh Apple dengan merespons dalam bentuk sertifikat yang disediakan Apple, yang kemudian diverifikasi oleh perangkat. Perangkat kemudian mengirimkan tantangan, yang harus dijawab aksesori dengan respons yang ditandatangani. Keseluruhan proses ini ditangani oleh sirkuit terpadu (IC) khusus yang disediakan Apple untuk produsen aksesori yang disetujui dan bersifat transparan bagi aksesori itu sendiri.

Aksesori dapat meminta akses ke metode dan fungsi transpor yang berbeda—misalnya, akses ke stream audio digital melalui kabel Lightning atau USB-C, atau informasi lokasi yang disediakan melalui Bluetooth. IC pengesahan dirancang untuk memastikan bahwa hanya aksesori yang disetujui yang diberi akses penuh ke perangkat. Jika aksesori tidak mendukung pengesahan, aksesnya terbatas pada audio analog dan subset kecil dari kontrol pemutaran audio serial (UART).

AirPlay juga menggunakan IC pengesahan untuk memverifikasi bahwa penerima telah disetujui oleh Apple. Stream audio AirPlay dan video CarPlay menggunakan MFi-SAP (Protokol Asosiasi Aman), yang mengenkripsi komunikasi antara aksesori dan perangkat menggunakan AES128 dalam mode penghitung (CTR). Kunci jangka pendek ditukar menggunakan pertukaran kunci ECDH (Curve25519) dan ditandatangani menggunakan kunci RSA 1024 bit milik IC pengesahan sebagai bagian dari protokol Stasiun ke Stasiun (STS).

Keamanan app di macOS

Pengantar keamanan app untuk macOS

Keamanan app di macOS terdiri dari sejumlah lapisan yang tumpang tindih—yang pertama adalah pilihan untuk hanya menjalankan app yang ditandatangani dan tepercaya dari App Store. Selain itu, macOS melapisi perlindungan untuk membantu memastikan app yang diunduh dari internet bebas dari malware yang diketahui. macOS menawarkan teknologi untuk mendeteksi dan menghapus malware, serta menawarkan perlindungan tambahan yang dirancang untuk mencegah app yang tidak tepercaya mengakses data pengguna. Layanan dari Apple seperti pembaruan Notarization dan Xprotect dirancang untuk membantu mencegah penginstalan malware. Saat diperlukan, layanan ini mencari malware yang mungkin telah menghindari deteksi sebelumnya lalu menghapusnya dengan cepat dan efisien. Terakhir, pengguna macOS bebas untuk beroperasi dalam mode keamanan yang masuk akal bagi mereka—termasuk menjalankan kode yang sepenuhnya tidak ditandatangani dan tidak tepercaya.

Proses penandatanganan kode app di macOS

Semua app dari App Store ditandatangani oleh Apple. Penandatanganan ini dirancang untuk memastikan bahwa app belum diubah atau dimodifikasi. Apple menandatangani app yang disediakan dengan perangkat Apple.

Di macOS 10.15, semua app yang didistribusikan di luar App Store harus ditandatangani oleh pengembang menggunakan sertifikat ID Pengembang yang diterbitkan Apple (digabungkan dengan kunci pribadi) dan dinotarisasi oleh Apple untuk dijalankan dengan pengaturan Gatekeeper default. App yang dikembangkan secara internal juga harus ditandatangani dengan ID Pengembang yang diterbitkan Apple sehingga pengguna dapat memvalidasi integritasnya.

Di macOS, penandatanganan dan notarisasi kode berfungsi secara independen—dan dapat dijalankan oleh penindak yang berbeda—untuk tujuan berbeda. Penandatanganan kode dijalankan oleh pengembang menggunakan sertifikat ID Pengembangnya (diterbitkan oleh Apple), dan verifikasi tanda tangan ini membuktikan ke pengguna bahwa perangkat lunak pengembang belum diubah sejak dibuat dan ditandatangani oleh pengembang. Notarisasi dapat dijalankan oleh semua orang dalam rantai distribusi perangkat lunak dan membuktikan bahwa Apple telah diberi salinan kode untuk memeriksa apakah kode tersebut memiliki malware dan tidak ditemukan adanya malware yang diketahui. Output Notarisasi adalah sebuah tiket, yang disimpan di server Apple dan dapat dikaitkan secara opsional ke app (oleh siapa saja) tanpa membatalkan validasi tanda tangan pengembang.

Kontrol Akses Wajib (MAC) mengharuskan penandatanganan kode untuk mengaktifkan hak yang dilindungi oleh sistem. Misalnya, app yang memerlukan akses melalui firewall harus ditandatangani kodenya dengan hak MAC yang sesuai.

Perlindungan Gatekeeper dan runtime di macOS

macOS menawarkan teknologi Gatekeeper dan perlindungan runtime untuk membantu memastikan hanya perangkat lunak tepercaya yang dijalankan di Mac pengguna.

Gatekeeper

macOS disertai dengan keamanan teknologi yang disebut *Gatekeeper* yang dirancang untuk membantu memastikan bahwa hanya perangkat lunak tepercaya yang dijalankan di Mac pengguna. Saat pengguna mengunduh dan membuka app, plug-in, atau paket penginstal dari luar App Store, Gatekeeper memverifikasi bahwa perangkat lunak berasal dari pengembang yang teridentifikasi dan dinotarisasi oleh Apple bebas dari konten berbahaya yang diketahui dan belum diubah. Gatekeeper juga meminta izin pengguna sebelum membuka perangkat lunak yang diunduh untuk pertama kalinya untuk memastikan bahwa pengguna tidak tertipu untuk menjalankan kode yang dapat dieksekusi yang mereka kira hanya merupakan file data.

Secara default, Gatekeeper membantu memastikan bahwa semua perangkat lunak yang diunduh telah ditandatangani oleh App Store atau oleh pengembang terdaftar dan dinotarisasi oleh Apple. Proses peninjauan App Store dan pipeline notarisasi dirancang untuk memastikan bahwa app tidak berisi malware yang diketahui. Oleh karena itu, secara default *semua perangkat lunak di macOS diperiksa untuk mengetahui apakah terdapat konten berbahaya yang diketahui saat pertama kali dibuka, terlepas dari bagaimana perangkat lunak tersebut masuk ke Mac*.

Pengguna dan organisasi memiliki pilihan untuk hanya mengizinkan perangkat lunak yang diinstal dari App Store. Selain itu, pengguna dapat menimpa kebijakan Gatekeeper untuk membuka perangkat lunak mana pun kecuali dibatasi oleh solusi mobile device management (MDM). Organisasi dapat menggunakan MDM untuk mengonfigurasi pengaturan Gatekeeper, termasuk mengizinkan perangkat lunak yang ditandatangani dengan identitas alternatif. Gatekeeper juga dapat dinonaktifkan sepenuhnya, jika perlu.

Gatekeeper juga melindungi dari distribusi plug-in yang berbahaya dengan app yang tidak berbahaya. Dalam hal ini, penggunaan app memicu dimuatnya plug-in berbahaya tanpa sepengetahuan pengguna. Jika perlu, Gatekeeper membuka app dari lokasi hanya baca acak. Ini dirancang untuk mencegah pemuatan otomatis plug-in yang didistribusikan bersama app.

Perlindungan runtime

File sistem, sumber daya, dan kernel dilindungi dari ruang app pengguna. Semua app dari App Store di-sandbox untuk membatasi akses ke data yang disimpan oleh app lainnya. Jika app dari App Store perlu mengakses data dari app lain, app tersebut hanya dapat melakukannya dengan menggunakan API dan layanan yang disediakan oleh macOS.

Perlindungan dari malware di macOS

Apple mengoperasikan proses kepintaran ancaman untuk mengidentifikasi dan memblokir malware dengan cepat.

Tiga lapisan pertahanan

Perlindungan malware terdiri dari tiga lapisan:

1. *Mencegah peluncuran atau eksekusi malware:* App Store, atau Gatekeeper yang digabungkan dengan Notarization

2. *Memblokir malware agar tidak dijalankan di sistem pelanggan:* Gatekeeper, Notarization, dan XProtect

3. *Menghilangkan malware yang telah dieksekusi:* XProtect

Lapisan pertama pertahanan dirancang untuk menghalangi penyebaran malware, dan mencegahnya diluncurkan sama sekali—ini adalah tujuan dari App Store, dan Gatekeeper yang digabungkan dengan Notarization.

Lapisan pertahanan berikutnya ditujukan untuk membantu memastikan bahwa jika malware muncul di Mac, malware diidentifikasi dan diblokir dengan cepat, untuk menghentikan penyebaran dan untuk memperbaiki sistem Mac yang telah dimasuki malware. XProtect menguatkan pertahanan ini, bersama dengan Gatekeeper dan Notarization.

Terakhir, XProtect bertindak untuk menghilangkan malware yang telah berhasil dieksekusi.

Perlindungan ini, dijelaskan lebih jauh di bawah, digabung untuk mendukung perlindungan terbaik dari virus dan malware. Terdapat juga perlindungan tambahan, khususnya di Mac dengan Apple silicon untuk membatasi kemungkinan kerusakan dari malware yang berhasil dieksekusi. Lihat Melindungi akses app ke data pengguna untuk cara macOS dapat membantu melindungi data pengguna dari malware, dan Integritas sistem operasi untuk cara macOS dapat membatasi tindakan yang dapat dilakukan malware di sistem.

Notarization

Notarization adalah layanan pemindaian malware yang disediakan oleh Apple. Pengembang yang ingin mendistribusikan app untuk macOS di luar App Store mengirimkan app-nya untuk dipindai sebagai bagian dari proses distribusi. Apple memindai perangkat lunak ini untuk malware yang diketahui, dan jika tidak ditemukan, akan menerbitkan tiket Notarization. Biasanya, pengembang mencantumkan tiket ini ke app-nya agar Gatekeeper dapat memverifikasi dan meluncurkan app, bahkan saat offline.

Apple juga dapat menerbitkan tiket pencabutan untuk app yang diketahui berbahaya—walaupun app tersebut telah dinotarisasi. macOS secara berkala memeriksa tiket pencabutan baru agar Gatekeeper memiliki informasi terbaru dan dapat memblokir peluncuran file seperti itu. Proses ini dapat memblokir app berbahaya dengan cepat karena pembaruan terjadi pada latar belakang lebih sering dibandingkan pembaruan latar belakang yang memberikan tanda tangan XProtect baru. Selain itu, perlindungan ini dapat diterapkan ke app yang sebelumnya telah dan yang belum dinotarisasi.

XProtect

macOS disertai dengan teknologi antivirus internal yang disebut *XProtect* untuk deteksi berbasis tanda tangan dan penghapusan malware. Sistem menggunakan tanda tangan YARA, alat yang digunakan untuk melakukan deteksi berbasis tanda tangan terhadap malware, yang diperbarui secara berkala oleh Apple. Apple memonitor infeksi dan jenis malware baru, dan memperbarui tanda tangan secara otomatis—terpisah dari pembaruan sistem—untuk membantu melindungi Mac dari infeksi Malware. XProtect secara otomatis mendeteksi dan memblokir eksekusi malware yang diketahui. Di macOS 10.15 atau lebih baru, XProtect memeriksa konten berbahaya yang diketahui setiap kali:

- App pertama kali diluncurkan
- App telah diubah (di sistem file)
- Tanda tangan XProtect diperbarui

Jika XProtect mendeteksi malware yang diketahui, perangkat lunak tersebut diblokir dan pengguna akan diberi tahu dan diberi pilihan untuk memindahkan perangkat lunak ke Tong Sampah.

Catatan: Notarization efektif untuk file yang diketahui (atau hash file) dan dapat digunakan di app yang sebelumnya telah diluncurkan. Aturan berbasis tanda tangan XProtect bersifat lebih umum dibandingkan hash file sehingga dapat menemukan varian yang belum pernah Apple lihat. XProtect memindai hanya app yang telah diubah atau app yang pertama kali diluncurkan.

Jika malware masuk ke Mac, XProtect juga disertai dengan teknologi untuk menangani infeksi. Misalnya, XProtect disertai dengan adalah mesin yang memulihkan infeksi berdasarkan pembaruan yang secara otomatis dikirim dari Apple (sebagai bagian dari pembaruan file data sistem dan keamanan otomatis). XProtect menghapus malware saat menerima informasi yang diperbarui, dan terus memeriksa infeksi secara berkala. XProtect tidak melakukan boot ulang Mac secara otomatis.

Pembaruan keamanan XProtect otomatis

Apple mengeluarkan pembaruan untuk XProtect secara otomatis berdasarkan informasi ancaman terbaru yang tersedia. Secara default, macOS memeriksa pembaruan ini setiap hari. Pembaruan Notarization, yang didistribusikan menggunakan penyelarasan CloudKit, yang lebih sering.

Cara Apple merespons saat malware baru ditemukan

Saat malware baru ditemukan, sejumlah langkah dapat dilakukan:

- Sertifikat ID Pengembang yang terkait dengan malware akan dicabut.
- Tiket pencabutan Notarization diterbitkan untuk semua file (app dan file terkait).
- Tanda tangan XProtect dikembangkan dan dirilis.

  Tanda tangan ini juga diterapkan secara retroaktif ke perangkat lunak yang sebelumnya dinotarisasi, dan hasil deteksi baru apa pun di satu atau beberapa tindakan sebelumnya yang terjadi.

Akhirnya, deteksi malware meluncurkan serangkaian langkah pada detik, jam, dan hari berikutnya untuk menyebarluaskan perlindungan terbaik ke pengguna Mac.

Mengontrol akses app ke file di macOS

Apple percaya bahwa pengguna harus memiliki transparansi, persetujuan, dan kontrol yang penuh atas apa yang dilakukan app dengan data mereka. Di macOS 10.15, model ini diperkuat oleh sistem untuk membantu memastikan bahwa semua app harus mendapatkan persetujuan pengguna sebelum mengakses file di Dokumen, Unduhan, Desktop, iCloud Drive, dan volume jaringan. Di macOS 10.13 atau lebih baru, app yang memerlukan akses ke seluruh perangkat penyimpanan harus ditambahkan secara eksplisit di Preferensi Sistem. Selain itu, kemampuan aksesibilitas dan automasi memerlukan izin pengguna untuk membantu memastikan bahwa app tidak menembus perlindungan lain. Tergantung kebijakan aksesnya, pengguna dapat diminta, atau diharuskan, untuk mengubah pengaturan di Preferensi Sistem > Keamanan & Privasi > Privasi:

Item	Pengguna diminta oleh app	Pengguna harus mengedit pengaturan privasi sistem
Aksesibilitas		✓
Akses penuh ke penyimpanan internal		✓
File dan folder *Catatan:* Disertai dengan Desktop, Dokumen, Unduhan, jaringan volume, dan volume yang dapat dilepas	✓	
Automasi (peristiwa Apple)	✓	

Item di Tong Sampah pengguna dilindungi dari semua app yang menggunakan Akses Disk Penuh; pengguna tidak akan diminta untuk akses app. Jika pengguna ingin app agar dapat mengakses file, app harus dipindahkan dari Tong Sampah ke lokasi lain.

Pengguna yang menyalakan FileVault di Mac akan diminta untuk menyediakan info pengesahan yang sah sebelum melanjutkan proses boot dan mendapatkan akses ke mode mulai khusus. Tanpa info pengesahan masuk yang valid atau kunci pemulihan, seluruh volume akan tetap terenkripsi dan dilindungi dari akses yang tidak sah, bahkan jika perangkat penyimpanan fisik dilepas dan disambungkan ke komputer lain.

Untuk melindungi data di pengaturan perusahaan, TI harus mendefinisikan dan menerapkan kebijakan konfigurasi FileVault menggunakan mobile device management (MDM). Organisasi memiliki beberapa pilihan untuk mengelola volume terenkripsi, termasuk kunci pemulihan institusi, kunci pemulihan pribadi (yang dapat secara opsional disimpan dengan MDM untuk eskrow), atau kombinasi keduanya. Rotasi kunci juga dapat diatur sebagai kebijakan di MDM.

Fitur aman di app Catatan

App Catatan dilengkapi dengan fitur catatan aman—di iPhone, iPad, Mac, dan situs web iCloud—yang memungkinkan pengguna untuk melindungi konten catatan tertentu. Pengguna juga dapat berbagi catatan dengan orang lain secara aman.

Catatan aman

Catatan aman dilindungi dengan enkripsi ujung ke ujung menggunakan frasa sandi yang diberikan pengguna dan diperlukan untuk melihat catatan di perangkat iOS, iPadOS, macOS, dan situs web iCloud. Setiap akun iCloud (termasuk akun perangkat "Di [perangkat] saya") dapat memiliki frasa sandi terpisah.

Saat pengguna mengamankan catatan, kunci 16 bita diturunkan dari frasa sandi pengguna menggunakan PBKDF2 dan SHA256. Catatan dan semua lampirannya dienkripsi menggunakan AES dengan Mode Galois/Counter (AES-GCM). Rekaman baru dibuat di Data Inti dan CloudKit untuk menyimpan catatan, lampiran, label, dan vektor inisialisasi yang dienkripsi. Setelah rekaman baru dibuat, data asli yang tidak dienkripsi akan dihapus. Lampiran yang mendukung enkripsi meliputi gambar, sketsa, tabel, peta, dan situs web. Catatan yang berisi jenis lampiran lainnya tidak dapat dienkripsi, dan lampiran yang tidak didukung tidak dapat ditambahkan ke catatan aman.

Untuk melihat catatan aman, pengguna harus memasukkan frasa sandi atau mengesahkan menggunakan Face ID atau Touch ID. Setelah berhasil mengesahkan pengguna, baik itu untuk melihat atau membuat catatan aman, Catatan akan membuka sesi aman. Saat sesi aman terbuka, pengguna dapat melihat atau mengamankan catatan lain tanpa pengesahan tambahan. Namun, sesi aman hanya berlaku bagi catatan yang dilindungi dengan frasa sandi yang disediakan. Pengguna masih harus mengesahkan untuk catatan yang dilindungi oleh frasa sandi lain. Sesi aman ditutup saat:

- Pengguna mengetuk tombol Kunci Sekarang di Catatan
- Catatan dialihkan ke latar belakang selama lebih dari 3 menit (8 menit di macOS)
- Perangkat iOS atau iPadOS terkunci

Untuk mengubah frasa sandi di catatan aman, pengguna harus memasukkan frasa sandi saat ini, karena Face ID dan Touch ID tidak tersedia saat mengubah frasa sandi. Setelah memilih frasa sandi baru, app Catatan akan membungkus ulang, dengan cara yang sama, kunci semua catatan yang dienkripsi oleh frasa sandi sebelumnya.

Jika pengguna salah mengetik frasa sandi tiga kali berturut-turut, Catatan akan menampilkan petunjuk yang diberikan pengguna jika pengguna membuat petunjuk tersebut pada saat pengaturan. Jika pengguna masih tidak mengingat frasa sandinya, mereka dapat mengaturnya kembali di pengaturan Catatan. Fitur ini memungkinkan pengguna untuk membuat catatan aman baru dengan frasa sandi baru, tapi frasa sandi baru tidak akan memungkinkan mereka untuk melihat catatan yang diamankan sebelumnya. Catatan yang diamankan sebelumnya masih dapat dilihat jika pengguna ingat frasa sandi lama. Pengaturan ulang frasa sandi memerlukan frasa sandi akun iCloud pengguna.

Catatan bersama

Catatan yang tidak dilindungi oleh enkripsi ujung ke ujung dengan frasa sandi dapat dibagikan dengan orang lain. Catatan bersama masih menggunakan jenis data yang dienkripsi CloudKit untuk semua teks atau lampiran yang disertakan di catatan oleh pengguna. Aset selalu dienkripsi dengan kunci yang dienkripsi di CKRecord. Metadata, seperti tanggal pembuatan atau perubahan, tidak dienkripsi. CloudKit mengelola proses yang dapat digunakan peserta untuk mengenkripsi dan mendekripsi data satu sama lain.

Fitur aman di app Pintasan

Di app Pintasan, pintasan diselaraskan secara opsional di semua perangkat Apple yang menggunakan iCloud. Pintasan juga dapat dibagikan dengan pengguna lainnya melalui iCloud. Pintasan disimpan secara lokal dalam format terenkripsi.

Pintasan khusus bersifat serba guna—mirip dengan skrip atau program. Saat mengunduh pintasan dari internet, pengguna akan diperingatkan bahwa pintasan belum ditinjau oleh Apple dan diberi kesempatan untuk menginspeksi pintasan tersebut. Untuk melindungi dari pintasan berbahaya, definisi malware yang diperbarui akan diunduh untuk mengidentifikasi pintasan berbahaya di runtime.

Pintasan khusus juga dapat menjalankan JavaScript yang ditetapkan pengguna di situs web di Safari saat diaktifkan dari lembar berbagi. Untuk melindungi dari JavaScript berbahaya yang, misalnya, menipu pengguna untuk menjalankan skrip di situs web media sosial yang mengambil data mereka, JavaScript divalidasi berdasarkan definisi malware yang disebut sebelumnya. Saat pertama kali pengguna menjalankan JavaScript di suatu domain, pengguna akan diminta untuk mengizinkan pintasan yang berisi JavaScript untuk dijalankan di halaman web saat ini untuk domain tersebut.

Keamanan layanan

Tinjauan keamanan layanan

Apple telah membangun rangkaian layanan yang kuat untuk membantu pengguna mengoptimalkan lebih banyak utilitas dan produktivitas dari perangkat mereka. Layanan ini menyediakan kemampuan yang andal untuk penyimpanan awan, penyelarasan, penyimpanan kata sandi, pengesahan, pembayaran, pesan, komunikasi, dan lainnya, serta melindungi privasi pengguna dan keamanan datanya.

Bab ini mencakup teknologi keamanan yang digunakan di iCloud, Masuk dengan Apple, Apple Pay, iMessage, Apple Messages for Business, FaceTime, Lacak, dan Berkelanjutan.

Catatan: Tidak semua layanan dan konten Apple tersedia di semua negara atau wilayah.

ID Apple dan ID Apple yang Dikelola

Tinjauan keamanan ID Apple

ID Apple adalah akun yang digunakan untuk masuk ke layanan Apple. Penting bagi pengguna untuk menjaga agar ID Apple mereka tetap aman untuk membantu mencegah akses yang tidak berwenang ke akun mereka. Untuk membantu hal ini, ID Apple memerlukan kata sandi kuat yang:

- Setidaknya harus memiliki delapan karakter
- Harus berisi huruf dan angka
- Tidak boleh berisi tiga atau lebih karakter identik yang berurutan
- Tidak boleh berupa kata sandi yang umum digunakan

Pengguna dianjurkan untuk melampaui panduan ini dengan menambahkan karakter dan tanda baca untuk membuat kata sandi mereka lebih kuat lagi.

Apple juga memberi tahu pengguna melalui email atau pemberitahuan push atau keduanya jika terdapat perubahan penting pada akun mereka—misalnya jika kata sandi atau informasi penagihan telah diubah atau ID Apple telah digunakan untuk masuk ke perangkat baru. Jika ada hal yang terasa ganjil, pengguna diinstruksikan untuk segera mengubah kata sandi ID Apple mereka.

Selain itu, Apple menerapkan berbagai kebijakan dan prosedur yang dirancang untuk melindungi akun pengguna. Ini meliputi pembatasan jumlah percobaan ulang untuk masuk dan upaya pengaturan ulang kata sandi, pengawasan penipuan aktif untuk membantu mengidentifikasi serangan pada saat kejadian, dan peninjauan kebijakan secara berkala yang memungkinkan Apple untuk beradaptasi terhadap informasi baru yang dapat berpengaruh pada keamanan pengguna.

Catatan: Kebijakan kata sandi ID Apple yang Dikelola diatur oleh administrator di Apple School Manager atau Apple Business Manager.

Autentikasi dua faktor

Untuk lebih lanjut membantu pengguna mengamankan akun mereka, Apple secara default menggunakan *autentikasi dua faktor*—lapisan keamanan tambahan untuk ID Apple. Fitur ini dirancang untuk memastikan bahwa hanya pemilik akun yang dapat mengakses akun, bahkan jika orang lain mengetahui kata sandinya. Dengan autentikasi dua faktor, akun pengguna hanya dapat diakses di perangkat tepercaya, seperti iPhone, iPad, iPod touch, atau Mac pengguna, atau di perangkat lainnya setelah menyelesaikan verifikasi dari salah satu perangkat tepercaya ini atau dari nomor telepon tepercaya. Agar dapat masuk untuk pertama kalinya di perangkat baru, dua jenis informasi diperlukan—kata sandi ID Apple dan kode verifikasi enam digit yang ditampilkan di perangkat tepercaya pengguna atau dikirimkan ke nomor telepon tepercaya. Dengan memasukkan kode, pengguna mengonfirmasi bahwa mereka mempercayai perangkat baru dan aman untuk masuk. Karena kata sandi tidak lagi cukup untuk mengakses akun pengguna, autentikasi dua faktor meningkatkan keamanan ID Apple pengguna dan semua informasi pribadi yang mereka simpan dengan Apple. Fitur ini terintegrasi secara langsung di iOS, iPadOS, macOS, tvOS, watchOS, dan sistem pengesahan yang digunakan oleh situs web Apple.

Saat pengguna masuk ke situs web Apple menggunakan browser web, permintaan faktor kedua akan dikirimkan ke semua perangkat tepercaya yang terkait dengan akun iCloud pengguna untuk meminta persetujuan sesi web. Jika pengguna masuk ke situs web Apple dari browser di perangkat tepercaya, mereka akan melihat kode verifikasi ditampilkan secara lokal di perangkat yang sedang mereka gunakan. Saat pengguna memasukkan kode di perangkat tersebut, sesi web disetujui.

Pengaturan ulang kata sandi dan pemulihan akun

Jika pengguna lupa kata sandi akun ID Apple, pengguna dapat mengaturnya ulang di perangkat tepercaya. Jika perangkat tepercaya tidak tersedia dan kata sandi diketahui, pengguna dapat menggunakan nomor telepon tepercaya untuk mengesahkan melalui verifikasi SMS. Selain itu, untuk menyediakan pemulihan segera untuk ID Apple, kode sandi yang sebelumnya digunakan dapat digunakan untuk mengatur ulang bersama SMS. Jika pilihan ini tidak memungkinkan, proses pemulihan akun harus diikuti. Untuk informasi lainnya, lihat artikel Dukungan Apple Cara menggunakan pemulihan akun saat Anda tidak dapat mengatur ulang kata sandi ID Apple.

Keamanan ID Apple yang dikelola

ID Apple yang Dikelola berfungsi sama seperti ID Apple tetapi dimiliki dan dikontrol oleh perusahaan atau lembaga pendidikan. Organisasi ini dapat mengatur ulang kata sandi, membatasi pembelian dan komunikasi seperti FaceTime dan Pesan, dan mengatur izin berbasis peran untuk karyawan, anggota staf, guru, dan murid.

Untuk ID Apple yang Dikelola, beberapa layanan dinonaktifkan, (misalnya Apple Pay, Rantai Kunci iCloud, HomeKit, dan Lacak).

Menginspeksi ID Apple yang Dikelola

ID Apple yang Dikelola juga mendukung *inspeksi*, yang memungkinkan organisasi untuk mematuhi peraturan hukum dan privasi. Administrator, manajer, atau guru Apple School Manager dapat memeriksa akun ID Apple yang Dikelola tertentu.

Inspektur hanya dapat mengawasi akun yang berada di bawah mereka dalam hierarki organisasi. Misalnya, guru dapat mengawasi murid, pengelola dapat menginspeksi guru dan murid, dan administrator dapat menginspeksi pengelola, guru, dan murid.

Saat menginspeksi info pengesahan yang diminta menggunakan Apple School Manager, akan diterbitkan akun khusus yang hanya memiliki akses ke ID Apple yang Dikelola yang akan diinspeksi. Inspektur kemudian dapat membaca dan memodifikasi konten pengguna yang disimpan di iCloud atau di app yang menggunakan CloudKit. Semua permintaan untuk akses audit dicatat di Apple School Manager. Log menampilkan siapa yang menginspeksi, ID Apple yang Dikelola yang akan diinspeksi, waktu permintaan, dan apakah inspeksi dilakukan atau tidak.

ID Apple yang Dikelola dan perangkat pribadi

ID Apple yang Dikelola juga dapat digunakan dengan perangkat iOS, perangkat iPadOS, dan komputer Mac milik pribadi. Murid masuk ke iCloud menggunakan ID Apple yang Dikelola yang diterbitkan oleh institusi dan kata sandi tambahan untuk penggunaan di rumah yang berfungsi sebagai faktor kedua pada proses autentikasi dua faktor ID Apple. Saat murid menggunakan ID Apple yang Dikelola di perangkat pribadi, Rantai Kunci iCloud tidak tersedia, dan institusi dapat membatasi fitur lain, seperti FaceTime atau Pesan. Semua dokumen iCloud yang dibuat oleh murid saat mereka masuk akan diaudit sebagaimana dijelaskan sebelumnya di bagian ini.

iCloud

Tinjauan keamanan iCloud

iCloud menyimpan kontak, kalender, foto, dokumen, dan data pengguna lainnya serta menjaganya agar tetap terbaru di semua perangkat pengguna secara otomatis. iCloud juga dapat digunakan oleh app pihak ketiga untuk menyimpan dan menyelaraskan dokumen, serta nilai kunci untuk data app sebagaimana yang didefinisikan oleh pengembang. Pengguna mengatur iCloud dengan masuk menggunakan ID Apple dan memilih layanan apa yang ingin digunakan. Beberapa fitur iCloud, seperti iCloud Drive, dan Cadangan iCloud dapat dinonaktifkan oleh administrator TI menggunakan profil konfigurasi mobile device management (MDM).

iCloud menggunakan metode keamanan kuat dan menerapkan kebijakan ketat untuk melindungi data pengguna. Sebagian besar data iCloud dienkripsi terlebih dahulu di perangkat pengguna, menggunakan kunci iCloud yang dibuat perangkat, sebelum diunggah ke server iCloud. Untuk data yang tidak dienkripsi ujung ke ujung, perangkat pengguna mengunggah kunci iCloud ini dengan aman ke Modul Keamanan Perangkat Keras iCloud di pusat data Apple. Ini memungkinkan Apple membantu pengguna dengan pemulihan data dan mendekripsi data atas nama pengguna kapan saja mereka memerlukannya (misalnya, saat mereka masuk di perangkat baru, memulihkannya dari cadangan, atau mengakses data iCloud mereka di web). Data yang berpindah antara perangkat pengguna dan server iCloud dienkripsi secara terpisah saat transit dengan TLS, dan server iCloud menyimpan data pengguna dengan lapisan tambahan enkripsi saat disimpan.

Kunci enkripsi, jika tersedia bagi Apple, diamankan di pusat data Apple. Saat memproses data yang disimpan di pusat data pihak ketiga, kunci enkripsi ini hanya diakses oleh perangkat lunak Apple yang dijalankan di server aman, dan hanya saat menjalankan pemrosesan yang dibutuhkan. Untuk privasi dan keamanan tambahan, banyak layanan Apple menggunakan enkripsi ujung ke ujung, yang berarti data iCloud pengguna hanya dapat diakses oleh pengguna itu sendiri, dan hanya dari perangkat tepercaya tempat mereka masuk dengan ID Apple miliknya.

Apple menawarkan dua pilihan kepada pengguna untuk mengenkripsi dan melindungi data yang mereka simpan di iCloud:

- **Perlindungan data standar (pengaturan default):** Data iCloud pengguna dienkripsi, kunci enkripsi diamankan di pusat data Apple, dan Apple dapat membantu dengan pemulihan data dan akun. Hanya data iCloud tertentu—14 kategori data, termasuk data Kesehatan dan kata sandi di Rantai Kunci iCloud—yang dienkripsi ujung ke ujung.
- **Perlindungan Data Lanjutan untuk iCloud:** Pengaturan opsional yang menawarkan tingkat tertinggi keamanan data awan Apple. Jika pengguna memilih untuk menyalakan Perlindungan Data Lanjutan, perangkat tepercaya mereka mempertahankan akses tunggalnya ke kunci enkripsi untuk sebagian besar data iCloud mereka, maka dari itu melindunginya menggunakan enkripsi ujung ke ujung. Saat Anda menyalakan Perlindungan Data Lanjutan, jumlah kategori data yang menggunakan enkripsi ujung ke ujung naik menjadi 23 dan menyertakan Cadangan iCloud, Foto, Catatan, dan lainnya.

Kategori khusus data iCloud yang dilindungi dengan enkripsi ujung ke ujung tercantum di artikel Dukungan Apple Tinjauan keamanan data iCloud.

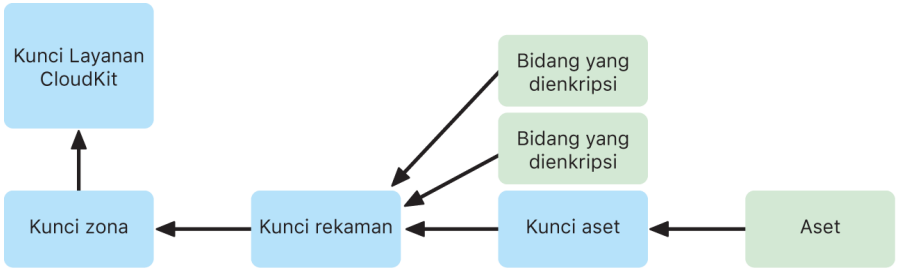
Enkripsi iCloud

Enkripsi data di iCloud terkait erat dengan model penyimpanan data, dimulai dengan kerangka dan API CloudKit yang memungkinkan app dan perangkat lunak sistem menyimpan data di iCloud atas nama pengguna, dan terus memperbaruinya di seluruh perangkat dan di web.

Enkripsi CloudKit

CloudKit adalah kerangka yang memungkinkan pengembang app menyimpan data nilai kunci, data terstruktur, dan aset (data besar yang disimpan secara terpisah dari database, seperti gambar atau video) di iCloud. CloudKit mendukung database publik dan pribadi, yang dikelompokkan di wadah. Database publik dibagikan secara global, biasanya digunakan untuk aset umum, dan tidak enkripsi. Database pribadi menyimpan data iCloud setiap pengguna.

CloudKit menggunakan hierarki kunci yang cocok dengan struktur data. Setiap database pribadi wadah dilindungi oleh hierarki kunci, yang terletak di kunci asimetris yang disebut *kunci Layanan CloudKit*. Kunci ini unik bagi setiap pengguna iCloud dan dibuat di perangkat tepercaya mereka. Saat data ditulis ke CloudKit, semua kunci rekaman dibuat di perangkat tepercaya pengguna dan dibungkus dengan hierarki kunci yang sesuai sebelum data apa pun diunggah.



Banyak layanan Apple, yang tercantum di artikel Dukungan Apple tinjauan keamanan data iCloud, menggunakan enkripsi ujung ke ujung dengan kunci layanan CloudKit yang dilindungi oleh penyelarasan Rantai Kunci iCloud. Untuk wadah CloudKit ini, kunci layanan disimpan di Rantai Kunci iCloud pengguna dan membagikan karakteristik keamanan Rantai Kunci iCloud; kunci layanan hanya tersedia di perangkat tepercaya pengguna, dan tidak dapat diakses oleh Apple atau pihak ketiga mana pun. Jika perangkat hilang, pengguna dapat memulihkan data Rantai Kunci iCloud mereka melalui penggunaan pemulihan Rantai Kunci iCloud aman, Kontak Pemulihan Akun, atau Kunci Pemulihan Akun.

Manajemen kunci enkripsi

Keamanan data terenkripsi di CloudKit mengandalkan keamanan kunci enkripsi masing-masing. Kunci layanan CloudKit dibagi menjadi dua kategori: dienkripsi ujung ke ujung dan tersedia setelah pengesahan.

- **Kunci layanan yang dienkripsi ujung ke ujung:** Untuk layanan iCloud yang dienkripsi ujung ke ujung, kunci pribadi layanan CloudKit yang relevan tidak pernah disediakan ke server Apple. Pasangan kunci layanan, termasuk kunci pribadi, dibuat secara lokal di perangkat tepercaya pengguna dan ditransfer ke perangkat lain pengguna menggunakan keamanan Rantai Kunci iCloud. Meskipun alur pemulihan dan sinkronisasi Rantai Kunci iCloud dilakukan oleh server Apple, server ini secara kriptografis tidak dapat mengakses data rantai kunci pengguna mana pun. Di kasus terburuk hilangnya akses Rantai Kunci iCloud dan semua mekanisme pemulihannya, data yang dienkripsi ujung ke ujung di CloudKit akan hilang. Apple tidak dapat membantu memulihkan data ini.
- **Kunci layanan tersedia setelah pengesahan:** Untuk layanan lainnya, seperti Foto dan iCloud Drive, kunci layanan disimpan di Modul Keamanan Perangkat Keras iCloud di pusat data Apple dan dapat diakses oleh beberapa layanan Apple. Saat pengguna masuk ke iCloud di perangkat baru dan mengesahkan ID Apple miliknya, kunci ini dapat diakses oleh server Apple tanpa interaksi atau input pengguna lebih lanjut. Misalnya, setelah masuk ke iCloud.com, pengguna dapat segera melihat foto mereka secara online. Kunci layanan ini merupakan kunci *tersedia setelah pengesahan*.

Perlindungan Data Lanjutan untuk iCloud

Perlindungan Data Lanjutan untuk iCloud merupakan pengaturan opsional yang menawarkan tingkat tertinggi keamanan data awan Apple. Saat pengguna menyalakan Perlindungan Data Lanjutan, perangkat tepercaya mereka mempertahankan akses tunggalnya ke kunci enkripsi untuk sebagian besar data iCloud mereka, maka dari itu melindunginya dengan *enkripsi ujung ke ujung*. Untuk pengguna yang menyalakan Perlindungan Data Lanjutan, jumlah total kategori data yang dilindungi menggunakan enkripsi ujung ke ujung naik dari 14 menjadi 23 dan menyertakan Cadangan iCloud, Foto, Catatan, dan lainnya.

Perlindungan Data Lanjutan untuk iCloud akan tersedia untuk pengguna A.S. pada akhir 2022 dan akan mulai diluncurkan ke seluruh dunia pada awal 2023.

Secara konsep, Perlindungan Data Lanjutan sifatnya sederhana: Semua kunci Layanan CloudKit yang dibuat di perangkat dan nantinya diunggah ke Modul Keamanan Perangkat Keras (HSM) iCloud *tersedia setelah pengesahan* di pusat data Apple akan dihapus dari HSM tersebut dan alih-alih disimpan sepenuhnya dalam domain perlindungan Rantai Kunci iCloud akun. Kunci tersebut ditangani seperti kunci layanan *yang dienkripsi ujung ke ujung* yang ada, yang berarti Apple tidak dapat lagi membaca atau mengakses kunci ini.

Perlindungan Data Lanjutan juga melindungi bidang CloudKit secara otomatis yang dipilih pengembang pihak ketiga untuk ditandai sebagai dienkripsi, dan semua aset CloudKit.

Mengaktifkan Perlindungan Data Lanjutan

Saat pengguna menyalakan Perlindungan Data Lanjutan, perangkat tepercaya mereka menjalankan dua tindakan: Pertama, perangkat mengomunikasikan maksud pengguna untuk menyalakan Perlindungan Data Lanjutan ke perangkat lain yang berpartisipasi di enkripsi ujung ke ujung. Perangkat tersebut melakukannya dengan menulis nilai baru, yang ditandatangani oleh kunci perangkat lokal, ke metadata perangkat Rantai Kunci iCloud. Server Apple tidak dapat menghapus atau memodifikasi pengesahan ini saat diselaraskan dengan perangkat lain pengguna.

Kedua, perangkat memulai penghapusan kunci layanan *tersedia setelah pengesahan* dari pusat data Apple. Karena kunci ini dilindungi oleh HSM iCloud, penghapusan ini bersifat segera, permanen, dan tidak dapat dibatalkan. Setelah kunci dihapus, Apple tidak dapat lagi mengakses data *mana pun* yang dilindungi oleh kunci layanan pengguna. Pada saat ini, perangkat memulai operasi rotasi kunci asinkron, yang membuat kunci layanan baru untuk setiap layanan yang kuncinya tersedia sebelumnya ke server Apple. Jika rotasi kunci gagal, karena gangguan jaringan atau kesalahan lainnya, perangkat mencoba lagi rotasi kunci hingga berhasil.

Setelah rotasi kunci layanan berhasil, data baru yang ditulis ke layanan tidak dapat didekripsi dengan kunci layanan lama. Ini dilindungi dengan kunci baru yang hanya dikontrol oleh perangkat tepercaya pengguna, dan tidak pernah tersedia untuk Apple.

Perlindungan Data Lanjutan dan akses web iCloud.com

Saat pengguna menyalakan Perlindungan Data Lanjutan untuk pertama kalinya, akses web ke data mereka di iCloud.com dimatikan secara otomatis. Ini karena server web iCloud tidak lagi memiliki akses ke kunci yang diperlukan untuk mendekripsi dan menampilkan data pengguna. Pengguna dapat memilih untuk menyalakan lagi akses web dan menggunakan partisipasi perangkat tepercaya mereka untuk mengakses data iCloud terenkripsinya di web.

Setelah menyalakan akses web, pengguna harus mengesahkan proses masuk web di salah satu perangkat tepercaya mereka setiap kali mereka mengunjungi iCloud.com. Pengesahan “mengaktifkan” perangkat untuk akses web. Selama satu jam berikutnya, perangkat ini menerima permintaan dari server Apple tertentu untuk mengunggah kunci layanan individual, tetapi hanya yang terkait dengan daftar layanan yang diizinkan yang biasanya dapat diakses di iCloud.com. Dengan kata lain, bahkan setelah pengguna mengesahkan proses masuk web, permintaan server tidak dapat membuat perangkat pengguna mengunggah kunci layanan untuk data yang tidak dimaksudkan untuk dilihat di iCloud.com (seperti data Kesehatan atau kata sandi di Rantai Kunci iCloud). Server Apple hanya meminta kunci layanan yang diperlukan untuk mendekripsi data spesifik yang diminta pengguna untuk diakses di web. Setiap kali kunci layanan diunggah, kunci dienkripsi menggunakan kunci jangka pendek yang diikat ke sesi web yang disahkan pengguna dan pemberitahuan ditampilkan di perangkat pengguna, yang menunjukkan layanan iCloud yang datanya disediakan sementara untuk server Apple.

Mempertahankan pilihan pengguna

Perlindungan Data Lanjutan dan pengaturan akses web iCloud.com hanya dapat dimodifikasi oleh pengguna. Nilai ini disimpan di metadata perangkat Rantai Kunci iCloud pengguna dan hanya dapat diubah dari salah satu perangkat tepercaya pengguna. Server Apple tidak dapat memodifikasi pengaturan ini atas nama pengguna, juga tidak dapat mengembalikannya ke konfigurasi sebelumnya.

