Sikkerhed på Apples platforme

Maj 2022

Indhold

Sikkerhed på Apples platforme

Introduktion til sikkerhed på Apples platforme

Apple indarbejder sikkerhed helt ind i kernen på sine platforme. På grundlag af sin erfaring med at skabe et af verdens mest avancerede operativsystemer til mobile enheder har Apple udviklet sikkerhedsarkitekturer, der opfylder de særlige krav til mobile enheder, ure, computere og enheder i hjemmet.

Alle Apple-enheder kombinerer *hardware*, *software* og *tjenester*, der er designet til at arbejde sammen for at give den maksimale sikkerhed og en transparent brugeroplevelse med det ultimative mål, at personlige oplysninger opbevares og behandles sikkert. Eksempelvis er chips og sikkerhedshardware designet af Apple drivkraften bag vigtige sikkerhedsfunktioner. Og beskyttelsesforanstaltninger i software har til formål at beskytte operativsystemet og apps fra tredjeparter. Endelig sørger tjenester for at levere sikre softwareopdateringer i rette tid, skabe et beskyttet miljø til apps og give mulighed for sikker kommunikation og betalinger. Det betyder, at Apple-enheder beskytter ikke blot enheden og dens data, men hele økosystemet, herunder det, som brugerne foretager sig lokalt, på netværk og med vigtige tjenester på internettet.

Vi designer vores produkter, så de er enkle, intuitive og effektive og samtidig sikre. Vigtige sikkerhedsfunktioner som f.eks. enhedskryptering baseret på hardware kan ikke slås fra ved en fejl. Andre funktioner, f.eks. Face ID og Touch ID, forbedrer brugeroplevelsen ved at gøre det enklere og mere intuitivt at sikre enheden. Mange af disse funktioner er slået til som standard, så brugerne eller it-afdelingerne ikke behøver at foretage omfattende konfigurationer.

Denne dokumentation indeholder detaljer om, hvordan sikkerhedsteknologi og -funktioner er implementeret på Apple-platforme. Den hjælper også organisationer med at kombinere Apple-platformenes sikkerhedsteknologi og -funktioner med deres egne strategier og procedurer med henblik på at opfylde deres særlige sikkerhedsbehov.

Indholdet er inddelt i følgende emneområder:

- **Hardwaresikkerhed og biometri:** De chips og den hardware, der danner grundlag for sikkerheden på Apple-enheder, herunder Apple Silicon, Secure Enclave, kryptografiske moduler, Face ID og Touch ID
- **Systemsikkerhed:** De integrerede hardware- og softwarefunktioner, der muliggør sikker start, opdatering og løbende afvikling af Apples operativsystemer
- **Kryptering og databeskyttelse:** Den arkitektur og det design, der beskytter brugerdata, hvis enheden bliver væk eller stjålet, eller hvis en uautoriseret person eller proces forsøger at bruge eller modificere den
- **App-sikkerhed:** Den software og de tjenester, der skaber et sikkert miljø til apps og gør det muligt at afvikle dem sikkert uden at bringe platformens integritet i fare
- **Sikkerhedstjenester:** Apples tjenester til identifikation, administration af adgangskoder, betalinger, kommunikation og lokalisering af mistede enheder
- **Netværkssikkerhed:** Netværksprotokoller, der er standard i branchen, og som leverer sikker godkendelse og kryptering af data under overførsler
- **Sikkerhed i Developer Kits:** Framework-"kits" til sikker og privat administration af hjem og sundhed og udbredelse af funktioner på Apple-enheder og i Apple-tjenester til apps fra tredjeparter
- **Sikker administration af enheder:** Metoder, der gør det muligt at administrere Apple-enheder, bidrage til at forhindre uautoriseret brug og slå ekstern sletning til, hvis en enhed bliver væk eller bliver stjålet

Fokus på sikkerhed

Apple fokuserer på at hjælpe med at beskytte kunderne ved hjælp af førende teknologier inden for anonymitet og sikkerhed, der har til formål at beskytte personlige oplysninger, og ved hjælp af metoder, der hjælper med at beskytte virksomhedens data i et virksomhedsmiljø. Apple belønner personer for deres arbejde med at afsløre sårbarheder ved at udlove en sikkerhedsdusør fra Apple. Der findes flere oplysninger om programmet og dusørkategorierne på https://developer.apple.com/security-bounty/.