Implikasi keamanan dari berbagi dan kolaborasi

Di banyak kasus, saat pengguna berbagi konten untuk saling berkolaborasi—misalnya, dengan Catatan bersama, Pengingat bersama, folder bersama di iCloud Drive, atau Perpustakaan Foto Bersama iCloud—dan semua pengguna menyalakan Perlindungan Data Lanjutan, server Apple hanya digunakan untuk membuat operasi berbagi, tetapi tidak memiliki akses ke kunci enkripsi untuk data yang dibagikan. Konten tetap dienkripsi ujung ke ujung dan hanya dapat diakses di perangkat tepercaya peserta. Untuk setiap operasi berbagi, judul dan gambar kecil yang mewakili dapat disimpan oleh Apple dengan perlindungan data standar untuk menampilkan pratinjau kepada pengguna penerima.

Memilih opsi "semua orang dengan tautan" saat mengaktifkan kolaborasi akan membuat konten tersedia untuk server Apple di bawah perlindungan data standar, karena server harus dapat memberikan akses kepada siapa saja yang membuka URL.

Kolaborasi iWork dan fitur Album Bersama di Foto tidak mendukung Perlindungan Data Lanjutan. Saat pengguna berkolaborasi pada dokumen iWork, atau membuka dokumen iWork dari folder bersama di iCloud Drive, kunci enkripsi untuk dokumen diunggah dengan aman ke server iWork di pusat data Apple. Ini karena kolaborasi real time di iWork memerlukan mediasi sisi server untuk mengoordinasikan perubahan dokumen antarpeserta. Foto yang ditambahkan ke Album Bersama disimpan dengan perlindungan data standar, karena fitur memungkinkan album dibagikan secara publik di web.

Menonaktifkan Perlindungan Data Lanjutan

Pengguna dapat menonaktifkan Perlindungan Data Lanjutan kapan saja. Jika mereka memilih untuk melakukannya:

1. Perangkat pengguna terlebih dahulu merekam pilihan barunya di metadata partisipasi Rantai Kunci iCloud dan pengaturan ini diselaraskan dengan aman ke semua perangkat mereka.

2. Perangkat pengguna mengunggah kunci layanan untuk semua layanan *tersedia setelah pengesahan* dengan aman ke HSM iCloud di pusat data Apple. Ini tidak pernah menyertakan kunci untuk layanan yang dienkripsi ujung ke ujung di bawah perlindungan data standar, seperti Rantai Kunci iCloud dan Kesehatan.

Perangkat mengunggah kunci layanan asli, yang dibuat sebelum Perlindungan Data Lanjutan dinyalakan, dan kunci layanan baru yang dibuat setelah pengguna menyalakan fitur tersebut. Ini membuat semua data di layanan ini dapat diakses setelah autentikasi dan mengembalikan akun ke perlindungan data standar, tempat Apple dapat sekali lagi membantu pengguna memulihkan sebagian besar data mereka jika mereka kehilangan akses ke akun mereka.

Data iCloud tidak dicakup oleh Perlindungan Data Lanjutan

Karena kebutuhan untuk beroperasi dengan email global, kontak, dan sistem kalender, iCloud Mail, Kontak, dan Kalender tidak dienkripsi ujung ke ujung.

iCloud menyimpan beberapa data tanpa perlindungan kunci layanan CloudKit khusus pengguna, meskipun Perlindungan Data Lanjutan dinyalakan. Bidang Catatan CloudKit harus dinyatakan secara eksplisit sebagai "dienkripsi" di skema wadah agar terlindungi, dan membaca serta menulis bidang yang dienkripsi memerlukan penggunaan API khusus. Tanggal dan waktu saat file atau objek dimodifikasi digunakan untuk mengurutkan informasi pengguna, dan ceksum data file dan foto digunakan untuk membantu Apple menghapus duplikat dan mengoptimalkan penyimpanan iCloud dan perangkat pengguna—semua tanpa memiliki akses ke file dan foto itu sendiri. Detail mengenai bagaimana enkripsi digunakan untuk kategori data tertentu tersedia di artikel Dukungan Apple Tinjauan keamanan data iCloud.

Keputusan seperti penggunaan ceksum untuk menghapus duplikasi data—teknik terkenal yang disebut *enkripsi konvergen*—adalah bagian dari desain asli layanan iCloud saat diluncurkan. Metadata ini selalu dienkripsi, tetapi kunci enkripsi disimpan oleh Apple dengan perlindungan data standar. Untuk terus memperkuat perlindungan keamanan bagi semua pengguna, Apple berkomitmen untuk memastikan lebih banyak data, termasuk jenis metadata ini, dienkripsi ujung ke ujung saat Perlindungan Data Lanjutan dinyalakan.

Persyaratan Perlindungan Data Lanjutan

Persyaratan untuk menyalakan Perlindungan Data Lanjutan untuk iCloud mencakup hal berikut ini:

- Akun pengguna harus mendukung enkripsi ujung ke ujung. Enkripsi ujung ke ujung memerlukan autentikasi dua faktor untuk ID Apple dan kode sandi atau kata sandi yang diatur di perangkat tepercaya mereka. Untuk informasi lainnya, lihat artikel Dukungan Apple Autentikasi dua faktor untuk ID Apple.
- Perangkat tempat pengguna masuk dengan ID Apple mereka harus diperbarui ke iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2, dan versi terbaru iCloud untuk Windows. Persyaratan ini mencegah versi iOS, iPadOS, macOS, tvOS, atau watchOS sebelumnya salah menangani kunci layanan yang baru dibuat dengan mengunggahnya kembali ke HSM *tersedia setelah pengesahan* di upaya yang salah untuk memperbaiki status akun.
- Pengguna harus menyiapkan setidaknya satu metode pemulihan alternatif—satu atau beberapa kontak pemulihan atau kunci pemulihan—yang dapat digunakan untuk memulihkan data iCloud jika kehilangan akses ke akun.

Jika metode pemulihan gagal, misalnya jika informasi kontak pemulihan kedaluwarsa atau pengguna melupakannya, Apple tidak dapat membantu memulihkan data iCloud yang dienkripsi ujung ke ujung pengguna.

Perlindungan Data Lanjutan untuk iCloud hanya dapat dinyalakan untuk ID Apple. ID Apple yang Dikelola dan akun turunan (bervariasi menurut negara atau wilayah) tidak didukung.

Keamanan Cadangan iCloud

iCloud mencadangkan informasi—termasuk pengaturan perangkat, data app, foto, dan video di Rol Kamera, serta percakapan di app Pesan—setiap hari melalui Wi-Fi. Cadangan iCloud dilakukan hanya saat perangkat dikunci, tersambung ke sumber daya, dan memiliki akses Wi-Fi ke internet. Sadar akan enkripsi penyimpanan yang digunakan di iOS dan iPadOS, Cadangan iCloud dirancang untuk menjaga agar data tetap aman sembari memungkinkan dilakukannya pencadangan dan pemulihan bertahap yang tidak diawasi. Secara default, kunci layanan Cadangan iCloud dicadangkan dengan aman ke Modul Keamanan Perangkat Keras iCloud di pusat data Apple, dan merupakan bagian dari kategori data yang tersedia setelah pengesahan. Bagi pengguna yang menyalakan Perlindungan Data Lanjutan untuk iCloud, kunci layanan Cadangan iCloud dilindungi dengan enkripsi ujung ke ujung, dan hanya tersedia untuk pengguna di perangkat tepercaya mereka.

Saat file dibuat di kelas Perlindungan Data yang tidak dapat diakses ketika perangkat terkunci, kunci per filenya akan dienkripsi, menggunakan kunci kelas dari kantong kunci Cadangan iCloud, dan mencadangkan file ke iCloud dalam status asli yang dienkripsi. Semua file dienkripsi selama transpor dan, saat disimpan, dienkripsi menggunakan kunci berbasis akun, seperti yang dijelaskan di Enkripsi CloudKit.

Kantong kunci Cadangan iCloud berisi kunci asimetris (Curve25519) untuk kelas Perlindungan Data yang tidak dapat diakses saat perangkat terkunci. Kumpulan cadangan disimpan di akun iCloud pengguna dan berisi salinan file pengguna dan kantong kunci Cadangan iCloud. Kantong kunci Cadangan iCloud dilindungi oleh kunci acak, yang juga disimpan dengan kumpulan cadangan. Kata sandi iCloud pengguna tidak digunakan untuk enkripsi, sehingga perubahan kata sandi iCloud tidak akan membuat cadangan yang ada menjadi tidak sah.

Saat dipulihkan, file yang dicadangkan, kantong kunci Cadangan iCloud, dan kunci untuk kantong kunci diambil dari akun iCloud pengguna. Kantong kunci Cadangan iCloud didekripsi menggunakan kuncinya, lalu kunci per file di kantong kunci akan digunakan untuk mendekripsi file di kumpulan cadangan, yang dituliskan sebagai file baru di sistem file, sehingga akan membuatnya dienkripsi ulang sesuai dengan kelas Perlindungan Datanya.

Konten berikut dicadangkan menggunakan Cadangan iCloud:

- Data untuk musik, film, acara TV, app, dan buku yang dibeli. Cadangan iCloud pengguna berisi informasi mengenai konten yang dibeli yang terdapat di perangkat pengguna, tapi tidak terdapat di konten yang dibeli itu sendiri. Saat pengguna memulihkan dari Cadangan iCloud, konten yang sudah dibeli akan otomatis diunduh dari iTunes Store, App Store, app Apple TV, atau Apple Books. Beberapa jenis konten tidak diunduh secara otomatis di semua negara atau wilayah, dan pembelian sebelumnya mungkin tidak tersedia jika telah mendapatkan pengembalian dana atau tidak lagi tersedia di setiap tokonya. Riwayat pembelian lengkap dikaitkan dengan ID Apple pengguna.
- Foto dan video di perangkat pengguna. Ingat bahwa jika pengguna menyalakan Foto iCloud di iOS 8.1, iPadOS 13.1, atau OS X 10.10.3, (atau lebih baru), foto dan video mereka telah disimpan di iCloud, sehingga tidak disertakan di Cadangan iCloud pengguna.
- Kontak, acara kalender, pengingat, dan catatan
- Pengaturan perangkat
- Data app
- Layar Utama dan pengelolaan app

- Konfigurasi HomeKit
- Data ID Medis
- Kata sandi Memo Suara (jika perlu, memerlukan kartu SIM fisik yang digunakan pada saat pencadangan)
- Pesan, Apple Messages for Business, pesan teks (SMS), dan MMS (jika perlu, memerlukan kartu SIM fisik yang digunakan pada saat pencadangan)

Cadangan iCloud juga digunakan untuk mencadangkan rantai kunci perangkat lokal, yang dienkripsi dengan kunci yang berasal dari kunci kriptografis dasar UID Secure Enclave perangkat. Kunci ini unik untuk perangkat dan tidak diketahui oleh Apple. Ini memungkinkan database dipulihkan hanya ke perangkat yang sama dari dengan perangkat asalnya, dan artinya tidak ada orang lain, termasuk Apple, yang dapat membacanya. Untuk informasi lainnya, lihat Secure Enclave.

Pesan di iCloud

Pesan di iCloud terus memperbarui seluruh riwayat pesan pengguna dan tersedia di semua perangkat.

Dengan perlindungan data standar, Pesan di iCloud dienkripsi ujung ke ujung saat Cadangan iCloud dimatikan. Saat Cadangan iCloud dinyalakan, cadangan mencakup salinan kunci enkripsi Pesan di iCloud sehingga Apple dapat membantu pengguna memulihkan pesan mereka bahkan jika mereka kehilangan akses ke Rantai Kunci iCloud dan perangkat tepercaya. Jika pengguna mematikan Cadangan iCloud, kunci baru dibuat di perangkat mereka untuk melindungi Pesan di iCloud mendatang. Kunci baru disimpan hanya di Rantai Kunci iCloud, hanya dapat diakses oleh pengguna di perangkat tepercaya mereka, dan data baru yang ditulis ke wadah tidak dapat didekripsi dengan kunci wadah lama.

Dengan Perlindungan Data Lanjutan, Pesan di iCloud selalu dienkripsi ujung ke ujung. Saat Cadangan iCloud dinyalakan, segala sesuatu di dalamnya dienkripsi ujung ke ujung, termasuk kunci enkripsi Pesan di iCloud. Kunci layanan Cadangan iCloud, serta kunci wadah Pesan di iCloud keduanya diaktifkan saat pengguna menyalakan Perlindungan Data Lanjutan. Untuk informasi lainnya, lihat artikel Dukungan Apple Tinjauan keamanan data iCloud.

Keamanan kontak pemulihan akun

Pengguna dapat menambahkan hingga lima orang yang mereka percayai sebagai kontak pemulihan akun untuk membantu mereka memulihkan akun dan data iCloud mereka, termasuk semua data yang dienkripsi ujung ke ujungnya, terlepas apakah mereka menyalakan Perlindungan Data Lanjutan atau tidak. Baik Apple maupun kontak pemulihan tidak memiliki informasi yang diperlukan secara terpisah untuk memulihkan data iCloud terenkripsi ujung ke ujung pengguna.

Kontak Pemulihan dirancang dengan mempertimbangkan privasi pengguna. Kontak pemulihan pilihan pengguna tidak diketahui oleh Apple. Server Apple hanya mempelajari informasi mengenai kontak pemulihan di akhir upaya pemulihan setelah pengguna meminta bantuan kontak dan kontak mereka mulai benar-benar membantu pemulihan. Informasi tersebut tidak disimpan setelah pemulihan selesai.

Proses keamanan kontak pemulihan

Saat pengguna menyiapkan Kontak Pemulihan Akun, kunci untuk mengakses data iCloud pengguna–termasuk data CloudKit terenkripsi ujung ke ujung–dienkripsi dengan kunci acak yang kuat. Kunci acak ini kemudian dibagi antara kontak pemulihan dan Apple. Pada waktu pemulihan, hanya ketika dua pembagian kunci digabungkan kembali, kunci asli dapat dipulihkan dan data iCloud pengguna dapat diakses.

Untuk menyiapkan Kontak Pemulihan Akun, perangkat pengguna berkomunikasi dengan server Apple untuk mengunggah bagian informasi kunci yang akan disimpan Apple. Lalu perangkat membuat wadah CloudKit yang dienkripsi ujung ke ujung dengan kontak pemulihan untuk membagikan sebagian yang dibutuhkan kontak pemulihan. Apple dan kontak pemulihan juga menerima rahasia pengesahan yang sama dari pengguna, yang dibutuhkan nanti untuk pemulihan. Komunikasi untuk mengundang dan menerima kontak pemulihan dilakukan melalui saluran IDS yang saling disahkan. Kontak pemulihan secara otomatis menyimpan informasi yang diterima di Rantai Kunci iCloud mereka. Apple tidak dapat mengakses konten wadah CloudKit, maupun Rantai Kunci iCloud yang menyimpan informasi ini. Saat berbagi dilakukan, server Apple hanya melihat ID anonim untuk kontak pemulihan.

Nantinya, saat pengguna perlu memulihkan akun dan data iCloud mereka, mereka dapat meminta bantuan dari kontak pemulihan mereka. Pada saat itu, kode pemulihan dibuat oleh perangkat kontak pemulihan, yang lalu kontak pemulihan sediakan ke pengguna (misalnya secara langsung atau melalui panggilan telepon). Pengguna lalu memasukkan kode pemulihan ke perangkat mereka untuk membuat koneksi aman antarperangkat menggunakan protokol SPAKE2+, konten tidak dapat diakses oleh Apple. Interaksi ini diatur oleh server Apple, tapi Apple tidak dapat memulai proses pemulihan.

Setelah koneksi aman dibuat dan semua pemeriksaan keamanan yang diperlukan diselesaikan, perangkat kontak pemulihan mengembalikan bagian informasi kunci mereka dan rahasia pengesahan yang dibuat sebelumnya ke pengguna yang meminta pemulihan. Pengguna menunjukkan rahasia pengesahan ini ke server Apple, yang memberikan akses ke informasi kunci yang disimpan Apple. Menyediakan rahasia pengesahan juga mengesahkan pengaturan ulang kata sandi akun untuk memulihkan akses akun.

Akhirnya, perangkat pengguna menggabungkan kembali informasi kunci yang diterima dari Apple serta Kontak Pemulihan Akun, lalu menggunakannya untuk mendekripsi dan memulihkan data iCloud mereka.

Terdapat perlindungan untuk mencegah kontak pemulihan agar tidak memulai pemulihan tanpa persetujuan pengguna, yang meliputi pemeriksaan aktivitas di akun pengguna. Jika akun aktif digunakan, pemulihan yang menggunakan Kontak Pemulihan juga memerlukan kode sandi perangkat terbaru atau Kode Keamanan iCloud.

Keamanan Kontak Pewaris

Jika pengguna ingin data iCloud-nya dapat diakses ke pewaris yang ditentukan setelah pengguna berpulang, mereka dapat mengatur Kontak Pewaris di akun mereka. Pewaris Kontak Pewaris mendapatkan akses ke semua data iCloud milik pengguna yang berpulang, termasuk hampir semua data yang dienkripsi ujung ke ujung, tetapi tidak termasuk data Rantai Kunci iCloud seperti kata sandi akun. Teknologi yang mendasari Kontak Pewaris serupa dengan cara kerja Kontak Pemulihan—kunci acak kuat yang dipisahkan antara Apple dan kontak pewaris, sehingga tidak ada yang dapat mendekripsi data sendiri. Pewaris mendapatkan kelas data yang sama terlepas dari apakah pengguna menyalakan Perlindungan Data Lanjutan atau tidak.

Informasi kunci yang diterima oleh pewaris disebut sebagai kunci akses di dokumentasi pengguna dan disimpan secara otomatis di perangkat yang didukung, tetapi juga dapat dicetak dan disimpan secara offline untuk digunakan. Untuk informasi lainnya, lihat artikel dukungan Apple Cara menambahkan Kontak Pewaris untuk ID Apple Anda.

Setelah pengguna berpulang, Kontak Pewaris masuk ke situs web klaim Apple untuk memulai akses. Ini memerlukan sertifikat kematian dan pengesahan sebagai bagian dari rahasia pengesahan yang disebutkan di bagian sebelumnya. Setelah semua pemeriksaan keamanan selesai, Apple menerbitkan nama pengguna dan kata sandi untuk akun baru dan merilis informasi kunci penting ke Kontak Pewaris.

Untuk dengan mudah menginput kunci akses saat dibutuhkan, kunci akses ditunjukkan sebagai kode alfanumerik dengan kode QR terkait. Setelah dimasukkan, akses ke data iCloud pengguna yang berpulang dipulihkan. Ini dapat dilakukan di perangkat, atau akses dapat dibuat secara online. Untuk informasi lainnya, lihat artikel Dukungan Apple Meminta akses ke akun Apple sebagai Kontak Pewaris.

Keamanan Relai Pribadi iCloud

Relai Pribadi iCloud membantu melindungi pengguna terutama saat menelusuri web dengan Safari, tetapi fitur ini juga meliputi semua permintaan resolusi nama DNS. Ini membantu memastikan bahwa tidak ada satu pihak pun, bahkan Apple, yang dapat menghubungkan alamat IP pengguna dengan aktivitas penelusuran mereka. Hal ini dilakukan dengan menggunakan proxy berbeda, proxy masuk, yang dikelola oleh Apple, proxy keluar, yang dikelola oleh penyedia konten. Untuk menggunakan Relai Pribadi iCloud, pengguna harus menjalankan iOS 15, iPadOS 15, atau macOS 12.0.1, atau lebih baru, dan masuk ke akun iCloud+ dengan ID Apple milik mereka. Relai Pribadi iCloud dapat dinyalakan di Pengaturan > iCloud atau Pengaturan Sistem > iCloud.

Untuk informasi lainnya, lihat Tinjauan Relai Pribadi iCloud.

Pengelolaan kode sandi dan kata sandi

Tinjauan keamanan kata sandi

iOS, iPadOS, dan macOS memudahkan pengguna untuk mengesahkan app dan situs web pihak ketiga yang menggunakan kata sandi. Cara terbaik untuk mengelola kata sandi adalah dengan tidak menggunakannya. Masuk dengan Apple memungkinkan pengguna untuk masuk ke app dan situs web pihak ketiga tanpa harus membuat dan mengelola akun atau kata sandi tambahan sembari melindungi masuk dengan autentikasi dua faktor untuk ID Apple. Untuk situs yang tidak mendukung Masuk dengan Apple, fitur Kata Sandi Kuat Otomatis memungkinkan perangkat pengguna untuk membuat, menyelaraskan, dan memasukkan kata sandi kuat yang unik secara otomatis untuk situs dan app. Di iOS dan iPadOS, kata sandi disimpan ke rantai kunci Isi-Auto Kata Sandi khusus yang dikontrol pengguna dan dapat dikelola dengan membuka Pengaturan > Kata Sandi.

Di macOS, kata sandi yang disimpan dapat dikelola di preferensi Kata Sandi Safari. Sistem penyelarasan ini juga dapat digunakan untuk menyelaraskan kata sandi yang dibuat secara manual oleh pengguna.

Keamanan Masuk dengan Apple

Masuk dengan Apple adalah alternatif yang ramah privasi terhadap sistem masuk tunggal lainnya. Fitur ini menyediakan kenyamanan dan efisiensi dari masuk satu ketukan serta memberikan pengguna transparansi dan kontrol lebih terhadap informasi pribadinya.

Masuk dengan Apple memungkinkan pengguna untuk mengatur akun dan masuk ke app dan situs web menggunakan ID Apple yang telah mereka miliki, dan memberi mereka kontrol yang lebih besar atas informasi pribadi mereka. App hanya dapat meminta nama dan alamat email pengguna saat mengatur akun, dan pengguna selalu memiliki pilihan: Pengguna dapat membagikan alamat email pribadi mereka dengan app atau memilih untuk menjadikan emailnya tetap pribadi dan menggunakan layanan relai email pribadi baru dari Apple. Layanan relai email ini membagikan alamat email anonim unik yang meneruskan pesan ke alamat pribadi pengguna sehingga mereka masih dapat menerima komunikasi yang bermanfaat dari pengembang tanpa mengganggu privasi dan kontrol atas informasi pribadi mereka.

Masuk dengan Apple dibangun untuk keamanan. Setiap pengguna Masuk dengan Apple diharuskan untuk mengaktifkan autentikasi dua faktor untuk ID Apple mereka. Autentikasi dua faktor bukan hanya membantu mengamankan ID Apple pengguna, tapi juga akun yang mereka buat dengan app. Selain itu, Apple telah mengembangkan dan mengintegrasikan sinyal anti-penipuan yang aman bagi privasi ke Masuk dengan Apple. Sinyal ini memberikan pengembang kepercayaan bahwa pengguna baru yang mereka dapatkan adalah manusia dan bukan bot atau akun yang dibuat skrip.

Kata sandi kuat otomatis

Saat Rantai Kunci iCloud diaktifkan, iOS, iPadOS, dan macOS akan membuat kata sandi acak yang unik dan kuat saat pengguna mendaftar atau mengganti kata sandi mereka di situs web di Safari. Di iOS dan iPadOS, pembuatan kata sandi kuat otomatis juga tersedia di app. Pengguna harus menolak menggunakan kata sandi kuat. Kata sandi yang dibuat akan disimpan di rantai kunci dan terus diperbarui di semua perangkat dengan Rantai Kunci iCloud jika diaktifkan.

Secara default, kata sandi yang dibuat oleh iOS dan iPadOS memiliki 20 karakter. Kata sandi tersebut memiliki satu digit, satu karakter huruf besar, dua tanda hubung, dan 16 karakter huruf kecil. Kata sandi yang dibuat ini bersifat kuat dan berisi entropi 71 bit.

Kata sandi dibuat berdasarkan heuristik yang menentukan apakah pengalaman bidang kata sandi diperuntukkan bagi pembuatan kata sandi. Jika heuristik gagal mengenali bahwa kata sandi spesifik konteks digunakan saat pembuatan kata sandi, pengembang app dapat mengatur `UITextContentType.newPassword` di bidang teksnya, dan pengembang web dapat mengatur `autocomplete= "new-password"` di elemen <input> mereka.

Untuk membantu memastikan kata sandi yang dibuat kompatibel dengan layanan yang relevan, app dan situs web dapat memberikan aturan. Pengembang menyediakan aturan ini menggunakan atribut `UITextInputPasswordRules` atau `passwordrules` di elemen input mereka. Lalu, perangkat membuat kata sandi terkuat yang dapat mereka penuhi menggunakan aturan ini.

Keamanan Isi-Auto Kata Sandi

Isi-Auto Kata Sandi secara otomatis akan mengisikan info pengesahan yang disimpan di rantai kunci. Manajer kata sandi Rantai Kunci iCloud dan Isi-Auto Kata Sandi menyediakan fitur berikut:

- Mengisikan info pengesahan di app dan situs web
- Membuat kata sandi yang kuat
- Menyimpan kata sandi di app dan situs web di Safari
- Membagikan kata sandi dengan aman ke kontak pengguna
- Menyediakan kata sandi ke Apple TV di sekitar yang meminta info pengesahan

Pembuatan dan penyimpanan kata sandi di dalam app, serta penyediaan kata sandi ke Apple TV, hanya tersedia di iOS dan iPadOS.

Isi-Auto Kata Sandi untuk app

iOS dan iPadOS memungkinkan pengguna untuk memasukkan nama pengguna dan kata sandi yang disimpan ke bidang terkait info pengesahan di app, mirip dengan fungsi Isi-Auto Kata Sandi di Safari. Di iOS dan iPadOS, pengguna mengetuk jenis tombol di bar QuickType papan ketik perangkat lunak. Di macOS, untuk app yang dibuat dengan Mac Catalyst, menu menurun Kata Sandi akan muncul di bawah bidang terkait info pengesahan.

Jika suatu app memiliki kaitan yang kuat dengan situs web yang menggunakan mekanisme pengaitan app-situs web yang sama dan didukung oleh file apple-app-site-association yang sama, bar QuickType iOS dan iPadOS serta menu menurun macOS akan menyarankan info pengesahan secara langsung untuk app, jika ada yang disimpan ke Rantai Kunci Isi-Auto Kata Sandi. Dengan demikian, pengguna dapat memilih untuk mengungkapkan info pengesahan yang disimpan Safari ke app dengan properti keamanan yang sama, tanpa mengharuskan agar app mengadopsi API.

Isi-Auto Kata Sandi tidak mengungkapkan informasi pengesahan ke app hingga pengguna menyetujui untuk merilis info pengesahan ke app tersebut. Daftar info pengesahan dibuat dari atau dihadirkan di luar proses app.

Jika app dan situs web memiliki hubungan tepercaya dan pengguna mengirimkan info pengesahan di dalam app, iOS dan iPadOS dapat meminta pengguna untuk menyimpan info pengesahan tersebut ke rantai kunci Isi-Auto Kata Sandi untuk digunakan di kemudian waktu.

Akses app ke kata sandi yang disimpan

App iOS, iPadOS, dan macOS dapat meminta bantuan rantai kunci Isi-Auto Kata Sandi untuk memasukkan pengguna menggunakan `ASAuthorizationPasswordProvider` dan `SecAddSharedWebCredential`. Penyedia dan peminta kata sandi dapat digunakan bersama Masuk dengan Apple, sehingga API yang sama dipanggil untuk membantu pengguna masuk ke app, terlepas dari apakah akun pengguna berbasis kata sandi atau tidak, atau apakah akun pengguna dibuat menggunakan Masuk dengan Apple atau tidak.

App dapat mengakses kata sandi yang disimpan hanya jika pengembang app, administrator situs web, dan pengguna telah memberikan persetujuan mereka. Pengembang app menyatakan tujuannya untuk mengakses kata sandi yang disimpan Safari dengan menyertakan hak di app mereka. Hak tersebut mencantumkan nama domain yang sepenuhnya berkualifikasi dari situs web terkait dan situs web tersebut harus menempatkan file di server mereka yang mencantumkan pengenal unik app dari app yang telah disetujui oleh Apple.

Saat app dengan hak com.apple.developer.associated-domains diinstal, iOS dan iPadOS membuat permintaan TLS ke setiap situs web yang dicantumkan, yang meminta salah satu dari file berikut:

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

Jika file mencantumkan pengenal app dari app yang sedang diinstal, iOS dan iPadOS akan menandai situs web dan app sebagai memiliki hubungan tepercaya. Hanya dengan hubungan tepercaya, panggilan kedua API ini akan menghasilkan permintaan ke pengguna, yang harus setuju sebelum kata sandi dirilis ke app, diperbarui, atau dihapus.

Rekomendasi keamanan kata sandi

Daftar kata sandi isi-Auto Kata Sandi di iOS, iPadOS, dan macOS menunjukkan kata sandi pengguna tersimpan mana yang akan *digunakan kembali* dengan situs web lain, kata sandi mana yang dianggap *lemah*, serta kata sandi yang telah diretas oleh *kebocoran data*.

Tinjauan

Dengan menggunakan kata sandi yang sama untuk lebih dari satu layanan, akun terkait dapat menjadi rentan terhadap serangan pengisian info pengesahan. Jika layanan dibobol dan kata sandi dibocorkan, penyerang dapat mencoba info pengesahan yang sama di layanan lain untuk menyerang akun lainnya.

- Kata sandi ditandai sebagai *digunakan kembali* jika kata sandi yang sama terlihat digunakan untuk lebih dari satu kata sandi tersimpan di berbagai domain berbeda.
- Kata sandi akan ditandai sebagai *lemah* jika mudah ditebak oleh penyerang. iOS, iPadOS, dan macOS mendeteksi pola umum yang digunakan untuk membuat kata sandi yang mudah diingat, seperti menggunakan kata yang terdapat di kamus, penggantian karakter yang umum (seperti menggunakan “p4ssw0rd” alih-alih “password”), pola yang terdapat di papan ketik (seperti “q12we34r” dari papan ketik QWERTY), atau rangkaian berulang (seperti “123123”). Pola ini sering digunakan untuk membuat kata sandi yang memenuhi persyaratan minimum kata sandi untuk layanan, tapi juga tidak jarang digunakan oleh penyerang yang mencoba untuk memperoleh kata sandi menggunakan serangan brute-force.

  Karena sebagian besar layanan memerlukan khususnya kode PIN empat atau enam digit, kode sandi pendek ini dievaluasi dengan aturan yang berbeda. Kode PIN dianggap lemah jika termasuk sebagai kode PIN yang paling umum digunakan, jika merupakan rangkaian yang bertambah atau berkurang seperti “1234” atau “8765”, atau jika memiliki pola pengulangan, seperti “123123” atau “123321”.
- Kata sandi ditandai sebagai *bocor* jika fitur Pengawasan Kata Sandi dapat mengeklaim bahwa kata sandi telah berada di sebuah kebocoran data. Untuk informasi lainnya, lihat Pengawasan Kata Sandi.

Kata sandi yang lemah, digunakan kembali, dan bocor ditunjukkan dalam daftar kata sandi (macOS) atau berada di antarmuka Rekomendasi Keamanan terdedikasi (iOS serta iPadOS). Jika pengguna masuk ke situs web di Safari menggunakan kata sandi yang telah disimpan sebelumnya yang sangat lemah atau telah diretas oleh kebocoran data, pengguna akan diberi peringatan yang menganjurkan mereka untuk meningkatkan ke kata sandi kuat otomatis.

Meningkatkan keamanan pengesahan akun di iOS dan iPadOS

App yang mengimplementasikan Ekstensi Modifikasi Pengesahan Akun (di kerangka Layanan Pengesahan) dapat menyediakan peningkatan yang mudah dan sekali tekan untuk akun berdasarkan kata sandi sehingga dapat beralih ke penggunaan Masuk dengan Apple atau kata sandi kuat otomatis. Titik ekstensi ini tersedia di iOS dan iPadOS.

Jika app telah mengimplementasikan titik ekstensi dan diinstal di perangkat, pengguna akan melihat pilihan peningkatan ekstensi saat melihat Rekomendasi Keamanan untuk info pengesahan yang dikaitkan dengan app di manajer kata sandi Rantai Kunci iCloud di Pengaturan. Peningkatan juga ditawarkan saat pengguna masuk ke app dengan info pengesahan yang berisiko. App memiliki kemampuan untuk memberi tahu sistem untuk tidak memberikan pengguna pilihan peningkatan setelah masuk. Menggunakan API AuthenticationServices baru, app juga dapat mengaktifkan ekstensinya dan melakukan peningkatan sendiri, idealnya dari layar pengaturan akun atau manajemen akun di app.

App dapat memilih untuk mendukung peningkatan kata sandi kuat, peningkatan Masuk dengan Apple, atau keduanya. Dalam peningkatan kata sandi kuat, sistem membuat kata sandi kuat otomatis untuk pengguna. Jika perlu, app dapat menyediakan aturan kata sandi khusus untuk diikuti saat membuat kata sandi baru. Saat pengguna beralih akun dari menggunakan kata sandi ke menggunakan Masuk dengan Apple, sistem menyediakan info pengesahan Masuk dengan Apple baru ke ekstensi untuk mengaitkan akun. Email ID Apple pengguna tidak disediakan sebagai bagian dari info pengesahan. Setelah berhasil meningkatkan Masuk dengan Apple, sistem menghapus info pengesahan kata sandi yang digunakan sebelumnya dari rantai kunci pengguna jika disimpan di sana.

Ekstensi Modifikasi Pengesahan Akun memiliki kesempatan untuk melakukan pengesahan pengguna tambahan sebelum melakukan peningkatan. Untuk peningkatan yang dimulai dalam manajer kata sandi atau setelah masuk ke app, ekstensi menyediakan nama pengguna dan kata sandi untuk peningkatan akun. Untuk peningkatan in-app, hanya nama pengguna yang disediakan. Jika ekstensi memerlukan pengesahan pengguna lebih lanjut, ekstensi dapat meminta untuk menampilkan antarmuka pengguna khusus sebelum melanjutkan peningkatan. Kasus penggunaan yang dimaksudkan untuk menampilkan antarmuka pengguna ini adalah untuk meminta pengguna memasukkan faktor kedua dari autentikasi untuk mengesahkan peningkatan.

Pengawasan Kata Sandi

Pengawasan Kata Sandi adalah fitur yang mencocokkan kata sandi yang disimpan di rantai kunci Isi-Auto Kata Sandi pengguna dengan daftar kata sandi yang secara terus menerus diperbarui dan dikuratori yang diketahui telah terpapar di kebocoran dari organisasi online berbeda. Jika fitur dinyalakan, protokol yang mengawasi akan terus menerus mencocokkan kata sandi rantai kunci Isi-Auto Kata Sandi pengguna dengan daftar yang dikuratori.

Cara pengawasan berfungsi

Perangkat pengguna secara terus menerus melakukan pemeriksaan round robin pada kata sandi pengguna, yang meminta pada interval yang tidak bergantung pada sandi pengguna atau pola penggunaan pengelola kata sandi mereka. Ini membantu memastikan bahwa status verifikasi tetap diperbarui dengan daftar kata sandi bocor yang dikuratori saat ini. Untuk membantu mencegah bocornya informasi terkait berapa banyak kata sandi yang dimiliki oleh pengguna, permintaan ditumpuk dan dilakukan secara paralel. Sejumlah kata sandi tetap diverifikasi secara paralel di setiap pemeriksaan, dan jika pengguna memiliki jumlah yang lebih rendah dibandingkan jumlah ini, kata sandi acak akan dibuat dan ditambahkan ke permintaan untuk mengisi perbedaannya.

Cara kata sandi dicocokkan

Kata sandi dicocokkan dalam proses dua bagian. Kata sandi yang paling umum bocor diletakkan dalam daftar lokal di perangkat pengguna. Jika kata sandi pengguna ada dalam daftar, pengguna akan segera diberi tahu tanpa interaksi eksternal. Ini dirancang untuk memastikan bahwa tidak ada informasi yang bocor mengenai kata sandi yang dimiliki pengguna yang paling berisiko karena bocornya kata sandi.

Jika kata sandi tidak berada di daftar paling sering, kata sandi dicocokkan dengan kata sandi yang jarang bocor.

Membandingkan kata sandi pengguna dengan daftar yang dikuratori

Untuk memverifikasi apakah kata sandi yang tidak ada di daftar lokal sesuai atau tidak melibatkan beberapa interaksi dengan server Apple. Untuk membantu memastikan kata sandi asli milik pengguna tidak dikirim ke Apple, bentuk *antarbagian kumpulan pribadi* kriptografi disebarkan yang membandingkan kata sandi pengguna dengan kumpulan besar kata sandi yang bocor. Ini dirancang untuk memastikan bahwa untuk kata sandi yang memiliki risiko kebocoran yang lebih rendah, hanya sedikit informasi yang dibagikan dengan Apple. Untuk kata sandi pengguna, informasi ini terbatas pada prefiks 15 bit dari hash kriptografis. Penghapusan kata sandi yang paling sering bocor dari proses interaktif ini, menggunakan daftar lokal dari kata sandi yang paling sering bocor, mengurangi delta pada frekuensi relatif kata sandi yang bocor di dalam keranjang layanan web, yang membuat kata sandi pengguna menjadi susah diduga dari pencarian ini.

Protokol yang mendasari mempartisi daftar kata sandi yang dikuratori, yang memasukkan kira-kira 1,5 miliar kata sandi saat dokumen ini ditulis, ke dalam 2^{15} keranjang berbeda. Keranjang tempat kata sandi berada didasarkan pada 15 bit pertama dari nilai hash SHA256 kata sandi. Selain itu, setiap kata sandi yang bocor, pw, diasosiasikan dengan titik kurva eliptis pada kurva NIST P256: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, dengan α adalah kunci acak rahasia yang hanya diketahui oleh Apple dan H_{SWU} adalah fungsi oracle acak yang memetakan kata sandi ke titik kurva berdasarkan metode Shallue-van de Woestijne-Ulas. Transformasi ini dirancang untuk menyembunyikan nilai kata sandi secara komputasional dan membantu mencegah pengungkapan kata sandi yang baru bocor melalui Pengawasan Kata Sandi.

Untuk mengomputasi antarbagian kumpulan pribadi, perangkat pengguna menentukan keranjang tempat kata sandi pengguna berada menggunakan λ, prefiks 15 bit SHA256(upw), dengan upw adalah salah satu kata sandi pengguna. Perangkat membuat konstanta acaknya sendiri, β, dan mengirimkan titik $P_c = \beta \cdot H_{SWU}(upw)$ ke server, bersamaan dengan permintaan untuk keranjang yang sesuai dengan λ. Di sini, β menyembunyikan informasi mengenai kata sandi pengguna dan membatasi ke λ mengenai informasi yang terpapar dari kata sandi ke Apple. Akhirnya, server mengambil titik yang dikirimkan ke perangkat pengguna, mengomputasi, $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$, dan mengembalikannya, bersamaan dengan keranjang yang sesuai pada titik—$B\lambda = \{ P_{pw} \mid SHA256(pw)$ yang diawali dengan prefiks $\lambda\}$—ke perangkat.

Informasi yang dikembalikan memungkinkan pengguna untuk mengomputasi $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$, dan memastikan bahwa kata sandi pengguna telah dibocorkan jika $\alpha P_c \in B'_\lambda$.

Mengirimkan kata sandi ke pengguna atau perangkat Apple lain

Apple mengirim kata sandi dengan aman ke pengguna lain atau perangkat Apple dengan AirDrop dan di Apple TV.

Menyimpan info pengesahan ke perangkat lain dengan AirDrop

Saat iCloud diaktifkan, pengguna dapat menggunakan AirDrop untuk mengirim info pengesahan yang disimpan di perangkat lain. Info pengesahan meliputi nama dan kata sandi pengguna serta situs web tujuan penyimpanan. Pengiriman info pengesahan dengan AirDrop selalu dioperasikan dalam mode Hanya Kontak, terlepas dari pengaturan pengguna. Di perangkat yang menerima, setelah persetujuan pengguna, info pengesahan akan disimpan di Rantai Kunci Isi-Auto Kata Sandi pengguna.

Mengisikan info pengesahan di app di Apple TV

Isi-Auto Kata Sandi tersedia untuk mengisi info pengesahan di app di Apple TV. Saat pengguna fokus pada bidang teks nama pengguna atau kata sandi di tvOS, Apple TV akan mulai mengiklankan permintaan untuk Isi-Auto Kata Sandi melalui Bluetooth Rendah Energi (BLE).

Setiap iPhone, iPad, atau iPod touch yang berada di sekitar akan menampilkan perintah yang mengundang pengguna untuk membagikan info pengesahan dengan Apple TV. Berikut adalah cara metode enkripsi dibuat:

- Jika perangkat dan Apple TV menggunakan akun iCloud yang sama, enkripsi antarperangkat terjadi secara otomatis.
- Jika perangkat masuk ke akun iCloud selain yang digunakan oleh Apple TV, pengguna diminta untuk membuat koneksi terenkripsi melalui penggunaan kode PIN. Untuk menerima perintah ini, iPhone harus terbuka dan berada di dekat Siri Remote yang dipasangkan ke Apple TV tersebut.

Setelah koneksi terenkripsi dibuat menggunakan enkripsi tautan BLE, info pengesahan akan dikirimkan ke Apple TV dan diisikan secara otomatis ke bidang teks terkait di app.

Ekstensi penyedia info pengesahan

Di iOS, iPadOS, dan macOS, pengguna dapat menetapkan app pihak ketiga yang berpartisipasi sebagai penyedia info pengesahan untuk Isi-Auto Kata Sandi di pengaturan Kata Sandi (iOS serta iPadOS) atau di pengaturan Ekstensi di Preferensi Sistem (macOS). Mekanisme ini dibuat berlandaskan ekstensi app. Ekstensi penyedia info pengesahan harus menyediakan tampilan untuk memilih info pengesahan, dan ekstensi dapat secara opsional menyediakan metadata mengenai info pengesahan yang disimpan sehingga dapat ditawarkan secara langsung di bar QuickType (iOS dan iPadOS) atau di saran lengkapi otomatis (macOS). Metadata menyertakan situs web info pengesahan dan nama pengguna terkait tapi tidak kata sandinya. iOS, iPadOS, dan macOS akan berkomunikasi dengan ekstensi untuk mendapatkan kata sandi saat pengguna memilih untuk mengisi info pengesahan ke app atau situs web di Safari. Metadata info pengesahan disimpan di dalam wadah app penyedia info pengesahan dan dihapus secara otomatis setelah app dicopot.

Rantai Kunci iCloud

Tinjauan keamanan Rantai Kunci iCloud

iCloud memungkinkan pengguna untuk dengan aman menyelaraskan kata sandi mereka antara perangkat iOS, perangkat iPadOS, dan komputer Mac tanpa memperlihatkan informasi tersebut ke Apple. Selain privasi dan keamanan yang kuat, tujuan lain yang sangat berpengaruh pada rancangan dan arsitektur Rantai Kunci iCloud adalah kemudahan penggunaan dan fitur untuk memulihkan rantai kunci. Rantai Kunci iCloud terdiri dari dua layanan: penyelarasan rantai kunci dan pemulihan rantai kunci.

Apple merancang Rantai Kunci iCloud dan pemulihan rantai kunci sehingga kata sandi pengguna masih terlindungi dalam kondisi berikut:

- Akun iCloud pengguna disusupi.
- iCloud disusupi oleh penyerang eksternal atau karyawan.
- Pihak ketiga mengakses akun pengguna.

Integrasi manajer kata sandi dengan Rantai Kunci iCloud

iOS, iPadOS, dan macOS dapat secara otomatis membuat string acak kuat secara kriptografi untuk digunakan sebagai kata sandi akun di Safari. iOS dan iPadOS juga dapat membuat kata sandi yang kuat untuk app. Kata sandi yang dibuat disimpan di rantai kunci dan diselaraskan ke perangkat lainnya. Item Rantai Kunci ditransfer dari perangkat ke perangkat, dikirim melalui server Apple, tapi dienkripsi sedemikian rupa sehingga Apple dan perangkat lainnya tidak dapat membaca kontennya.

Penyelarasan rantai kunci aman

Saat pengguna mengaktifkan Rantai Kunci iCloud untuk pertama kalinya, perangkat membangun lingkaran kepercayaan dan membuat identitas penyelarasan untuk dirinya sendiri. Identitas penyelarasan berisi kunci pribadi dan kunci publik, dan disimpan di rantai kunci perangkat. Kunci publik identitas penyelarasan disimpan di lingkaran, dan lingkaran ditandatangani dua kali: pertama oleh kunci pribadi identitas penyelarasan, dan lalu oleh kunci eliptis asimetris (menggunakan P-256) turunan kata sandi akun iCloud pengguna. Juga yang disimpan bersama dengan lingkaran adalah parameter (salt dan iterasi acak) yang digunakan untuk membuat kunci berdasarkan kata sandi iCloud pengguna.

Untuk akun autentikasi dua faktor, lingkaran penyelarasan tambahan serupa dibuat dan disimpan di CloudKit. Identitas perangkat di sistem ini berisi dua pasang kunci eliptis asimetris (menggunakan P-384), juga disimpan di rantai kunci. Setiap perangkat masing-masing mempertahankan daftar identitas yang dipercayai, dan menandatangani daftar ini sebagai salah satu kunci identitasnya.

Penyelarasan iCloud dari lingkaran penyelarasan

Lingkaran penyelarasan yang ditandatangani disimpan di area penyimpanan nilai kunci iCloud pengguna. Lingkaran tidak dapat dibaca tanpa mengetahui kata sandi iCloud pengguna dan tidak dapat dimodifikasi dengan sah tanpa memiliki kunci pribadi identitas penyelarasan dari anggotanya.

Untuk akun autentikasi dua faktor, setiap daftar penyelarasan perangkat disimpan di CloudKit. Daftar tidak dapat dibaca tanpa mengetahui kata sandi iCloud pengguna, dan tidak dapat dimodifikasi tanpa memiliki kunci pribadi perangkat yang memilikinya.

Cara perangkat lain milik pengguna ditambahkan ke lingkaran penyelarasan

Perangkat baru, saat masuk ke iCloud, bergabung dengan lingkaran penyelarasan Rantai Kunci iCloud dengan satu dari dua cara: dengan memasangkan dan disponsori oleh perangkat Rantai Kunci iCloud yang ada, atau dengan menggunakan pemulihan Rantai Kunci iCloud.

Selama alur pemasangan, perangkat pendaftar membuat identitas penyelarasan baru untuk lingkaran penyelarasan dan daftar penyelarasan (untuk akun autentikasi dua faktor) dan menunjukkannya ke sponsor. Sponsor menambahkan kunci publik anggota baru ke lingkaran penyelarasan dan menandatanganinya kembali dengan identitas penyelarasan dan kunci turunan dari kata sandi iCloud pengguna. Lingkaran penyelarasan baru ditempatkan di iCloud, lalu ditandatangani secara serupa oleh anggota baru dari lingkaran. Di akun autentikasi dua faktor, perangkat sponsor juga menyediakan perangkat yang bergabung dengan *voucer* yang ditandatangani oleh kunci identitasnya, yang menunjukkan bahwa perangkat pendaftar harus dipercayai. Lalu perangkat memperbarui daftar identitas penyelarasan tepercayanya sendiri untuk menyertakan pendaftar.

Ada dua anggota lingkaran penanda tangan pada tahap ini, dan setiap anggota memiliki kunci publik rekannya. Kedua anggota akan mulai bertukar item rantai kunci individual melalui penyimpanan nilai kunci iCloud atau mereka menyimpannya di CloudKit, yang mana pun yang paling sesuai. Jika kedua anggota lingkaran memiliki pembaruan ke item yang sama, salah satunya akan dipilih, yang nantinya menghasilkan konsistensi. Setiap item yang diselaraskan akan dienkripsi sehingga hanya dapat didekripsi oleh perangkat di dalam lingkaran kepercayaan pengguna; item tidak dapat didekripsi oleh perangkat lain atau oleh Apple.

Saat perangkat baru bergabung ke lingkaran penyelarasan, “proses bergabung” ini diulangi. Misalnya, saat perangkat ketiga bergabung, perangkat dapat dipasangkan dengan salah satu perangkat yang ada. Saat rekan baru ditambahkan, tiap rekan akan diselaraskan dengan rekan baru. Ini dirancang untuk memastikan bahwa semua anggota memiliki item rantai kunci yang sama.

Hanya item tertentu yang diselaraskan

Beberapa item rantai kunci dikhususkan bagi perangkat, seperti kunci iMessage, maka dari itu harus tetap berada di perangkat. Sebagai hasilnya, setiap item yang akan diselaraskan harus ditandai secara eksplisit dengan atribut `kSecAttrSynchronizable`.

Apple mengatur atribut ini untuk data pengguna Safari (termasuk nama pengguna, kata sandi, dan nomor kartu kredit) serta untuk kata sandi Wi-Fi, kunci enkripsi HomeKit, dan item rantai kunci lainnya yang mendukung enkripsi iCloud ujung ke ujung.

Selain itu, secara default, item rantai kunci yang ditambahkan oleh app pihak ketiga tidak diselaraskan. Pengembang harus mengatur atribut `kSecAttrSynchronizable` saat menambahkan item ke rantai kunci.

Pemulihan Rantai Kunci iCloud aman

Rantai Kunci iCloud mengeskrow data rantai kunci pengguna kepada Apple *tanpa* mengizinkan Apple untuk membaca kata sandi dan data lainnya yang tersimpan. Meskipun pengguna hanya memiliki satu perangkat, pemulihan rantai kunci menyediakan jaring pengaman atas hilangnya data. Ini penting khususnya jika Safari digunakan untuk membuat kata sandi yang kuat dan acak untuk akun web, karena satu-satunya rekaman terkait kata sandi tersebut berada di rantai kunci.

Landasan pemulihan rantai kunci adalah pengesahan kedua dan layanan eskrow yang aman, yang dibuat oleh Apple khusus untuk mendukung fitur ini. Rantai kunci pengguna dienkripsi menggunakan kode sandi yang kuat, dan layanan eskrow akan menyediakan salinan rantai kunci hanya jika persyaratan yang ketat terpenuhi.

Penggunaan pengesahan kedua

Terdapat beberapa cara untuk membuat kode sandi kuat:

- Jika autentikasi dua faktor diaktifkan untuk akun pengguna, kode sandi pengguna akan digunakan untuk memulihkan rantai kunci yang dieskrow.
- Jika autentikasi dua faktor tidak diatur, pengguna diminta untuk membuat kode keamanan iCloud dengan menyediakan kode sandi enam digit. Di sisi lain, tanpa autentikasi dua faktor, pengguna dapat menetapkan kode mereka sendiri yang lebih panjang, atau mereka dapat mengizinkan perangkat untuk membuat kode acak kriptografis yang dapat mereka rekam dan simpan sendiri.

Proses eskrow rantai kunci

Setelah kode sandi dibuat, rantai kunci dieskrow dengan Apple. Perangkat iOS, iPadOS, atau macOS terlebih dahulu mengekspor salinan rantai kunci pengguna, lalu mengenkripsinya melalui pembungkusan kunci di kantong kunci asimetris, dan menempatkannya di area penyimpanan nilai kunci iCloud milik pengguna. Kantong kunci dibungkus dengan kode keamanan iCloud milik pengguna dan dengan kunci gugus modul keamanan perangkat keras (HSM) publik yang menyimpan rekaman eskrow. Ini menjadi *rekaman eskrow iCloud* pengguna. Untuk akun autentikasi dua faktor, rantai kunci juga disimpan di CloudKit dan dibungkus dengan kunci menengah yang hanya dapat dipulihkan dengan konten rekaman eskrow iCloud, yang oleh karenanya menyediakan tingkat perlindungan yang sama.

Konten rekaman eskrow juga memungkinkan perangkat yang memulihkan untuk bergabung kembali dengan Rantai Kunci iCloud, yang membuktikan ke perangkat yang ada bahwa perangkat yang memulihkan berhasil melakukan proses ekrow dan oleh karena itu disahkan oleh pemilik akun.

Catatan: Jika pengguna memutuskan untuk menerima kode keamanan acak kriptografis alih-alih menetapkan kodenya sendiri atau menggunakan nilai empat digit, rekaman eskrow tidak akan diperlukan. Sebagai gantinya, kode keamanan iCloud akan digunakan untuk membungkus kunci acak secara langsung.

Selain membuat kode keamanan, pengguna harus mendaftarkan nomor telepon. Ini menyediakan pengesahan level kedua pada saat pemulihan rantai kunci. Pengguna akan menerima pesan SMS yang harus dibalas agar pemulihan dapat dilanjutkan.

Keamanan eskrow untuk Rantai Kunci iCloud

iCloud menyediakan infrastruktur aman untuk eskrow rantai kunci untuk membantu memastikan bahwa hanya pengguna dan perangkat yang disahkan yang dapat melakukan pemulihan. Gugus modul keamanan perangkat keras (HSM) ditempatkan secara topografis di belakang iCloud berfungsi menjaga rekaman eskrow. Sebagaimana yang dijelaskan sebelumnya, setiap gugus memiliki kunci yang digunakan untuk mengenkripsi rekaman eskrow yang diawasi.

Untuk memulihkan rantai kunci, pengguna harus mengesahkan dengan kata sandi dan akun iCloud mereka dan merespons SMS yang dikirimkan ke nomor telepon mereka yang terdaftar. Setelah selesai, pengguna harus memasukkan kode keamanan iCloud mereka. Gugus HSM memverifikasi bahwa pengguna mengetahui kode keamanan iCloud-nya menggunakan protokol Kata Sandi Jarak Jauh Aman (SRP); kodenya sendiri tidak dikirimkan ke Apple. Setiap anggota gugus memverifikasi secara terpisah bahwa pengguna belum melampaui jumlah upaya maksimum yang diizinkan untuk mengambil rekamannya, sebagaimana yang dijelaskan di bawah. Jika sebagian besar setuju, gugus akan membuka bungkus rekaman eskrow dan mengirimkannya ke perangkat pengguna.

Berikutnya, perangkat menggunakan kode keamanan iCloud untuk membuka bungkus kunci acak yang digunakan untuk mengenkripsi rantai kunci pengguna. Dengan kunci tersebut, rantai kunci—diambil dari penyimpanan nilai kunci iCloud dan CloudKit—didekripsi dan dipulihkan ke perangkat. iOS, iPadOS, dan macOS hanya mengizinkan 10 percobaan untuk mengesahkan dan mengambil rekaman eskrow. Setelah beberapa upaya gagal, rekaman akan dikunci dan pengguna harus menghubungi Dukungan Apple untuk dapat mencoba kembali. Setelah 10 upaya gagal, gugus HSM akan menghancurkan rekaman eskrow dan rantai kunci akan hilang selamanya. Ini memberikan perlindungan dari upaya brute-force untuk mengambil rekaman, dengan mengorbankan data rantai kunci sebagai bentuk penanggulangan.

Kebijakan ini dikodekan di firmware HSM. Kartu akses administratif yang mengizinkan firmware untuk diubah telah dihancurkan. Setiap upaya untuk mengubah firmware atau mengakses kunci pribadi akan menyebabkan gugus HSM untuk menghapus kunci pribadi. Jika ini terjadi, pemilik setiap rantai kunci yang dilindungi oleh gugus akan menerima pesan yang memberi tahu bahwa rekaman eskrow mereka telah hilang. Mereka kemudian dapat memilih untuk mendaftar ulang.

Apple Pay

Tinjauan keamanan Apple Pay

Dengan Apple Pay, pengguna dapat menggunakan perangkat iPhone, iPad, Mac, dan Apple Watch yang didukung untuk bertransaksi secara mudah, aman, dan pribadi di toko, app, dan web di Safari. Pengguna juga dapat menambahkan kartu transit dengan Apple Pay yang diaktifkan, ID pelajar, dan kartu akses ke Dompet Apple. Mudah digunakan bagi pengguna, dan dibuat dengan keamanan terpadu di perangkat keras dan perangkat lunak.

Apple Pay juga dirancang untuk melindungi informasi pribadi pengguna. Apple Pay tidak mengumpulkan informasi transaksi yang dapat dikaitkan kembali dengan pengguna. Transaksi pembayaran terdapat di antara pengguna, penjual, dan penerbit kartu.

Keamanan komponen Apple Pay

Apple Pay menggunakan beberapa fitur perangkat keras dan perangkat lunak untuk menyediakan pembelian yang aman dan andal.

Elemen Aman

Elemen Aman adalah keping berstandar industri yang bersertifikat, yang menjalankan platform Java Card, dan tunduk pada persyaratan industri keuangan untuk pembayaran elektronik. IC Elemen Aman dan platform Java Card disertifikasi sesuai dengan proses Evaluasi Keamanan EMVCo. Setelah evaluasi keamanan berhasil diselesaikan, EMVCo mengeluarkan sertifikat IC dan platform yang unik.

IC Elemen Aman telah disertifikasi berdasarkan standar Common Criteria. Untuk informasi lainnya, lihat Sertifikasi keamanan Prosesor Secure Enclave di Sertifikasi Platform Apple.

Pengontrol NFC

Pengontrol NFC menangani protokol Komunikasi Medan Dekat dan menyalurkan komunikasi antara Prosesor Aplikasi dan Elemen Aman, serta antara Elemen Aman dan terminal tempat penjualan.

Dompet Apple

App Dompet Apple digunakan untuk menambah dan mengelola kartu kredit, debit, dan toko serta untuk melakukan pembayaran dengan Apple Pay. Pengguna dapat melihat kartu mereka dan mungkin dapat melihat informasi tambahan yang disediakan oleh penerbit kartu, seperti kebijakan privasi penerbit kartu, transaksi terbaru, dan lainnya di Dompet Apple. Pengguna juga dapat menambahkan kartu ke Apple Pay di:

- Asisten Pengaturan dan Pengaturan untuk iOS dan iPadOS
- App Apple Watch untuk Apple Watch
- Dompet & Apple Pay di Preferensi Sistem untuk komputer Mac dengan Touch ID

Selain itu, Dompet Apple memungkinkan pengguna untuk menambahkan dan mengelola kartu transit, kartu imbalan, boarding pass, tiket, kartu hadiah, kartu ID pelajar, kartu akses, dan lainnya.

Secure Enclave

Di iPhone, iPad, Apple Watch, komputer Mac dengan Touch ID, dan komputer Mac dengan Apple silicon yang menggunakan Magic Keyboard dengan Touch ID, Secure Enclave mengelola proses pengesahan dan mengizinkan transaksi pembayaran untuk melanjutkan.

Di Apple Watch, perangkat harus dibuka, dan pengguna harus mengeklik tombol samping dua kali. Klik dua kali akan terdeteksi dan diteruskan secara langsung ke Elemen Aman atau Secure Enclave jika tersedia, tanpa melalui Prosesor Aplikasi.

Server Apple Pay

Server Apple Pay mengelola pengaturan dan penyediaan kartu kredit, debit, transit, ID pelajar, dan kartu akses di Dompet Apple. Server juga mengelola Nomor Akun Perangkat yang disimpan di Elemen Aman. Server berkomunikasi dengan perangkat dan server jaringan pembayaran atau penerbit kartu. Server Apple Pay juga bertanggung jawab untuk mengenkripsi ulang info pengesahan pembayaran untuk pembayaran di dalam app atau web.

Cara Apple Pay memastikan keamanan pembelian pengguna

Elemen Aman

Elemen Aman menghosting applet yang dirancang secara khusus untuk mengelola Apple Pay. Elemen Aman juga disertai dengan applet yang disertifikasi oleh jaringan pembayaran atau penerbit kartu. Data kartu prabayar, kredit, atau debit dikirimkan dari jaringan pembayaran atau penerbit kartu yang dienkripsi untuk applet ini menggunakan kunci yang hanya diketahui oleh jaringan pembayaran atau penerbit kartu dan domain keamanan applet. Data ini disimpan di dalam applet ini dan dilindungi menggunakan fitur keamanan Elemen Aman. Selama transaksi, terminal akan berkomunikasi secara langsung dengan Elemen Aman melalui pengontrol komunikasi medan dekat (NFC) melalui bus perangkat keras khusus.

Pengontrol NFC

Sebagai gateway menuju Elemen Aman, pengontrol NFC membantu memastikan bahwa semua transaksi pembayaran nirkontak dilakukan menggunakan terminal tempat penjualan yang dekat dengan perangkat. Hanya permintaan pembayaran dari terminal jarak dekat yang ditandai oleh pengontrol NFC sebagai transaksi nirkontak.

Setelah pembayaran kartu kredit, debit, atau prabayar (termasuk kartu toko) disahkan oleh pemegang kartu menggunakan Face ID, Touch ID, atau kode sandi, atau di Apple Watch yang terbuka dengan mengeklik tombol samping dua kali, respons nirkontak yang disiapkan oleh applet pembayaran di dalam Elemen Aman dirutekan secara eksklusif oleh pengontrol ke area NFC. Karenanya, detail pengesahan pembayaran untuk transaksi pembayaran nirkontak disimpan di area NFC lokal dan tidak pernah dipaparkan pada Prosesor Aplikasi. Di sisi lain, detail pengesahan untuk pembayaran di dalam app dan di web dirutekan ke Prosesor Aplikasi, tapi hanya setelah enkripsi oleh Elemen Aman ke server Apple Pay.

Kartu kredit, debit, dan prabayar

Tinjauan keamanan penyediaan kartu

Saat pengguna menambahkan kartu prabayar, debit, atau kredit (termasuk kartu toko) ke Dompet Apple, Apple akan mengirimkan informasi kartu dengan aman, bersama dengan informasi lainnya mengenai akun dan perangkat pengguna, ke penerbit kartu atau penyedia layanan resmi dari penerbit kartu. Penerbit kartu akan menentukan apakah mereka akan menyetujui penambahan kartu ke Dompet Apple atau tidak dengan menggunakan informasi tersebut. Sebagai bagian dari proses penyediaan kartu, Apple Pay menggunakan tiga panggilan di server untuk mengirimkan dan menerima komunikasi dengan penerbit kartu atau jaringan:

- Bidang yang Diperlukan
- Periksa Kartu
- Penautan dan Penyediaan

Penerbit kartu atau jaringan menggunakan tiga panggilan ini untuk memverifikasi, menyetujui, dan menambahkan kartu ke Dompet Apple. Sesi klien-server ini menggunakan TLS 1.2 untuk mentransfer data.

Nomor lengkap kartu tidak disimpan di perangkat atau di server Apple Pay. Sebagai gantinya, Nomor Akun Perangkat unik dibuat, dienkripsi, dan kemudian disimpan di Elemen Aman. Nomor Akun Perangkat unik ini dienkripsi dengan cara yang tidak memungkinkan Apple untuk mengaksesnya. Nomor Akun Perangkat bersifat unik dan berbeda dari sebagian besar nomor kartu kredit atau debit; jaringan penerbit kartu atau pembayaran dapat mencegah penggunaannya pada kartu garis magnetis, melalui telepon, atau di situs web. Nomor Akun Perangkat di Elemen Aman tidak pernah disimpan di server Apple Pay atau dicadangkan ke iCloud, dan diisolasi dari iOS, iPadOS, dan watchOS serta dari komputer Mac dengan Touch ID.

Kartu yang diperuntukkan bagi Apple Watch disediakan kepada Apple Pay menggunakan app Apple Watch di iPhone, atau di dalam app iPhone penerbit kartu. Untuk menambahkan kartu ke Apple Watch, jam harus berada di jangkauan komunikasi Bluetooth. Kartu didaftarkan secara khusus untuk digunakan dengan Apple Watch dan memiliki Nomor Akun Perangkat-nya sendiri, yang disimpan di dalam Elemen Aman di Apple Watch.

Jika kartu kredit, debit, atau prabayar (termasuk kartu toko) ditambahkan, kartu tersebut akan muncul di daftar kartu selama Asisten Pengaturan di perangkat yang masuk ke akun iCloud yang sama. Kartu ini tetap berada di daftar ini selama berstatus aktif setidaknya di satu perangkat. Kartu dihapus dari daftar ini setelah dihapus dari semua perangkat selama 7 hari. Fitur ini mengharuskan autentikasi dua faktor untuk diaktifkan di akun iCloud masing-masing.

Menambahkan kartu kredit atau debit ke Apple Pay

Kartu kredit dapat ditambahkan secara manual ke Apple Pay di perangkat Apple.

Menambahkan kartu kredit atau debit secara manual

Untuk menambahkan kartu secara manual, nama, nomor kartu, tanggal kedaluwarsa, dan CVV akan digunakan untuk memfasilitasi proses penyediaan. Dari dalam Pengaturan, Dompet Apple, atau app Apple Watch, pengguna dapat memasukkan informasi tersebut dengan mengetik atau dengan menggunakan kamera perangkat. Saat kamera mengambil informasi kartu, Apple akan mencoba untuk mengisi nama, nomor kartu, dan tanggal kedaluwarsa. Foto tidak pernah disimpan ke perangkat atau disimpan di perpustakaan foto. Setelah semua bidang diisi, proses Periksa Kartu akan memverifikasi bidang selain CVV. Lalu, data dienkripsi dan dikirimkan ke server Apple Pay.

Jika ID syarat dan ketentuan dikembalikan bersama dengan proses Periksa Kartu, Apple akan mengunduh dan menampilkan syarat dan ketentuan penerbit kartu ke pengguna. Jika pengguna menerima syarat dan ketentuan, Apple akan mengirimkan ID syarat yang diterima, serta CVV ke proses Penautan dan Penyediaan. Selain itu, sebagai bagian dari proses Penautan dan Penyediaan, Apple membagikan informasi dari perangkat dengan penerbit kartu atau jaringan. Ini meliputi informasi mengenai (a) aktivitas akun iTunes dan App Store pengguna (misalnya, apakah pengguna memiliki riwayat transaksi yang panjang di iTunes), (b) perangkat pengguna (misalnya, nomor telepon, nama, dan model perangkat, serta perangkat Apple pelengkap yang diperlukan untuk mengatur Apple Pay), dan (c) perkiraan lokasi pengguna pada saat menambahkan kartu (jika pengguna mengaktifkan Layanan Lokasi). Penerbit kartu akan menentukan apakah mereka akan menyetujui penambahan kartu ke Apple Pay atau tidak dengan menggunakan informasi tersebut.

Sebagai hasil dari proses Penautan dan Penyediaan, dua hal terjadi:

- Perangkat mulai mengunduh file pass Dompet Apple yang mewakili kartu kredit atau debit.
- Perangkat mulai mengikat kartu ke Elemen Aman.

File pass berisi URL untuk mengunduh gambar kartu, metadata mengenai kartu seperti informasi kontak, app penerbit terkait, dan fitur yang didukung. File pass juga berisi status pass, yang dilengkapi dengan informasi seperti apakah penyesuaian Elemen Aman telah selesai, apakah kartu sedang ditangguhkan oleh penerbit kartu, apakah pengesahan tambahan diperlukan sebelum kartu dapat digunakan untuk bertransaksi dengan Apple Pay.

Menambahkan kartu kredit atau debit dari akun iTunes Store

Untuk kartu kredit atau debit yang digunakan dengan iTunes, pengguna dapat diwajibkan untuk memasukkan kembali kata sandi ID Apple mereka. Nomor kartu diambil dari iTunes, dan proses Periksa Kartu akan dimulai. Jika kartu layak untuk Apple Pay, perangkat akan mengunduh dan menampilkan syarat dan ketentuan, lalu mengirimkan ID syarat dan kode keamanan kartu ke proses Penautan dan Penyediaan. Verifikasi tambahan dapat dilakukan untuk kartu akun iTunes yang digunakan.

Menambahkan kartu kredit atau debit dari app penerbit kartu

Saat app didaftarkan untuk digunakan dengan Apple Pay, kunci akan dibuat untuk app dan untuk server penerbit kartu. Kunci ini digunakan untuk mengenkripsi informasi kartu yang dikirimkan ke penerbit kartu. Ini dirancang untuk mencegah informasi agar tidak dibaca oleh perangkat Apple. Alur penyediaan ini mirip dengan yang digunakan untuk kartu yang ditambahkan secara manual, yang dijelaskan sebelumnya, kecuali bahwa kata sandi sekali pakai digunakan sebagai ganti CVV.

Menambahkan kartu kredit atau debit dari situs web penerbit kartu

Beberapa penerbit kartu menyediakan kemampuan untuk memulai proses penyediaan kartu untuk Dompet Apple secara langsung dari situs web mereka. Dalam kasus ini, pengguna memulai tugas dengan memilih kartu untuk disediakan di situs web penerbit kartu. Pengguna lalu diarahkan ke pengalaman masuk Apple yang berdiri sendiri (berada dalam domain Apple) dan diminta untuk masuk dengan ID Apple mereka. Saat berhasil masuk, pengguna lalu memilih satu atau beberapa perangkat sebagai tujuan penyediaan kartu dan diharuskan untuk mengonfirmasi hasil penyediaan di setiap perangkat target.

Menambahkan verifikasi tambahan

Penerbit kartu dapat memutuskan apakah kartu kredit atau debit memerlukan verifikasi tambahan atau tidak. Bergantung pada apa yang ditawarkan oleh penerbit kartu, pengguna dapat memilih berbagai opsi untuk verifikasi tambahan, seperti pesan teks, email, panggilan layanan konsumen, atau metode di app pihak ketiga yang disetujui untuk menyelesaikan verifikasi. Untuk pesan teks atau email, pengguna memilih dari informasi kontak yang dimiliki penerbit. Kode akan dikirimkan, yang harus dimasukkan ke Dompet Apple, Pengaturan, atau app Apple Watch. Untuk layanan pelanggan atau verifikasi menggunakan app, penerbit menjalankan proses komunikasinya sendiri.

Pengesahan pembayaran dengan Apple Pay

Untuk perangkat yang memiliki Secure Enclave, pembayaran hanya dapat dilakukan setelah menerima pengesahan dari Secure Enclave. Di iPhone atau iPad, proses ini disertai dengan konfirmasi bahwa pengguna telah mengesahkan dengan Face ID, Touch ID, atau kode sandi perangkat. Face ID atau Touch ID, jika tersedia, adalah metode default, tapi kode sandi dapat digunakan kapan pun. Kode sandi ditawarkan secara otomatis setiap tiga percobaan gagal untuk mencocokkan sidik jari, atau dua percobaan gagal untuk mencocokkan wajah, setelah lima percobaan gagal, kode sandi akan diwajibkan. Kode sandi juga diperlukan saat Face ID atau Touch ID tidak dikonfigurasi atau tidak diaktifkan untuk Apple Pay. Agar pembayaran dapat dilakukan di Apple Watch, perangkat harus dibuka dengan kode sandi dan tombol samping harus diklik dua kali.

Menggunakan kunci pemasangan bersama

Komunikasi antara Secure Enclave dan Elemen Aman berlangsung melalui antarmuka serial, dengan Elemen Aman yang terhubung ke pengontrol NFC, yang pada gilirannya akan dihubungkan ke Prosesor Aplikasi. Meskipun tidak terhubung secara langsung, Secure Enclave dan Elemen Aman dapat berkomunikasi secara aman menggunakan kunci pemasangan bersama yang disediakan selama proses produksi. Enkripsi dan pengesahan komunikasi didasarkan pada AES, dengan nonce kriptografis yang digunakan oleh kedua pihak untuk melindungi dari serangan pemutaran ulang. Kunci pemasangan dibuat di dalam Secure Enclave dari kunci UID-nya dan pengenal unik Elemen Aman. Kunci pemasangan kemudian ditransfer secara aman dari Secure Enclave ke modul keamanan perangkat keras (HSM) di pabrik, yang memiliki materi pokok yang diperlukan untuk memasukkan kunci pemasangan ke Elemen Aman.

Mengesahkan transaksi aman

Saat pengguna mengesahkan transaksi, yang meliputi gerakan fisik yang dikomunikasikan secara langsung ke Secure Enclave, lalu Secure Enclave akan mengirimkan data bertanda tangan mengenai jenis pengesahan dan detail mengenai jenis transaksi (nirkontak atau di dalam app) ke Elemen Aman, yang dikaitkan dengan nilai Pengesahan Acak (AR). Nilai AR dibuat di Secure Enclave saat pengguna menyediakan kartu kredit untuk pertama kalinya dan dipertahankan saat Apple Pay diaktifkan, dilindungi oleh enkripsi Secure Enclave dan mekanisme anti-rollback. AR dikirimkan dengan aman ke Elemen Aman dengan memanfaatkan kunci pemasangan. Setelah menerima nilai AR baru, Elemen Aman menandai setiap kartu yang ditambahkan sebelumnya sebagai dihapus.

Menggunakan kriptogram pembayaran untuk keamanan dinamis

Transaksi pembayaran dari applet pembayaran termasuk kriptogram pembayaran beserta Nomor Akun Perangkat. Kriptogram ini, kode sekali pakai, dihitung menggunakan penghitung transaksi dan kunci. Penghitung transaksi akan bertambah untuk setiap transaksi baru. Kunci disediakan di applet pembayaran selama personalisasi dan diketahui oleh jaringan pembayaran atau penerbit kartu atau keduanya. Bergantung pada skema pembayaran, data lainnya juga dapat digunakan dalam penghitungan, termasuk:

- Nomor yang Tidak Dapat Diprediksi Terminal, untuk transaksi komunikasi medan dekat (NFC)
- Nonce server Apple Pay, untuk transaksi dalam app

Kode keamanan ini disediakan untuk jaringan pembayaran dan untuk penerbit kartu, yang memungkinkan penerbit untuk memverifikasi setiap transaksi. Panjang kode keamanan ini dapat berbeda-beda tergantung jenis transaksi.

Membayar dengan kartu menggunakan Apple Pay

Apple Pay dapat digunakan untuk membayar pembelian di toko, dalam app, dan di situs web.

Membayar dengan kartu di toko

Jika iPhone atau Apple Watch menyala dan mendeteksi area NFC, perangkat akan memberi pengguna kartu yang diminta (jika pilihan otomatis dinyalakan untuk kartu tersebut) atau kartu default, yang dikelola di Pengaturan. Pengguna juga dapat membuka Dompet Apple dan memilih kartu, atau saat perangkat dikunci, dapat:

- Mengeklik dua kali tombol samping di perangkat dengan Face ID
- Mengeklik dua kali tombol Utama di perangkat dengan Touch ID
- Menggunakan fitur Aksesibilitas yang memungkinkan Apple Pay dari Layar Terkunci

Selanjutnya, sebelum informasi pembayaran dikirimkan, pengguna harus mengesahkan menggunakan Face ID, Touch ID, atau kode sandi mereka. Setelah Apple Watch dibuka, kartu default untuk pembayaran akan diaktifkan jika tombol samping diklik dua kali. Tidak ada informasi pembayaran yang dikirimkan tanpa pengesahan pengguna.

Setelah pengguna mengesahkan, Nomor Akun Perangkat dan kode keamanan dinamis khusus transaksi akan digunakan saat memproses pembayaran. Apple atau perangkat pengguna tidak akan mengirim nomor lengkap kartu kredit atau debit ke penjual. Apple dapat menerima informasi transaksi anonim seperti perkiraan waktu dan lokasi transaksi, yang membantu Apple Pay dan produk serta layanan Apple lainnya.

Membayar dengan kartu dalam app

Apple Pay juga dapat digunakan untuk melakukan pembayaran di app iPhone, iPad, dan Apple Watch. Saat pengguna membayar dalam app menggunakan Apple Pay, Apple menerima informasi transaksi terenkripsi. Sebelum informasi tersebut dikirimkan ke pengembang atau penjual, Apple mengenkripsi ulang transaksi dengan kunci khusus pengembang. Apple Pay akan menyimpan informasi transaksi anonim, seperti perkiraan jumlah pembelian. Informasi ini tidak dapat dikaitkan ke pengguna dan tidak akan menyertakan apa yang dibeli pengguna.

Saat app memulai transaksi pembayaran Apple Pay, server Apple Pay akan menerima transaksi terenkripsi dari perangkat sebelum penjual menerimanya. Server Apple Pay kemudian akan mengenkripsinya kembali dengan kunci khusus penjual sebelum mengirimkannya ke penjual.

Ketika app meminta pembayaran, app memanggil API untuk menentukan apakah perangkat mendukung Apple Pay dan apakah pengguna memiliki kartu kredit atau debit yang dapat digunakan untuk membayar di jaringan pembayaran yang diterima oleh penjual. App meminta informasi yang diperlukan untuk memproses dan melengkapi transaksi, seperti alamat penagihan dan pengiriman, dan informasi kontak. App kemudian akan meminta iOS, iPadOS, atau watchOS untuk mengeluarkan lembar Apple Pay, yang akan meminta informasi untuk app, serta informasi lainnya yang diperlukan, seperti kartu yang akan digunakan.

Pada tahap ini, app akan diberi informasi kota, negara bagian, dan kode pos untuk menghitung total biaya pengiriman. Informasi lengkap tidak akan diberikan kepada app hingga pengguna mengesahkan pembayaran dengan Face ID, Touch ID, atau kode sandi perangkat. Setelah pembayaran disahkan, informasi yang diberikan di lembar Apple Pay akan ditransfer ke penjual.

Pengesahan pembayaran app

Ketika pengguna mengesahkan pembayaran, panggilan akan dilakukan ke server Apple Pay untuk mendapatkan nonce kriptografis, yang mirip dengan nilai yang dikembalikan oleh terminal NFC yang digunakan untuk transaksi dalam toko. Nonce, bersama dengan data transaksi lainnya, diteruskan ke Elemen Aman untuk mengomputasi info pengesahan pembayaran yang dienkripsi dengan kunci Apple. Info pengesahan pembayaran terenkripsi dikembalikan ke server Apple Pay, yang mendekripsi info pengesahan, memverifikasi nonce di info pengesahan berdasarkan nonce yang pada awalnya dikirimkan oleh server Apple Pay, dan mengenkripsi ulang info pengesahan pembayaran dengan kunci penjual yang dikaitkan dengan ID Penjual. Lalu, pembayaran akan dikembalikan ke perangkat, yang akan menyerahkannya kembali ke app melalui API. App kemudian akan meneruskannya ke sistem penjual untuk diproses. Penjual dapat mendekripsi info pengesahan pembayaran dengan kunci pribadinya untuk diproses. Ini, bersama dengan tanda tangan dari server Apple, memungkinkan penjual untuk memverifikasi transaksi yang ditujukan untuk penjual ini.

API memerlukan hak yang menetapkan ID Penjual yang didukung. App juga dapat menyertakan data tambahan (seperti nomor pesanan atau identitas konsumen) untuk dikirimkan ke Elemen Aman untuk ditandatangani, sehingga memastikan bahwa transaksi tidak dapat dialihkan ke konsumen lain. Hal ini dapat dilakukan oleh pengembang app, yang dapat menetapkan applicationData di PKPaymentRequest. Hash dari data ini disertakan di data pembayaran terenkripsi. Penjual kemudian bertanggung jawab untuk memverifikasi bahwa hash applicationData cocok dengan apa yang disertakan di data pembayaran.

Membayar dengan kartu di situs web

Apple Pay dapat digunakan untuk melakukan pembayaran di situs web di iPhone, iPad, Apple Watch, dan komputer Mac dengan Touch ID. Transaksi Apple Pay juga dapat dimulai di Mac dan diselesaikan di iPhone atau Apple Watch dengan Apple Pay yang diaktifkan menggunakan akun iCloud yang sama.

Apple Pay di web mengharuskan semua situs web yang berpartisipasi untuk mendaftar ke Apple. Setelah domain terdaftar, validasi nama domain dilakukan hanya setelah Apple menerbitkan sertifikat klien TLS. Situs web yang mendukung Apple Pay diharuskan untuk menyajikan konten mereka melalui HTTPS. Untuk setiap transaksi pembayaran, situs web harus mendapatkan sesi penjual yang aman dan unik dengan server Apple menggunakan sertifikat klien TLS yang diterbitkan Apple. Data sesi penjual ditandatangani oleh Apple. Setelah tanda tangan sesi penjual diverifikasi, situs web dapat bertanya apakah pengguna memiliki perangkat yang mendukung Apple Pay dan apakah terdapat kartu prabayar, debit, atau kredit yang diaktifkan di perangkat tersebut. Tidak ada detail lainnya yang dibagikan. Jika pengguna tidak ingin membagikan informasi ini, mereka dapat menonaktifkan permintaan Apple Pay di pengaturan privasi Safari di perangkat iPhone, iPad, dan Mac.

Setelah sesi penjual divalidasi, semua langkah privasi dan keamanan berlangsung sama seperti ketika pengguna membayar di dalam app.

Jika pengguna mengirimkan informasi terkait pembayaran dari Mac ke iPhone atau Apple Watch, Handoff Apple Pay menggunakan protokol Layanan Identitas (IDS) Apple terenkripsi ujung ke ujung untuk mengirimkan informasi terkait pembayaran antara Mac pengguna dan perangkat memberi pengesahan. Klien IDS di Mac menggunakan kunci perangkat pengguna untuk menjalankan enkripsi sehingga tidak ada perangkat lainnya dapat mendekripsi informasi ini, dan kunci tersebut tidak tersedia bagi Apple. Penemuan perangkat untuk Handoff Apple Pay melibatkan informasi mengenai jenis dan pengenal unik dari kartu kredit pengguna serta beberapa metadata. Nomor akun khusus perangkat dari kartu pengguna tidak dibagikan dan terus disimpan dengan aman di iPhone atau Apple Watch pengguna. Apple juga dengan aman mentransfer alamat kontak, pengiriman, dan penagihan pengguna yang baru digunakan melalui Rantai Kunci iCloud.

Setelah pengguna mengesahkan pembayaran menggunakan Face ID, Touch ID, kode sandi, atau mengeklik tombol samping dua kali di Apple Watch, token pembayaran yang dienkripsi secara unik ke sertifikat penjual milik setiap situs web dikirimkan secara aman dari iPhone atau Apple Watch pengguna ke Mac mereka dan kemudian dikirimkan ke situs web penjual.

Hanya perangkat yang saling berdekatan yang dapat meminta dan menyelesaikan pembayaran. Jarak ditetapkan melalui penerapan Bluetooth Rendah Energi (BLE).

Pass nirkontak di Apple Pay

Untuk mengirimkan data dari pass yang didukung ke terminal NFC yang kompatibel, Apple menggunakan protokol Layanan Nilai Tambah Apple (Apple VAS). Protokol VAS dapat diterapkan di terminal nirkontak atau di app iPhone dan menggunakan NFC untuk berkomunikasi dengan perangkat Apple yang didukung. Protokol VAS dapat berfungsi dalam jarak pendek dan dapat digunakan untuk mengaktifkan pass nirkontak secara terpisah atau sebagai bagian dari transaksi Apple Pay.

Saat perangkat didekatkan ke terminal NFC, terminal tersebut akan mulai menerima informasi pass dengan mengirimkan permintaan untuk pass. Jika pengguna memiliki pass dengan pengenal penyedia pass, pengguna akan diminta untuk mengesahkan penggunaannya dengan Face ID, Touch ID, atau kode sandi. Informasi pass, tanda waktu, kunci P-256 ECDH acak sekali pakai akan digunakan dengan kunci publik penyedia pass untuk membuat kunci enkripsi untuk data pass, yang akan dikirimkan ke terminal.

Dari iOS 12.0.1 hingga dan termasuk iOS 13, pengguna dapat memilih pass secara manual sebelum menggunakannya di terminal NFC penjual. Di iOS 13.1 atau lebih baru, penyedia pass dapat mengonfigurasi pass yang dipilih secara manual agar memerlukan pengesahan pengguna atau agar dapat digunakan tanpa pengesahan.

Menjadikan kartu tidak dapat digunakan dengan Apple Pay

Kartu prabayar, debit, dan kredit yang ditambahkan ke Elemen Aman hanya dapat digunakan jika Elemen Aman diberikan dengan pengesahan menggunakan kunci pemasangan yang sama dan nilai Pengacakan Pengesahan (AR) dari saat kartu ditambahkan. Setelah menerima nilai AR baru, Elemen Aman menandai setiap kartu yang ditambahkan sebelumnya sebagai dihapus. Ini juga memungkinkan sistem operasi untuk menginstruksikan Secure Enclave untuk membuat kartu menjadi tidak dapat digunakan dengan menandai salinan AR-nya sebagai tidak sah dengan skenario berikut:

Metode	Perangkat
Kode sandi dinonaktifkan.	iPhone, iPad, Apple Watch
Kata sandi dinonaktifkan.	Mac
Pengguna keluar dari iCloud.	iPhone, iPad, Mac, Apple Watch
Pengguna memilih Hapus Semua Konten & Pengaturan.	iPhone, iPad, Mac, Apple Watch
Perangkat dipulihkan dari Mode Pemulihan.	iPhone, iPad, Mac, Apple Watch
Pelepasan	Apple Watch

Menangguhkan dan menghapus kartu

Pengguna dapat menangguhkan Apple Pay di iPhone, iPad, dan Apple Watch dengan menyalakan Mode Hilang di perangkat menggunakan Lacak. Pengguna juga dapat menghapus kartu mereka dari Apple Pay menggunakan Lacak, iCloud.com, atau langsung di perangkat mereka menggunakan Dompet Apple. Di Apple Watch, kartu dapat dihapus menggunakan pengaturan iCloud, app Apple Watch di iPhone, atau langsung di Apple Watch. Fitur untuk melakukan pembayaran menggunakan kartu di perangkat akan ditangguhkan atau dihapus dari Apple Pay oleh penerbit kartu atau jaringan pembayaran terkait meskipun perangkat offline dan tidak terhubung ke jaringan seluler atau Wi-Fi. Pengguna juga dapat menghubungi penerbit kartunya untuk menangguhkan atau menghapus kartu dari Apple Pay.