Vi har et sikkerhedsteam, der udelukkende beskæftiger sig med at yde support til Apples produkter. Teamet foretager sikkerhedsrevisioner og -test af produkter, både dem, der er ved at blive udviklet, og dem, der er frigivet. Apples team leverer også sikkerhedsværktøjer og -uddannelse og holder aktivt øje med mulige trusler og rapporter om nye sikkerhedsproblemer. Apple er medlem af FIRST (Forum of Incident Response and Security Teams).

Apple arbejder hele tiden på at skubbe grænserne for, hvad der er muligt inden for sikkerhed og anonymitet. Apple bruger specialchips til hele produktserien – fra Apple Watch til iPhone, iPad og til T2-sikkerhedschippen og Apple Silicon i Mac – til at foretage effektive beregninger og danne grundlag for sikkerheden. Apple Silicon danner f.eks. grundlaget for sikker start, Face ID og Touch ID og Databeskyttelse. Derudover er sikkerhedsfunktioner på enheder med Apple Silicon, f.eks. beskyttelse af kernens integritet, koder til markørgodkendelse og hurtige begrænsninger i adgang, med til at hindre almindelige typer cyberangreb. Derved minimeres den skade, der kan opstå, hvis det på en eller anden måde lykkes en hacker at afvikle kode.

Organisationer opfordres til at gennemgå deres it- og sikkerhedspolitik for at sikre, at de til fulde udnytter de omfattende sikkerhedsfunktioner og lag med sikkerhedsteknologi, som er indbygget i disse platforme.

Du kan få mere at vide om, hvordan du rapporterer problemer til Apple og abonnerer på sikkerhedsnotifikationer, i Rapportering af en sikkerheds- og anonymitetssårbarhed.

Apple mener, at anonymitet er en grundlæggende menneskeret, og har utallige indbyggede kontrolforanstaltninger og -muligheder, der giver brugerne mulighed for at bestemme, hvordan og hvornår apps må bruge deres oplysninger, og hvilke oplysninger de må bruge. Du kan læse mere om Apples tilgang til anonymitet, kontrolforanstaltninger vedr. anonymitet på Apple-enheder og Apples anonymitetspolitik på https://www.apple.com/dk/privacy**.**

Bemærk: Medmindre andet er anført, dækker denne dokumentation følgende operativsystemversioner: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 og watchOS 8.5.

Hardwaresikkerhed og biometri

Oversigt over hardwaresikkerhed

Sikker software afhænger af, at hardwaren har indbygget sikkerhed. Det er årsagen til, at Apple-enheder – med iOS, iPadOS, macOS, tvOS og watchOS – har sikkerhedsfunktioner, der er integreret i silicium. Disse funktioner omfatter blandt andet en CPU, som driver sikkerhedsfunktioner til systemet, og en ekstra chip, der er dedikeret til sikkerhedsfunktioner. Hardware med fokus på sikkerhed følger princippet om at understøtte begrænsede og separat definerede funktioner for at gøre angrebsfladen mindre. Disse komponenter inkluderer en Boot ROM, som danner en hardwaretillidsrod til sikker start, dedikerede AES-moduler til effektiv og sikker kryptering og en Secure Enclave. *Secure Enclave* er en SoC (System on Chip), der findes i alle nyere iPhone-, iPad-, Apple Watch-, Apple TV- og HomePod-enheder og på en Mac med Apple Silicon og Mac-computere med Apple T2-sikkerhedschippen. Selve Secure Enclave følger samme designprincip som SoC'en og indeholder sin egen adskilte Boot ROM og sit eget AES-modul. Secure Enclave danner også grundlag for sikker generering og opbevaring af de nøgler, der bruges til at kryptere data under opbevaring, og den beskytter og evaluerer de biometriske data til Face ID og Touch ID.

Kryptering af lagringsplads skal være hurtig og effektiv. Den skal samtidig sørge for, at de data (eller det *nøglemateriale*), den bruger til at etablere kryptografiske nøglerelationer, ikke risikerer at blive opsnappet. AES-hardwaremodulet løser dette problem ved at foretage hurtig kryptering og dekryptering, *samtidig med at arkiver skrives og læses*. En særlig kanal fra Secure Enclave stiller nødvendigt nøglemateriale til rådighed for AES-modulet, uden at oplysningerne kan ses af app-processoren (eller CPU'en) eller operativsystemet. Det er med til at sikre, at Apples databeskyttelses- og FileVault-teknologier beskytter brugernes arkiver uden at videregive krypteringsnøgler med lang levetid.