Saat pengguna menghapus keseluruhan perangkat—menggunakan Hapus Semua Konten & Pengaturan, dengan Lacak, atau memulihkan perangkatnya—iPhone, iPad, iPod touch, Mac, dan Apple Watch memerintahkan Elemen Aman untuk menandai semua kartu sebagai dihapus. Tindakan ini langsung membuat kartu menjadi tidak dapat digunakan hingga server Apple Pay dapat dihubungi untuk menghapus kartu sepenuhnya dari Elemen Aman. Terlepas dari itu, Secure Enclave menandai AR sebagai tidak sah, sehingga kartu yang didaftarkan sebelumnya tidak mungkin mendapatkan pengesahan pembayaran lebih lanjut. Saat online, perangkat akan mencoba untuk menghubungi server Apple Pay untuk membantu memastikan bahwa semua kartu di Elemen Aman dihapus.

Keamanan Apple Card

Di model iPhone dan Mac yang didukung, pengguna dapat mengajukan Apple Card dengan aman.

Pengajuan Apple Card

Di iOS 12.4 atau lebih baru, macOS 10.14.6 atau lebih baru, dan watchOS 5.3 atau lebih baru, Apple Card dapat digunakan dengan Apple Pay untuk melakukan pembayaran di toko, app, dan situs web.

Untuk mengajukan Apple Card, pengguna harus masuk ke akun iCloud mereka di perangkat iOS atau iPadOS yang kompatibel dengan Apple Pay dan mengatur autentikasi dua faktor di akun iCloud. Jika pengajuan disetujui, Apple Card akan tersedia di Dompet Apple atau di Pengaturan > Dompet & Apple Pay di semua perangkat yang memenuhi syarat tempat pengguna telah masuk dengan ID Apple mereka.

Saat pengguna mengajukan Apple Card, informasi identitas pengguna diverifikasi dengan aman oleh mitra penyedia identitas Apple, lalu dibagikan dengan Goldman Sachs Bank USA untuk tujuan evaluasi identitas dan kredit.

Informasi seperti nomor jaminan sosial, atau gambar dokumen identitas yang disediakan selama pengajuan, dikirimkan dengan aman ke mitra penyedia identitas Apple dan/atau Goldman Sachs Bank USA dalam kondisi terenkripsi dengan kuncinya masing-masing. Apple tidak dapat mendekripsi data ini.

Informasi pemasukan yang disediakan selama pengajuan, dan informasi rekening bank yang digunakan untuk pembayaran tagihan, dikirimkan dengan aman ke Goldman Sachs Bank USA dalam kondisi terenkripsi dengan kuncinya. Informasi rekening bank disimpan di rantai kunci. Apple tidak dapat mendekripsi data ini.

Saat menambahkan Apple Card ke Dompet Apple, informasi yang sama seperti saat pengguna menambahkan kartu kredit atau debit dapat dibagikan dengan mitra bank Apple, Goldman Sachs Bank USA, dan dengan Apple Payments Inc. Informasi ini hanya digunakan untuk penyelesaian masalah, pencegahan penipuan, dan tujuan pengaturan.

Di iOS 14.6 atau lebih baru, iPadOS 14.6 atau lebih baru, dan watchOS 7.5 atau lebih baru, pengelola keluarga iCloud dengan Apple Card dapat membagikan kartu mereka dengan anggota Keluarga iCloud yang berumur 13 tahun ke atas. Pengesahan pengguna diperlukan untuk mengonfirmasi undangan. Dompet Apple menggunakan kunci di Secure Enclave untuk mengomputasi tanda tangan yang mengikat pengguna dan undangan. Tanda tangan tersebut divalidasi di server Apple.

Secara opsional, pengelola dapat mengatur batas transaksi untuk peserta. Kartu peserta juga dapat dikunci untuk menjeda pengeluaran mereka kapan pun melalui Dompet Apple. Saat pemilik bersama atau peserta yang berumur 18 tahun ke atas menerima undangan dan mengajukan, mereka mengikuti proses pengajuan yang sama di bagian pengajuan Apple Card di Dompet Apple.

Penggunaan Apple Card

Kartu fisik dapat dipesan dari Apple Card di Dompet Apple. Setelah pengguna menerima kartu fisik, kartu tersebut diaktifkan menggunakan label NFC yang ada di amplop lipat kartu fisik. Label tersebut bersifat unik untuk setiap kartu dan tidak dapat digunakan untuk mengaktifkan kartu pengguna lain. Selain itu, kartu tersebut juga dapat diaktifkan secara manual di pengaturan Dompet Apple. Lalu, pengguna juga dapat memilih untuk mengunci atau membuka kartu fisik tersebut kapan pun dari Dompet Apple.

Pembayaran Apple Card dan detail pass Dompet Apple

Pembayaran yang jatuh tempo pada akun Apple Card dapat dilakukan dari Dompet Apple di iOS dengan Apple Cash dan rekening bank. Pembayaran tagihan dapat dijadwalkan sebagai pembayaran berulang atau pembayaran satu kali pada tanggal tertentu dengan Apple Cash dan rekening bank. Saat pengguna melakukan pembayaran, panggilan dilakukan ke server Apple Pay untuk mendapatkan nonce kriptografis yang mirip dengan Apple Cash. Nonce, bersama dengan detail pengaturan pembayaran, diteruskan ke Elemen Aman untuk mengomputasi tanda tangan. Tanda tangan lalu dikembalikan ke server Apple Pay. Pengesahan, integritas, dan ketepatan pembayaran diverifikasi melalui tanda tangan dan nonce oleh server Apple Pay dan perintah diteruskan ke Goldman Sachs Bank USA untuk diproses.

Nomor Apple Card diterima oleh Dompet Apple dengan menunjukkan sertifikat. Server Apple Pay memvalidasi sertifikat untuk mengonfirmasi bahwa kunci dibuat di Secure Enclave. Lalu sertifikat menggunakan kunci ini untuk mengenkripsi nomor Apple Card sebelum mengembalikannya ke Dompet Apple, sehingga hanya iPhone yang meminta nomor Apple Card yang dapat mendekripsinya. Setelah dekripsi, nomor Apple Card disimpan di Rantai Kunci iCloud.

Untuk menampilkan detail nomor Apple Card di pass menggunakan Dompet Apple, pengguna harus memberikan pengesahan dengan Face ID, Touch ID, atau kode sandi. Pengesahan dapat diganti oleh pengguna di bagian informasi kartu dan menonaktifkan pengesahan sebelumnya.

Perlindungan Lanjutan dari Penipuan

Di iOS 15 atau lebih baru dan iPadOS 15 atau lebih baru, pengguna Apple Card dapat mengaktifkan Perlindungan Lanjutan dari Penipuan di Dompet Apple. Saat diaktifkan, Kode Keamanan Kartu disegarkan setiap beberapa hari.

Keamanan Apple Cash

Di iOS 11.2 atau lebih baru, iPadOS 13.1 atau lebih baru, dan watchOS 4.2 atau lebih baru, Apple Pay dapat digunakan di iPhone, iPad, atau Apple Watch untuk mengirim, menerima, dan meminta uang dari pengguna lain. Saat pengguna menerima uang, uang tersebut ditambahkan ke akun Apple Cash yang dapat diakses di Dompet Apple atau di Pengaturan > Dompet & Apple Pay di semua perangkat yang memenuhi syarat tempat pengguna telah masuk dengan ID Apple mereka.

Di iOS 14, iPadOS 14, dan watchOS 7, pengelola iCloud keluarga yang telah memverifikasi identitasnya dengan Apple Cash dapat mengaktifkan Apple Cash untuk anggota keluarga yang berusia di bawah 18 tahun. Secara opsional, pengelola dapat membatasi kemampuan mengirim uang pada pengguna ini hanya ke anggota keluarga atau hanya kontak. Jika anggota keluarga yang berusia di bawah 18 tahun melakukan pemulihan akun ID Apple, pengelola keluarga harus mengaktifkan kembali kartu Apple Cash untuk pengguna tersebut secara manual. Jika anggota keluarga yang berusia di bawah 18 tahun tidak lagi menjadi bagian dari iCloud keluarga, saldo Apple Cash mereka akan ditransfer secara otomatis ke akun pengelola.

Saat pengguna mengatur Apple Cash, informasi yang sama ketika pengguna menambahkan kartu kredit atau debit dapat dibagikan dengan bank mitra Green Dot Bank dan dengan Apple Payments Inc., anak perusahaan yang sepenuhnya dimiliki Apple yang dibentuk untuk melindungi privasi pengguna dengan menyimpan dan memproses informasi secara terpisah dari bagian Apple lainnya dan dengan cara yang tidak diketahui oleh bagian Apple lainnya. Informasi ini hanya digunakan untuk tujuan peraturan, menyelesaikan masalah, dan mencegah penipuan.

Menggunakan Apple Cash di iMessage

Untuk menggunakan pembayaran orang ke orang dan Apple Cash, pengguna harus masuk ke akun iCloud mereka di perangkat yang kompatibel dengan Apple Cash dan mengatur autentikasi dua faktor di akun iCloud. Permintaan dan transfer uang antarpengguna dimulai dari dalam app Pesan atau dengan meminta Siri. Saat pengguna mencoba untuk mengirim uang, iMessage akan menampilkan lembar Apple Pay. Saldo Apple Cash selalu digunakan terlebih dahulu. Jika perlu, dana tambahan akan diambil dari kartu kredit atau debit kedua yang telah ditambahkan pengguna ke Dompet Apple.

Menggunakan Apple Cash di toko, app, dan web

Kartu Apple Cash di Dompet Apple dapat digunakan dengan Apple Pay untuk melakukan pembayaran di toko, app, dan web. Uang di akun Apple Cash juga dapat ditransfer ke rekening bank. Selain menerima uang dari pengguna lain, uang dapat ditambahkan ke akun Apple Cash dari kartu debit atau prabayar di Dompet Apple.

Apple Payments Inc. akan menyimpan dan dapat menggunakan data transaksi pengguna untuk tujuan penyelesaian masalah, pencegahan penipuan, dan peraturan setelah transaksi selesai. Bagian Apple lainnya tidak mengetahui siapa yang pengguna kirimi uang, siapa yang mengirimi Anda uang, atau tempat pengguna melakukan pembelian dengan kartu Apple Cash mereka.

Saat pengguna mengirim uang dengan Apple Pay, menambahkan uang ke akun Apple Cash, atau mentransfer uang ke rekening bank, panggilan akan dibuat ke server Apple Pay untuk mendapatkan nonce kriptografis, yang mirip dengan nilai yang dihasilkan untuk Apple Pay di dalam app. Nonce, bersama dengan data transaksi lainnya, diteruskan ke Elemen Aman untuk mengomputasi tanda tangan pembayaran. Tanda tangan dikembalikan ke server Apple Pay. Pengesahan, integritas, dan ketepatan transaksi diverifikasi melalui tanda tangan pembayaran dan nonce oleh server Apple Pay. Transfer uang kemudian dimulai, dan pengguna diberi tahu mengenai transaksi yang telah selesai.

Jika transaksi menyangkut:

- Kartu debit untuk menambahkan uang ke Apple Cash
- Penyediaan penambahan uang jika saldo Apple Cash tidak cukup

Info pengesahan pembayaran terenkripsi juga dihasilkan dan dikirimkan ke server Apple Pay, sama dengan cara Apple Pay berfungsi dalam app serta situs web.

Setelah saldo akun Apple Cash melampaui jumlah tertentu, atau jika aktivitas yang tidak biasa terdeteksi, pengguna akan diminta untuk memverifikasi identitas mereka. Informasi yang diberikan untuk memverifikasi identitas pengguna—seperti nomor jaminan sosial atau jawaban atas pertanyaan (misalnya, untuk mengonfirmasi nama jalan tempat tinggal pengguna sebelumnya)—dikirimkan ke mitra Apple dengan aman dan dienkripsi menggunakan kunci. Apple tidak dapat mendekripsi data ini. Pengguna diminta untuk memverifikasi identitasnya lagi jika mereka melakukan pemulihan akun ID Apple, sebelum mendapatkan kembali akses ke saldo Apple Cash mereka.

Keamanan Tap to Pay on iPhone

Tap to Pay on iPhone, yang tersedia di iOS 15.4, memungkinkan penjual di A.S. untuk menerima Apple Pay dan pembayaran nirkontak lainnya dengan menggunakan iPhone dan app iOS yang diaktifkan mitra. Dengan layanan ini, pengguna dengan perangkat iPhone yang didukung dapat menerima pembayaran nirkontak dengan aman dan pass berkemampuan NFC *Apple Pay*. Dengan Tap to Pay on iPhone, penjual tidak memerlukan perangkat keras tambahan untuk menerima pembayaran nirkontak.

Tap to Pay on iPhone dirancang untuk melindungi informasi pribadi pembayar. Layanan ini tidak mengumpulkan informasi transaksi yang dapat dikaitkan kembali dengan pembayar. Informasi kartu pembayaran seperti Nomor Kartu Kredit/Debit (PAN) diamankan dengan Elemen Aman dan tidak tersedia bagi penjual. Informasi kartu pembayaran hanya diperuntukkan bagi Penyedia Layanan Pembayaran penjual, pembayar, dan penerbit kartu. Selain itu, layanan Tap to Pay tidak mengumpulkan nama, alamat, atau nomor telepon pembayar.

Tap to Pay on iPhone telah dinilai secara eksternal oleh laboratorium keamanan terakreditasi serta disetujui oleh American Express, Discover, Mastercard dan Visa.

Keamanan komponen pembayaran nirkontak

- *Elemen Aman:* Elemen Aman [Tautan ke bagian Elemen Aman Apple Pay] menjadi host kernel pembayaran yang membaca dan mengamankan data kartu pembayaran nirkontak.
- *Pengontrol NFC:* Pengontrol NFC menangani protokol Komunikasi Medan Dekat dan menyalurkan komunikasi antara Prosesor Aplikasi dan Elemen Aman, serta antara Elemen Aman dan kartu pembayaran nirkontak.
- *Server Tap to Pay on iPhone:* Server Tap to Pay on iPhone mengelola pengaturan dan penyediaan kernel pembayaran di perangkat. Server juga mengawasi keamanan perangkat Tap to Pay on iPhone dengan cara yang kompatibel dengan standar Contactless Payments on COTS (CPoC) dari Payment Card Industry Security Standards Council (PCI SSC) dan tunduk pada PCI DSS.

Cara Tap to Pay membaca kartu kredit, debit, dan prabayar

Tinjauan keamanan penyediaan

Saat penggunaan pertama Tap to Pay on iPhone yang menggunakan app dengan hak yang cukup, server Tap to Pay on iPhone menentukan apakah perangkat memenuhi kriteria seperti Model Perangkat, versi iOS, dan apakah kode sandi telah diatur. Setelah verifikasi ini selesai, applet penerimaan pembayaran diunduh dari server Tap to Pay on iPhone dan diinstal di Elemen Aman, bersamaan dengan konfigurasi kernel pembayaran terkait. Operasi ini dilakukan dengan aman di antara server Tap to Pay on iPhone dan Elemen Aman. Elemen Aman memvalidasi integritas dan keabsahan data ini sebelum penginstalan.

Tinjauan keamanan pembacaan kartu

Saat app Tap to Pay on iPhone meminta pembacaan kartu dari kerangka ProximityReader, lembar—yang dikontrol oleh iOS—ditampilkan dan meminta pengguna untuk mengetuk kartu pembayaran. iOS memulai Pembaca Kartu Pembayaran lalu meminta kernel pembayaran di Elemen Aman untuk memulai pembacaan kartu.

Pada tahap ini, Elemen Aman mengendalikan pengontrol NFC di Mode Pembaca. Mode ini hanya memungkinkan data kartu untuk ditukar di antara kartu pembayaran dan Elemen Aman melalui pengontrol NFC. Kartu pembayaran hanya dapat dibaca saat dalam mode ini.

Setelah applet penerimaan pembayaran di Elemen Aman telah menyelesaikan pembacaan kartu, applet mengenkripsi dan menandatangani data kartu. Data kartu tetap dienkripsi dan disahkan hingga mencapai Penyedia Layanan Pembayaran. Hanya Penyedia Layanan Pembayaran yang digunakan oleh app untuk meminta pembacaan kartu yang dapat mendekripsi data kartu. Penyedia Layanan Pembayaran harus meminta kunci dekripsi data kartu dari server Tap to Pay on iPhone. Server Tap to Pay on iPhone memancarkan kunci dekripsi ke Penyedia Layanan Pembayaran setelah validasi integritas serta keabsahan data, dan setelah memverifikasi bahwa kartu dibaca dalam 60 detik Penyedia pembacaan kartu di perangkat.

Model ini membantu memastikan bahwa data kartu tidak didekripsi oleh siapa pun selain Penyedia Layanan Pembayaran, yang memproses transaksi ini untuk penjual.

Menggunakan Dompet Apple

Mengakses dengan Dompet Apple

Di Dompet Apple di perangkat iPhone dan Apple Watch yang didukung, pengguna dapat menyimpan kunci rumah, mobil, dan kamar hotel. Mereka bahkan dapat menyimpan tanda pengenal perusahaan dan kartu ID pelajar. Saat pengguna tiba di depan pintu, kunci yang benar secara otomatis ditunjukkan, yang memungkinkan mereka masuk hanya dengan mengetuk menggunakan Komunikasi Medan Dekat (NFC).

Kenyamanan pengguna

Setelah kunci, pass, kartu ID pelajar, atau tanda pengenal perusahaan ditambahkan ke app Dompet Apple, Mode Kilat akan dinyalakan secara default. Kartu dalam Mode Kilat berinteraksi dengan terminal yang menerima tanpa pengesahan Face ID, Touch ID, kode sandi, atau klik dua kali pada tombol samping di Apple Watch. Untuk menonaktifkan fitur ini, pengguna dapat mematikan Mode Kilat dengan mengetuk tombol Lainnya di bagian depan kartu di Dompet Apple. Untuk menyalakan kembali Mode Kilat, merek harus menggunakan Face ID, Touch ID, atau kode sandi.

Privasi dan keamanan

Kunci di Dompet Apple memanfaatkan penuh privasi dan keamanan yang berada di iPhone dan Apple Watch. Kapan atau di mana seseorang menggunakan kunci mereka di Dompet Apple tidak pernah dibagikan dengan Apple atau disimpan di server Apple, dan info pengesahan disimpan dengan aman di dalam Elemen Aman (SE) pada perangkat yang didukung. SE menjadi host applet yang dirancang secara khusus untuk mengelola dan menyimpan kunci akses dengan aman, yang memastikan bahwa kunci tidak dapat diekstrak.

Sebelum menyediakan kunci akses, pengguna harus masuk ke akun iCloud mereka di iPhone yang kompatibel dan menyalakan autentikasi dua faktor untuk akun iCloud mereka, dengan pengecualian untuk ID pelajar, yang tidak perlu menyalakan autentikasi dua faktor.

Saat pengguna memulai proses penyediaan, langkah serupa dengan penyediaan kartu kredit dan debit dilakukan, seperti penautan dan penyediaan. Selama transaksi, pembaca berkomunikasi dengan Elemen Aman melalui pengontrol komunikasi medan dekat (NFC) menggunakan saluran aman yang dibuat.

Jumlah perangkat, termasuk iPhone dan Apple Watch, yang dapat disediakan dengan kunci akses ditentukan dan dikontrol oleh setiap mitra dan dapat bervariasi dari satu mitra ke mitra lain. Pendekatan tersebut memungkinkan setiap mitra untuk memiliki kontrol atas jumlah maksimum kunci akses yang disediakan per jenis perangkat untuk menyesuaikan kebutuhannya. Demi tujuan ini, Apple memberikan mitra dengan jenis perangkat dan pengenal perangkat anonim. Pengenal berbeda untuk setiap mitra demi alasan privasi dan keamanan.

Kunci dapat dinonaktifkan atau dihapus dengan:

- Menghapus perangkat dari jarak jauh dengan Lacak
- Mengaktifkan Mode Hilang dengan Lacak
- Menerima perintah penghapusan mobile device management (MDM) dari jarak jauh

- Menghapus semua kartu dari halaman akun ID Apple mereka
- Menghapus semua kartu dari iCloud.com
- Menghapus semua kartu dari Dompet Apple
- Menghapus kartu di app penerbit

Di iOS 15.4 atau lebih baru, saat pengguna mengeklik dua kali tombol samping di iPhone dengan Face ID atau mengeklik dua kali tombol Utama di iPhone dengan Touch ID, pass dan detail kunci akses mereka tidak ditampilkan hingga mereka mengesahkan perangkat. Face ID, Touch ID, atau pengesahan kode sandi diperlukan sebelum informasi khusus pass termasuk detail pemesanan hotel ditampilkan di Dompet Apple.

Jenis info pengesahan akses

Terdapat berbagai jenis akses dari Dompet Apple, seperti perhotelan, tanda pengenal perusahaan, ID pelajar, kunci rumah, dan kunci mobil.

Perhotelan

Kunci kamar hotel di Dompet Apple membantu memberikan pengalaman check-in dan check-out nirkontak yang mudah, selagi menyediakan keuntungan privasi dan keamanan tambahan untuk tamu selain kartu kunci hotel plastik tradisional. Tamu hotel di lokasi yang didukung dapat mengetuk untuk membuka dengan kunci kamar di Dompet Apple di iPhone yang kompatibel dan Apple Watch Series 4 atau lebih baru.

Kemampuan di Dompet Apple dirancang secara khusus untuk mengurangi friksi untuk pengguna:

- Penyediaan prakedatangan dari app hotel, untuk menambahkan pass ke Dompet Apple sebelum tiba
- Kotak pass check-in, untuk memulai check-in dan penetapan kamar dari Dompet Apple
- Pembaruan kunci pascapenyediaan, untuk mendukung perpanjangan atau pengubahan rencana menginap saat ini
- Dukungan kunci beberapa kamar untuk satu pass di Dompet Apple
- Pengarsipan otomatis kunci yang kedaluwarsa di Dompet Apple

Tanda pengenal perusahaan

Tanda pengenal karyawan dari mitra yang didukung dapat ditambahkan ke Dompet Apple di iPhone dan Apple Watch, yang memungkinkan karyawan di seluruh dunia mengakses ruang kerjanya secara nirkontak. Untuk menambahkan tanda pengenal, karyawan harus menyalakan pengesahan beberapa faktor untuk akun mereka yang digunakan untuk masuk ke app yang disediakan oleh perusahaan.

Tanda pengenal perusahaan memanfaatkan kemampuan akses Apple, yang memungkinkan pengguna untuk:

- Secara otomatis menambahkan tanda pengenal karyawan ke Apple Watch mereka yang dipasangkan melalui penyediaan push yang tidak memerlukan penginstalan app mitra
- Mengakses perlengkapan kantor tanpa sela menggunakan mode kilat
- Mendapatkan akses ke ruang kerja bahkan setelah daya baterai iPhone habis

Kartu ID pelajar

Di iOS 12 atau lebih baru, pelajar, fakultas, dan staf di kampus yang berpartisipasi dapat menambahkan kartu ID pelajar mereka ke Dompet Apple di model iPhone dan Apple Watch yang didukung untuk mengakses lokasi dan membayar di tempat yang menerima kartu mereka.

Pengguna menambahkan kartu ID pelajar mereka ke Dompet Apple melalui app yang disediakan oleh penerbit kartu atau sekolah yang berpartisipasi. Proses teknisnya sama dengan yang dijelaskan di Menambahkan kartu kredit atau debit dari app penerbit kartu. Selain itu, app penerbit harus mendukung autentikasi dua faktor pada akun yang menjaga akses ke ID pelajar mereka. Kartu dapat diatur secara bersamaan di maksimal dua perangkat Apple yang didukung, yang masuk dengan ID Apple yang sama.

Rumah beberapa keluarga

Penghuni dan staf dari fasilitas mitra yang didukung dapat menggunakan kunci rumah mereka di Dompet Apple untuk mengakses bangunan, unit, dan area umum. Kunci rumah dapat disediakan dari app yang disediakan oleh mitra. Untuk mitra yang mendukung penyediaan tanpa friksi, pengelola properti dapat mengirimi penghuni tautan untuk memulai penyediaan menggunakan saluran pesan pilihan mereka (misalnya, email atau SMS) agar penghuni hanya perlu mengeklik tautan untuk menukarkan kunci. Cuplikan App juga menyediakan pengalaman yang aman dan tanpa sela, memungkinkan penyediaan kunci tanpa menginstal app mitra. Untuk informasi lainnya, lihat artikel Dukungan Apple Menggunakan Cuplikan App di iPhone.

Kunci rumah

Kunci rumah di Dompet Apple dapat digunakan dengan kunci pintu berkemampuan NFC yang didukung hanya dengan mengetuk iPhone atau Apple Watch. Untuk informasi lainnya mengenai cara pengguna dapat mengatur dan menggunakan kunci rumah, lihat artikel Dukungan Apple Membuka pintu Anda dengan kunci rumah di iPhone.

Saat pengguna mengatur kunci rumah, semua penghuni di rumah mereka juga secara otomatis menerima kunci rumah. Untuk membagikan kunci rumah atau menghapus anggota rumah bersama lebih lanjut, pemilik rumah dapat menggunakan app Rumah untuk mengelola undangan dan anggota. Saat pengguna memilih untuk menerima undangan untuk bergabung dengan rumah dengan kunci rumah, ini memulai penyediaan kunci rumah ke Dompet Apple di perangkat mereka. Jika pengguna memilih untuk meninggalkan rumah atau jika pemilik rumah mencabut aksesnya, tindakan ini juga menghapus kunci rumah dari Dompet Apple.

Kunci mobil

Penyimpanan kunci mobil secara digital di Dompet Apple didukung langsung di perangkat iPhone yang didukung dan perangkat Apple Watch yang dipasangkan. Kunci mobil diwakili sebagai pass (dibuat oleh Apple atas nama pembuat mobil) di Dompet Apple dan mendukung siklus masa pakai kartu Apple Pay penuh (Mode Hilang iCloud, Penghapusan Jarak Jauh, penghapusan pass lokal, serta Hapus Semua Konten dan Pengaturan). Selain manajemen kartu Apple Pay standar, kunci mobil bersama dapat dihapus dari iPhone dan Apple Watch pemilik, serta di Antarmuka Mesin Manusia (HMI) kendaraan.

Kunci mobil dapat digunakan untuk membuka dan mengunci kendaraan serta untuk menyalakan atau mengatur kendaraan ke mode berkendara. “Transaksi standar” menawarkan pengesahan bersama dan wajib untuk menyalakan mesin. Transaksi buka dan kunci dapat menggunakan “transaksi cepat” saat diperlukan demi alasan kinerja.

Kunci dibuat melalui pemasangan iPhone dengan kendaraan yang dimiliki dan didukung. Semua kunci dibuat di Secure Element yang dilekatkan berdasarkan pembuatan kunci internal kurva eliptis (NIST P-256), yang disingkat menjadi ECC-OBKG, dan kunci pribadi tidak pernah meninggalkan Secure Element. Komunikasi antara perangkat dan kendaraan menggunakan NFC, atau kombinasi dari Bluetooth LE dan UWB, serta manajemen kunci menggunakan API server Apple ke pembuat mobil dengan TLS yang saling disahkan. Setelah kunci dipasangkan ke iPhone, Apple Watch yang dipasangkan ke iPhone tersebut juga dapat menerima kunci. Saat dihapus di kendaraan atau di perangkat, kunci tidak dapat dipulihkan. Kunci di perangkat yang hilang atau dicuri dapat ditangguhkan dan dilanjutkan, tapi membuatnya kembali di perangkat baru memerlukan pemasangan atau pembagian baru.

Keamanan kunci mobil di iOS

Pengembang dapat mendukung cara tanpa kunci yang aman di iPhone yang didukung dan Apple Watch yang dipasangkan.

Pemasangan pemilik

Pemilik harus membuktikan kepemilikan kendaraan (metode ini tergantung pada pembuat mobil) dan dapat memulai proses pemasangan di app pembuat mobil menggunakan tautan email yang diterima dari pembuat mobil atau dari menu kendaraan. Dalam setiap kasus, pemilik harus menyediakan kata sandi pemasangan sekali pakai rahasia ke iPhone, yang digunakan untuk membuat saluran pemasangan aman menggunakan protokol SPAKE2+ dengan kurva NIST P-256. Saat menggunakan app atau tautan email, kata sandi secara otomatis ditransfer ke iPhone, tempat kata sandi harus dimasukkan secara manual saat pemasangan dimulai dari kendaraan.

Berbagi kunci

iPhone pemilik yang dipasangkan dapat membagikan kunci ke perangkat iPhone anggota keluarga dan teman yang memenuhi syarat (dan perangkat Apple Watch mereka yang dipasangkan) dengan mengirimkan undangan spesifik perangkat menggunakan iMessage dan Layanan Identitas Apple (IDS). Semua perintah berbagi dilakukan menggunakan fitur IDS yang dienkripsi ujung ke ujung. iPhone pemilik yang dipasangkan menjaga agar saluran IDS tidak berubah selama proses berbagi agar dapat melindungi dari penerusan undangan.

Saat menerima undangan, iPhone anggota keluarga atau teman membuat kunci digital dan mengirimkan rantai sertifikat pembuatan kunci kembali ke iPhone pemilik yang dipasangkan untuk memverifikasi bahwa kunci dibuat di perangkat asli Apple. iPhone pemilik yang dipasangkan menandatangani kunci publik ECC iPhone anggota keluarga atau teman dan mengirimkan tanda tangan kembali ke iPhone anggota keluarga atau teman. Operasi penandatanganan di perangkat pemilik memerlukan pengesahan pengguna (Face ID, Touch ID, atau entri kode sandi) dan tujuan pengguna aman yang dijelaskan di Penggunaan Face ID dan Face ID. Pengesahan diminta saat mengirimkan undangan dan disimpan di secure element untuk dikonsumsi saat perangkat teman mengirimkan kembali permintaan penandatanganan. Hak kunci disediakan ke kendaraan secara online oleh server OEM kendaraan atau selama penggunaan pertama kunci bersama di kendaraan.

Penghapusan kunci

Kunci dapat dihapus di perangkat pemegang kunci dari perangkat pemilik dan di kendaraan. Penghapusan di iPhone pemegang kunci segera berlaku, bahkan jika pemegang kunci menggunakan kunci. Maka dari itu, peringatan keras ditampilkan sebelum penghapusan. Penghapusan kunci di kendaraan dapat dilakukan kapan pun atau hanya mungkin dilakukan saat kendaraan online.

Dalam kedua kasus, penghapusan di perangkat pemegang kunci atau kendaraan dilaporkan ke server inventaris kunci (KIS) pada sisi pembuat mobil, yang mendaftarkan kunci yang diterbitkan untuk kendaraan demi tujuan asuransi.

Pemilik dapat meminta penghapusan dari belakang pass pemilik. Permintaan pertama-tama dikirimkan ke pembuat mobil untuk penghapusan kunci di kendaraan. Kondisi untuk menghapus kunci dari kendaraan ditetapkan oleh pembuat mobil. Server pembuat mobil akan mengirimkan permintaan penghapusan jarak jauh ke perangkat pemegang kunci hanya saat kunci dihapus di mobil.

Saat kunci dihapus di perangkat, applet yang mengelola kunci mobil digital membuat pengesahan penghapus yang ditandatangani secara kriptografis, yang digunakan sebagai bukti penghapusan oleh pembuat mobil dan digunakan untuk menghapus kunci dari KIS.

Transaksi standar NFC

Untuk kendaraan yang menggunakan kunci NFC, saluran aman antara pembaca dan iPhone diawali dengan membuat pasangan kunci jangka pendek di sisi pembaca dan iPhone. Menggunakan metode persetujuan kunci, rahasia bersama dapat diturunkan di kedua sisi dan digunakan untuk pembuatan kunci simetris bersama menggunakan Diffie-Hellman, fungsi turunan kunci, dan tanda tangan dari kunci jangka panjang yang dibuat selama pemasangan.

Kunci publik jangka pendek yang dibuat di sisi kendaraan ditandatangani dengan kunci pribadi jangka panjang pembaca, yang menghasilkan pengesahan pembaca oleh iPhone. Dari sudut pandang iPhone, protokol ini dirancang untuk mencegah data sensitif pribadi agar tidak ditampilkan ke pihak yang menyadap komunikasi.

Terakhir, iPhone menggunakan saluran aman yang dibuat untuk mengenkripsi pengenal kunci publiknya bersamaan dengan tanda tangan yang dikomputasi di tantangan yang diturunkan dari data pembaca dan beberapa data spesifik app tambahan. Verifikasi tanda tangan iPhone oleh pembaca ini memungkinkan pembaca untuk mengesahkan perangkat.

Transaksi cepat

iPhone membuat kriptogram berdasarkan rahasia yang dibagikan sebelumnya selama transaksi standar. Kriptogram ini memungkinkan kendaraan untuk mengesahkan perangkat dengan cepat dalam skenario yang memerlukan kinerja. Secara opsional, saluran aman di antara kendaraan dan perangkat dibuat dengan menurunkan kunci sesi dari rahasia yang dibagikan sebelumnya selama transaksi standar dan pasangan kunci jangka pendek baru. Kemampuan kendaraan untuk membuat saluran aman mengesahkan kendaraan ke iPhone.

Transaksi standar BLE/UWB

Untuk kendaraan yang menggunakan kunci UWB, sesi Bluetooth LE dibuat di antara perangkat dan iPhone. Serupa dengan transaksi NFC, rahasia bersama diturunkan di kedua pihak dan digunakan untuk pembuatan sesi aman. Sesi ini digunakan untuk kemudian menurunkan dan menyetujui Kunci Rahasia Mencakup UWB (URSK). URSK disediakan ke radio UWB di perangkat pengguna dan di kendaraan untuk memungkinkan pelokalan akurat dari perangkat pengguna ke posisi tertentu di dekat atau di dalam kendaraan. Kendaraan lalu menggunakan posisi perangkat untuk membuat keputusan apakah akan mengizinkan untuk membuka atau menyalakan kendaraan. URSK memiliki TTL yang telah ditentukan. Untuk menghindari gangguan pencakupan saat TTL kedaluwarsa, URSK dapat diturunkan terlebih dahulu di SE perangkat dan HSM/SE kendaraan selagi pencakupan aman tidak aktif tapi BLE terhubung. Ini menghindari dibutuhkannya transaksi standar untuk menurunkan URSK baru di situasi yang membutuhkan keputusan cepat. URSK yang diturunkan sebelumnya dapat ditransfer dengan cepat ke radio UWB mobil dan perangkat agar tidak mengganggu pencakupan UWB.

Privasi

Server inventaris kunci pembuat mobil (KIS) pembuat mobil tidak menyimpan ID, SEID, atau ID Apple perangkat. Server hanya menyimpan pengenal yang dapat berubah, contohnya adalah pengenal CA. Pengenal ini tidak terikat ke data pribadi mana pun di perangkat atau di server, dan dihapus saat pengguna menghapus perangkatnya secara penuh (menggunakan Hapus Semua Konten dan Pengaturan).

Menambahkan kartu transit dan eMoney ke Dompet Apple

Di beberapa pasar global, pengguna dapat menambahkan kartu transit dan eMoney yang didukung ke Dompet Apple di model iPhone dan Apple Watch yang didukung. Tergantung operator, ini dapat dilakukan dengan mentransfer nilai atau pass komuter (atau keduanya) dari kartu fisik ke representasi digitalnya di Dompet Apple atau dengan menyediakan kartu transit atau eMoney baru dari Dompet Apple atau app penerbit kartu transit. Setelah kartu transit ditambahkan ke Dompet Apple, pengguna dapat naik transit hanya dengan mendekatkan iPhone atau Apple Watch pengguna ke pembaca transit. Beberapa kartu transit juga dapat digunakan untuk melakukan pembayaran.

Cara kartu transit dan eMoney berfungsi

Kartu transit dan eMoney yang ditambahkan dikaitkan dengan akun iCloud pengguna. Jika pengguna menambahkan lebih dari satu kartu ke Dompet Apple, Apple atau penerbit kartu mungkin dapat menautkan informasi pribadi pengguna dan informasi akun yang dikaitkan antarkartu. Kartu transit dan eMoney dan transaksi dilindungi oleh kumpulan kunci kriptografis hierarkis.

Selama proses transfer saldo dari kartu fisik ke Dompet Apple, pengguna diharuskan untuk memasukkan informasi khusus terkait kartu. Pengguna juga mungkin harus menyediakan informasi untuk bukti kepemilikan kartu. Saat mentransfer pass dari iPhone ke Apple Watch, kedua perangkat harus online.

Saldo dapat diisi ulang dengan dana dari kartu prabayar, kredit, dan debit melalui Dompet Apple atau dari app penerbit kartu transit atau eMoney. Untuk memahami keamanan pemuatan ulang saldo saat menggunakan Apple Pay, lihat Membayar dengan kartu dalam app. Untuk mempelajari cara kartu disediakan dari dalam app penerbit kartu, lihat Menambahkan kartu kredit atau debit dari app penerbit kartu.

Jika penyediaan dari kartu fisik didukung, penerbit kartu transit atau eMoney memiliki kunci kriptografis yang diperlukan untuk mengesahkan kartu fisik dan memverifikasi data pengguna yang dimasukkan. Setelah data diverifikasi, sistem dapat membuat Nomor Akun Perangkat untuk Elemen Aman dan mengaktifkan pass yang baru dibuat di Dompet Apple dengan saldo yang ditransfer. Untuk beberapa kartu, setelah penyediaan kartu fisik selesai, kartu fisik akan dinonaktifkan.

Di akhir kedua jenis penyediaan, jika saldo kartu disimpan di perangkat, informasi tersebut akan dienkripsi dan disimpan ke applet yang ditetapkan di Elemen Aman. Operator memiliki kunci untuk menjalankan operasi kriptografis pada data kartu untuk transaksi saldo.

Secara default, pengguna kartu transit diuntungkan oleh pengalaman Transit Kilat yang memungkinkan mereka untuk membayar dan bepergian tanpa memerlukan Face ID, Touch ID, atau kode sandi. Informasi seperti stasiun yang baru kunjungi, riwayat transaksi, dan tiket tambahan dapat diakses oleh pembaca kartu nirkontak di sekitar dengan Mode Kilat yang diaktifkan. Pengguna dapat menyalakan Face ID, Touch ID, atau persyaratan pengesahan kode sandi di pengaturan Dompet & Apple Pay dengan menonaktifkan Transit Kilat. Mode kilat tidak didukung untuk kartu eMoney.

Seperti kartu Apple Pay lainnya, pengguna dapat menangguhkan atau menghapus kartu eMoney dengan:

- Menghapus perangkat dari jarak jauh dengan Lacak
- Mengaktifkan Mode Hilang dengan Lacak
- Memasukkan perintah penghapusan mobile device management (MDM) dari jarak jauh
- Menghapus semua kartu dari halaman akun ID Apple mereka
- Menghapus semua kartu dari iCloud.com
- Menghapus semua kartu dari Dompet Apple
- Menghapus kartu di app penerbit

Server Apple Pay memberi tahu operator kartu untuk menangguhkan atau menonaktifkan kartu tersebut. Jika pengguna menghapus kartu transit atau eMoney dari perangkat online, saldonya akan dapat dipulihkan dengan menambahkannya kembali ke perangkat yang masuk dengan ID Apple yang sama. Jika perangkat offline, dimatikan, atau tidak dapat digunakan, pemulihan mungkin tidak dapat dilakukan.

Menambahkan kartu transit dan eMoney ke Apple Watch anggota keluarga

Di iOS 15 dan watchOS 8, pengelola keluarga iCloud dapat menambahkan kartu transit dan eMoney ke perangkat Apple Watch anggota keluarga mereka melalui app Apple Watch iPhone mereka. Saat menyediakan salah satu kartu ini ke Apple Watch anggota keluarga, jam perlu berada di sekitar dan terhubung ke iPhone pengelola menggunakan Wi-Fi atau Bluetooth. Anggota keluarga perlu mengaktifkan autentikasi dua faktor untuk ID Apple mereka agar ini dapat dilakukan.

Anggota keluarga dapat mengirimkan permintaan untuk menambahkan uang ke kartu transit atau eMoney dari Apple Watch mereka menggunakan iMessage. Konten pesan dilindungi oleh enkripsi ujung ke ujung, seperti yang dijelaskan di tinjauan keamanan iMessage. Menambahkan uang ke kartu di Apple Watch anggota keluarga dapat dilakukan secara jarak jauh menggunakan koneksi Wi-Fi atau seluler. Kartu tidak perlu didekatkan.

Catatan: Fitur ini mungkin tidak tersedia di semua negara atau wilayah.

Kartu kredit dan debit

Di beberapa kota, pembaca transit menerima kartu EMV (cerdas) untuk membayar perjalanan transit. Saat pengguna menyediakan kartu kredit atau debit EMV ke pembaca tersebut, pengesahan pengguna diperlukan, seperti dengan “Membayar dengan kartu kredit dan debit di toko”.

Di iOS 12.3 atau lebih baru, beberapa kartu kredit/debit EMV di Dompet Apple dapat diaktifkan untuk Transit Kilat. Transit Kilat memungkinkan pengguna untuk membayar perjalanan di operator transit yang didukung tanpa memerlukan Face ID, Touch ID, atau kode sandi. Saat pengguna menyediakan kartu kredit atau debit EMV, kartu pertama yang disediakan ke Dompet Apple akan diaktifkan untuk Transit Kilat. Pengguna dapat mengetuk tombol Lainnya di bagian depan kartu di Dompet Apple dan menonaktifkan Transit Kilat untuk kartu tersebut dengan mengatur Pengaturan Transit Kilat ke Tidak Ada. Pengguna juga dapat memilih kartu kredit atau debit lain sebagai kartu Transit Kilat mereka menggunakan Dompet Apple. Face ID, Touch ID, atau kode sandi diperlukan untuk mengaktifkan ulang atau memilih kartu lain untuk Transit Kilat.

Apple Card dan Apple Cash dapat digunakan untuk Transit Kilat.

ID di Dompet Apple

Di iPhone 8 atau lebih baru yang menjalankan iOS 15.4 atau lebih baru dan Apple Watch Series 4 atau lebih baru yang menjalankan watchOS 8.4 atau lebih baru, pengguna dapat menambahkan ID negara bagian atau SIM ke Dompet Apple dan mengetuk iPhone atau Apple Watch mereka untuk menunjukkannya tanpa sela dan aman di lokasi yang berpartisipasi.

Catatan: Fitur ini hanya tersedia dengan negara bagian A.S. yang berpartisipasi.

ID di Dompet Apple menggunakan fitur keamanan yang terdapat di perangkat keras dan perangkat lunak perangkat pengguna untuk membantu melindungi identitas dan membantu mereka menjaga informasi pribadi tetap aman.

Menambahkan SIM atau ID negara bagian ke Dompet Apple

Di iPhone, pengguna cukup mengetuk tombol Tambah (+) di bagian atas layar di Dompet Apple untuk mulai menambahkan SIM atau ID mereka. Jika pengguna memiliki Apple Watch yang dipasangkan saat pengaturan, mereka juga diminta untuk menambahkan SIM atau ID ke Dompet Apple mereka di Apple Watch.

Pengguna pertama-tama diminta untuk menggunakan iPhone mereka untuk memindai bagian depan dan belakang SIM atau kartu ID negara bagian mereka. iPhone mengevaluasi kualitas dan jenis gambar untuk membantu memastikan bahwa gambar yang disediakan dapat diterima oleh otoritas penerbit negara bagian. Gambar kartu identitas ini dienkripsi ke kunci otoritas penerbit negara bagian di perangkat lalu dikirim ke otoritas penerbit negara bagian.

Berikutnya, pengguna diminta untuk menyelesaikan rangkaian gerakan wajah dan kepala. Gerakan ini dievaluasi oleh perangkat pengguna dan oleh Apple untuk membantu mengurangi risiko seseorang menggunakan foto, video, atau masker untuk mencoba menambahkan ID orang lain ke Dompet Apple. Hasil dari analisis gerakan ini lalu dikirim ke otoritas penerbit negara bagian, bukan video gerakannya sendiri.

Untuk membantu memastikan bahwa orang yang menambahkan kartu identitas ke Dompet Apple adalah orang yang sama dengan yang memiliki kartu identitas, pengguna diminta untuk mengambil selfie. Sebelum foto pengguna dikirim ke otoritas penerbit negara bagian, server Apple dan perangkat pengguna membandingkan foto dengan kemiripan orang yang melakukan rangkaian gerakan wajah serta kepala dan membantu memastikan bahwa foto yang sedang dikirim adalah orang yang sama dengan di ID. Setelah perbandingan dibuat, foto dienkripsi di perangkat lalu dikirimkan ke otoritas penerbit negara bagian untuk dibandingkan dengan gambar di file untuk ID mereka.

Terakhir, pengguna diminta untuk melakukan pengesahan Face ID atau Touch ID. Perangkat pengguna mengaitkan biometrik Face ID atau Touch ID yang dicocokkan sekali ini ke ID negara bagian untuk membantu memastikan bahwa hanya orang yang menambahkan ID ke iPhone ini yang dapat menunjukkannya; informasi biometrik terdaftar lain tidak dapat digunakan untuk mengesahkan penunjukan ID. Ini hanya terjadi di perangkat dan tidak dikirim ke otoritas penerbit negara bagian.

Otoritas penerbit negara bagian akan menerima informasi yang diperlukan untuk mengatur ID digital. Ini meliputi gambar bagian depan dan belakang ID pengguna, data yang dibaca dari kode bar PDF417 serta selfie yang pengguna ambil sebagai bagian dari proses verifikasi ID. Negara bagian penerbit juga menerima nilai satu digit, yang digunakan untuk membantu mencegah penipuan, yang didasarkan pada pola penggunaan perangkat pengguna, data pengaturan, dan informasi mengenai ID Apple pribadi mereka. Pada akhirnya semua tergantung pada keputusan negara bagian penerbit apakah akan menyetujui atau menolak ID yang sedang ditambahkan ke Dompet Apple.

Setelah otoritas penerbit negara bagian mengesahkan penambahan ID negara bagian atau SIM ke Dompet Apple, pasangan kunci dibuat di Elemen Aman oleh iPhone yang mengaitkan ID pengguna ke perangkat tersebut. Jika ditambahkan ke Apple Watch, pasangan kunci dibuat di Elemen Aman oleh Apple Watch.

Setelah ID ada di iPhone, informasi yang tercermin di ID pengguna di Dompet Apple disimpan dalam format terenkripsi yang dilindungi oleh Secure Enclave.

Menggunakan SIM atau ID negara bagian di Dompet Apple

Untuk menggunakan ID mereka di Dompet Apple, pengguna harus mengesahkan dengan perangkat Face ID atau Touch ID yang dikaitkan dengan ID di Dompet Apple sebelum iPhone menunjukkan informasi ke pembaca identitas.

Untuk menggunakan ID mereka di Dompet Apple di Apple Watch, pengguna perlu membuka iPhone mereka menggunakan tampilan Face ID atau sidik jari Touch ID setiap kali mereka mengenakan Apple Watch. Lalu, mereka dapat menggunakan ID di Dompet Apple tanpa mengesahkan hingga mereka melepas Apple Watch lagi. Kemampuan ini menggunakan kemampuan Buka Otomatis dasar yang dijelaskan di Keamanan sistem untuk watchOS.

Saat pengguna mendekatkan iPhone atau Apple Watch mereka ke pembaca identitas, pengguna melihat permintaan di perangkat yang menampilkan informasi tertentu mana yang diminta, oleh siapa, dan apakah mereka akan menyimpannya. Setelah mengesahkan dengan Face ID atau Touch ID terkait, informasi identitas yang diminta dilepas dari perangkat.

Penting: Pengguna tidak perlu membuka, menunjukkan, atau menyerahkan perangkat untuk menunjukkan ID mereka.

Jika pengguna menyalakan fitur aksesibilitas seperti Kontrol Suara, Kontrol Pengalihan, atau Assistive Touch alih-alih Face ID atau Touch ID, mereka dapat menggunakan kode sandi untuk mengakses dan menunjukkan informasi mereka.

Transmisi data identitas ke pembaca identitas mengikuti standar ISO/IEC 18013-5, yang menyediakan beberapa mekanisme keamanan yang dapat mendeteksi, mencegah, dan memitigasi risiko keamanan. Ini terdiri dari integritas dan anti-pemalsuan data identitas, pengaitan perangkat, persetujuan resmi, dan kerahasiaan data pengguna melalui tautan radio.

Integritas dan anti-pemalsuan data identitas

ID di Dompet Apple menggunakan tanda tangan yang disediakan penerbit untuk memungkinkan pembaca yang patuh terhadap ISO/IEC 18013-5 untuk memverifikasi ID pengguna di Dompet Apple. Selain itu, semua elemen data di ID di Dompet dilindungi dari pemalsuan secara terpisah. Ini memungkinkan pembaca identitas untuk meminta subset khusus elemen data yang ada di ID di Dompet Apple dan agar ID di Dompet Apple untuk merespons dengan subset yang sama tersebut, yang maka dari itu hanya membagikan data yang diminta dan memaksimalkan privasi pengguna.

Pengaitan perangkat

ID di pengesahan Dompet Apple menggunakan tanda tangan perangkat untuk melindungi dari penduplikatan ID dan pemutaran ulang transaksi identitas. Dengan menyimpan kunci pribadi untuk pengesahan ID di Elemen Aman perangkat iPhone, ID dikaitkan ke perangkat yang sama dengan tujuan ID dibuat oleh otoritas penerbit negara bagian.

Persetujuan resmi

ID di pengesahan pembaca Dompet Apple mengesahkan pembaca identitas menggunakan protokol yang didefinisikan di standar ISO/IEC 18013-5. Selama penunjukan, ikon yang diturunkan dari sertifikat pembaca ditunjukkan kepada mereka untuk memberikan pengguna jaminan bahwa mereka berinteraksi dengan pihak yang tepat.

Kerahasiaan data pengguna melalui tautan radio

Enkripsi sesi membantu memastikan bahwa semua informasi yang dapat mengidentifikasi secara pribadi (PII) yang bertukar di antara ID di Dompet Apple dan pembaca identitas dienkripsi. Enkripsi dilakukan oleh lapisan aplikasi. Maka dari itu keamanan enkripsi sesi tidak bergantung pada keamanan yang disediakan oleh lapisan transmisi (misalnya, NFC, Bluetooth, dan Wi-Fi).

ID di Dompet Apple membantu menjaga kerahasiaan informasi pengguna

ID di Dompet Apple mengikuti proses “pengambilan perangkat” yang tercantum di ISO/IEC 18013-5. Pengambilan perangkat tidak memerlukan panggilan server selama penunjukan, yang maka dari itu melindungi pengguna agar tidak dilacak oleh Apple dan penerbit.

iMessage

Tinjauan keamanan iMessage

iMessage Apple adalah layanan pesan untuk perangkat iOS dan iPadOS, Apple Watch, dan komputer Mac. iMessage mendukung teks dan lampiran, seperti foto, kontak, lokasi, tautan, dan lampiran secara langsung di pesan, seperti ikon jempol ke atas. Pesan muncul di semua perangkat pengguna yang didaftarkan sehingga percakapan dapat dilanjutkan dari perangkat mana pun milik pengguna. iMessage memanfaatkan layanan Pemberitahuan Push Apple (APN) secara ekstensif. Apple tidak mencatat konten pesan atau lampiran, yang dilindungi oleh enkripsi ujung ke ujung sehingga tidak ada orang yang dapat mengaksesnya, kecuali pengirim dan penerima. Apple tidak dapat mendekripsi data tersebut.

Saat pengguna menyalakan iMessage di perangkat, perangkat tersebut akan membuat enkripsi dan pasangan kunci penanda tangan untuk digunakan dengan layanan tersebut. Untuk enkripsi, terdapat kunci enkripsi RSA 1280 bit serta kunci enkripsi EC 256 bit pada kurva NIST P-256. Untuk tanda tangan, kunci penandatanganan Algoritme Tanda Tangan Digital Kurva Eliptis (ECDSA) 256 bit digunakan. Kunci pribadi disimpan di rantai kunci perangkat dan hanya tersedia setelah pembukaan pertama. Kunci publik dikirimkan ke Layanan Identitas (IDS) Apple, tempat kunci akan dikaitkan dengan nomor telepon atau alamat email pengguna, bersama dengan alamat APN perangkat.

Saat pengguna mengaktifkan perangkat tambahan untuk digunakan dengan iMessage, enkripsi dan kunci publik penanda tangan, alamat APN, dan nomor telepon terkaitnya akan ditambahkan ke layanan direktori. Pengguna juga dapat menambahkan alamat email lain, yang diverifikasi dengan mengirimkan tautan konfirmasi. Nomor telepon diverifikasi oleh jaringan dan SIM operator. Dengan jaringan tertentu, ini memerlukan penggunaan SMS (pengguna akan diberi dialog konfirmasi jika SMS tidak dinilai nol). Verifikasi nomor telepon mungkin diperlukan untuk beberapa layanan sistem selain iMessage, seperti FaceTime dan iCloud. Semua perangkat pengguna yang terdaftar akan menampilkan pesan peringatan saat perangkat, nomor telepon, atau alamat email baru ditambahkan.

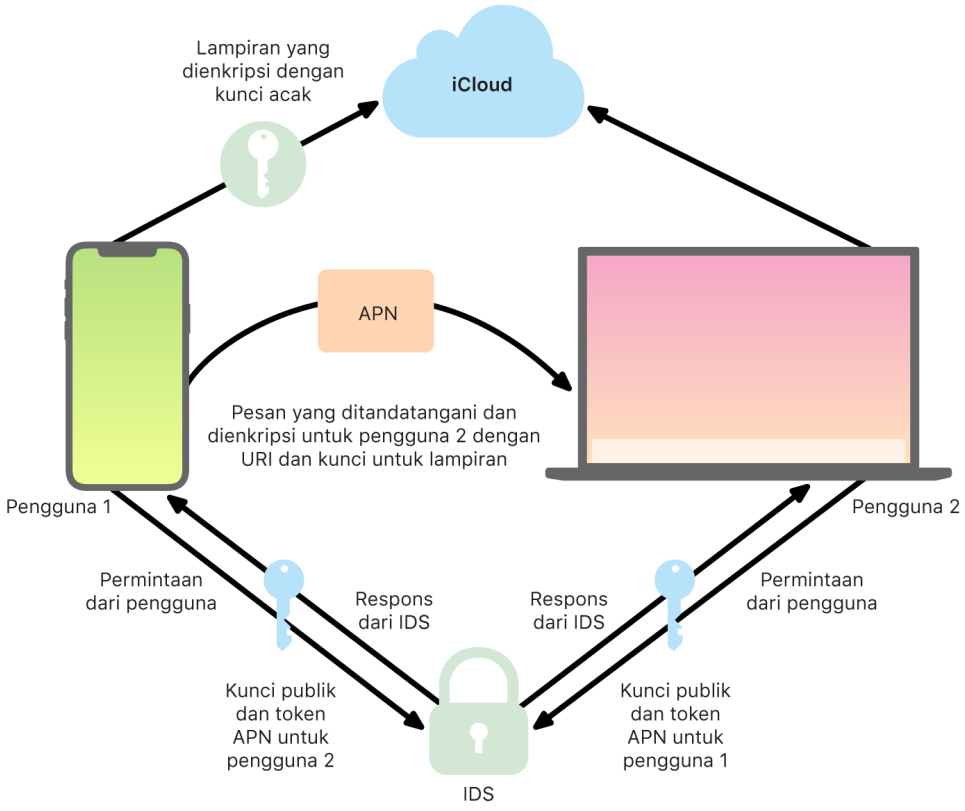
Cara iMessage mengirimkan dan menerima pesan dengan aman

Pengguna memulai percakapan iMessage baru dengan memasukkan alamat atau nama. Jika mereka memasukkan nomor telepon atau alamat email, perangkat akan menghubungi Layanan Identitas (IDS) Apple untuk mengambil kunci publik dan alamat APN untuk semua perangkat yang dikaitkan dengan penerima. Jika pengguna memasukkan nama, perangkat pertama-tama akan menggunakan app Kontak pengguna untuk mengumpulkan nomor telepon dan alamat email yang terkait dengan nama tersebut, lalu mendapatkan kunci publik dan alamat APN dari IDS.

Pesan keluar pengguna dienkripsi secara terpisah untuk setiap perangkat penerima. Kunci enkripsi publik dan kunci penanda tangan dari perangkat penerima diambil dari IDS. Untuk setiap perangkat penerima, perangkat pengirim membuat nilai 88 bit acak dan menggunakannya sebagai kunci HMAC-SHA256 untuk membuat nilai 40 bit yang diturunkan dari kunci publik pengirim dan penerima serta plaintext. Rangkaian nilai 88 bit dan 40 bit menghasilkan kunci 128 bit, yang digunakan untuk mengenkripsi pesan dengan AES dalam Mode Penghitung (CTR). Nilai 40 bit digunakan oleh penerima untuk memverifikasi integritas plaintext yang didekripsi. Kunci AES per pesan ini dienkripsi menggunakan RSA-OAEP ke kunci publik dari perangkat penerima. Kombinasi pesan teks terenkripsi dan kunci pesan terenkripsi kemudian di-hash dengan SHA-1, dan hash ditandatangani dengan Algoritme Tanda Tangan Digital Kurva Eliptis (ECDSA) menggunakan kunci penanda tangan pribadi milik perangkat pengirim. Di iOS 13 atau lebih baru dan iPadOS 13.1 atau lebih baru, perangkat mungkin menggunakan enkripsi Skema Enkripsi Terintegrasi Kurva Eliptis (ECIES) alih-alih enkripsi RSA.

Pesan yang dihasilkan, satu untuk setiap perangkat penerima, berisi teks pesan terenkripsi, kunci pesan terenkripsi, dan tanda tangan digital pengirim. Pesan kemudian diteruskan ke APN untuk dikirim. Metadata, seperti tanda waktu dan informasi rute APN, tidak dienkripsi. Komunikasi dengan APN dienkripsi menggunakan saluran TLS dengan kerahasiaan maju.

APN hanya dapat mengirimkan pesan berukuran hingga 4 atau 16 KB, tergantung versi iOS dan iPadOS. Jika teks pesan terlalu panjang atau jika lampiran seperti foto disertakan, lampiran dienkripsi menggunakan AES dalam mode CTR dengan kunci 256 bit yang dibuat secara acak dan diunggah ke iCloud. Kunci AES untuk lampiran, Pengenal Sumber Seragam (URI), dan hash SHA-1 dari format terenkripsinya kemudian dikirimkan ke penerima sebagai konten iMessage, dengan kerahasiaan dan integritasnya yang terlindungi melalui enkripsi iMessage normal, sebagaimana yang ditampilkan di diagram.



Untuk percakapan grup, proses ini diulangi untuk setiap penerima dan perangkatnya.

Perangkat penerima menerima salinan pesannya dari APN, dan, jika perlu, mengambil lampiran dari iCloud. Nomor telepon atau alamat email masuk milik pengirim dicocokkan dengan kontak penerima sehingga nama dapat ditampilkan, jika memungkinkan.

Sebagaimana halnya dengan semua pemberitahuan push, pesan dihapus dari APN saat dikirimkan. Berbeda dengan pemberitahuan APN lainnya, pesan iMessage diantrekan untuk dikirim ke perangkat offline. Pesan disimpan di server Apple hingga selama 30 hari.

Berbagi foto dan nama iMessage dengan aman

Berbagi Foto dan Nama iMessage memungkinkan pengguna untuk berbagi Nama dan Foto menggunakan iMessage. Pengguna dapat memilih informasi Kartu Saya milik mereka, atau menyesuaikan nama dan menyertakan gambar apa pun yang mereka pilih. Berbagi Foto dan Nama iMessage menggunakan sistem dua tahap untuk mendistribusikan nama dan foto.

Data dibagi ke dalam bidang, masing-masing dienkripsi dan disahkan secara terpisah dan disahkan bersama dengan proses di bawah. Ada tiga bidang:

- Nama
- Foto
- Nama file foto

Salah satu langkah pertama dari pembuatan data adalah untuk membuat kunci rekaman 128 bit secara acak di perangkat. Kunci rekaman ini kemudian diturunkan dengan HKDF-HMAC-SHA256 untuk membuat tiga subkunci: Kunci 1:Kunci 2:Kunci 3 = HKDF(kunci rekaman “nama panggilan”). Untuk setiap bidang, Vektor Inisialisasi (IV) 96 bit acak dibuat dan data dienkripsi menggunakan AES-CTR dan Kunci 1. Kode pengesahan pesan (MAC) kemudian dihitung dengan HMAC-SHA256 menggunakan Kunci 2 dan menyertakan nama bidang, IV bidang, dan ciphertext bidang. Terakhir, kumpulan nilai MAC bidang terpisah disatukan dan MAC-nya dihitung dengan HMAC-SHA256 menggunakan Kunci 3. MAC 256 bit disimpan bersama data yang dienkripsi. 128 bit pertama dari MAC ini digunakan sebagai RecordID.

Rekaman terenkripsi ini kemudian disimpan di database publik CloudKit di bagian RecordID. Rekaman ini tidak pernah dimutasi dan jika pengguna memilih untuk mengubah nama dan foto mereka, rekaman terenkripsi baru akan dibuat. Jika pengguna 1 memilih untuk membagikan nama dan foto mereka dengan pengguna 2, mereka mengirimkan kunci rekaman bersama dengan recordID di dalam muatan iMessage mereka, yang dienkripsi.

Saat perangkat pengguna 2 menerima muatan iMessage ini, perangkat akan mendeteksi bahwa muatan berisi recordID dan kunci Nama Panggilan dan Foto. Perangkat pengguna 2 kemudian akan mengakses database CloudKit publik untuk mengambil nama dan foto terenkripsi di ID rekaman dan mengirimkannya menggunakan iMessage.

Setelah pesan diterima, perangkat pengguna 2 mendekripsi muatan dan memverifikasi tanda tangan menggunakan recordID. Jika berhasil, pengguna 2 akan diberi nama dan foto, dan mereka dapat memilih untuk menambahkannya ke kontak mereka, atau menggunakannya untuk Pesan.

Mengamankan Apple Messages for Business

Apple Messages for Business adalah layanan pesan yang memungkinkan pengguna untuk berkomunikasi dengan bisnis menggunakan app Pesan. Dengan Apple Messages for Business, pengguna selalu memiliki kontrol pada percakapan. Pengguna juga dapat menghapus percakapan dan memblokir bisnis agar tidak mengirimkan pesan di masa mendatang. Demi privasi, bisnis tidak menerima informasi nomor telepon, alamat email, atau akun iCloud pengguna. Sebagai gantinya, pengenal unik khusus yang disebut *ID Buram* dibuat oleh Layanan Identitas Apple (IDS) dan dibagikan dengan bisnis. ID Buram bersifat unik terhadap hubungannya antara ID Apple pengguna dan ID Bisnis milik bisnis. Pengguna memiliki ID Buram berbeda untuk setiap bisnis yang pengguna hubungi menggunakan Apple Messages for Business. Pengguna menentukan apakah dan kapan pengguna membagikan informasi yang mengidentifikasi secara pribadi dengan bisnis dan layanan Apple Messages for Business tidak pernah menyimpan riwayat percakapan.

Apple Messages for Business mendukung ID Apple yang Dikelola dari Apple Business Manager dan menentukan apakah ID Apple diaktifkan untuk iMessage serta FaceTime di Apple School Manager.

Pesan yang dikirimkan ke bisnis dienkripsi di antara perangkat pengguna dan server pesan Apple, menggunakan keamanan yang sama serta server pesan Apple seperti iMessage. Server pesan Apple mendekripsi pesan ini di RAM, dan merelainya ke bisnis melalui tautan terenkripsi menggunakan TLS 1.2. Pesan tidak pernah disimpan dalam bentuk yang tidak dienkripsi saat transit melalui layanan Apple Messages for Business. Balasan bisnis juga dikirim menggunakan TLS 1.2 ke server pesan Apple, tempat balasan dienkripsi menggunakan kunci publik unik dari setiap perangkat penerima.

Jika perangkat pengguna online, pesan akan segera dikirim dan tidak di-cache di server pesan Apple. Jika perangkat pengguna tidak online, pesan yang dienkripsi di-cache hingga 30 hari untuk memungkinkan pengguna menerimanya saat perangkat kembali online. Segera setelah perangkat kembali online, pesan dikirim dan dihapus dari cache. Setelah 30 hari, cache pesan yang tidak terkirim kedaluwarsa dan dihapus secara permanen.

Keamanan FaceTime

FaceTime adalah layanan panggilan audio dan video Apple. Seperti iMessage, panggilan FaceTime menggunakan layanan Pemberitahuan Push Apple (APN) untuk membuat koneksi awal ke perangkat terdaftar milik pengguna. Konten audio/video dari panggilan FaceTime dilindungi oleh enkripsi ujung ke ujung, sehingga tidak ada orang yang dapat mengaksesnya kecuali pengirim dan penerima. Apple tidak dapat mendekripsi data tersebut.

Koneksi awal FaceTime dilakukan melalui infrastruktur server Apple yang merelai paket data di antara perangkat yang didaftarkan pengguna. Dengan pemberitahuan APN dan pesan Utilitas Traversal Sesi untuk NAT (STUN) melalui koneksi yang direlai, perangkat memverifikasi sertifikat identitasnya dan membuat rahasia bersama untuk setiap sesi. Rahasia bersama digunakan untuk menurunkan kunci sesi untuk saluran media yang di-stream menggunakan Protokol Transpor Real Time Aman. (SRTP). Paket SRTP dienkripsi menggunakan AES256 dalam Mode Penghitung dan disahkan dengan HMAC-SHA1. Setelah pengaturan koneksi dan keamanan awal, FaceTime menggunakan STUN dan Pembuatan Konektivitas Internet (ICE) untuk membuat koneksi ujung ke ujung antarperangkat, jika memungkinkan.

FaceTime Grup memperluas FaceTime hingga mendukung maksimum 33 peserta pada saat yang bersamaan. Sama halnya dengan FaceTime perseorangan klasik, panggilan dienkripsi dalam bentuk ujung ke ujung di antara perangkat pengguna yang diundang. Meskipun FaceTime Grup menggunakan kembali banyak bagian dari infrastruktur dan desain FaceTime perseorangan, panggilan grup ini dilengkapi dengan mekanisme pembuatan kunci berlandaskan keautentikan yang disediakan oleh Layanan Identitas (IDS) Apple. Protokol ini menyediakan kerahasiaan maju, yang berarti bahwa penyusupan pada perangkat pengguna tidak akan membocorkan konten panggilan lampau. Kunci sesi dibungkus menggunakan AES-SIV dan didistribusikan di antara peserta menggunakan konstruksi ECIES dengan kunci P-256 ECDH jangka pendek.

Saat nomor telepon atau alamat email baru ditambahkan ke panggilan FaceTime Grup yang sedang berlangsung, perangkat yang aktif akan membuat kunci media baru dan tidak akan membagikan kunci yang sebelumnya digunakan dengan perangkat yang baru diundang.

Lacak

Keamanan Lacak

App Lacak untuk perangkat Apple dibangun dengan landasan kriptografi kunci publik mutakhir.

Tinjauan

App Lacak menggabungkan Cari iPhone Saya dan Cari Teman Saya ke dalam satu app di iOS, iPadOS, dan macOS. Lacak dapat membantu pengguna menemukan perangkat yang hilang, bahkan saat Mac offline. Perangkat online dapat melaporkan lokasi ke pengguna melalui iCloud. Lacak berfungsi offline dengan mengirimkan sinyal Bluetooth jarak dekat dari perangkat yang hilang, yang dapat dideteksi oleh perangkat Apple lain yang digunakan di sekitar. Perangkat di sekitar tersebut lalu meneruskan lokasi terdeteksi dari perangkat yang hilang ke iCloud sehingga pengguna dapat menemukannya di app Lacak—semua ini dilakukan sembari melindungi privasi dan keamanan semua pengguna yang terlibat. Lacak bahkan berfungsi dengan Mac yang offline dan dalam mode tidur.

Dengan menggunakan Bluetooth dan ratusan juta perangkat iOS, iPadOS, dan macOS yang sedang digunakan secara aktif di seluruh dunia, pengguna dapat menemukan perangkat yang hilang, meskipun perangkat tidak terhubung ke jaringan Wi-Fi atau seluler. Setiap perangkat iOS, iPadOS, atau macOS yang mengaktifkan “penemuan offline” di pengaturan Lacak dapat berfungsi sebagai “perangkat penemu”. Ini berarti perangkat dapat mendeteksi kehadiran perangkat offline lain yang hilang menggunakan Bluetooth, lalu menggunakan koneksi jaringannya untuk melaporkan kembali perkiraan lokasinya ke pemilik. Jika perangkat mengaktifkan penemuan offline, itu juga berarti bahwa perangkat dapat ditemukan oleh peserta lain dengan cara yang sama. Seluruh interaksi ini dienkripsi ujung ke ujung, bersifat anonim, serta dirancang agar hemat baterai dan data. Terdapat sedikit dampak pada masa pakai baterai serta penggunaan paket data seluler, dan privasi pengguna dilindungi dengan lebih baik.

Catatan: Lacak mungkin tidak tersedia di semua negara atau wilayah.

Enkripsi ujung ke ujung

Lacak dibangun dengan landasan kriptografi kunci publik mutakhir. Saat penemuan offline diaktifkan di pengaturan Lacak, pasangan kunci enkripsi pribadi kurva eliptis (EC) P-224 dengan notasi {d,P} dibuat secara langsung di perangkat dengan *d* sebagai kunci pribadi dan *P* kunci publik. Selain itu, SK_0 rahasia 256 bit dan penghitung $_i$ dimulai dari nol. Pasangan kunci pribadi ini dan rahasianya tidak pernah dikirimkan ke Apple dan hanya diselaraskan di antara perangkat pengguna lainnya dengan enkripsi ujung ke ujung menggunakan Rantai Kunci iCloud. Rahasia dan penghitung digunakan untuk menurunkan SK_i kunci simetris saat ini dengan konstruksi berulang berikut: $SK_i = KDF(SK_{i-1}, \text{“update”})$.

Berdasarkan kunci SK_i, dua integer besar u_i, dan v_i dihitung dengan $(u_i,v_i) = KDF(SK_i, \text{“diversify”})$. Kunci pribadi P-224 bernotasi *d* dan kunci publiknya yang bernotasi *P* kemudian diturunkan menggunakan relasi affine yang melibatkan kedua integer untuk menghitung pasangan kunci jangka pendek: Kunci pribadi yang diturunkan adalah d_i dengan $d_i = u_i * d + v_i$ (modulus urutan kurva P-224) dan bagian publiknya = P_i dan memverifikasi $P_i = u_i*P + v_i*G$.

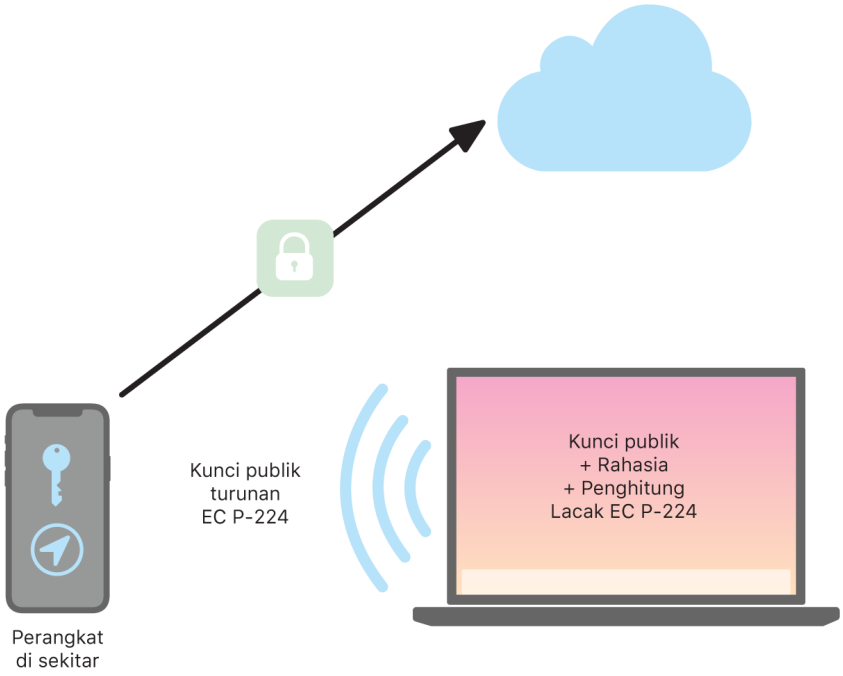
Jika perangkat hilang dan tidak dapat terhubung ke Wi-Fi atau seluler—misalnya, sebuah MacBook Pro tertinggal di bangku taman—perangkat tersebut akan mulai menyiarkan kunci publik turunan P_i secara berkala dalam periode waktu terbatas dalam muatan Bluetooth. Dengan menggunakan P-224, representasi kunci publik dapat disertakan dalam satu muatan Bluetooth. Kemudian, perangkat di sekitar dapat membantu menemukan perangkat offline tersebut dengan mengenkripsi lokasinya ke kunci publik. Kira-kira setiap 15 menit, kunci publik diganti oleh yang baru menggunakan nilai tertambah dari penghitung dan proses di atas sehingga pengguna tidak dapat dilacak oleh pengenal tetap. Mekanisme penurunan dirancang untuk menghalangi berbagai kunci publik P_i untuk dikaitkan ke perangkat yang sama.

Menjaga anonimitas pengguna dan perangkat

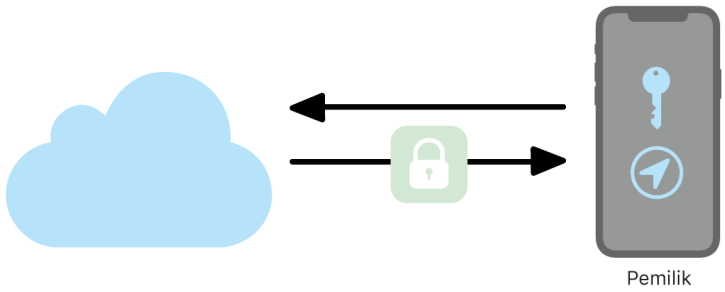
Selain memastikan bahwa informasi lokasi dan data lainnya terenkripsi sepenuhnya, privasi identitas peserta tetap terjaga dari satu sama lain dan dari Apple. Lalu lintas yang dikirimkan ke Apple oleh perangkat penemu tidak berisi informasi pengesahan pada konten atau header-nya. Oleh karena itu, Apple tidak mengetahui siapa penemu atau perangkat siapa yang telah ditemukan. Selain itu, Apple tidak mencatat informasi yang akan mengungkap identitas penemu, dan tidak menyimpan informasi yang akan memungkinkan seseorang untuk mengorelasikan penemu dan pemilik. Pemilik perangkat hanya menerima informasi lokasi terenkripsi yang telah didekripsi dan ditampilkan di app Lacak tanpa petunjuk mengenai siapa yang menemukan perangkat.

Menggunakan Lacak untuk menemukan perangkat Apple yang hilang

Setiap perangkat Apple dalam jangkauan Bluetooth yang mengaktifkan penemuan offline dapat mendeteksi sinyal dari perangkat Apple lain yang dikonfigurasi untuk mengizinkan Lacak dan membaca kunci P_i yang sedang disiarkan. Dengan menggunakan konstruksi ECIES dan kunci publik P_i dari siaran, perangkat penemu mengenkripsi informasi lokasi mereka saat ini dan merelainya ke Apple. Lokasi terenkripsi dikaitkan dengan indeks server yang dihitung sebagai hash SHA256 dari kunci publik P-224 P_i yang diambil dari muatan Bluetooth. Apple tidak memiliki kunci dekripsi, sehingga Apple tidak dapat membaca lokasi yang dienkripsi oleh penemu. Pemilik perangkat yang hilang dapat merekonstruksi indeks dan mendekripsi lokasi yang dienkripsi.



Saat mencoba menemukan perangkat yang hilang, nilai penghitung yang diharapkan akan diperkirakan selama periode waktu pencarian lokasi. Dengan diketahuinya kunci *d* P-224 pribadi yang asli dan nilai rahasia SK_i dalam rentang nilai penghitung selama periode pencarian, pemilik dapat merekonstruksi kumpulan nilai $\{d_i, SHA256(P_i)\}$ di sepanjang periode pencarian. Kemudian, perangkat pemilik yang digunakan untuk mencari perangkat yang hilang dapat mengirimkan permintaan ke server menggunakan kumpulan nilai indeks $SHA256(P_i)$ dan mengunduh lokasi terenkripsi dari server. App Lacak kemudian secara lokal mendekripsi lokasi yang terenkripsi dengan mencocokkan kunci pribadi d_i dan menampilkan perkiraan lokasi dari perangkat yang hilang di app. Laporan lokasi dari beberapa perangkat penemu digabungkan dengan app pemilik untuk membuat lokasi yang lebih tepat.



Menemukan perangkat yang offline

Jika pengguna mengaktifkan Cari iPhone Saya di perangkat mereka, penemuan offline akan diaktifkan secara default saat mereka meningkatkan perangkat ke iOS 13 atau lebih baru, iPadOS 13.1 atau lebih baru, dan macOS 10.15 atau lebih baru. Ini dirancang untuk memastikan bahwa setiap pengguna memiliki peluang sebesar mungkin untuk menemukan perangkat mereka yang hilang. Namun, jika pada suatu saat pengguna memutuskan untuk tidak berpartisipasi, mereka dapat menonaktifkan penemuan offline di pengaturan Lacak di perangkat mereka. Jika penemuan offline dinonaktifkan, perangkat tidak akan lagi dapat menemukan perangkat yang hilang atau terdeteksi oleh perangkat penemu lain. Namun, pengguna masih dapat menemukan perangkat selama perangkat tersebut terhubung ke jaringan Wi-Fi atau seluler.

Jika perangkat offline yang hilang ditemukan, pengguna akan menerima pemberitahuan dan pesan email untuk memberi tahu mereka bahwa perangkat telah ditemukan. Untuk melihat lokasi perangkat yang hilang, pengguna membuka app Lacak dan memilih tab Perangkat. Alih-alih menampilkan perangkat pada peta kosong seperti sebelum perangkat ditemukan, Lacak menampilkan lokasi peta dengan perkiraan alamat dan informasi mengenai kapan perangkat terdeteksi. Jika terdapat laporan lokasi lain yang masuk, lokasi dan stempel waktu saat ini kan diperbarui secara otomatis. Meskipun pengguna tidak dapat memutar bunyi pada perangkat offline atau menghapusnya dari jauh, mereka dapat menggunakan informasi lokasi untuk melacak langkah mereka atau mengambil tindakan lain untuk membantu mereka memperoleh kembali perangkat yang hilang.

Berkelanjutan

Tinjauan keamanan Berkelanjutan

Berkelanjutan memanfaatkan teknologi seperti iCloud, Bluetooth, dan Wi-Fi untuk memungkinkan pengguna melanjutkan aktivitas dari satu perangkat ke perangkat lain, melakukan dan menerima panggilan telepon, mengirim dan menerima pesan teks, dan berbagi koneksi internet seluler.

Keamanan Handoff

Apple menangani handoff dengan aman, dari satu pengguna ke pengguna lain, antara app asal dan situs web, dan bahkan penyerahan sejumlah besar data.

Cara Handoff bekerja dengan aman

Dengan Handoff, saat perangkat iOS, iPadOS, dan macOS pengguna berada di dekat satu sama lain, pengguna dapat meneruskan apa yang mereka kerjakan dari satu perangkat ke perangkat lain secara otomatis. Handoff memungkinkan pengguna untuk beralih perangkat dan langsung melanjutkan pekerjaan.

Saat pengguna masuk ke iCloud di perangkat kedua dengan fitur Handoff, kedua perangkat tersebut akan membuat pemasangan luar jalur Bluetooth Rendah Energi (BLE) 4.2 menggunakan APN. Pesan terpisah dienkripsi seperti pesan di iMessage. Setelah dipasangkan, setiap perangkat akan membuat kunci AES 256 bit simetris yang disimpan di rantai kunci perangkat. Kunci ini dapat mengenkripsi dan mengesahkan iklan BLE yang mengomunikasikan aktivitas perangkat saat ini dengan perangkat iCloud lain yang dipasangkan menggunakan AES256 dalam mode GCM, dengan tindakan perlindungan pemutaran ulang.

Saat perangkat menerima iklan dari kunci baru untuk pertama kalinya, perangkat akan membuat koneksi BLE ke perangkat asal dan melakukan pertukaran kunci enkripsi iklan. Koneksi ini diamankan menggunakan enkripsi BLE 4.2 standar serta enkripsi pesan individual, yang serupa dengan bagaimana iMessage dienkripsi. Di situasi tertentu, pesan ini dikirimkan menggunakan APN alih-alih BLE. Muatan aktivitas dilindungi dan ditransfer dengan cara yang sama dengan iMessage.

Handoff antara app asli dan situs web

Handoff memungkinkan app asli iOS, iPadOS, atau macOS untuk melanjutkan aktivitas pengguna di halaman web di domain yang dikontrol secara sah oleh pengembang app. Handoff juga memungkinkan aktivitas pengguna app asli untuk dilanjutkan di browser web.

Untuk membantu mencegah app asli melanjutkan situs web yang tidak dikontrol oleh pengembang, app harus menunjukkan kontrol sah terhadap domain web yang ingin dilanjutkan app. Kontrol terhadap domain situs web dibangun menggunakan mekanisme untuk info pengesahan web bersama. Untuk detail, lihat Akses app ke kata sandi yang disimpan. Sistem harus memvalidasi kontrol nama domain app sebelum app diizinkan untuk menerima Handoff aktivitas pengguna.

Sumber Handoff halaman web dapat berupa browser apa pun yang mengadopsi API Handoff. Saat pengguna melihat halaman web, sistem mengiklankan nama domain halaman web dalam bita iklan Handoff yang dienkripsi. Hanya perangkat lain milik pengguna yang dapat mendekripsi bita iklan.

Di perangkat penerima, sistem mendeteksi bahwa app asli yang diinstal menerima Handoff dari nama domain yang diiklankan dan menampilkan ikon app asli sebagai pilihan Handoff. Saat diluncurkan, app asli menerima URL lengkap dan judul halaman web. Tidak ada informasi lain yang diteruskan dari browser ke app asli.

Di sisi lain, app asli dapat menetapkan URL balik jika app asli yang sama tidak terinstal di perangkat penerima Handoff. Pada kasus ini, sistem akan menampilkan browser default pengguna sebagai pilihan app Handoff (jika browser tersebut telah mengadopsi API Handoff). Saat Handoff diminta, browser diluncurkan dan diberi URL balik oleh app sumber. Tidak ada keharusan bagi URL balik untuk dibatasi menjadi nama domain yang dikontrol oleh pengembang app asli.

Handoff data yang lebih besar

Selain menggunakan fitur dasar Handoff, beberapa app dapat memilih untuk menggunakan API yang mendukung pengiriman data dalam jumlah lebih besar melalui teknologi Wi-Fi rekan ke rekan yang dibuat Apple (seperti AirDrop). Misalnya, app Mail menggunakan API ini untuk mendukung handoff draf mail, yang dapat berisi lampiran besar.

Saat app menggunakan API ini, pertukaran antara dua perangkat dimulai seperti di Handoff. Namun, setelah menerima muatan awal menggunakan Bluetooth Rendah Energi (BLE), perangkat penerima memulai koneksi baru melalui Wi-Fi. Koneksi ini dienkripsi (dengan TLS), dan menurunkan kepercayaan melalui identitas yang dibagikan melalui Rantai Kunci iCloud. Identitas di sertifikat diverifikasi terhadap identitas pengguna. Data muatan lebih lanjut dikirimkan melalui koneksi terenkripsi ini hingga transfer selesai.

Papan Klip Universal

Papan Klip Universal memanfaatkan Handoff untuk mentransfer konten papan klip pengguna antarperangkat dengan aman sehingga mereka dapat menyalin di satu perangkat dan menempelkannya di perangkat lain. Konten dilindungi dengan cara yang sama dengan data Handoff lainnya dan dibagikan secara default dengan Papan Klip Universal kecuali jika pengembang app memilih untuk tidak mengizinkan berbagi.

App memiliki akses ke data papan klip terlepas dari apakah pengguna telah menempelkan papan klip ke app atau tidak. Dengan Papan Klip Universal, akses data ini tersedia bagi app yang dijalankan di perangkat pengguna lainnya (sebagaimana yang dibuat oleh info masuk iCloud mereka).

Keamanan relai panggilan seluler iPhone

Saat Mac, iPad, iPod touch, atau HomePod pengguna terhubung ke jaringan Wi-Fi yang sama dengan iPhone mereka, perangkat dapat melakukan dan menerima panggilan telepon menggunakan koneksi seluler di iPhone. Konfigurasi mengharuskan perangkat untuk masuk ke iCloud dan FaceTime menggunakan akun ID Apple yang sama.

Saat panggilan masuk tiba, semua perangkat yang dikonfigurasi akan diberi tahu menggunakan layanan Pemberitahuan Push Apple (APN), dengan tiap pemberitahuan menggunakan enkripsi ujung ke ujung yang sama dengan yang digunakan iMessage. Perangkat yang berada di jaringan yang sama menampilkan antarmuka pengguna pemberitahuan panggilan masuk. Saat pengguna menjawab panggilan, audio ditransmisikan dengan lancar dari iPhone pengguna menggunakan koneksi rekan ke rekan yang aman antara kedua perangkat.

Saat panggilan dijawab di satu perangkat, deringan di perangkat di sekitar yang dipasangkan iCloud dihentikan oleh pengiklanan singkat menggunakan Bluetooth Rendah Energi (BLE). Bita pengiklanan dienkripsi menggunakan metode yang sama dengan pengiklanan Handoff.

Panggilan keluar juga direlai ke iPhone menggunakan APN, dan audio ditransmisikan dengan cara yang serupa melalui tautan rekan ke rekan yang aman antarperangkat. Pengguna dapat menonaktifkan penyampaian panggilan telepon di perangkat dengan mematikan Panggilan Seluler iPhone di pengaturan FaceTime.