Apple har designet Sikker start med henblik på at beskytte software på laveste niveau mod modificering og på kun at tillade, at godkendt operativsystemsoftware fra Apple indlæses under starten. Sikker start har sit udgangspunkt i uforanderlig kode med navnet Boot ROM, som integreres under fremstillingen af Apple SoC og betragtes som *hardwaretillidsroden*. På Mac-computere med en T2-chip starter tilliden til sikker macOS-start med T2-chippen. (Både T2-chippen og Secure Enclave udfører også deres egen sikre startproces med hver sin separate Boot ROM – det svarer præcis til den måde, som chips i A-serien og M1-chipfamilien starter sikkert på).

Secure Enclave behandler også ansigts- og fingeraftryksdata fra Face ID- og Touch ID-sensorer i Apple-enheder. Det gør godkendelsen sikker, uden at brugerens biometriske data afsløres. Det giver også brugerne mulighed for at opnå større sikkerhed i kraft af længere og mere komplekse adgangskoder og i mange situationer også hurtig godkendelse af adgang eller køb.

Sikkerhed i Apple SoC

Chips designet af Apple udgør en fælles arkitektur på tværs af alle Apple-produkter og er nu grundlaget for Mac såvel som iPhone, iPad, Apple TV og Apple Watch. I mere end 10 år har Apples designere af chips i verdensklasse arbejdet med at udvikle og finjustere Apples SoC'er (System on Chip). Resultatet er en skalerbar arkitektur, der er designet til alle enheder, som er førende i branchen med hensyn til sikkerhedsfunktioner. Dette fælles grundlag for sikkerhedsfunktioner er kun muligt for en virksomhed, der designer sine egne chips til at fungere med dens software.

Apple Silicon er udviklet og fremstillet til specifikt at levere de sikkerhedsfunktioner, som er beskrevet nedenfor.

Funktion	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	M1-familien
Beskyttelse af kernens integritet	✓	✓	✓	✓	✓	✓
Hurtige begrænsninger i adgangen		✓	✓	✓	✓	✓
Beskyttelse af systemhjælpeprocessorers integritet			✓	✓	✓	✓
Koder til markørgodkendelse			✓	✓	✓	✓
Sidebeskyttelseslag		✓	✓	✓	✓	Se bemærkning nedenfor.

Bemærk: PPL (Page Protection Layer) kræver, at platformen *kun* afvikler signeret og godkendt kode. Det er en sikkerhedsmodel, der ikke er relevant i macOS.

Chips designet af Apple giver specifikt mulighed for at levere de databeskyttelsesfunktioner, som er beskrevet nedenfor.