Keamanan Penerusan Pesan Teks iPhone

Penerusan Pesan Teks mengirimkan pesan teks SMS yang diterima di iPhone secara otomatis ke iPad, iPod touch, atau Mac yang didaftarkan milik pengguna. Setiap perangkat harus masuk ke layanan iMessage menggunakan akun ID Apple yang sama. Jika Penerusan Pesan Teks dinyalakan, pendaftaran akan dilakukan secara otomatis di perangkat dalam lingkaran kepercayaan pengguna jika autentikasi dua faktor diaktifkan. Jika tidak, pendaftaran diverifikasi di setiap perangkat dengan memasukkan kode numerik enam digit acak yang dibuat oleh iPhone.

Setelah perangkat tertaut, iPhone mengenkripsi dan meneruskan pesan teks SMS masuk ke setiap perangkat, menggunakan metode yang dijelaskan di tinjauan keamanan iMessage. Balasan dikirim kembali ke iPhone menggunakan metode yang sama, lalu iPhone mengirimkan balasan sebagai pesan teks menggunakan mekanisme transmisi SMS operator. Penerusan Pesan Teks dapat dinyalakan atau dimatikan di pengaturan Pesan.

Keamanan Instant Hotspot

Instant Hotspot menghubungkan perangkat Apple lainnya ke hotspot iOS atau iPadOS pribadi. Perangkat iOS dan iPadOS yang mendukung Instant Hotspot menggunakan Bluetooth Rendah Energi (BLE) untuk menemukan dan berkomunikasi dengan semua perangkat yang telah masuk ke akun iCloud yang sama atau akun yang digunakan dengan Keluarga Berbagi (di iOS 13 dan iPadOS). Komputer Mac yang kompatibel dengan OS X 10.10 atau lebih baru menggunakan teknologi yang sama untuk menemukan dan berkomunikasi dengan perangkat iOS dan iPadOS Instant Hotspot.

Saat pertama kali pengguna masuk ke Pengaturan Wi-Fi di perangkat, perangkat memancarkan pengiklanan BLE berisi pengenal yang disetujui oleh semua perangkat yang masuk ke akun iCloud yang sama. Pengenal dibuat dari DSID (Pengenal Sinyal Tujuan) yang dikaitkan dengan akun iCloud dan dirotasi secara berkala. Saat perangkat lain yang masuk ke akun iCloud yang sama berada di sekitar dan mendukung Hotspot Pribadi, perangkat dapat mendeteksi sinyal dan merespons, menunjukkan ketersediaan untuk menggunakan Instant Hotspot.

Saat pengguna yang bukan bagian dari Keluarga Berbagi memilih iPhone atau iPad untuk Hotspot Pribadi, permintaan untuk menyalakan Hotspot Pribadi akan dikirimkan ke perangkat tersebut. Permintaan dikirimkan melalui tautan terenkripsi menggunakan enkripsi BLE, dan permintaan dienkripsi dengan cara yang serupa dengan enkripsi iMessage. Perangkat kemudian merespons melalui tautan BLE yang sama menggunakan enkripsi per pesan yang sama dengan informasi koneksi Hotspot Pribadi.

Untuk pengguna yang merupakan bagian dari Keluarga Berbagi, informasi koneksi Hotspot Pribadi dibagikan dengan aman menggunakan mekanisme serupa dengan yang digunakan oleh perangkat HomeKit untuk menyelaraskan informasi. Khususnya, koneksi yang berbagi informasi hotspot di antara pengguna diamankan dengan kunci sementara ECDH (Curve25519) yang disahkan dengan masing-masing kunci publik Ed25519 spesifik perangkat pengguna. Kunci publik yang digunakan adalah kunci yang sebelumnya telah diselaraskan di antara anggota Keluarga Berbagi menggunakan IDS saat Keluarga Berbagi dibuat.

Keamanan jaringan

Tinjauan keamanan jaringan

Selain pengamanan internal yang digunakan Apple untuk melindungi data yang disimpan di perangkat Apple, ada banyak tindakan yang dapat digunakan organisasi untuk menjaga keamanan informasi saat dikirimkan dari dan ke perangkat. Semua perlindungan dan tindakan ini ada di keamanan jaringan.

Karena pengguna harus dapat mengakses jaringan perusahaan dari mana pun di dunia, ini penting untuk membantu memastikan bahwa mereka disahkan dan bahwa data mereka terlindungi selama transmisi. Untuk mencapai tujuan keamanan ini, iOS, iPadOS, serta macOS memadukan teknologi yang teruji dan standar terbaru untuk koneksi jaringan Wi-Fi dan data seluler. Karenanya sistem operasi kami menggunakan—dan menyediakan akses pengembang ke—protokol jaringan standar untuk komunikasi yang dienkripsi, diizinkan, dan disahkan.

Keamanan TLS

iOS, iPadOS, serta macOS mendukung Keamanan Lapisan Transpor (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) dan Keamanan Lapisan Transpor Datagram (DTLS). Protokol TLS mendukung AES128 dan AES256, dan memprioritaskan rangkaian cipher dengan kerahasiaan maju. App internet seperti Safari, Kalender, dan Mail menggunakan protokol ini secara otomatis untuk mengaktifkan saluran komunikasi terenkripsi antara perangkat dan layanan jaringan. API Level Tinggi (seperti CFNetwork) memudahkan pengembang untuk mengadopsi TLS di app mereka, sementara API level rendah (seperti Network.framework) menyediakan kontrol cermat. CFNetwork tidak mengizinkan SSL 3, dan app yang menggunakan WebKit (seperti Safari) dilarang membuat koneksi SSL 3.

Di iOS 11 atau lebih baru dan macOS 10.13 atau lebih baru, sertifikat SHA-1 tidak lagi diizinkan untuk koneksi TLS kecuali jika dipercaya oleh pengguna. Sertifikat dengan kunci RSA yang lebih pendek dari 2048 bit juga tidak diizinkan. Rangkaian cipher simetris RC4 tidak lagi digunakan di iOS 10 dan macOS 10.12. Secara default, klien atau server TLS yang diterapkan dengan API SecureTransport tidak memiliki rangkaian cipher RC4 dan tidak dapat terhubung jika RC4 adalah satu-satunya rangkaian cipher yang tersedia. Agar lebih aman, layanan atau app yang memerlukan RC4 harus ditingkatkan untuk menggunakan rangkaian cipher aman. Di iOS 12.1, sertifikat yang diterbitkan setelah 15 Oktober 2018 dari sertifikat root yang dipercayai sistem harus masuk ke dalam log Transparansi Sertifikat tepercaya untuk memungkinkan koneksi TLS. Di iOS 12.2, TLS 1.3 diaktifkan secara default untuk API Network.framework dan NSURLSession. Klien TLS yang menggunakan API SecureTransport tidak dapat menggunakan TLS 1.3.

Keamanan Transpor App

Keamanan Transpor App menyediakan persyaratan koneksi default sehingga app diharuskan untuk mengutamakan koneksi aman saat menggunakan API NSURLConnection, CFURL, atau NSURLSession. Secara default, Keamanan Transpor App membatasi pilihan cipher menjadi hanya rangkaian yang menyediakan kerahasiaan maju, khususnya:

- ECDHE_ECDSA_AES dan ECDHE_RSA_AES dalam Mode Galois/Penghitung (GCM)
- Mode Rantai Blok Cipher (CBC)

App dapat menonaktifkan persyaratan kerahasiaan maju per domain, dalam kasus ini, RSA_AES ditambahkan ke rangkaian cipher yang tersedia.

Server harus mendukung TLS 1.2 dan kerahasiaan maju, dan sertifikat harus sah serta ditandatangani menggunakan SHA256 atau lebih kuat dengan setidaknya kunci RSA 2048 bit atau kunci kurva eliptis 256 bit.

Koneksi jaringan yang tidak memenuhi persyaratan ini akan gagal kecuali jika app menimpa Keamanan Transpor App. Sertifikat yang tidak sah selalu mengakibatkan kegagalan perangkat dan tidak adanya koneksi. Keamanan Transpor App diterapkan ke app yang dibuat untuk iOS 9 atau lebih baru dan macOS 10.11 atau lebih baru secara otomatis.

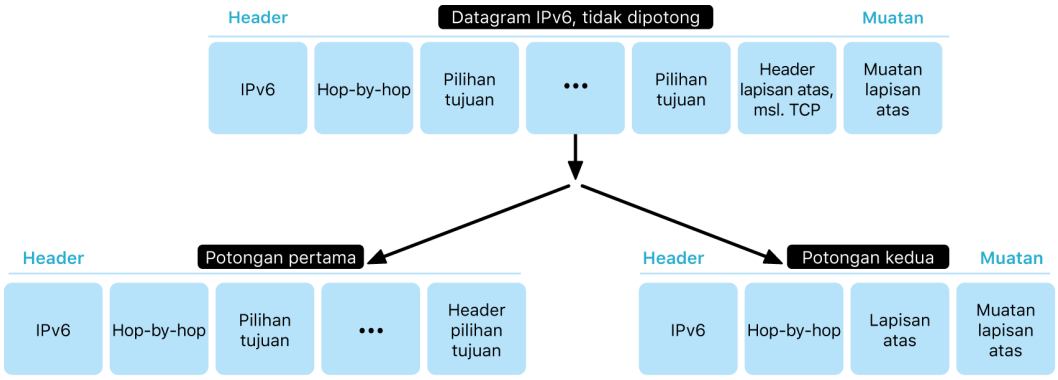
Pemeriksaan validitas sertifikat

Pengevaluasian status sertifikat TLS tepercaya dilakukan sesuai dengan standar industri yang dibuat, seperti yang diputuskan di RFC 5280, dan menggabungkan standar yang muncul seperti RFC 6962 (Transparansi Sertifikat). Di iOS 11 atau lebih baru dan macOS 10.13 atau lebih baru, perangkat Apple diperbarui secara berkala dengan daftar sertifikat yang dibatalkan serta dibatasi saat ini. Daftar diagregatkan dari daftar pembatalan sertifikat (CRL) yang diterbitkan oleh setiap otoritas sertifikat daftar internal yang dipercayai oleh Apple, serta oleh penerbit CA bawahan. Daftar juga dapat menyertakan batasan lainnya atas kehendak Apple. Informasi ini dikonsultasikan kapan pun fungsi API jaringan digunakan untuk membuat koneksi aman. Jika ada terlalu banyak sertifikat yang dibatalkan dari CA untuk dicantumkan secara terpisah, evaluasi kepercayaan dapat memerlukan respons status sertifikat online (OCSP), dan jika responsnya tidak tersedia, evaluasi kepercayaan akan gagal.

Keamanan IPv6

Semua sistem operasi Apple mendukung IPv6, mengimplementasikan beberapa mekanisme untuk melindungi privasi pengguna dan stabilitas tumpukan jaringan. Saat Konfigurasi Otomatis Alamat Tanpa Status (SLAAC) digunakan, alamat IPv6 pada semua antarmuka dibuat dalam cara yang membantu mencegah pelacakan perangkat di semua jaringan dan juga memungkinkan pengalaman pengguna yang menakjubkan dengan memastikan stabilitas alamat saat tidak ada perubahan jaringan. Algoritme pembuatan alamat didasarkan pada alamat yang dibuat secara kriptografis sesuai dengan RFC 3972, yang ditingkatkan oleh pengubah spesifik antarmuka untuk memastikan bahwa antarmuka yang berbeda di jaringan yang sama pada akhirnya akan memiliki alamat yang berbeda. Selain itu, alamat sementara dibuat dengan masa pakai 24 jam yang dipilih, dan ini digunakan secara default untuk koneksi baru. Sesuai dengan fitur alamat Wi-Fi Pribadi yang diperkenalkan di iOS 14, iPadOS 14, dan watchOS 7, alamat lokal tautan unik dibuat untuk semua jaringan Wi-Fi tempat perangkat bergabung. SSID jaringan digunakan sebagai elemen tambahan untuk pembuatan alamat, serupa dengan parameter Network_ID yang memenuhi standar RFC 7217. Pendekatan ini digunakan di iOS 14, iPadOS 14, dan watchOS 7.

Untuk melindungi dari serangan berdasarkan header dan fragmentasi IPv6, perangkat Apple mengimplementasikan tindakan perlindungan yang ditetapkan di RFC 6980, RFC 7112, serta RFC 8021. Di antara tindakan lain, ini menghambat serangan tempat lokasi header lapisan atas hanya dapat ditemukan di fragmen kedua (seperti yang ditampilkan di bawah), yang pada gilirannya dapat menyebabkan ambiguitas untuk kontrol keamanan seperti filter paket tanpa status.



Selain itu, untuk membantu memastikan keterandalan tumpukan IPv6 pada sistem operasi Apple, perangkat Apple memberlakukan berbagai batas pada struktur data terkait IPv6, seperti jumlah prefiks per antarmuka.

Keamanan jaringan pribadi virtual (VPN)

Layanan jaringan aman seperti jaringan pribadi virtual biasanya memerlukan sedikit pengaturan dan konfigurasi agar dapat digunakan dengan perangkat iOS, iPadOS, serta macOS.

Protokol yang didukung

Perangkat ini dapat digunakan dengan server VPN yang mendukung protokol dan metode pengesahan berikut:

- IKEv2/IPsec dengan pengesahan oleh rahasia bersama, Sertifikat RSA, Sertifikat Algoritme Tanda Tangan Digital Kurva Eliptis (ECDSA), EAP-MSCHAPv2, atau EAP-TLS
- SSL-VPN yang menggunakan app klien yang sesuai dari App Store
- L2TP/IPsec dengan pengesahan pengguna menggunakan kata sandi MS-CHAPV2 dan pengesahan mesin menggunakan rahasia bersama (iOS, iPadOS, serta macOS) dan RSA SecurID atau CRYPTOCard (hanya macOS)
- Cisco IPsec dengan pengesahan pengguna menggunakan kata sandi, RSA SecurID atau CRYPTOCard, dan pengesahan mesin menggunakan rahasia bersama dan sertifikat (hanya macOS)

Penerapan VPN yang didukung

iOS, iPadOS, serta macOS mendukung hal berikut:

- *VPN Atas Permintaan:* Untuk jaringan yang menggunakan pengesahan berbasis sertifikat. Kebijakan TI menetapkan domain mana yang memerlukan koneksi VPN menggunakan profil konfigurasi VPN.
- *VPN Per App:* Untuk memfasilitasi koneksi VPN pada level yang lebih kecil. Solusi Mobile device management (MDM) dapat menetapkan koneksi untuk tiap app yang dikelola dan domain tertentu di Safari. Ini membantu memastikan bahwa data aman selalu menuju dan berasal dari jaringan perusahaan—dan data pribadi pengguna tidak.

iOS dan iPadOS mendukung hal berikut:

- *VPN Selalu Nyala:* Untuk perangkat yang dikelola melalui solusi MDM dan diawasi menggunakan Apple Configurator untuk Mac, Apple School Manager, atau Apple Business Manager. Dengan VPN Selalu Nyala, pengguna tidak perlu menyalakan VPN untuk mengaktifkan perlindungan saat terhubung ke jaringan seluler atau Wi-Fi. VPN Selalu Nyala juga memberi organisasi kontrol penuh atas lalu lintas perangkat dengan menyalurkan lalu lintas IP ke perusahaan. Pertukaran parameter dan kunci default untuk enkripsi berikutnya, IKEv2 mengamankan transmisi lalu lintas dengan enkripsi data. Organisasi dapat mengawasi dan memfilter lalu lintas dari dan ke perangkatnya, mengamankan data di jaringannya, dan membatasi akses perangkat ke internet.

Keamanan Wi-Fi

Akses aman ke jaringan nirkabel

Semua platform Apple mendukung pengesahan Wi-Fi dan protokol enkripsi berstandar industri, untuk menyediakan akses serta kerahasiaan yang disahkan saat menghubungkan ke jaringan nirkabel aman berikut:

- WPA2 Pribadi
- WPA2 Perusahaan
- WPA2/WPA3 Transisional
- WPA3 Pribadi
- WPA3 Perusahaan
- WPA3 Perusahaan dengan keamanan 192 bit

WPA2 dan WPA3 mengesahkan koneksi satu sama lain dan menyediakan enkripsi AES 128 bit untuk membantu memastikan kerahasiaan data yang dikirimkan secara nirkabel. Ini memberi pengguna jaminan tertinggi bahwa datanya tetap terlindungi saat mengirimkan dan menerima komunikasi melalui koneksi jaringan Wi-Fi.

Dukungan WPA3

WPA3 didukung di perangkat Apple berikut:

- iPhone 7 atau lebih baru
- iPad generasi ke-5 atau lebih baru
- Apple TV 4K atau lebih baru
- Apple Watch series 3 atau lebih baru
- Komputer Mac (akhir 2013 atau lebih baru, dengan 802.11ac atau lebih baru)

Perangkat yang lebih baru mendukung pengesahan dengan WPA3 Perusahaan dengan keamanan 192 bit, termasuk dukungan untuk enkripsi AES 256 bit saat menghubungkan ke titik akses (AP) nirkabel yang kompatibel. Ini menyediakan perlindungan kerahasiaan yang lebih kuat untuk lalu lintas yang dikirimkan melalui udara. WPA3 Perusahaan dengan keamanan 192 bit didukung di iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, dan perangkat iOS serta iPadOS yang lebih baru.

Dukungan PMF

Selain melindungi data yang dikirimkan secara nirkabel, platform Apple memperluas perlindungan level WPA2 dan WPA3 untuk bingkai pengelolaan unicast dan multicast melalui layanan Bingkai Pengelolaan Terlindungi (PMF) yang didefinisikan di 802.11w. Dukungan PMF tersedia di perangkat Apple berikut:

- iPhone 6 atau lebih baru
- iPad Air 2 atau lebih baru
- Apple TV HD atau lebih baru
- Apple Watch series 3 atau lebih baru
- Komputer Mac (akhir 2013 atau lebih baru, dengan 802.11ac atau lebih baru)

Dengan dukungan untuk 802.1X, perangkat Apple dapat dipadukan dengan berbagai lingkungan pengesahan RADIUS. Metode pengesahan nirkabel 802.1X yang didukung meliputi EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, dan PEAPv1.

Perlindungan platform

Sistem operasi Apple melindungi perangkat dari kerentanan di firmware prosesor jaringan. Ini berarti pengontrol jaringan dengan Wi-Fi memiliki akses terbatas ke memori Prosesor Aplikasi.

- Saat USB atau SDIO (Input Output Digital Aman) digunakan untuk menjalankan antarmuka dengan prosesor jaringan, prosesor jaringan tersebut tidak dapat memulai transaksi akses memori langsung (DMA) ke Prosesor Aplikasi.
- Saat PCIe digunakan, setiap prosesor jaringan berada di bus PCIe-nya sendiri yang terisolasi. Unit Manajemen Memori Input/Output (IOMMU) di setiap bus PCIe lebih jauh membatasi akses DMA prosesor jaringan hanya ke memori dan sumber daya yang berisi paket jaringannya serta struktur kontrol.

Protokol yang tidak lagi digunakan

Produk Apple mendukung pengesahan Wi-Fi dan protokol enkripsi yang sudah tidak digunakan berikut ini:

- WEP Terbuka, dengan kunci 40 bit dan 104 bit
- WEP Bersama, dengan kunci 40 bit dan 104 bit
- WEP Dinamis
- Protokol Integritas Kunci Sementara (TKIP)
- WPA
- WPA/WPA2 Transisional

Protokol ini tidak lagi dianggap aman, dan penggunaannya sangat tidak dianjurkan untuk alasan kompatibilitas, keterandalan, kinerja, dan keamanan. Mereka didukung hanya untuk tujuan kompatibilitas terbalik dan dapat dihapus di versi perangkat lunak mendatang.

Sangat dianjurkan agar semua penerapan Wi-Fi dimigrasi ke WPA3 Pribadi atau WPA3 Perusahaan, untuk menyediakan koneksi Wi-Fi yang kuat, aman, dan kompatibel.

Privasi Wi-Fi

Pengacakan alamat MAC

Platform Apple menggunakan alamat kontrol akses media (alamat MAC) yang diacak saat melakukan pemindaian Wi-Fi saat tidak terkait dengan jaringan Wi-Fi. Pemindaian ini dapat dijalankan untuk menemukan dan menghubungkan ke jaringan Wi-Fi yang diketahui atau untuk membantu Layanan Lokasi untuk app yang menggunakan geofence, seperti pengingat berbasis lokasi atau menetapkan lokasi di Peta Apple. Ingat bahwa pemindaian Wi-Fi yang dilakukan saat mencoba terhubung ke jaringan Wi-Fi yang dipilih tidak diacak. Dukungan pengacakan alamat MAC Wi-Fi tidak tersedia di iPhone 5 atau lebih baru.

Platform Apple juga menggunakan alamat MAC acak saat melakukan pemindaian Pengeluaran Jaringan Pilihan yang ditingkatkan (ePNO) jika perangkat tidak dikaitkan dengan jaringan Wi-Fi atau prosesornya tidur. Pemindaian ePNO dijalankan saat perangkat menggunakan Layanan Lokasi untuk app yang menggunakan geofence, seperti pengingat berbasis lokasi yang menentukan apakah perangkat berada di dekat lokasi tertentu.

Karena alamat MAC perangkat berubah saat terputus dari jaringan Wi-Fi, alamat MAC tidak dapat digunakan untuk melacak perangkat secara terus menerus dengan pengamat pasif dari lalu lintas Wi-Fi, bahkan saat perangkat terhubung ke jaringan seluler. Apple telah memberi tahu produsen Wi-Fi bahwa pemindaian Wi-Fi iOS serta iPadOS menggunakan alamat MAC acak dan bahwa Apple atau produsen tidak dapat memprediksi alamat MAC acak ini.

Di iOS 14 atau lebih baru, iPadOS 14 atau lebih baru, dan watchOS 7 atau lebih baru, saat iPhone, iPad, iPod touch, atau Apple Watch terhubung ke jaringan Wi-Fi, perangkat diidentifikasi dengan alamat MAC unik (acak) per jaringan. Fitur ini dapat dinonaktifkan oleh pengguna atau menggunakan pilihan baru di muatan Wi-Fi. Dalam kondisi tertentu, perangkat akan menggunakan kembali alamat MAC asli.

Untuk informasi lainnya, lihat artikel Dukungan Apple Menggunakan alamat Wi-Fi pribadi di iPhone, iPad, iPod touch, dan Apple Watch.

Pengacakan angka rangkaian bingkai Wi-Fi

Bingkai Wi-Fi menyertakan angka rangkaian, yang digunakan oleh protokol 802.11 level rendah untuk mengaktifkan komunikasi Wi-Fi yang efisien dan dapat diandalkan. Karena angka rangkaian bertambah di setiap bingkai yang ditransmisikan, angka dapat digunakan untuk mengorelasikan informasi yang ditransmisikan selama pemindaian Wi-Fi, dengan bingkai lainnya yang ditransmisikan oleh perangkat yang sama.

Untuk melindungi terhadap hal ini, perangkat Apple mengacak angka rangkaian kapan pun alamat MAC diubah ke alamat baru yang diacak. Ini menyertakan pengacakan angka rangkaian untuk setiap permintaan pemindaian baru yang dimulai saat perangkat tidak dikaitkan. Pengacakan ini didukung di perangkat berikut:

- iPhone 7 atau lebih baru
- iPad generasi ke-5 atau lebih baru
- Apple TV 4K atau lebih baru
- Apple Watch series 3 atau lebih baru
- iMac Pro (Retina 5K, 27 inci, 2017) atau lebih baru
- MacBook Pro (13 inci, 2018) atau lebih baru

- MacBook Pro (15 inci, 2018) atau lebih baru
- MacBook Air (Retina, 13 inci, 2018) atau lebih baru
- Mac mini (2018) atau lebih baru
- iMac (Retina 4K, 21,5 inci, 2019) atau lebih baru
- iMac (Retina 5K, 27 inci, 2019) atau lebih baru
- Mac Pro (2019) atau lebih baru

Koneksi Wi-Fi

Apple membuat alamat MAC acak untuk koneksi Wi-Fi rekan ke rekan yang digunakan untuk AirDrop dan AirPlay. Alamat acak juga digunakan untuk Hotspot Pribadi di iOS dan iPadOS (dengan kartu SIM) serta Berbagi Internet di macOS.

Alamat acak baru dibuat kapan pun antarmuka jaringan ini dimulai, dan alamat unik secara terpisah dibuat untuk setiap antarmuka sesuai keperluan.

Jaringan tersembunyi

Jaringan Wi-Fi dikenali menurut nama jaringannya, yang dikenal sebagai *pengenal set layanan (SSID)*. Beberapa jaringan Wi-Fi dikonfigurasi untuk menyembunyikan SSID-nya, yang menyebabkan titik akses nirkabel tidak menyiarkan nama jaringannya. Ini dikenal sebagai *jaringan tersembunyi*. iPhone 6s dan perangkat yang lebih baru secara otomatis mendeteksi jaringan tersembunyi. Jika jaringan disembunyikan, perangkat iOS atau iPadOS akan mengirimkan kuar dengan menyertakan SSID di permintaan—bukan sebaliknya. Ini membantu mencegah perangkat menyiarkan nama jaringan yang sebelumnya tersembunyi yang terhubung dengan pengguna, sehingga memastikan privasi lebih jauh.

Keamanan Bluetooth

Terdapat dua jenis Bluetooth di perangkat Apple, Bluetooth Klasik dan Bluetooth Rendah Energi (BLE). Model keamanan Bluetooth untuk kedua versi menyertakan fitur keamanan berbeda berikut:

- *Pemasangan:* Proses untuk membuat satu atau beberapa kunci rahasia bersama
- *Pengikatan:* Tindakan penyimpanan kunci yang dibuat selama pemasangan untuk digunakan dalam koneksi berikutnya untuk membangun pasangan perangkat tepercaya
- *Pengesahan:* Memverifikasi bahwa dua perangkat memiliki kunci yang sama
- *Enkripsi:* Kerahasiaan pesan
- *Integritas pesan:* Perlindungan terhadap pemalsuan pesan
- *Pemasangan Sederhana dan Aman:* Perlindungan terhadap pengintaian pasif dan perlindungan terhadap serangan perantara

Bluetooth versi 4.1 menambahkan fitur Koneksi Aman ke transpor fisik Bluetooth Klasik (BR/EDR).

Fitur keamanan untuk setiap jenis Bluetooth dicantumkan di bawah.

Dukungan	**Bluetooth Klasik**	**Bluetooth Rendah Energi**
Pemasangan	Kurva eliptis P-256	Algoritme yang disetujui FIPS (AES-CMAC dan kurva eliptis P-256)
Pengikatan	Informasi pemasangan yang disimpan dalam lokasi yang aman di perangkat iOS, iPadOS, macOS, tvOS, dan watchOS	Informasi pemasangan yang disimpan dalam lokasi yang aman di perangkat iOS, iPadOS, macOS, tvOS, dan watchOS
Pengesahan	Algoritme yang disetujui FIPS (HMAC-SHA256 dan AES-CTR)	Algoritme yang disetujui FIPS
Enkripsi	Kriptografi AES-CCM, yang dilakukan di Pengontrol	Kriptografi AES-CCM, yang dilakukan di Pengontrol
Integritas pesan	AES-CCM, yang digunakan untuk integritas pesan	AES-CCM, yang digunakan untuk integritas pesan
Pemasangan Sederhana dan Aman: Perlindungan terhadap pengintaian pasif	Pertukaran Diffie-Hellman Kurva Eliptis Sementara (ECDHE)	Pertukaran Diffie-Hellman Kurva Eliptis (ECDHE)
Pemasangan Sederhana dan Aman: Perlindungan terhadap serangan perantara (MITM)	Dua metode numerik yang dibantu pengguna: perbandingan numerik atau entri kunci sandi	Dua metode numerik yang dibantu pengguna: perbandingan numerik atau entri kunci sandi Pemasangan memerlukan respons pengguna, termasuk semua mode pemasangan bukan MITM
Bluetooth 4.1 atau lebih baru	iMac 2015 Akhir atau lebih baru MacBook Pro 2015 Awal atau lebih baru	iOS 9 atau lebih baru iPadOS 13.1 atau lebih baru macOS 10.12 atau lebih baru tvOS 9 atau lebih baru watchOS 2.0 atau lebih baru
Bluetooth 4.2 atau lebih baru	iPhone 6 atau lebih baru	iOS 9 atau lebih baru iPadOS 13.1 atau lebih baru macOS 10.12 atau lebih baru tvOS 9 atau lebih baru watchOS 2.0 atau lebih baru

Privasi Bluetooth Rendah Energi

Untuk membantu mengamankan privasi pengguna, BLE menyertakan dua fitur berikut: pengacakan alamat dan derivasi kunci lintas transpor.

Pengacakan alamat adalah fitur yang mengurangi kemampuan untuk melacak perangkat BLE selama beberapa waktu dengan mengubah alamat perangkat Bluetooth secara berkala. Agar perangkat yang menggunakan fitur privasi dapat terhubung ulang ke perangkat yang diketahui, alamat perangkat, yang dikenal sebagai *alamat pribadi*, harus dapat diselesaikan oleh perangkat lainnya. Alamat pribadi dibuat menggunakan kunci penyelesaian identitas perangkat yang ditukar selama prosedur pemasangan.

iOS 13 atau lebih baru dan iPadOS 13.1 atau lebih baru memiliki kemampuan untuk menurunkan kunci tautan melalui transpor, fitur yang dikenal sebagai *derivasi kunci lintas transpor*. Misalnya, kunci tautan yang dibuat dengan BLE dapat digunakan untuk menurunkan kunci tautan Bluetooth Klasik. Selain itu, Apple menambahkan Bluetooth Klasik ke dukungan BLE untuk perangkat yang mendukung fitur Koneksi yang Diamankan, yang diperkenalkan di Spesifikasi Inti Bluetooth 4.1 (lihat Spesifikasi Inti Bluetooth 5.1).

Keamanan Ultra Wideband di iOS

Keping U1 baru rancangan Apple menggunakan teknologi Ultra Wideband untuk kesadaran ruang—memungkinkan iPhone 11, iPhone 11 Pro, dan iPhone 11 Pro Max atau model iPhone yang lebih baru menemukan perangkat Apple lain yang dilengkapi dengan U1 secara tepat. Teknologi Ultra Wideband menggunakan teknologi yang sama untuk mengacak data yang ditemukan di perangkat Apple lainnya yang didukung:

- Pengacakan alamat MAC
- Pengacakan angka rangkaian bingkai Wi-Fi

Masuk tunggal

Keamanan masuk tunggal

Masuk tunggal

iOS dan iPadOS mendukung pengesahan ke jaringan perusahaan melalui Masuk tunggal (SSO). SSO dapat digunakan dengan jaringan berbasis Kerberos untuk mengesahkan pengguna atas layanan yang berhak mereka akses. SSO dapat digunakan untuk berbagai aktivitas jaringan, dari sesi Safari aman hingga app pihak ketiga. Pengesahan berbasis sertifikat seperti PKINIT juga didukung.

macOS mendukung pengesahan ke jaringan perusahaan menggunakan Kerberos. App dapat menggunakan Kerberos untuk mengesahkan pengguna ke layanan yang disahkan untuk diakses. Kerberos juga dapat digunakan untuk berbagai aktivitas jaringan, dari sesi Safari aman dan pengesahan sistem file jaringan hingga app pihak ketiga. Pengesahan berbasis sertifikat didukung, meskipun memerlukan adopsi app dari API pengembang.

SSO iOS, iPadOS, serta macOS menggunakan token SPNEGO dan protokol Negosiasi HTTP untuk bekerja dengan gateway pengesahan berbasis Kerberos dan sistem Pengesahan Terpadu Windows yang mendukung tiket Kerberos. Dukungan SSO didasarkan pada proyek Heimdal sumber terbuka.

Jenis enkripsi berikut didukung di iOS, iPadOS, dan macOS:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari mendukung SSO, dan app pihak ketiga yang menggunakan API jaringan iOS serta iPadOS standar yang juga dapat dikonfigurasi untuk menggunakannya. Untuk mengonfigurasi SSO, iOS dan iPadOS mendukung muatan profil konfigurasi yang memungkinkan solusi mobile device management (MDM) untuk menonaktifkan pengaturan yang diperlukan. Ini meliputi pengaturan nama pokok pengguna (yaitu, akun pengguna Active Directory) dan pengaturan realm Kerberos, serta konfigurasi mengenai app dan URL web Safari mana yang harus diizinkan untuk menggunakan SSO.

Untuk mengonfigurasi Kerberos di macOS, dapatkan tiket dengan Penampil Tiket, masuk ke domain Active Directory Windows, atau gunakan alat baris perintah `kinit`.

Masuk tunggal yang dapat diperluas

Pengembang app dapat menyediakan penerapan masuk tunggalnya sendiri menggunakan ekstensi SSO. Ekstensi SSO diaktifkan saat app asli atau web perlu menggunakan beberapa penyedia identitas untuk pengesahan pengguna. Pengembang dapat menyediakan dua jenis ekstensi: jenis yang mengalihkan ke HTTPS dan jenis yang menggunakan mekanisme tantangan/respons seperti Kerberos. Hal ini memungkinkan skema pengesahan OpenID, OAuth, SAML2, dan Kerberos didukung oleh Masuk tunggal Yang Dapat Diperluas.

Untuk menggunakan ekstensi Masuk tunggal, app dapat menggunakan API AuthenticationServices atau dapat mengandalkan mekanisme intersepsi URL yang ditawarkan oleh sistem operasi. WebKit dan CFNetwork menyediakan lapisan intersepsi yang memungkinkan dukungan tanpa hambatan dari Masuk tunggal untuk app asli atau WebKit. Agar ekstensi Masuk tunggal diaktifkan, konfigurasi yang disediakan oleh administrator harus diinstal melalui profil mobile device management (MDM). Selain itu, ekstensi jenis pengalih harus menggunakan muatan Domain Terkait untuk membuktikan bahwa server identitas yang didukung mengetahui keberadaannya.

Satu-satunya ekstensi yang disediakan dengan sistem operasi adalah ekstensi SSO Kerberos.

Keamanan AirDrop

Perangkat Apple yang mendukung AirDrop menggunakan teknologi Bluetooth Rendah Energi (BLE) dan teknologi Wi-Fi rekan ke rekan yang dibuat Apple untuk mengirimkan file serta informasi ke perangkat di sekitar, termasuk perangkat iOS dan perangkat iPad berkemampuan AirDrop yang menjalankan iOS 7 atau lebih baru dan komputer Mac yang menjalankan OS X 10.11 atau lebih baru. Radio Wi-Fi digunakan untuk berkomunikasi langsung antarperangkat tanpa menggunakan koneksi internet atau titik akses (AP) nirkabel. Koneksi ini dienkripsi dengan TLS.

AirDrop diatur agar berbagi dengan Hanya Kontak secara default. Pengguna juga dapat memilih untuk menggunakan AirDrop untuk berbagi dengan semua orang atau sepenuhnya mematikan fitur ini. Organisasi dapat membatasi penggunaan AirDrop untuk perangkat atau app yang sedang dikelola oleh solusi mobile device management (MDM).

Operasi AirDrop

AirDrop menggunakan layanan iCloud untuk membantu pengesahan pengguna. Saat pengguna masuk ke iCloud, identitas RSA 2048 bit disimpan di perangkat, dan saat pengguna menyalakan AirDrop, hash identitas pendek AirDrop dibuat berdasarkan alamat email dan nomor telepon yang dikaitkan dengan ID Apple pengguna.

Saat pengguna memilih AirDrop sebagai metode untuk berbagi item, perangkat pengirim akan memancarkan sinyal AirDrop melalui BLE yang menyertakan hash identitas pendek AirDrop milik pengguna. Perangkat Apple lainnya yang bangun, dalam jarak dekat, dan menyalakan AirDrop mendeteksi sinyal tersebut dan merespons menggunakan Wi-Fi rekan ke rekan, sehingga perangkat pengirim dapat menemukan identitas perangkat yang merespons.

Dalam mode Hanya Kontak, hash identitas pendek AirDrop yang diterima dibandingkan dengan hash orang di app Kontak perangkat penerima. Jika terdapat kecocokan, perangkat penerima merespons melalui Wi-Fi rekan ke rekan dengan informasi identitasnya. Jika tidak ada kecocokan, perangkat tidak akan merespons.

Dalam mode Semua Orang, seluruh proses yang sama digunakan. Namun, perangkat yang menerima merespons bahkan jika tidak ada kecocokan di app Kontak perangkat.

Perangkat pengirim kemudian memulai koneksi AirDrop menggunakan Wi-Fi rekan ke rekan, dengan koneksi ini untuk mengirimkan hash identitas panjang ke perangkat penerima. Jika hash identitas panjang cocok dengan hash orang yang dikenal di Kontak penerima, penerima akan merespons dengan hash identitas panjangnya.

Jika hash terverifikasi, nama depan dan foto penerima (jika ada di Kontak) akan ditampilkan di lembar berbagi AirDrop pengirim. Di iOS dan iPadOS, hash ditampilkan di bagian “Orang” atau “Perangkat”. Perangkat yang tidak terverifikasi atau disahkan ditampilkan di lembar berbagi AirDrop pengirim dengan ikon siluet dan nama perangkat, seperti yang didefinisikan di Pengaturan > Umum > Mengenai > Nama. Di iOS dan iPadOS, hash ditempatkan di bagian “Orang Lain” pada lembar berbagi AirDrop.

Pengguna pengirim lalu dapat memilih orang yang ingin diajak berbagi. Setelah pengguna memilih, perangkat penerima memulai koneksi terenkripsi (TLS) dengan perangkat pengirim, yang akan menukar sertifikat identitas iCloud kedua perangkat. Identitas di sertifikat diverifikasi berdasarkan app Kontak masing-masing pengguna.

Jika sertifikat diverifikasi, pengguna penerima diminta untuk menerima transfer masuk dari pengguna atau perangkat yang telah diidentifikasi. Jika beberapa penerima telah dipilih, proses ini akan diulangi untuk setiap tujuan.

Keamanan berbagi kata sandi Wi-Fi di iPhone dan iPad

Perangkat iOS dan iPadOS yang mendukung berbagi kata sandi Wi-Fi menggunakan mekanisme yang mirip dengan AirDrop untuk mengirimkan kata sandi Wi-Fi dari satu perangkat ke perangkat lain.

Saat pengguna memilih jaringan Wi-Fi (peminta) dan dimintai kata sandi Wi-Fi, perangkat Apple akan memulai pengiklanan Bluetooth Rendah Energi (BLE) yang menunjukkan bahwa perangkat menginginkan kata sandi Wi-Fi. Perangkat Apple lainnya yang bangun, dalam jarak dekat, dan memiliki kata sandi jaringan Wi-Fi yang dipilih akan terhubung menggunakan BLE ke perangkat yang meminta.

Perangkat yang memiliki kata sandi Wi-Fi (pemberi) memerlukan Informasi Kontak peminta, dan peminta harus membuktikan identitasnya menggunakan mekanisme yang mirip dengan AirDrop. Setelah identitas dibuktikan, pemberi akan mengirimi peminta kode sandi yang dapat digunakan untuk bergabung dengan jaringan.

Organisasi dapat membatasi penggunaan berbagi kata sandi Wi-Fi untuk perangkat atau app yang sedang dikelola melalui solusi mobile device management (MDM).

Keamanan firewall di macOS

macOS menyertakan firewall internal untuk melindungi Mac dari serangan akses jaringan dan penolakan layanan. Firewall dapat dikonfigurasi di panel Keamanan & Privasi pada Preferensi Sistem dan mendukung konfigurasi berikut:

- Memblokir semua koneksi masuk, apa pun app-nya.
- Secara otomatis mengizinkan perangkat lunak internal menerima koneksi masuk.
- Secara otomatis mengizinkan perangkat lunak yang diunduh dan ditandatangani menerima koneksi masuk.
- Menambahkan atau menolak akses berdasarkan app yang ditetapkan oleh pengguna.
- Mencegah Mac merespons permintaan penyelidikan dan pemindaian port ICMP (Protokol Pesan Kontrol Internet).

Keamanan kit pengembang

Tinjauan keamanan kit pengembang

Apple menyediakan sejumlah kerangka “kit” agar pengembang pihak ketiga dapat memperluas layanan Apple. Kerangka ini dibangun dengan mengutamakan privasi dan keamanan pengguna:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

Keamanan HomeKit

Keamanan komunikasi HomeKit

HomeKit menyediakan infrastruktur automasi rumah yang menggunakan keamanan iCloud dan iOS, iPadOS, dan macOS untuk melindungi dan menyelaraskan data pribadi tanpa memaparkannya ke Apple.

Identitas dan keamanan HomeKit didasarkan pada pasangan kunci pribadi-publik Ed25519. Pasangan kunci Ed25519 dibuat di perangkat iOS, iPadOS, dan macOS bagi tiap pengguna untuk HomeKit, yang kemudian menjadi identitas HomeKit-nya. Pasangan kunci ini digunakan untuk mengesahkan komunikasi antarperangkat iOS, iPadOS, dan macOS, serta antara perangkat iOS, iPadOS, dan macOS serta aksesori.

Kunci—yang disimpan di rantai kunci dan disertakan hanya di cadangan Rantai Kunci yang dienkripsi—terus diperbarui antarperangkat menggunakan Rantai Kunci iCloud, jika tersedia. HomePod dan Apple TV menerima kunci melalui ketuk-atur atau mode pengaturan yang dijelaskan di bawah. Kunci dibagikan dari iPhone ke Apple Watch yang dipasangkan menggunakan Layanan Identitas (IDS) Apple.

Komunikasi antara aksesori HomeKit

Aksesori HomeKit membuat pasangan kunci Ed25519-nya sendiri untuk digunakan saat berkomunikasi dengan perangkat iOS, iPadOS, dan macOS. Jika aksesori dipulihkan ke pengaturan pabrik, pasangan kunci baru akan dibuat.

Untuk membangun hubungan antara perangkat iOS, iPadOS, dan macOS dan aksesori HomeKit, kunci ditukar menggunakan protokol Kata Sandi Jarak Jauh Aman (3072 bit), menggunakan kode delapan digit yang disediakan oleh produsen aksesori, dimasukkan di perangkat iOS dan iPadOS oleh pengguna, lalu dienkripsi menggunakan ChaCha20-Poly1305 AEAD dengan kunci turunan dari HKDF-SHA512. Sertifikasi MFi aksesori juga diverifikasi selama pengaturan. Aksesori tanpa keping MFi dapat membangun dukungan untuk pengesahan perangkat lunak di iOS 11.3 atau lebih baru.

Saat berkomunikasi selama penggunaan, perangkat iOS, iPadOS, macOS, dan aksesori HomeKit saling mengesahkan penggunaan kunci yang ditukar pada proses di atas. Setiap sesi dibuat menggunakan protokol Stasiun ke Stasiun dan dienkripsi dengan kunci turunan dari HKDF-SHA512 berdasarkan kunci Curve25519 per sesi. Ini berlaku bagi aksesori berbasis IP dan aksesori Bluetooth Rendah Energi (BLE).

Untuk perangkat BLE yang mendukung pemberitahuan siaran, aksesorinya akan dilengkapi dengan kunci enkripsi siaran melalui sesi aman oleh perangkat iOS, iPadOS, dan macOS yang dipasangkan. Kunci ini digunakan untuk mengenkripsi data mengenai perubahan status aksesori, yang diberi tahu menggunakan pengiklanan BLE. Kunci enkripsi siaran merupakan kunci turunan HKDF-SHA512, dan datanya dienkripsi menggunakan algoritme AEAD ChaCha20-Poly1305. Kunci enkripsi siaran diubah secara berkala oleh perangkat iOS, iPadOS, dan macOS dan diperbarui ke perangkat lainnya yang menggunakan iCloud sebagaimana dijelaskan di Keamanan data HomeKit.

HomeKit dan Siri

Siri dapat digunakan untuk meminta dan mengontrol aksesori, dan untuk mengaktifkan tampilan. Informasi minimal mengenai konfigurasi rumah diberikan secara anonim ke Siri, untuk menyediakan nama ruangan, aksesori, dan skenario yang penting bagi pengenalan perintah. Audio yang dikirimkan oleh Siri dapat menyebutkan aksesori atau perintah tertentu, tapi data Siri tersebut tidak dikaitkan dengan fitur Apple lainnya seperti HomeKit.

Aksesori HomeKit berkemampuan Siri

Pengguna dapat mengaktifkan fitur baru seperti Siri, dan fitur HomePod lainnya seperti timer, alarm, interkom, dan bel pintu, di aksesori berkemampuan Siri menggunakan app Rumah. Saat fitur ini diaktifkan, aksesori berkoordinasi dengan HomePod yang dipasangkan di jaringan lokal yang menjadi host fitur Apple ini. Audio bertukar antarperangkat melalui saluran yang dienkripsi menggunakan protokol HomeKit dan AirPlay.

Saat Dengarkan Hey Siri dinyalakan, aksesori mendengarkan frasa “Hey Siri” menggunakan mesin deteksi yang dipicu frasa yang dijalankan di perangkat. Jika frasa terdeteksi, mesin ini mengirimkan bingkai audio secara langsung ke HomePod yang dipasangkan menggunakan HomeKit. HomePod melakukan pemeriksaan audio kedua dan dapat membatalkan sesi audio jika frasa tidak tampak berisi frasa pemicu.

Saat Sentuh untuk Siri dinyalakan, pengguna dapat menekan tombol terdedikasi di aksesori untuk memulai percakapan dengan Siri. Bingkai audio dikirim secara langsung ke HomePod yang dipasangkan.

Setelah pengaktifan Siri yang berhasil terdeteksi, HomePod mengirimkan audio ke server Siri dan memenuhi tujuan pengguna menggunakan keamanan, privasi, dan perlindungan enkripsi yang HomePod terapkan ke pengaktifan pengguna yang dilakukan oleh HomePod. Jika Siri memiliki balasan audio, respons Siri dikirim melalui saluran audio AirPlay ke aksesori. Beberapa permintaan Siri memerlukan informasi tambahan dari pengguna (misalnya, bertanya apakah pengguna ingin mendengarkan pilihan lainnya). Dalam kasus tersebut, aksesori menerima indikasi bahwa pengguna harus diminta, dan audio tambahan di-stream ke HomePod.

Aksesori diperlukan untuk memiliki indikator visual untuk memberi tahu pengguna saat mendengarkan secara aktif (misalnya, indikator LED). Aksesori tidak mengetahui tujuan permintaan Siri, kecuali untuk akses ke stream audio, dan tidak ada data pengguna yang disimpan di aksesori.

Keamanan data HomeKit

Data HomeKit dapat keamanan diperbarui dengan aman antarperangkat iOS, iPadOS, macOS pengguna menggunakan iCloud dan rantai kunci iCloud. Selama proses ini, data HomeKit dienkripsi menggunakan kunci turunan dari identitas HomeKit pengguna dan nonce acak serta ditangani sebagai objek besar biner buram, atau *blob*. Blob terbaru disimpan di iCloud, tapi tidak digunakan untuk tujuan lainnya. Karena blob dienkripsi menggunakan kunci yang hanya tersedia di perangkat iOS, iPadOS, macOS pengguna, kontennya tidak dapat diakses selama transmisi dan penyimpanan iCloud.

Data HomeKit juga diselaraskan antara beberapa pengguna rumah yang sama. Proses ini menggunakan pengesahan dan enkripsi yang sama dengan yang digunakan antara perangkat iOS, iPadOS, macOS, dan aksesori HomeKit. Pengesahan didasarkan pada kunci publik Ed25519 yang ditukar antara perangkat saat pengguna ditambahkan ke rumah. Setelah pengguna baru ditambahkan ke rumah, semua komunikasi lebih lanjut disahkan dan dienkripsi menggunakan protokol Stasiun ke Stasiun dan kunci per sesi.

Pengguna yang membuat rumah di HomeKit atau pengguna lain dengan izin pengeditan dapat menambahkan pengguna baru. Perangkat pemilik mengonfigurasi aksesori dengan kunci publik pengguna baru sehingga aksesori tersebut dapat mengesahkan dan menerima perintah dari pengguna baru. Saat pengguna dengan izin pengeditan menambahkan anggota baru, proses tersebut didelegasikan ke hub rumah untuk menyelesaikan operasi.

HomeKit dan Apple TV

Proses penyediaan Apple TV untuk digunakan dengan HomeKit dijalankan secara otomatis saat pengguna masuk ke iCloud. Autentikasi dua faktor di akun iCloud harus diaktifkan. Apple TV dan perangkat pemilik bertukar kunci publik Ed25519 sementara melalui iCloud. Saat perangkat dan Apple TV pemilik terhubung ke jaringan lokal yang sama, kunci sementara tersebut digunakan untuk mengamankan koneksi melalui jaringan lokal menggunakan protokol Stasiun ke Stasiun dan kunci per sesi. Proses ini menggunakan pengesahan dan enkripsi yang sama dengan yang digunakan antara perangkat iOS, iPadOS, macOS, dan aksesori HomeKit. Melalui koneksi lokal aman ini, perangkat pemilik mentransfer pasangan kunci publik-pribadi Ed25519 milik pengguna ke Apple TV. Kunci ini kemudian digunakan untuk mengamankan komunikasi antara Apple TV dan aksesori HomeKit dan juga antara Apple TV dan perangkat iOS, iPadOS, dan macOS lainnya yang merupakan bagian dari rumah HomeKit.

Jika pengguna tidak memiliki beberapa perangkat dan tidak memberi pengguna tambahan akses ke rumahnya, tidak ada data HomeKit yang akan ditransmisikan ke iCloud.

Data dan app Rumah

Akses app ke data rumah dikontrol oleh pengaturan Privasi pengguna. Pengguna diminta untuk memberikan akses saat app meminta data rumah, sama dengan Kontak, Foto, dan sumber data iOS, iPadOS, dan macOS lainnya. Jika pengguna menyetujui, app akan memiliki akses ke nama ruangan, nama aksesori, ruangan tempat aksesori berada, dan informasi lainnya sebagaimana yang dirinci di dokumentasi pengembang HomeKit di https://developer.apple.com/homekit/.

Penyimpanan data lokal

HomeKit menyimpan data mengenai rumah, aksesori, skenario, dan pengguna di perangkat iOS, iPadOS, dan macOS pengguna. Data yang disimpan ini dienkripsi menggunakan kunci turunan dari kunci identitas HomeKit pengguna, ditambah nonce acak. Selain itu, data HomeKit disimpan menggunakan kelas Perlindungan Data Dilindungi Hingga Pengesahan Pengguna Pertama. Data HomeKit hanya dicadangkan di cadangan yang dienkripsi, sehingga, misalnya, cadangan yang tidak dienkripsi ke Finder (macOS 10.15 atau lebih baru) atau iTunes (di macOS 10.14 atau lebih lama) melalui USB tidak berisi data HomeKit.

Mengamankan ruter dengan HomeKit

Ruter yang mendukung HomeKit memungkinkan pengguna meningkatkan keamanan jaringan rumahnya dengan mengelola akses Wi-Fi yang dimiliki aksesori HomeKit ke jaringan lokalnya dan ke internet. Ruter juga mendukung pengesahan PSK Pribadi (PPSK), sehingga aksesori dapat ditambahkan ke jaringan Wi-Fi menggunakan kunci yang khusus untuk aksesori dan dapat dicabut saat dibutuhkan. Pengesahan PPSK meningkatkan keamanan dengan tidak memperlihatkan kata sandi Wi-Fi utama ke aksesori, serta memungkinkan ruter mengidentifikasi aksesori secara aman bahkan jika alamat MAC-nya diubah.

Dengan menggunakan app Rumah, pengguna dapat mengonfigurasi pembatasan akses untuk grup aksesori sebagai berikut:

- *Tidak ada batasan:* Izinkan akses tanpa batas ke internet dan jaringan lokal.
- *Otomatis:* Ini adalah pengaturan default. Izinkan akses ke internet dan jaringan lokal berdasarkan daftar situs internet dan port lokal yang disediakan ke Apple oleh pabrik aksesori. Daftar ini menyertakan semua situs dan port yang dibutuhkan oleh aksesori agar dapat berfungsi dengan benar. (Tidak Ada Batasan digunakan hingga daftar tersedia.)
- *Batasi ke Rumah:* Tidak ada akses ke internet atau jaringan lokal kecuali untuk koneksi yang diperlukan oleh HomeKit untuk menemukan dan mengontrol aksesori dari jaringan lokal (termasuk dari hub rumah untuk mendukung kontrol jarak jauh).

PPSK adalah frasa sandi WPA2 Pribadi yang kuat dan khusus aksesori yang dibuat oleh HomeKit secara otomatis dan dicabut jika dan saat aksesori nantinya dihapus dari Rumah. PPSK digunakan saat aksesori ditambahkan ke jaringan Wi-Fi oleh HomeKit di Rumah yang telah dikonfigurasikan dengan ruter HomeKit; tambahan ini dicerminkan sebagai Info Pengesahan Wi-Fi: Yang dikelola oleh HomeKit di layar pengaturan untuk aksesori di app Rumah. Aksesori yang ditambahkan ke jaringan Wi-Fi sebelum menambahkan ruter dikonfigurasi ulang untuk menggunakan PPSK jika aksesori mendukungnya, jika tidak, info pengesahan yang ada akan dipertahankan.

Sebagai tindakan keamanan tambahan, pengguna harus mengonfigurasi ruter HomeKit menggunakan app produsen ruter, sehingga app dapat mengesahkan bahwa pengguna memiliki akses ke ruter dan dapat menambahkannya ke app Rumah.

Keamanan kamera HomeKit

Kamera yang memiliki alamat Protokol Internet (alamat IP) di HomeKit mengirimkan stream audio dan video secara langsung ke perangkat iOS, iPadOS, tvOS, serta macOS menggunakan jaringan lokal yang mengakses streaming tersebut. Streaming dienkripsi menggunakan kunci yang dibuat secara acak pada perangkat dan kamera Protokol Internet (atau kamera IP), dan ditukar melalui sesi HomeKit aman ke kamera. Jika perangkat tidak terhubung ke jaringan lokal, stream yang dienkripsi direlai melalui hub rumah ke perangkat. Hub rumah tidak mendekripsi stream; hub hanya berfungsi sebagai relai antara perangkat dan kamera IP. Saat app menampilkan tampilan video kamera IP HomeKit ke pengguna, HomeKit mengolah bingkai video dengan aman dari proses sistem terpisah. Hasilnya, app tidak dapat mengakses atau menyimpan streaming video. Selain itu, app tidak diizinkan untuk mengambil jepretan layar dari stream ini.

Video aman HomeKit

HomeKit menyediakan mekanisme aman ujung ke ujung dan pribadi untuk merekam, menganalisis, dan melihat klip dari kamera IP HomeKit tanpa memperlihatkan konten video tersebut ke Apple atau pihak ketiga mana pun. Saat gerakan terdeteksi oleh kamera IP, klip video akan dikirimkan secara langsung ke perangkat Apple yang bertindak sebagai hub rumah, menggunakan koneksi jaringan lokal terdedikasi antara hub rumah dan kamera IP tersebut. Koneksi jaringan lokal dienkripsi dengan pasangan kunci turunan HKDF-SHA512 per sesi yang dinegosiasikan melalui sesi HomeKit antara hub rumah dan kamera IP. HomeKit mendekripsi streaming audio dan video di hub rumah dan menganalisis bingkai video secara lokal untuk kejadian signifikan apa pun. Jika kejadian signifikan terdeteksi, HomeKit akan mengenkripsi klip video menggunakan AES-256-GCM dengan kunci AES256 yang dibuat secara acak. HomeKit juga membuat bingkai poster untuk setiap klip dan bingkai poster ini dienkripsi menggunakan kunci AES256 yang sama. Bingkai poster yang dienkripsi dan data audio serta video diunggah ke server iCloud. Metadata terkait untuk setiap klip termasuk kunci enkripsi diunggah ke CloudKit menggunakan enkripsi ujung ke ujung iCloud.

Untuk klasifikasi wajah, HomeKit menyimpan semua data yang digunakan untuk mengklasifikasikan wajah orang tertentu di CloudKit menggunakan enkripsi ujung ke ujung iCloud. Data yang disimpan menyertakan informasi mengenai setiap orang, seperti nama, serta gambar yang mewakili wajah orang tersebut. Gambar wajah ini dapat bersumber dari Foto pengguna jika mereka mengaktifkannya, atau gambar dapat dikumpulkan dari video kamera IP yang dianalisis sebelumnya. Sesi analisis Video Aman HomeKit menggunakan data klasifikasi ini untuk mengidentifikasi wajah di streaming video aman yang diterima secara langsung dari kamera IP dan menyertakan informasi identifikasi tersebut di metadata klip yang disebutkan sebelumnya.

Saat app Rumah digunakan untuk melihat klip untuk kamera, data diunduh dari iCloud dan kunci untuk mendekripsi streaming dibuka secara lokal menggunakan enkripsi ujung ke ujung iCloud. Konten video yang dienkripsi distreaming dari server dan dienkripsi secara lokal di perangkat iOS sebelum menampilkannya di penampil. Setiap sesi klip video dapat dipecah ke dalam beberapa subbagian dengan setiap subbagian mengenkripsi streaming konten dengan kunci uniknya sendiri.

Keamanan HomeKit dengan Apple TV

HomeKit secara aman menghubungkan beberapa aksesori remote pihak ketiga ke Apple TV dan mendukung penambahan profil pengguna ke pemilik Apple TV rumah.

Menggunakan aksesori remote pihak ketiga dengan Apple TV

Beberapa aksesori remote pihak ketiga menyediakan peristiwa Rancangan Antarmuka Manusia (HID) dan audio Siri ke Apple TV terkait yang ditambahkan menggunakan app Rumah. Remote mengirimkan kejadian HID melalui sesi aman ke Apple TV. Remote TV yang mendukung Siri mengirimkan data audio ke Apple TV saat pengguna mengaktifkan mikrofon secara jelas pada remote menggunakan tombol khusus Siri. Remote mengirimkan bingkai audio secara langsung ke Apple TV menggunakan koneksi jaringan lokal khusus. Pasangan kunci turunan HKDF-SHA512 per sesi yang dinegosiasikan melalui sesi HomeKit antara Apple TV dan remote TV digunakan untuk mengenkripsi koneksi jaringan lokal. HomeKit mendekripsi bingkai audio di Apple TV dan meneruskannya ke app Siri, tempat bingkai audio akan diperlakukan dengan perlindungan privasi yang sama dengan semua input audio Siri.

Profil Apple TV untuk rumah HomeKit

Jika pengguna rumah HomeKit menambahkan profilnya ke Apple TV pemilik rumah, mereka akan dapat mengakses acara TV, musik, dan podcast pemilik. Pengaturan untuk setiap pengguna terkait penggunaan profil mereka di Apple TV dibagikan ke akun iCloud pemilik menggunakan enkripsi ujung ke ujung iCloud. Data dimiliki oleh setiap pengguna dan dibagikan dengan status hanya baca ke pemilik. Setiap pengguna rumah dapat mengubah nilai ini di app Rumah dan Apple TV pemilik menggunakan pengaturan ini.

Jika pengaturan dinyalakan, akun iTunes dari pengguna tersebut akan tersedia di Apple TV. Jika pengaturan dimatikan, semua akun dan data terkait pengguna tersebut akan dihapus di Apple TV. Berbagi CloudKit awal dimulai oleh perangkat pengguna dan token untuk berbagi CloudKit yang aman dikirimkan melalui saluran aman yang sama dengan yang digunakan untuk menyelaraskan data antarpengguna rumah.

Keamanan SiriKit untuk iOS, iPadOS, dan watchOS

Siri menggunakan sistem ekstensi app untuk berkomunikasi dengan app pihak ketiga. Di perangkat, Siri dapat mengakses informasi kontak pengguna dan lokasi perangkat saat ini. Namun, sebelum menyediakan data yang dilindungi ke app, Siri akan memeriksa izin akses yang dikontrol pengguna dari aplikasi tersebut. Menurut izin tersebut, Siri hanya meneruskan potongan yang relevan dari ucapan asli pengguna ke ekstensi app. Misalnya, jika app tidak memiliki akses ke informasi kontak, Siri tidak akan memproses hubungan dalam permintaan pengguna seperti "Pay my mother 10 dollars using Payment App". Dalam kasus ini, app hanya akan melihat istilah literal "my mother".

Namun, jika pengguna telah memberi app tersebut akses ke informasi kontak, app tersebut akan menerima informasi yang diproses mengenai ibu pengguna. Jika pengguna dirujuk di bagian isi pesan—misalnya, "Tell my mother on MessageApp that my brother is awesome"—Siri tidak akan memproses "my brother" terlepas dari izin app.

App yang mengaktifkan SiriKit dapat mengirimkan kosakata khusus pengguna atau khusus app ke Siri, seperti nama kontak pengguna. Informasi ini memungkinkan pengenalan ucapan dan pemahaman bahasa alami Siri untuk mengenali kosakata untuk app tersebut dan dikaitkan dengan pengenal acak. Informasi khusus tetap tersedia selama pengenal tersebut digunakan, atau hingga pengguna menonaktifkan integrasi Siri dengan app tersebut di Pengaturan, atau hingga app yang mengaktifkan SiriKit dicopot.

Untuk ucapan seperti "Get me a ride to my mom's home using RideShareApp," permintaan tersebut memerlukan data lokasi dari kontak pengguna. Hanya untuk permintaan tersebut, Siri menyediakan informasi yang diperlukan ke ekstensi app, terlepas pengaturan izin pengguna untuk informasi lokasi atau kontak untuk app tersebut.

Keamanan DriverKit untuk macOS

DriverKit adalah kerangka yang memungkinkan pengembang untuk membuat driver perangkat yang diinstal pengguna di Mac mereka. Driver yang dibangun dengan DriverKit dijalankan di ruang pengguna, alih-alih ekstensi kernel, untuk keamanan dan stabilitas sistem yang lebih baik. Ini memudahkan penginstalan dan meningkatkan stabilitas dan keamanan macOS.

Pengguna cukup mengunduh app (penginstal tidak diperlukan saat menggunakan ekstensi sistem atau DriverKit) dan ekstensi hanya diaktifkan saat diperlukan. Ini menggantikan kext untuk banyak kasus penggunaan, yang memerlukan hak administrator untuk menginstal di /Sistem/Perpustakaan atau /Perpustakaan.

Administrator TI yang menggunakan driver perangkat, solusi penyimpanan awan, jaringan, dan app keamanan yang memerlukan ekstensi kernel didorong untuk pindah ke versi lebih baru yang dibangun berdasarkan ekstensi sistem. Versi lebih baru ini secara drastis mengurangi kemungkinan panik kernel di Mac serta mengurangi permukaan serangan. Ekstensi baru ini dijalankan di ruang pengguna, tidak akan memerlukan hak khusus yang diperlukan untuk penginstalan, dan dihapus secara otomatis saat app bundel dipindahkan ke Tong Sampah.

Kerangka DriverKit menyediakan kelas C++ untuk layanan I/O, pencocokan perangkat, deskriptor memori, dan antrean penyebaran. Kerangka ini juga mendefinisikan jenis I/O yang sesuai untuk angka, koleksi, string, dan jenis umum lainnya. Pengguna menggunakan ini dengan kerangka driver khusus kumpulan seperti USBDriverKit dan HIDDriverKit. Gunakan kerangka Ekstensi Sistem untuk menginstal dan meningkatkan driver.

Keamanan ReplayKit di iOS dan iPadOS

ReplayKit adalah kerangka yang memungkinkan pengembang untuk menambahkan fitur perekaman dan siaran langsung ke app mereka. Selain itu, ReplayKit juga memungkinkan pengguna untuk menganotasi rekaman dan siaran mereka menggunakan kamera depan dan mikrofon perangkat.

Perekaman film

Ada beberapa lapisan keamanan yang terdapat di perekaman film:

- *Dialog izin:* Sebelum perekaman dimulai, ReplayKit memberi pengguna peringatan persetujuan yang meminta pengguna untuk menyatakan niat mereka untuk merekam layar, mikrofon, dan kamera depan. Peringatan ini diberikan sekali per proses app, dan akan diberikan lagi jika app berada di latar belakang selama lebih dari 8 menit.
- *Pengambilan layar dan audio:* Pengambilan layar dan audio berlangsung di luar proses app di replayd daemon ReplayKit. Ini dirancang untuk memastikan bahwa konten yang direkam tidak dapat diakses oleh proses app.
- *Pengambilan layar dan audio in-app:* Ini memungkinkan app untuk mendapatkan buffer video dan sampel, yang dijaga oleh dialog izin.
- *Pembuatan dan penyimpanan film:* File film dituliskan ke direktori yang hanya dapat diakses oleh subsistem ReplayKit dan tidak dapat diakses oleh app mana pun. Ini membantu mencegah rekaman agar tidak digunakan oleh pihak ketiga tanpa persetujuan pengguna.
- *Pratinjau dan berbagi oleh pengguna akhir:* Pengguna memiliki akses untuk mempratinjau dan membagikan film dengan antarmuka pengguna dari ReplayKit. Antarmuka pengguna diberikan di luar proses melalui infrastruktur Ekstensi iOS dan memiliki akses ke file film yang dibuat.

Penyiaran ReplayKit

Ada beberapa lapisan keamanan yang terdapat di penyiaran film:

- *Pengambilan layar dan audio:* Mekanisme pengambilan layar dan audio selama siaran sama seperti perekaman film dan berlangsung di `replayd`.
- *Ekstensi siaran:* Layanan pihak ketiga harus membuat dua ekstensi baru yang dikonfigurasi dengan titik akhir com.apple.broadcast-services agar dapat berpartisipasi dalam siaran ReplayKit:
  - Ekstensi antarmuka pengguna yang memungkinkan pengguna untuk mengatur siaran mereka
  - Ekstensi pengunggahan yang menangani pengunggahan data video dan audio ke server ujung belakang layanan

Arsitektur membantu memastikan app host tidak memiliki hak ke konten video dan audio yang disiarkan. Hanya ReplayKit dan ekstensi penyiaran pihak ketiga yang memiliki akses.

- *Pemilih siaran:* Dengan pemilih siaran, pengguna memulai siaran sistem secara langsung dari app mereka yang menggunakan antarmuka pengguna tetapan sistem yang sama, yang dapat diakses menggunakan Pusat Kontrol. Antarmuka pengguna diterapkan menggunakan API pribadi dan merupakan ekstensi yang berada di dalam kerangka ReplayKit. Pemilih siaran berada di luar proses app host.
- *Ekstensi pengunggahan:* Ekstensi yang diterapkan layanan siaran pihak ketiga untuk menangani konten video dan audio selama siaran menggunakan buffer sampel mentah yang tidak dikodekan. Selama mode penanganan ini, data video dan audio disusun secara serial dan diteruskan ke ekstensi pengunggahan pihak ketiga secara real time melalui koneksi XPC langsung. Data video dikodekan dengan mengekstrak objek IOSurface dari buffer sampel video, mengodekannya secara aman sebagai objek XPC, mengirimkannya melalui XPC ke ekstensi pihak ketiga, dan mendekodekannya kembali secara aman ke objek IOSurface.

Keamanan ARKit di iOS dan iPadOS

ARKit adalah kerangka yang memungkinkan pengembang membuat pengalaman realitas di app atau game mereka. Pengembang dapat menambahkan elemen 2D atau 3D menggunakan kamera depan atau belakang perangkat iOS atau iPadOS.

Apple merancang kamera dengan mengutamakan privasi, dan app pihak ketiga harus mendapatkan persetujuan pengguna sebelum mengakses kamera. Di iOS dan iPadOS, saat pengguna memberi app akses ke kamera mereka, app tersebut dapat mengakses gambar real time dari kamera depan dan belakang. App tidak diizinkan untuk menggunakan kamera tanpa transparansi bahwa kamera sedang digunakan.

Foto dan video yang diambil dengan kamera dapat berisi informasi lainnya, seperti tempat dan waktu pengambilan, kedalaman bidang, dan pengambilan di luar bingkai. Jika pengguna tidak ingin foto dan video yang diambil dengan app Kamera untuk menyertakan lokasi, mereka dapat mengontrol ini kapan pun dengan membuka Pengaturan > Privasi > Layanan Lokasi > Kamera. Jika pengguna tidak ingin foto dan video untuk menyertakan lokasi saat dibagikan, mereka dapat mematikan lokasi di menu Pilihan di lembar berbagi.

Untuk memosisikan pengalaman AR pengguna yang lebih baik, app yang menggunakan ARKit dapat menggunakan informasi pelacakan dunia atau wajah dari kamera lainnya. Pelacakan dunia menggunakan algoritme pada perangkat pengguna untuk memproses informasi dari sensor ini untuk menentukan posisi mereka relatif terhadap ruang fisik. Pelacakan dunia mengaktifkan fitur seperti Heading Optik di Peta.

Manajemen perangkat aman

Tinjauan manajemen perangkat aman

iOS, iPadOS, macOS, dan tvOS mendukung kebijakan dan konfigurasi keamanan fleksibel yang mudah diterapkan dan dikelola. Melaluinya, organisasi dapat melindungi informasi perusahaan dan membantu memastikan bahwa karyawan memenuhi persyaratan perusahaan, meskipun mereka menggunakan perangkat yang disediakan sendiri—misalnya, sebagai bagian dari program “bawa perangkat sendiri” (BYOD).

Organisasi dapat menggunakan sumber seperti perlindungan kode sandi, profil konfigurasi, penghapusan jarak jauh, dan mobile device management (MDM) pihak ketiga untuk mengelola rangkaian perangkat dan membantu menjaga agar data perusahaan tetap aman, bahkan saat karyawan mengakses data ini di perangkat pribadi mereka.

Di iOS 13 atau lebih baru, iPadOS 13.1 atau lebih baru, dan macOS 10.15 atau lebih baru, perangkat Apple mendukung pilihan pendaftaran pengguna baru yang secara khusus didesain untuk program BYOD. Pendaftaran pengguna menyediakan otonomi yang lebih besar untuk pengguna di perangkat mereka sendiri, sekaligus meningkatkan keamanan data pengguna dengan menyimpannya di volume APFS (Apple File System) terpisah yang dilindungi secara kriptografis. Ini menyediakan keseimbangan yang lebih baik antara keamanan, privasi, dan pengalaman pengguna untuk program BYOD.

Keamanan model pemasangan untuk iPhone dan iPad

iOS dan iPadOS menggunakan model pemasangan untuk mengontrol akses ke perangkat dari komputer host. Pemasangan membangun hubungan kepercayaan antara perangkat dan host yang terhubung, ditandai oleh pertukaran kunci publik. iOS dan iPadOS juga menggunakan tanda kepercayaan ini untuk mengaktifkan fungsi tambahan dengan host yang terhubung, seperti penyelarasan data. Di iOS 9 atau lebih baru, layanan:

- Yang memerlukan pemasangan tidak dapat dimulai hingga setelah perangkat telah dibuka oleh pengguna
- Tidak akan dimulai kecuali jika perangkat baru dibuka
- Dapat (seperti dengan penyelarasan foto) mengharuskan perangkat untuk dibuka agar dapat memulai

Proses pemasangan mengharuskan pengguna untuk membuka perangkat dan menerima permintaan pemasangan dari host. Di iOS 9 atau lebih baru, pengguna juga diharuskan untuk memasukkan kode sandi mereka, setelahnya host dan perangkat menukar dan menyimpan kunci publik RSA 2048 bit. Host kemudian diberi kunci 256 bit yang dapat membuka kantong kunci eskrow yang disimpan di perangkat. Kunci yang ditukar digunakan untuk memulai sesi SSL terenkripsi, yang diperlukan perangkat sebelum mengirimkan data terlindungi ke host atau memulai layanan (penyelarasan iTunes atau Finder, transfer file, pengembangan Xcode, dan seterusnya). Untuk menggunakan sesi yang dienkripsi ini untuk semua komunikasi, perangkat memerlukan koneksi dari host melalui Wi-Fi, maka perangkat harus telah dipasangkan sebelumnya melalui USB. Pemasangan juga mengaktifkan beberapa fitur diagnostik. Di iOS 9, jika rekaman pemasangan belum digunakan selama lebih dari 6 bulan, rekaman akan kedaluwarsa. Di iOS 11 atau lebih baru, jangka waktu ini dipersingkat ke 30 hari.

Layanan diagnostik tertentu, termasuk com.apple.mobile.pcapd, dibatasi untuk hanya dapat digunakan melalui USB. Selain itu, layanan com.apple.file_relay mengharuskan profil konfigurasi yang ditandatangani Apple untuk diinstal. Di iOS 11 atau lebih baru, Apple TV dapat menggunakan protokol Kata Sandi Jarak Jauh Aman untuk membuat hubungan pemasangan secara nirkabel.

Pengguna dapat menghilangkan daftar host tepercaya dengan pilihan Atur Ulang Pengaturan Jaringan atau Atur Ulang Lokasi & Privasi.

Mobile device management

Tinjauan keamanan mobile device management

Sistem operasi Apple mendukung mobile device management (MDM), yang memungkinkan organisasi untuk mengonfigurasi dan mengelola penyebaran perangkat Apple terskala dengan aman.

Cara MDM bekerja dengan aman

Kemampuan MDM dibangun berdasarkan teknologi sistem operasi yang ada, seperti profil konfigurasi, pendaftaran nirkabel, dan layanan Pemberitahuan Push Apple (APN). Misalnya, APN digunakan untuk membangunkan perangkat sehingga dapat berkomunikasi langsung dengan solusi MDM melalui koneksi aman. Dengan APN, tidak ada informasi rahasia atau khusus yang dikirimkan.

Dengan MDM, departemen TI dapat mendaftarkan perangkat Apple di lingkungan perusahaan, mengonfigurasi dan memperbarui pengaturan secara nirkabel, mengawasi kepatuhan terhadap kebijakan perusahaan, mengelola kebijakan pembaruan perangkat lunak, dan bahkan menghapus atau mengunci perangkat yang dikelola dari jauh.

Selain pendaftaran perangkat tradisional yang didukung oleh iOS, iPadOS, macOS, dan tvOS, jenis pendaftaran telah ditambahkan di iOS 13 atau lebih baru, iPadOS 13.1 atau lebih baru, dan macOS 10.15 atau lebih baru—Pendaftaran Pengguna. Pendaftaran pengguna adalah pendaftaran MDM yang secara khusus menargetkan penyebaran "bawa perangkat sendiri" (BYOD) tempat perangkat dimiliki secara pribadi tapi digunakan dalam lingkungan terkelola. Pendaftaran pengguna memberi solusi MDM hak yang lebih terbatas dari pendaftaran perangkat yang tidak diawasi, dan menyediakan pemisahan kriptografis antara data pengguna dan perusahaan.

Jenis pendaftaran

- *Pendaftaran Perangkat Otomatis:* Pendaftaran Perangkat Otomatis memungkinkan organisasi untuk mengonfigurasi dan mengelola perangkat sejak perangkat digunakan (dalam proses yang dikenal sebagai *penyebaran Maju Otomatis*). Perangkat ini dikenal sebagai yang *diawasi*, dan pengguna memiliki pilihan untuk mencegah profil MDM agar tidak dihapus oleh pengguna. Pendaftaran Perangkat Otomatis dirancang untuk perangkat yang dimiliki oleh organisasi.
- *Pendaftaran Perangkat:* Pendaftaran Perangkat memungkinkan organisasi untuk memungkinkan pengguna secara manual mendaftarkan perangkat, lalu mengelola berbagai aspek penggunaan perangkat, termasuk kemampuan untuk menghapus perangkat. Pendaftaran Perangkat juga memiliki kumpulan muatan dan pembatasan yang lebih besar yang dapat diterapkan ke perangkat. Saat pengguna menghapus profil pendaftaran, semua profil konfigurasi, pengaturannya, dan app terkelola berdasarkan profil pendaftaran tersebut juga akan dihapus.
- *Pendaftaran Pengguna:* Pendaftaran Pengguna dirancang untuk perangkat yang dimiliki oleh pengguna dan terintegrasi dengan ID Apple yang Dikelola untuk membuat identitas pengguna di perangkat. ID Apple yang Dikelola adalah bagian dari profil Pendaftaran Pengguna, dan pengguna harus berhasil disahkan agar pendaftaran dapat diselesaikan. ID Apple yang Dikelola dapat digunakan bersama ID Apple pribadi yang telah digunakan pengguna untuk masuk. App serta akun terkelola menggunakan ID Apple yang Dikelola, dan app serta akun pribadi menggunakan ID Apple.

Pembatasan perangkat

Pembatasan dapat diaktifkan—atau dalam beberapa kasus dinonaktifkan—oleh administrator untuk membantu mencegah pengguna mengakses app, layanan, atau fungsi iPhone, iPad, Mac, atau Apple TV yang terdaftar di solusi MDM. Pembatasan dikirimkan ke perangkat dalam muatan pembatasan, yang merupakan bagian dari profil konfigurasi. Pembatasan tertentu di iPhone dapat dicerminkan di Apple Watch yang dipasangkan.

Manajemen pengaturan kode sandi dan kata sandi

Secara default, kode sandi pengguna dapat didefinisikan sebagai PIN numerik. Di perangkat iOS dan iPadOS dengan Face ID atau Touch ID, panjang kode sandi minimum adalah empat digit. Apple menyarankan kode sandi yang lebih panjang dan rumit karena lebih sulit ditebak atau diserang.

Administrator dapat menerapkan persyaratan kode sandi yang rumit dan kebijakan lain menggunakan MDM atau Microsoft Exchange ActiveSync, atau dengan mengharuskan pengguna untuk menginstal profil konfigurasi secara manual. Kata sandi administrator diperlukan untuk penginstalan muatan kebijakan kode sandi macOS. Beberapa kebijakan kode sandi dapat memerlukan panjang kode sandi tertentu, komposisi, atau atribut lainnya.

Pemberlakuan profil konfigurasi

Profil konfigurasi adalah cara utama solusi MDM memberikan dan mengelola kebijakan dan batasan pada perangkat terkelola. Jika organisasi harus mengonfigurasi sejumlah besar perangkat atau untuk menyediakan banyak pengaturan email khusus, pengaturan jaringan, atau sertifikat ke sejumlah besar perangkat—profil konfigurasi adalah cara yang aman untuk melakukannya.

Profil konfigurasi

Profil konfigurasi adalah file XML (berakhir .mobileconfig) yang berisi muatan yang memuat pengaturan dan informasi pengesahan di perangkat Apple. Profil konfigurasi mengotomatiskan konfigurasi pengaturan, akun, pembatasan, dan informasi pengesahan. File ini dapat dibuat oleh solusi MDM atau Apple Configurator untuk Mac, atau file dapat dibuat secara manual. Sebelum organisasi mengirimkan profil konfigurasi ke perangkat Apple, mereka harus mendaftarkan perangkat di solusi MDM menggunakan profil pendaftaran.

Profil pendaftaran

Profil pendaftaran adalah profil konfigurasi dengan muatan MDM yang mendaftarkan perangkat di solusi MDM yang ditetapkan untuk perangkat tersebut. Ini memungkinkan solusi MDM untuk mengirimkan perintah serta profil konfigurasi ke perangkat dan untuk meminta aspek perangkat tertentu. Saat pengguna menghapus profil pendaftaran, semua profil konfigurasi, pengaturannya, dan app terkelola berdasarkan profil pendaftaran tersebut juga akan dihapus. Hanya boleh ada satu profil pendaftaran di perangkat dalam satu waktu.

Pengaturan profil konfigurasi

Profil konfigurasi berisi sejumlah pengaturan dalam muatan tertentu yang dapat ditetapkan, termasuk (tapi tidak terbatas pada):

- Kebijakan kode sandi dan kata sandi
- Pembatasan fitur perangkat (misalnya, menonaktifkan kamera)
- Pengaturan jaringan dan VPN
- Pengaturan Microsoft Exchange
- Pengaturan Mail
- Pengaturan akun
- Pengaturan layanan direktori LDAP
- Pengaturan layanan kalender CalDAV
- Info pengesahan dan kunci
- Pembaruan perangkat lunak

Penandatanganan dan enkripsi profil

Profil konfigurasi dapat ditandatangani untuk memvalidasi asalnya dan dienkripsi untuk membantu memastikan integritas dan melindungi kontennya. Profil konfigurasi untuk iOS dan iPadOS dienkripsi menggunakan Sintaksis Pesan Kriptografi (CMS) yang ditetapkan di RFC 5652, mendukung 3DES dan AES128.

Penginstalan profil

Pengguna dapat menginstal profil konfigurasi secara langsung di perangkat mereka menggunakan Apple Configurator untuk Mac, atau profil dapat diunduh menggunakan Safari, dikirim terlampir ke pesan mail, ditransfer menggunakan AirDrop atau app File di iOS dan iPadOS, atau dikirim secara nirkabel menggunakan solusi mobile device management (MDM). Saat pengguna mengatur perangkat di Apple School Manager atau Apple Business Manager, perangkat akan mengunduh dan menginstal profil untuk pendaftaran MDM. Untuk informasi mengenai cara menghapus profil, lihat Pengantar mobile device management di Penyebaran Platform Apple.

Catatan: Di perangkat yang diawasi, profil konfigurasi juga dapat dikunci ke perangkat. Ini dirancang untuk mencegah penghapusannya atau untuk hanya mengizinkan penghapusan dengan kode sandi. Karena banyak organisasi yang memiliki perangkat iOS dan iPadOS, profil konfigurasi yang mengikat perangkat ke solusi MDM dapat dihapus—tapi hal tersebut juga menghapus semua informasi konfigurasi, data, dan app yang dikelola.

Pendaftaran Perangkat Otomatis

Organisasi dapat secara otomatis mendaftarkan perangkat iOS, iPadOS, macOS, dan tvOS di mobile device management (MDM) tanpa harus secara fisik menyentuh atau menyiapkan perangkat sebelum pengguna mendapatkannya. Setelah terdaftar di salah satu layanan, administrator masuk ke situs web layanan, dan menautkan program ke solusi MDM mereka. Perangkat yang mereka beli dapat ditetapkan ke pengguna melalui MDM. Selama proses konfigurasi perangkat, keamanan data sensitif dapat ditingkatkan dengan memastikan diberlakukannya tindakan pengamanan yang sesuai. Misalnya:

- Meminta pengguna untuk melakukan pengesahan sebagai bagian dari alur pengaturan awal di Asisten Pengaturan perangkat Apple selama aktivasi.
- Menyediakan konfigurasi awal dengan akses terbatas dan mengharuskan konfigurasi perangkat tambahan untuk mengakses data sensitif.

Setelah pengguna ditetapkan, semua konfigurasi, pembatasan, atau kontrol yang ditentukan MDM akan diinstal secara otomatis. Semua komunikasi antara perangkat dan server Apple dienkripsi saat dikirimkan melalui HTTPS (TLS).

Proses pengaturan untuk pengguna dapat disederhanakan lebih lanjut dengan menghapus langkah tertentu di Asisten Pengaturan untuk perangkat, sehingga perangkat pengguna dapat siap digunakan dengan cepat. Administrator juga dapat mengontrol apakah pengguna dapat menghapus profil MDM dari perangkat dan memastikan bahwa pembatasan perangkat telah aktif selama siklus proses perangkat. Setelah perangkat dibuka dan diaktifkan, perangkat akan terdaftar di solusi MDM organisasi—dan semua pengaturan manajemen, app, dan buku akan terinstal sebagaimana yang ditetapkan administrator MDM.

Apple School Manager, Apple Business Manager, dan Apple Business Essentials

Apple School Manager, Apple Business Manager, dan Apple Business Essentials adalah layanan untuk administrator TI untuk menyebarkan perangkat Apple yang telah dibeli organisasi secara langsung dari Apple atau Penjual Resmi Apple dan operator yang berpartisipasi.

Saat digunakan dengan solusi MDM, administrator dapat menyederhanakan proses pengaturan untuk pengguna, mengonfigurasi pengaturan perangkat, dan mendistribusikan app serta buku yang dibeli di ketiga layanan ini. Apple School Manager juga terintegrasi dengan Sistem Informasi Murid (SIS) secara langsung atau menggunakan SFTP, dan ketiga layanan dapat menggunakan Sistem untuk Manajemen Identitas Lintas Domain (SCIM) atau pengesahan gabungan dengan Microsoft Azure Active Directory (Azure AD) sehingga administrator dapat membuat akun dengan cepat.

Apple mempertahankan sertifikasi sesuai dengan ISO/IEC 27001 dan standar 27018 untuk memungkinkan pelanggan Apple untuk menangani peraturan dan kewajiban kontraknya. Sertifikasi ini memberikan pengesahan independen pada pelaksanaan Privasi dan Keamanan Informasi Apple untuk sistem dalam lingkup. Untuk informasi lainnya, lihat Sertifikasi keamanan layanan internet Apple di Sertifikasi Platform Apple.

Catatan: Untuk mempelajari ketersediaan program Apple di negara atau wilayah tertentu, lihat artikel Dukungan Apple Ketersediaan program Apple dan metode pembayaran untuk pendidikan serta bisnis.

Pengawasan perangkat

Pengawasan secara umum menunjukkan bahwa perangkat dimiliki oleh organisasi, yang memberikan mereka kontrol tambahan atas konfigurasi dan pembatasan perangkat. Untuk informasi lainnya, lihat Mengenai pengawasan perangkat Apple di Penyebaran Platform Apple.

Keamanan Kunci Aktivasi

Cara Apple memberlakukan Kunci Aktivasi berbeda-beda tergantung apakah perangkat berupa iPhone atau iPad, Mac dengan Apple silicon, atau Mac berbasis Intel dengan Keping Keamanan T2 Apple.