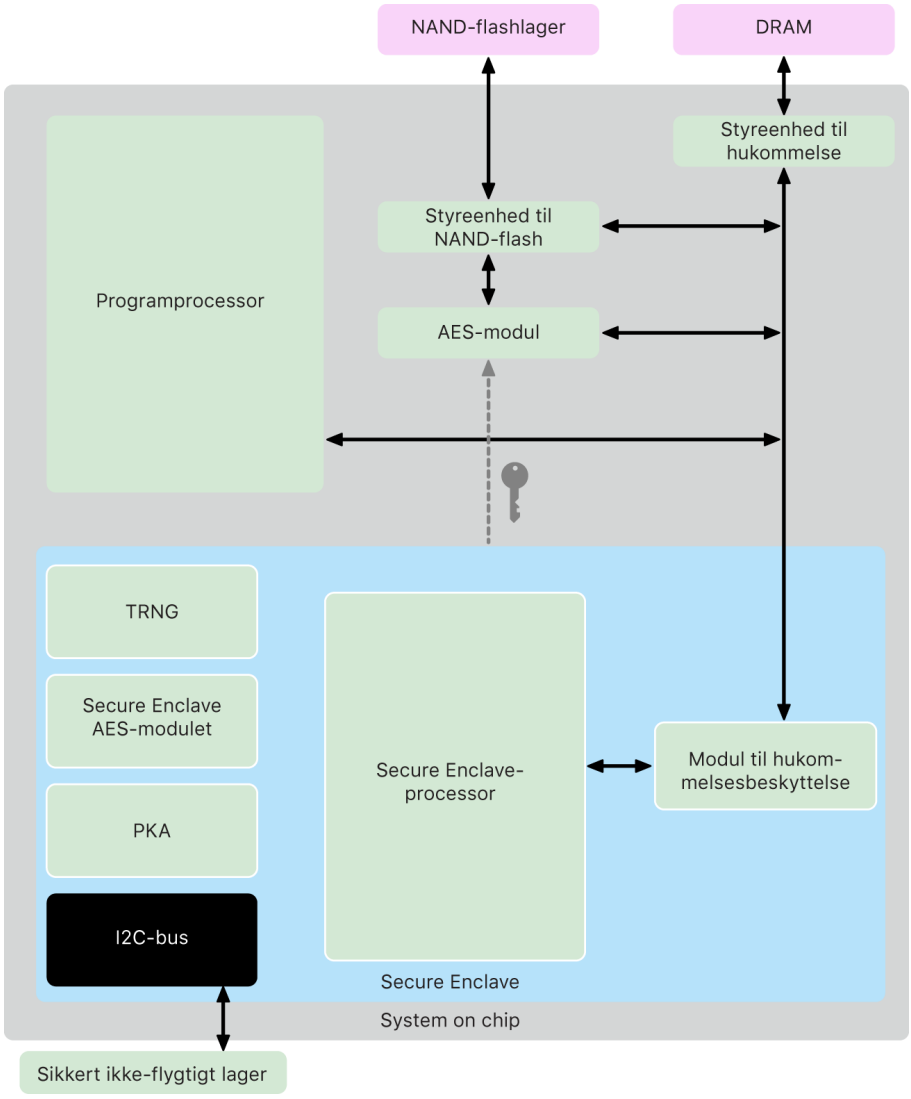
Funktion	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1-familien
Sealed Key Protection (SKP)	✓	✓	✓	✓	✓
macOS-gendannelse - alle klasser i Databeskyttelse er beskyttet	✓	✓	✓	✓	✓
Andre starttilstande i forbindelse med DFU, Diagnosticering og opdatering – data i klasse A, B og C er beskyttet			✓	✓	✓

Secure Enclave

Secure Enclave er et dedikeret, sikkert subsystem i de nyeste versioner af iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch og HomePod.

Oversigt

Secure Enclave er et dedikeret, sikkert subsystem, som er integreret i Apples SoC'er (System on Chip). Secure Enclave er isoleret fra hovedprocessoren for at give et ekstra lag sikkerhed og er designet til at beskytte følsomme brugerdata, også selvom app-processorens kerne bliver kompromitteret. Den følger samme designprincipper som SoC – en Boot ROM, der etablerer en hardwaretillidsrod, et AES-modul, der giver effektive og sikre kryptografiske funktioner, og beskyttet hukommelse. Selvom Secure Enclave ikke har nogen lagringsplads, har den en metode til at opbevare oplysninger sikkert på tilsluttet lagringsplads, der er adskilt fra det NAND-flashlager, der bruges af app-processoren og operativsystemet.



Secure Enclave er en hardwarefunktion på de fleste versioner af iPhone, iPad, Mac, Apple TV, Apple Watch og HomePod:

- iPhone 5s og nyere modeller
- iPad Air og nyere modeller
- MacBook Pro-computere med Touch Bar (2016 og 2017) og Apple T1-chippen
- Intel-baserede Mac-computere med Apple T2-sikkerhedschippen
- Mac-computere med Apple Silicon
- Apple TV HD og nyere modeller
- Apple Watch Series 1 og nyere modeller
- HomePod og HomePod mini

Secure Enclave-processor

Secure Enclave-processoren leverer den primære computerkraft til Secure Enclave. Secure Enclave-processoren er dedikeret til kun at blive brugt af Secure Enclave for at skabe størst mulig isolation. Det er med til at forhindre angreb på sidekanaler, som afhænger af, at ondsindet software deler samme kerne til afvikling som den software, der angribes.