Perilaku di iPhone dan iPad

Di perangkat iPhone dan iPad, Kunci Aktivasi diberlakukan melalui proses aktivasi setelah layar pilihan Wi-Fi di Asisten Pengaturan iOS dan iPadOS. Saat perangkat terindikasi aktif, perangkat mengirimkan permintaan ke server Apple untuk mendapatkan sertifikat aktivasi. Perangkat yang Dikunci Aktivasi meminta pengesahan iCloud pengguna yang mengaktifkan Kunci Aktivasi pada saat ini. Asisten Pengaturan iOS dan iPadOS tidak akan berlanjut kecuali sertifikat yang sah dapat diperoleh.

Perilaku di Mac dengan Apple silicon

Di Mac dengan Apple silicon, LLB memverifikasi bahwa LocalPolicy yang sah untuk perangkat ada dan bahwa nilai nonce kebijakan LocalPolicy sesuai dengan nilai yang disimpan di Komponen Penyimpanan Aman. LLB melakukan boot ke recoveryOS jika:

- Tidak ada LocalPolicy untuk macOS saat ini
- LocalPolicy tidak sah untuk macOS tersebut
- Nilai hash nonce LocalPolicy tidak sesuai dengan hash nilai yang disimpan di Komponen Penyimpanan Aman

recoveryOS mendeteksi bahwa komputer Mac tidak diaktifkan dan menghubungi server aktivasi untuk mendapatkan sertifikat aktivasi. Jika perangkat Dikunci Aktivasi, recoveryOS meminta pengesahan iCloud pengguna yang mengaktifkan Kunci Aktivasi pada saat ini. Setelah sertifikat aktivasi yang sah diperoleh, kunci sertifikat aktivasi digunakan untuk memperoleh sertifikat RemotePolicy. Komputer Mac menggunakan kunci LocalPolicy dan sertifikat RemotePolicy untuk memproduksi LocalPolicy yang sah. LLB tidak akan mengizinkan boot macOS kecuali LocalPolicy yang sah ada.

Perilaku di komputer Mac berbasis Intel

Di Mac berbasis Intel dengan keping T2, firmware keping T2 memverifikasi bahwa sertifikat aktivasi yang sah ada sebelum mengizinkan komputer di-boot ke macOS. Firmware UEFI yang dimuat oleh keping T2 bertanggung jawab untuk meminta status aktivasi perangkat dari keping T2 dan melakukan boot ke recoveryOS alih-alih melakukan boot ke macOS jika sertifikat aktivasi yang sah tidak ada. recoveryOS mendeteksi bahwa Mac tidak diaktifkan dan menghubungi server aktivasi untuk mendapatkan sertifikat aktivasi. Jika perangkat Dikunci Aktivasi, recoveryOS meminta pengesahan iCloud pengguna yang mengaktifkan Kunci Aktivasi pada saat ini. Firmware UEFI tidak akan mengizinkan boot macOS kecuali sertifikat aktivasi yang sah ada.

Mode Hilang yang Dikelola dan penghapusan jarak jauh

Mode Hilang yang Dikelola digunakan untuk menemukan perangkat yang diawasi saat dicuri. Setelah ditemukan, perangkat dapat dikunci atau dihapus dari jarak jauh.

Mode Hilang yang Dikelola

Jika perangkat iOS atau iPadOS yang diawasi dengan iOS 9 atau lebih baru hilang atau dicuri, administrator mobile device management (MDM) dapat mengaktifkan Mode Hilang (disebut Mode Hilang yang Dikelola) dari jauh di perangkat tersebut. Jika Mode Hilang yang Dikelola diaktifkan, pengguna saat ini akan keluar dan perangkat tidak dapat dibuka. Layar menampilkan pesan yang dapat disesuaikan oleh administrator, seperti menampilkan nomor telepon untuk dihubungi jika perangkat ditemukan. Administrator juga dapat meminta perangkat untuk mengirim lokasinya saat ini (bahkan jika Layanan Lokasi mati) dan memutar bunyi jika diperlukan. Jika administrator mematikan Mode Hilang yang Dikelola, yang merupakan satu-satunya cara untuk keluar dari mode tersebut, pengguna akan diberi tahu perihal tindakan ini melalui pesan di Layar Terkunci atau peringatan di Layar Utama.

Penghapusan jarak jauh

Perangkat iOS, iPadOS, dan macOS dapat dihapus dari jauh oleh administrator atau pengguna (penghapusan jarak jauh instan hanya tersedia jika Mac mengaktifkan FileVault). Penghapusan jarak jauh instan dilakukan secara aman dengan membuang kunci media dari Penyimpanan Dapat Dihapus, sehingga membuat semua data tidak dapat dibaca. Untuk penghapusan jarak jauh melalui Microsoft Exchange ActiveSync, perangkat melakukan pemeriksaan dengan Server Microsoft Exchange sebelum melakukan penghapusan.

Saat perintah penghapusan jarak jauh dipicu oleh MDM atau iCloud, perangkat iPhone, iPad, iPod touch, atau Mac akan mengirimkan pengakuan dan melakukan penghapusan.

Penghapusan jarak jauh tidak dimungkinkan dalam situasi berikut:

- Dengan Pendaftaran Pengguna
- Menggunakan Microsoft Exchange ActiveSync jika akun yang terinstal dengan Pendaftaran Pengguna
- Menggunakan Microsoft Exchange ActiveSync jika perangkat diawasi

Pengguna juga dapat menghapus perangkat iOS atau iPadOS yang mereka miliki menggunakan app Pengaturan. Dan sebagaimana yang disebutkan, perangkat iOS dan iPadOS dapat diatur agar dihapus secara otomatis setelah serangkaian upaya memasukkan kode sandi yang gagal.

Keamanan iPad bersama di iPadOS

iPad Bersama adalah mode beberapa pengguna untuk digunakan dalam penyebaran iPad. Ini memungkinkan pengguna untuk berbagi iPad sambil mempertahankan pemisahan dokumen dan data untuk setiap pengguna. Setiap pengguna mendapatkan lokasi penyimpanan mereka sendiri, yang diimplementasikan sebagai volume APFS (Apple File System) yang dilindungi oleh info pengesahan pengguna. iPad Bersama memerlukan penggunaan ID Apple yang Dikelola yang diterbitkan dan dimiliki oleh organisasi.

Dengan iPad Bersama, pengguna dapat masuk ke perangkat milik organisasi yang dikonfigurasi untuk digunakan oleh beberapa pengguna. Data pengguna dipartisi ke direktori terpisah, yang masing-masing berada di domain perlindungan datanya sendiri dan dilindungi oleh izin UNIX dan sandbox. Di iPadOS 13.4 atau lebih baru, pengguna juga dapat masuk ke sesi sementara. Saat pengguna keluar dari sesi sementara, volume APFS-nya dihapus dan ruang terpisahnya dikembalikan ke sistem.

Masuk ke iPad Bersama

Baik ID Apple yang Dikelola yang asli maupun gabungan didukung saat masuk ke iPad Bersama. Saat menggunakan akun gabungan untuk pertama kalinya, pengguna akan dialihkan ke portal masuk Penyedia Identitas (IdP). Setelah disahkan, token akses jangka pendek dikeluarkan untuk ID Apple yang Dikelola pendukung, dan proses masuk dilanjutkan dengan cara yang sama seperti proses masuk ID Apple yang Dikelola. Setelah masuk, Asisten Pengaturan di iPad Bersama meminta pengguna untuk membuat kode sandi (rahasia) yang digunakan untuk mengamankan data lokal di perangkat dan untuk mengesahkan ke layar masuk di masa mendatang. Seperti perangkat satu pengguna, tempat pengguna masuk sekali ke ID Apple yang Dikelola menggunakan akun gabungan, lalu membuka perangkat mereka dengan kode sandi, di iPad Bersama pengguna masuk sekali menggunakan akun gabungan mereka, kemudian menggunakan kode sandi yang dibuat.

Saat pengguna masuk tanpa pengesahan gabungan, ID Apple yang Dikelola disahkan dengan Layanan Identitas Apple (IDS) menggunakan protokol SRP. Jika pengesahan berhasil, token akses sementara khusus perangkat akan diberikan. Jika pengguna telah menggunakan perangkat sebelumnya, mereka akan memiliki akun pengguna lokal yang dibuka menggunakan info pengesahan yang sama.

Jika pengguna belum menggunakan perangkat sebelum atau sedang menggunakan fitur sesi sementara, iPad Bersama menyediakan ID pengguna UNIX baru, volume APFS untuk menyimpan data pribadi pengguna, dan rantai kunci lokal. Karena penyimpanan dialokasikan (dipisahkan) untuk pengguna saat volume APFS dibuat, mungkin tidak terdapat cukup ruang untuk membuat volume baru. Pada kejadian tersebut, sistem mengidentifikasi pengguna yang ada yang datanya telah selesai diselaraskan ke awan dan mengeluarkan pengguna tersebut dari perangkat agar dapat memungkinkan pengguna baru untuk masuk. Jika semua pengguna yang ada belum selesai mengunggah data awannya, pengguna baru akan gagal masuk. Untuk masuk, pengguna baru harus menunggu satu data pengguna selesai diselaraskan, atau meminta administrator untuk menghapus akun pengguna yang ada secara paksa, yang dapat mengakibatkan hilangnya data.

Jika perangkat tidak terhubung ke internet (misalnya, jika pengguna tidak memiliki titik akses Wi-Fi), pengesahan dapat dilakukan dengan akun lokal selama beberapa hari. Dalam situasi tersebut, hanya pengguna dengan akun lokal yang telah ada sebelumnya atau sesi sementara yang dapat masuk. Setelah batas waktu terlewati, pengguna akan diharuskan untuk mengesahkan secara online, meskipun akun lokal telah ada.

Setelah akun lokal pengguna dibuka atau dibuat, jika disahkan dari jauh, token sementara yang diterbitkan server Apple akan dikonversi ke token iCloud yang mengizinkan proses masuk ke iCloud. Setelah itu, pengaturan pengguna akan dipulihkan dan dokumen serta data mereka akan diselaraskan dari iCloud.

Saat sesi pengguna aktif dan perangkat online, dokumen dan data akan disimpan di iCloud saat dibuat atau dimodifikasi. Selain itu, mekanisme penyelarasan latar belakang membantu memastikan bahwa perubahan didorong ke iCloud, atau ke layanan web lainnya menggunakan sesi latar belakang NSURLSession, setelah pengguna keluar. Setelah penyelarasan latar belakang untuk pengguna tersebut selesai, volume APFS pengguna akan dilepas dan tidak dapat dipasang lagi tanpa pengguna masuk kembali.

Sesi sementara tidak menyelaraskan data dengan iCloud, dan meskipun sesi sementara dapat masuk ke layanan penyelarasan pihak ketiga seperti Box atau Google Drive, tidak ada fasilitas untuk terus menyelaraskan data saat sesi sementara berakhir.

Keluar dari iPad Bersama

Setelah pengguna keluar dari iPad Bersama, kantong kunci pengguna tersebut akan segera dikunci dan semua app akan dimatikan. Untuk mempercepat proses masuk pengguna baru, iPadOS akan menangguhkan sebagian tindakan keluar biasa untuk sementara dan memunculkan jendela masuk kepada pengguna baru. Jika pengguna masuk selama periode waktu ini (kira-kira 30 detik), iPad Bersama akan menjalankan pembersihan yang ditangguhkan sebagai bagian dari proses masuk ke akun pengguna baru. Namun, jika iPad Bersama tetap idle, perangkat tersebut akan mengaktifkan pembersihan yang ditangguhkan. Selama fase pembersihan, Jendela Masuk akan dimulai ulang seakan-akan proses keluar lain telah terjadi.

Saat sesi sementara berakhir, iPad Bersama melakukan rangkaian keluar penuh dan segera menghapus volume APFS sesi sementara.

Keamanan Apple Configurator

Apple Configurator untuk Mac dilengkapi dengan desain yang fleksibel, aman, dan fokus pada perangkat yang memungkinkan administrator dengan cepat dan mudah mengonfigurasi satu atau lusinan perangkat iOS, iPadOS, dan tvOS yang terhubung ke Mac melalui USB (atau perangkat tvOS yang dipasangkan melalui Bonjour) sebelum memberikannya ke pengguna. Dengan Apple Configurator untuk Mac, administrator dapat memperbarui perangkat lunak, menginstal app dan profil konfigurasi, mengubah nama dan mengganti wallpaper di perangkat, mengekspor informasi perangkat dan dokumen, dan lainnya.

Apple Configurator untuk Mac juga dapat memulihkan atau mengaktifkan kembali komputer Mac dengan Apple silicon dan perangkat dengan Keping Keamanan T2 Apple. Saat Mac dipulihkan atau diaktifkan kembali dengan cara ini, file yang berisi pembaruan kecil terbaru untuk sistem operasi (macOS, recoveryOS untuk Apple silicon, atau sepOS untuk T2) diunduh dengan aman dari server Apple dan diinstal secara langsung di Mac. Setelah berhasil memulihkan atau mengaktifkan kembali, file dihapus dari Mac yang menjalankan Apple Configurator. Pengguna tidak dapat memeriksa atau menggunakan file ini di luar Apple Configurator.

Administrator juga dapat memilih untuk menambahkan perangkat ke Apple School Manager, Apple Business Manager, atau Apple Business Essentials menggunakan Apple Configurator untuk Mac atau Apple Configurator untuk iPhone, bahkan jika perangkat tidak dibeli langsung dari Apple, Penjual Resmi Apple, dan operator seluler resmi. Saat administrator mengatur perangkat yang telah didaftarkan secara manual, perangkat akan berfungsi seperti perangkat lainnya di salah satu layanan tersebut, dengan pengawasan wajib dan pendaftaran mobile device management (MDM). Untuk perangkat yang tidak dibeli secara langsung, pengguna memiliki jangka waktu provisional selama 30 hari untuk melepas perangkat dari layanan, pengawasan, dan MDM tersebut.

Organisasi juga dapat menggunakan Apple Configurator untuk Mac untuk mengaktifkan perangkat iOS, iPadOS, dan tvOS yang sama sekali tidak memiliki koneksi internet dengan menghubungkannya ke Mac host dengan koneksi internet selagi perangkat diatur. Administrator dapat memulihkan, mengaktifkan, dan menyiapkan perangkat dengan konfigurasi pentingnya termasuk app, profil, serta dokumen tanpa perlu terhubung ke jaringan Wi-Fi atau seluler. Fitur ini tidak mengizinkan administrator untuk melewati persyaratan Kunci Aktivasi apa pun yang ada yang biasanya diperlukan selama aktivasi non-tertambat.

Keamanan Durasi Layar

Durasi Layar adalah fitur internal untuk melihat dan mengelola seberapa banyak waktu yang dihabiskan orang dewasa dan anak mereka di app, situs web, dan lainnya. Ada dua jenis pengguna: orang dewasa dan anak (dikelola).

Meskipun Durasi Layar bukan merupakan fitur keamanan sistem baru, Anda perlu memahami cara Durasi Layar melindungi privasi dan keamanan data yang dikumpulkan dan dibagikan antarperangkat. Durasi Layar tersedia di iOS 12 atau lebih baru, iPadOS 13.1 atau lebih baru, macOS 10.15 atau lebih baru, dan beberapa fitur watchOS 6 atau lebih baru.

Tabel di bawah menjelaskan fitur utama Durasi Layar.

Fitur	Sistem operasi yang didukung
Melihat data penggunaan	iOS iPadOS macOS
Memberlakukan pembatasan tambahan	iOS iPadOS macOS watchOS
Mengatur batas penggunaan web	iOS iPadOS macOS
Mengatur batas app	iOS iPadOS macOS watchOS
Mengonfigurasi waktu henti	iOS iPadOS macOS watchOS

Untuk pengguna yang mengelola penggunaan perangkat mereka sendiri, kontrol dan penggunaan data Durasi Layar dapat diselaraskan di semua perangkat yang dikaitkan dengan akun iCloud yang sama menggunakan enkripsi ujung ke ujung CloudKit. Ini mengharuskan akun pengguna untuk mengaktifkan autentikasi dua faktor (penyelarasan menyala secara default). Durasi Layar mengganti fitur Pembatasan yang ada di versi iOS serta iPadOS sebelumnya, dan fitur Pengawasan Orang Tua yang ada di versi macOS sebelumnya.

Di iOS 13 atau lebih baru, iPadOS 13.1 atau lebih baru, dan macOS 10.15 atau lebih baru, pengguna Durasi Layar dan anak yang dikelola secara otomatis berbagi penggunaan mereka di seluruh perangkat jika akun iCloud mereka mengaktifkan autentikasi dua faktor. Setelah pengguna membersihkan riwayat Safari atau menghapus app, data penggunaannya akan dihapus dari perangkat dan semua perangkat yang diselaraskan.

Orang Tua dan Durasi Layar

Orang tua juga dapat menggunakan Durasi Layar di perangkat iOS, iPadOS, dan macOS untuk memahami dan mengontrol penggunaan oleh anak mereka. Jika orang tua merupakan pengelola keluarga (di Keluarga Berbagi iCloud), mereka dapat melihat data penggunaan dan mengelola pengaturan Durasi Layar untuk anak mereka. Anak akan diberi tahu jika orang tua mereka menyalakan Durasi Layar, dan mereka dapat mengawasi penggunaan mereka sendiri. Jika orang tua menyalakan Durasi Layar untuk anak mereka, orang tua dapat mengatur kode sandi sehingga anak mereka tidak dapat membuat perubahan. Setelah mereka dewasa (usia akan berbeda tergantung negara atau wilayah), anak dapat mematikan pengawasan ini.

Data penggunaan dan pengaturan konfigurasi ditransfer antara perangkat orang tua dan anak menggunakan protokol Layanan Identitas (IDS) Apple yang dilindungi dengan enkripsi ujung ke ujung. Data terenkripsi dapat disimpan untuk sementara di server IDS hingga dibaca oleh perangkat yang menerima (misalnya, segera setelah iPhone, iPad, atau iPod touch dinyalakan, jika perangkat tersebut mati). Data ini tidak dapat dibaca oleh Apple.

Analisis Durasi Layar

Jika pengguna menyalakan Bagikan Analisis iPhone & Apple Watch, hanya data anonim berikut yang dikumpulkan sehingga Apple dapat lebih memahami bagaimana Durasi Layar sedang digunakan:

- Apakah Durasi Layar dinyalakan selama Asisten Pengaturan atau di lain waktu di Pengaturan
- Perubahan dalam penggunaan Kategori setelah membuat batas untuk kategori tersebut (dalam waktu 90 hari)
- Apakah Durasi Layar dinyalakan
- Apakah Waktu Henti diaktifkan
- Berapa kali permintaan “Minta durasi tambahan” digunakan
- Jumlah batas app
- Berapa kali pengguna melihat penggunaan di pengaturan Durasi Layar, per jenis pengguna dan per jenis tampilan (lokal, jarak jauh, widget)
- Berapa kali pengguna mengabaikan batas, per jenis pengguna
- Berapa kali pengguna menghapus batas, per jenis pengguna

Tidak ada data spesifik penggunaan app atau web yang dikumpulkan oleh Apple. Saat pengguna melihat daftar app di informasi penggunaan Durasi Layar, ikon app diambil secara langsung dari App Store, yang tidak menyimpan data apa pun dari permintaan ini.

Glosarium

AES (Standar Enkripsi Lanjutan) Standar enkripsi global populer yang digunakan untuk mengenkripsi data agar tetap pribadi.

AES-XTS Mode AES yang didefinisikan di IEEE 1619-2007 ditujukan untuk mengenkripsi media penyimpanan.

akses memori langsung (DMA) Fitur yang memungkinkan subsistem perangkat keras untuk mengakses memori utama secara langsung, melewati CPU.

Algoritme Tanda Tangan Digital Kurva Eliptis (ECDSA) Algoritme tanda tangan digital yang didasarkan pada kriptografi kurva elips.

Antarmuka Periferal Serial yang Ditingkatkan (eSPI) Bus semua dalam satu yang dirancang untuk komunikasi serial selaras.

APFS (Apple File System) Sistem file default untuk iOS, iPadOS, tvOS, watchOS, dan komputer Mac yang menggunakan macOS 10.13 atau lebih baru. APFS disertai dengan enkripsi kuat, berbagi ruang, snapshot, pembuatan ukuran direktori cepat, dan fundamental sistem file yang ditingkatkan.

Apple Business Manager Portal sederhana berbasis web untuk administrator TI yang menyediakan cara yang cepat dan sederhana bagi organisasi untuk menyebarkan perangkat Apple yang telah mereka beli secara langsung dari Apple atau dari Penjual Resmi Apple dan operator yang berpartisipasi. Mereka dapat secara otomatis mendaftarkan perangkat di solusi mobile device management (MDM) tanpa harus secara fisik menyentuh atau menyiapkan perangkat sebelum pengguna mendapatkannya.

Apple School Manager Portal sederhana berbasis web untuk administrator TI yang menyediakan cara yang cepat dan sederhana bagi organisasi untuk menyebarkan perangkat Apple yang telah mereka beli secara langsung dari Apple atau dari Penjual Resmi Apple dan operator yang berpartisipasi. Mereka dapat secara otomatis mendaftarkan perangkat di solusi mobile device management (MDM) tanpa harus secara fisik menyentuh atau menyiapkan perangkat sebelum pengguna mendapatkannya.

Apple Security Bounty Imbalan yang diberikan oleh Apple kepada peneliti yang melaporkan kerentanan yang memengaruhi sistem operasi rilis terbaru dan, jika relevan, perangkat keras terbaru.

bit seeding perangkat lunak Bit terdedikasi di Mesin AES Secure Enclave yang ditambahkan ke UID saat membuat kunci dari UID. Setiap bit seeding perangkat lunak memiliki bit kunci masing-masing. Sistem operasi dan ROM Boot Secure Enclave dapat mengubah nilai setiap bit seeding perangkat lunak secara terpisah selama bit kunci masing-masingnya belum diatur. Setelah bit kunci diatur, bit seeding perangkat lunak dan bit kunci tidak dapat dimodifikasi. Bit seeding perangkat lunak dan kuncinya diatur ulang setelah Secure Enclave di-boot ulang.

Boot Camp Utilitas Mac yang mendukung penginstalan Microsoft Windows di komputer Mac yang didukung.

Bootloader Level Rendah (LLB) Di komputer Mac dengan arsitektur boot dua tahap, LLB berisi kode yang diaktifkan oleh ROM Boot dan pada gilirannya memuat iBoot, sebagai bagian dari rantai boot aman.

CKRecord Kamus pasangan nilai kunci yang berisi data yang disimpan atau diambil dari CloudKit.

Firmware Antarmuka Firmware Terpadu yang Dapat Diperluas (UEFi) Teknologi pengganti untuk BIOS untuk menghubungkan firmware ke sistem operasi komputer.

Gatekeeper Di macOS, teknologi yang dirancang untuk membantu memastikan hanya perangkat lunak tepercaya yang dijalankan di Mac pengguna.

HMAC Kode pengesahan pesan berbasis hash yang berdasarkan pada fungsi hash kriptografis.

iBoot Boot loader tingkat 2 untuk semua perangkat Apple. Kode yang memuat XNU, sebagai bagian dari rantai boot aman. Tergantung generasi sistem pada keping (SoC), iBoot dapat dimuat oleh Bootloader Level Rendah atau secara langsung oleh ROM Boot.

ID grup (GID) Seperti UID, tapi bersifat umum untuk semua prosesor di satu kelas.

ID unik (UID) Kunci AES 256 bit yang ditanamkan ke setiap prosesor pada proses produksi. UID tidak dapat dibaca oleh firmware atau perangkat lunak, dan hanya digunakan oleh Mesin AES perangkat keras milik prosesor. Untuk mendapatkan kunci yang sebenarnya, penyerang harus melancarkan serangan fisik yang sangat rumit dan mahal pada silikon prosesor. UID tidak terkait dengan pengenal lain di perangkat termasuk, tapi tidak terbatas pada, UDID.

Identifikasi Keping Eksklusif (ECID) Pengenal 64 bit yang bersifat unik untuk prosesor di setiap perangkat iOS dan iPadOS. Saat panggilan dijawab di satu perangkat, deringan di perangkat di sekitar yang dipasangkan iCloud dihentikan oleh pengiklanan singkat melalui Bluetooth Rendah Energi (BLE) 4.0. Bita pengiklanan dienkripsi menggunakan metode yang sama dengan pengiklanan Handoff. Digunakan sebagai bagian dari proses penyesuaian, pengenal tidak dianggap sebagai rahasia.

Joint Test Action Group (JTAG) Alat debug perangkat keras standar yang digunakan oleh pemrogram dan pengembang sirkuit.

kantong kunci Struktur data yang digunakan untuk menyimpan kumpulan kunci kelas. Setiap jenis (pengguna, perangkat, sistem, cadangan, eskrow, atau Cadangan iCloud) memiliki format yang sama.

Header berisi: Versi (diatur ke empat dalam iOS 12 atau lebih baru), Jenis (sistem, cadangan, eskrow, atau Cadangan iCloud), UUID Kantong Kunci, HMAC jika kantong kunci ditandatangani, dan metode yang digunakan untuk membungkus kunci kelas—dikaitkan dengan UID atau PBKDF2, bersama dengan jumlah salt dan iterasi.

Daftar kunci kelas: UUID Kunci, Kelas (file atau kelas Perlindungan Data Rantai Kunci yang digunakan), jenis pembungkusan (hanya kunci turunan UID, atau kunci turunan UID dan kunci turunan kode sandi), kunci kelas yang dibungkus, dan kunci publik untuk kelas asimetris.

Komponen Penyimpanan Aman Keping dirancang dengan kode RO tetap, pembuat nomor acak perangkat keras, mesin kriptografi, dan deteksi kerusakan fisik. Di perangkat yang didukung, Secure Enclave dipasangkan dengan Komponen Penyimpanan Aman untuk penyimpanan nonce anti-pemutaran ulang. Untuk membaca dan memperbarui nonce, Secure Enclave dan keping penyimpanan menerapkan protokol aman yang membantu memastikan akses eksklusif ke nonce. Terdapat beberapa generasi dari teknologi ini dengan jaminan keamanan yang berbeda.

kunci media Bagian hierarki kunci enkripsi yang membantu menyediakan penghapusan aman dan instan. Di iOS, iPadOS, tvOS, dan watchOS, kunci media membungkus metadata di volume data (dan karenanya tanpa akses ke semua kunci per file tidak akan mungkin, membuat file yang dilindungi dengan Perlindungan Data tidak dapat diakses). Di macOS, kunci media membungkus material kunci, semua metadata, dan data di volume yang dilindungi oleh FileVault. Dalam kedua kasus, penghapusan kunci media membuat data yang dienkripsi tidak dapat diakses.

kunci per file Kunci yang digunakan oleh Perlindungan Data untuk mengenkripsi file di sistem file. Kunci per file dibungkus oleh kunci kelas dan disimpan di metadata file.

kunci sistem file Kunci yang mengenkripsi setiap metadata file, termasuk kunci kelasnya. Kunci ini disimpan di Penyimpanan Dapat Dihapus untuk penghapusan cepat dapat dilakukan, bukan untuk kerahasiaan.

Kunci turunan kode sandi (PDK) Kunci enkripsi yang diturunkan dari pengaitan kata sandi pengguna dengan kunci SKP jangka panjang dan UID Secure Enclave.

Layanan Identitas (IDS) Apple Direktori kunci publik iMessage Apple, alamat APN, serta nomor telepon dan alamat email yang digunakan untuk mencari kunci dan alamat perangkat.

Layanan Pemberitahuan Push Apple (APN) Layanan global dari Apple yang mengirimkan pemberitahuan push ke perangkat Apple.

Mesin kriptografis AES Komponen perangkat keras khusus yang menerapkan AES.

mobile device management (MDM) Layanan yang memungkinkan administrator mengelola perangkat yang didaftarkan secara jarak jauh. Setelah perangkat didaftarkan, administrator dapat menggunakan layanan MDM melalui jaringan untuk mengonfigurasi pengaturan dan melakukan tugas lainnya di perangkat tanpa interaksi pengguna.

Mode Pemulihan Mode yang digunakan untuk memulihkan banyak perangkat Apple jika tidak mengenali perangkat pengguna sehingga pengguna dapat menginstal ulang sistem operasinya.

Mode Peningkatan Firmware Perangkat (DFU) Mode ketika kode ROM Boot perangkat menunggu untuk dipulihkan melalui USB. Layar menjadi hitam saat dalam mode DFU, tapi saat tersambung ke komputer yang menjalankan iTunes atau Finder, perintah berikut akan muncul: "iTunes (atau Finder) telah mendeteksi (iPad, iPhone, atau iPod touch) dalam mode Pemulihan. Pengguna harus memulihkan (iPad, iPhone, atau iPod touch) ini sebelum perangkat dapat digunakan dengan iTunes (atau Finder)."

modul keamanan perangkat keras (HSM) Komputer khusus tahan perusakan yang melindungi dan mengelola kunci digital.

NAND Memori kilat non-volatil.

nonce Angka unik sekali pakai yang digunakan di berbagai protokol keamanan.

pembungkusan kunci Dengan mengenkripsi satu kunci dengan kunci lain, iOS dan iPadOS menggunakan pembungkusan kunci NIST AES, sesuai dengan RFC 3394.

pemetaan sudut alur kerutan Representasi matematis dari arah dan lebar kerutan yang diekstrak dari bagian sidik jari.

Pengacakan Tata Letak Ruang Alamat (ASLR) Teknik yang diterapkan oleh sistem operasi untuk mempersulit eksploitasi oleh bug perangkat lunak. Dengan memastikan bahwa alamat dan ofset memori tidak dapat diprediksi, kode eksploitasi tidak dapat mengodekan paksa nilai ini.

pengaitan Proses pengubahan kode sandi pengguna menjadi kunci kriptografis dan diperkuat dengan UID perangkat. Proses ini membantu memastikan bahwa serangan brute-force harus dilakukan di perangkat tertentu, dan oleh karena itu, menjadi terbatas dan tidak dapat dilakukan secara paralel. Algoritme pengaitan adalah PBKDF2, yang menggunakan kunci AES dengan UID perangkat sebagai fungsi semu acak (PRF) untuk setiap iterasi.

Pengenal Sumber Seragam (URI) String karakter yang mengidentifikasi sumber berbasis web.

pengesahan perangkat lunak sistem Proses yang menggabungkan kunci kriptografis yang tersedia di perangkat keras dengan layanan online untuk memeriksa bahwa hanya perangkat lunak asli dari Apple, yang sesuai dengan perangkat yang didukung, disuplai dan diinstal saat pembaruan.

pengontrol memori Subsistem di sistem pada keping yang mengontrol antarmuka antara sistem pada keping dan memori utamanya.

Pengontrol SSD Subsistem perangkat keras yang mengelola media penyimpanan (solid-state drive).

Penyimpanan Dapat Dihapus Area khusus penyimpanan NAND, digunakan untuk menyimpan kunci kriptografis, yang dapat diakses secara langsung dan dihapus dengan aman. Meskipun tidak menyediakan perlindungan jika perangkat berada di tangan penyerang, kunci yang disimpan di Penyimpanan Dapat Dihapus dapat digunakan sebagai bagian dari hierarki kunci untuk memfasilitasi penghapusan cepat dan keamanan berkelanjutan.

Perlindungan Data Mekanisme perlindungan file dan rantai kunci untuk perangkat Apple yang didukung. Perlindungan Data juga dapat merujuk ke API yang digunakan app untuk melindungi file dan item rantai kunci.

Perlindungan Integritas Koprosesor Sistem (SCIP) Mekanisme yang digunakan oleh Apple yang dirancang untuk mencegah modifikasi firmware koprosesor.

Perlindungan Kunci yang Disegel (SKP) Teknologi di Perlindungan Data yang melindungi, atau *menyegel*, kunci enkripsi dengan pengukuran perangkat lunak sistem dan kunci yang hanya tersedia di perangkat keras (seperti UID Secure Enclave).

Pertukaran Diffie-Hellman Kurva Eliptis Sementara (ECDHE) Mekanisme pertukaran kunci berdasarkan kurva eliptis. ECDHE memungkinkan dua pihak untuk menyepakati kunci rahasia dengan cara yang mencegah kunci untuk ditemukan oleh pengintai yang mengawasi pesan antara kedua pihak.

profil penyedia Daftar properti (file .plist) yang ditandatangani Apple yang berisi kumpulan entitas dan hak yang memungkinkan app untuk diinstal dan diuji di perangkat iOS atau iPadOS. Profil penyedia pengembangan membuat daftar perangkat yang telah dipilih pengembang untuk distribusi ad hoc, dan profil penyedia distribusi berisi ID app dari app yang dikembangkan perusahaan.

rantai kunci Infrastruktur dan kumpulan API yang digunakan oleh sistem operasi Apple dan app pihak ketiga untuk menyimpan dan mengambil kata sandi, kunci, dan info pengesahan sensitif lainnya.

Register Kemajuan Boot (BPR) Kumpulan tanda pada perangkat keras di sistem pada keping (SoC) yang dapat digunakan perangkat lunak untuk melacak mode boot yang diaktifkan perangkat, seperti mode Peningkatan Firmware Perangkat (DFU) dan mode Pemulihan. Setelah diatur, tanda Register Kemajuan Boot tidak dapat dibersihkan. Ini memungkinkan perangkat lunak berikutnya untuk mendapatkan indikator tepercaya dari status sistem.

ROM Boot Kode paling pertama yang dijalankan oleh prosesor perangkat saat boot pertama. Sebagai bagian integral dari prosesor, ROM Boot tidak dapat diubah oleh Apple atau penyerang.

sepOS Firmware Secure Enclave, berdasarkan versi mikrokernel L4 khusus Apple.

sirkuit terpadu (IC) Juga disebut *keping mikro*.

sistem pada keping (SoC) Sirkuit terpadu (IC) yang menggabungkan beberapa komponen ke dalam satu keping. Prosesor Aplikasi, Secure Enclave, dan koprosesor lain merupakan komponen SoC.

Unit Manajemen Memori Input/Output (IOMMU) Unit manajemen memori input/output. Subsistem dalam keping terintegrasi yang mengontrol akses ke ruang alamat dari perangkat dan periferal input/output lainnya.

Vault Data Mekanisme—diberlakukan oleh kernel—untuk melindungi dari akses tanpa izin ke data terlepas dari apakah app yang meminta di-sandbox.

xART Singkatan dari Anti-Pemutaran Ulang yang Diperluas. Sekumpulan layanan yang menyediakan penyimpanan persisten yang dienkripsi dan disahkan untuk Secure Enclave dengan kemampuan anti-pemutaran ulang berdasarkan arsitektur penyimpanan fisik. Lihat Komponen Penyimpanan Aman.

XNU Kernel di pusat sistem operasi Apple. XNU diasumsikan sebagai tepercaya, dan memberlakukan tindakan pengamanan seperti penandatanganan kode, penggunaan mekanisme sandbox, pemeriksaan hak, dan Pengacakan Tata Letak Ruang Alamat (ASLR).

XProtect Di macOS, teknologi antivirus untuk deteksi berbasis tanda tangan dan penghapusan malware.

Riwayat revisi dokumen

Riwayat revisi dokumen

Tanggal	Ringkasan
Desember 2022	Topik ditambahkan: • Perlindungan Data Lanjutan untuk iCloud Topik diperbarui: • Tinjauan keamanan iCloud • Enkripsi iCloud • Keamanan Cadangan iCloud • Keamanan kontak pemulihan akun • Keamanan Kontak Pewaris

Tanggal	Ringkasan
Mei 2022	Diperbarui untuk: • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 Topik ditambahkan: • Pembatasan recoveryOS yang dipasangkan • Versi Sistem Operasi Lokal (love) • Berbagi kesehatan • Keamanan kontak pemulihan akun • Keamanan Kontak Pewaris • Keamanan Tap to Pay on iPhone • Mengakses dengan Dompet Apple • Jenis info pengesahan akses • ID di Dompet Apple • Aksesori HomeKit berkemampuan Siri Topik diperbarui: • Magic Keyboard dengan Touch ID • Face ID, Touch ID, kode sandi, dan kata sandi • Keamanan pencocokan wajah • Kartu Kilat dengan cadangan daya • Mode boot untuk Mac dengan Apple silicon • Konten file LocalPolicy untuk Mac dengan Apple silicon • Keamanan volume sistem yang ditandatangani di iOS, iPadOS, dan macOS • Keamanan sistem untuk watchOS • Perangkat Riset Keamanan Apple • Peran Apple File System • Melindungi akses app ke data pengguna • Pengantar keamanan app untuk macOS • Perlindungan dari malware di macOS • Tinjauan keamanan iCloud • Penyelarasan rantai kunci aman • Pemulihan Rantai Kunci iCloud aman • Membayar dengan kartu menggunakan Apple Pay • Pass nirkontak di Apple Pay • Menjadikan kartu tidak dapat digunakan dengan Apple Pay • Pengajuan Apple Card • Keamanan Apple Cash • Menambahkan kartu transit dan eMoney ke Dompet Apple • Mengamankan Apple Messages for Business • Keamanan FaceTime • Keamanan kunci mobil di iOS • Keamanan Apple Configurator Topik dihapus: • Aksesori HomeKit dan iCloud

Tanggal	Ringkasan
Mei 2021	Diperbarui untuk: • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 Topik ditambahkan: • Magic Keyboard dengan Touch ID. • Tujuan dan koneksi aman ke Secure Enclave. • Buka Otomatis dan Apple Watch. • Hash Manifes Image4 CustomOS (coih). Topik yang diedit: • Menambahkan dua transaksi Mode Kilat baru di Kartu Kilat dengan cadangan daya. • Mengedit ringkasan fitur Secure Enclave. • Konten pembaruan perangkat lunak ditambahkan ke Multi-Boot Aman (smb3). • Konten tambahan untuk Perlindungan Kunci yang Disegel (SKP).

Tanggal	Ringkasan
Februari 2021	Diperbarui untuk: • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 Topik ditambahkan: • Implementasi iBoot yang aman bagi memori • Proses boot untuk Mac dengan Apple silicon • Mode boot untuk Mac dengan Apple silicon • Kontrol kebijakan keamanan Disk Mulai untuk Mac dengan Apple silicon • Pembuatan dan manajemen kunci penandatanganan LocalPolicy • Konten file LocalPolicy untuk Mac dengan Apple silicon • Keamanan volume sistem yang ditandatangani di iOS, iPadOS, dan macOS • Perangkat Riset Keamanan Apple • Pengawasan Kata Sandi • Keamanan IPv6 • Keamanan kunci mobil di iOS Topik diperbarui: • Secure Enclave • Pemutusan mikrofon perangkat keras • Lingkungan recoveryOS dan diagnostik untuk Mac berbasis Intel • Perlindungan akses memori langsung untuk komputer Mac • Ekstensi kernel di macOS • Perlindungan Integritas Sistem • Keamanan sistem untuk watchOS • Mengelola FileVault di macOS • Akses app ke kata sandi yang disimpan • Rekomendasi keamanan kata sandi • Keamanan Apple Cash • Mengamankan Apple Messages for Business • Privasi Wi-Fi • Keamanan Kunci Aktivasi • Keamanan Apple Configurator
April 2020	Diperbarui untuk: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Pembaruan: • Pemutusan mikrofon iPad ditambahkan ke Pemutusan mikrofon perangkat keras. • Vault Data ditambahkan ke Melindungi akses app ke data pengguna. • Pembaruan ke Mengelola FileVault di macOS dan Alat baris perintah. • Tambahan alat Penghapus Malware di Perlindungan dari malware di macOS. • Pembaruan ke Keamanan iPad bersama di iPadOS.

Tanggal	Ringkasan
Desember 2019	Digabung dengan Petunjuk Keamanan iOS, Tinjauan Keamanan macOS, dan Tinjauan Keping Keamanan T2 Apple Diperbarui untuk: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Kontrol Privasi, Siri dan Saran Siri, dan Pencegahan Pelacakan Pintar Safari telah dihapus. Lihat https://www.apple.com/id/privacy/ untuk informasi terbaru terkait fitur tersebut.
Mei 2019	Diperbarui untuk iOS 12.3 • Dukungan untuk TLS 1.3 • Revisi deskripsi untuk keamanan AirDrop • Mode DFU dan mode Pemulihan • Persyaratan kode sandi untuk koneksi aksesori
November 2018	Diperbarui untuk iOS 12.1 • FaceTime Grup
September 2018	Diperbarui untuk iOS 12 Secure Enclave • Perlindungan Integritas OS • Kartu Kilat dengan cadangan daya • Mode DFU dan mode Pemulihan • Aksesori Remote TV HomeKit • Pass nirkontak • Kartu ID pelajar • Saran Siri • Pintasan di Siri • App Pintasan • Manajemen kata sandi pengguna • Durasi Layar • Sertifikasi dan program keamanan
Juli 2018	Diperbarui untuk iOS 11.4 • Kebijakan biometrik • HomeKit • Apple Pay • Obrolan Bisnis • Pesan di iCloud • Apple Business Manager
Desember 2017	Diperbarui untuk iOS 11.2 • Apple Pay Cash

Tanggal	Ringkasan
Oktober 2017	Diperbarui untuk iOS 11.1 • Sertifikasi dan program keamanan • Touch ID/Face ID • Catatan Bersama • CloudKit dan enkripsi ujung ke ujung • Pembaruan TLS • Apple Pay, Membayar dengan Apple Pay di web • Saran Siri • iPad Bersama
Juli 2017	Diperbarui untuk iOS 10.3 • Secure Enclave • Perlindungan Data File • Kantong Kunci • Sertifikasi dan program keamanan • SiriKit • HealthKit • Keamanan Jaringan • Bluetooth • iPad Bersama • Mode Hilang • Kunci Aktivasi • Kontrol Privasi
Maret 2017	Diperbarui untuk iOS 10 Keamanan Sistem • Kelas Perlindungan Data • Sertifikasi dan program keamanan • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Masuk tunggal • Apple Pay, Membayar dengan Apple Pay di web • Penyediaan kartu prabayar, kredit, dan debit • Saran Safari
Mei 2016	Diperbarui untuk iOS 9.3 • ID Apple yang Dikelola • Autentikasi dua faktor untuk ID Apple • Kantong Kunci • Sertifikasi Keamanan • Mode Hilang, Kunci Aktivasi • Catatan Aman • Apple School Manager • iPad Bersama

Tanggal	Ringkasan
September 2015	Diperbarui untuk iOS 9 Kunci Aktivasi Apple Watch • Kebijakan kode sandi • Dukungan API Touch ID • Perlindungan Data di A8 menggunakan AES-XTS • Kantong kunci untuk pembaruan perangkat lunak tanpa pengawasan • Pembaruan sertifikasi • Model kepercayaan app perusahaan • Perlindungan Data untuk penanda Safari • Keamanan Transpor App • Spesifikasi VPN • Akses Jarak Jauh iCloud untuk HomeKit • Kartu Imbalan Apple Pay, app penerbit kartu Apple Pay • Indeks Spotlight di perangkat • Model Pemasangan iOS • Apple Configurator 2 • Pembatasan

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

ID028-00625