Secure Enclave-processoren bruger en Apple-tilpasset version af L4-mikrokernen. Den er designet til at fungere effektivt ved en lavere clockfrekvens, der bidrager til at beskytte den mod angreb rettet mod tidsmåling eller strømforbrug. Fra A11 og S4 inkluderer Secure Enclave-processoren et modul til hukommelsesbeskyttelse og krypteret hukommelse med funktioner, der forhindrer genafspilning, sikker start, en dedikeret tilfældighedsgenerator og sit eget AES-modul.

Modul til hukommelsesbeskyttelse

Secure Enclave arbejder fra et dedikeret område i enhedens DRAM-hukommelse. Flere beskyttelseslag holder Secure Enclaves beskyttede hukommelse isoleret fra app-processoren.

Når enheden starter, opretter Secure Enclave Boot ROM en tilfældig midlertidig nøgle til beskyttelse af hukommelsen, som anvendes af modulet til hukommelsesbeskyttelse. Hver gang, Secure Enclave skriver til sit dedikerede hukommelsesområde, udfører modulet til hukommelsesbeskyttelse kryptering af hukommelsesblokken vha. AES i Mac-tilstanden XEX (xor-encrypt-xor) og beregning af et CMAC-godkendelsesmærke (Cipher-based Message Authentication Code) til hukommelsen. Modulet til hukommelsesbeskyttelse gemmer godkendelsesmærket sammen med den krypterede hukommelse. Når Secure Enclave læser hukommelsen, kontrolleres godkendelsesmærket af modulet til hukommelsesbeskyttelse. Hvis godkendelsesmærket stemmer overens, dekrypteres hukommelsesblokken af modulet til hukommelsesbeskyttelse. Hvis mærket ikke matcher, sender modulet til hukommelsesbeskyttelse signal om en fejl til Secure Enclave. Efter en fejl i godkendelse af hukommelse holder Secure Enclave op med at acceptere anmodninger, indtil systemet genstartes.

Fra Apple A11 og S4 SoC'er og frem tilføjer modulet til hukommelsesbeskyttelse også beskyttelse mod genafspilning for Secure Enclave-hukommelsen. Modulet til hukommelsesbeskyttelse er med til at forhindre genafspilning af data, der er kritiske for sikkerheden, ved at gemme et entydigt engangsnummer (kaldes en *nonce-værdi*) til hukommelsesblokken sammen med godkendelsesmærket. Nonce-værdien bruges som et ekstra "tweak" til CMAC-godkendelsesmærket. Nonce-værdierne for alle hukommelsesblokke beskyttes vha. et integritetshierarki med rod i dedikeret SRAM i selve Secure Enclave. Til skrivninger *opdaterer* modulet til hukommelsesbeskyttelse nonce-værdien og hvert niveau i integritetshierarkiet op til SRAM. Til læsninger *kontrollerer* modulet til hukommelsesbeskyttelse nonce-værdien og hvert niveau i integritetshierarkiet op til SRAM. Nonce-værdier, der ikke matcher, håndteres på samme måde som godkendelsesmærker, der ikke matcher.

På Apple A14, A15, M1-familien og nyere SoC'er understøtter modulet til hukommelsesbeskyttelse to midlertidige nøgler til beskyttelse af hukommelsen. Den første bruges til data, som kun Secure Enclave skal kende, og den anden bruges til data, der deles med Sikker Neural Engine.

Modulet til hukommelsesbeskyttelse arbejder inline og er gennemsigtigt over for Secure Enclave. Secure Enclave læser og skriver hukommelse, som om den var almindelig ikke-krypteret DRAM, hvorimod en iagttager uden for Secure Enclave kun ser den krypterede og godkendte version af hukommelsen. Resultatet er en effektiv beskyttelse af hukommelsen, uden at det går ud over ydeevnen eller softwarens kompleksitet.

Secure Enclave Boot ROM

Secure Enclave omfatter en dedikeret Secure Enclave Boot ROM. Ligesom app-processor-Boot ROM er Secure Enclave Boot ROM en uforanderlig kode, som etablerer hardware-tillidsroden til Secure Enclave.

Ved systemstart tildeler iBoot et dedikeret område i hukommelsen til Secure Enclave. Før hukommelsen bruges, starter Secure Enclave Boot ROM modulet til hukommelsesbeskyttelse for at give kryptografisk beskyttelse af Secure Enclaves hukommelse.

Derefter sender app-processoren sepOS-billedet til Secure Enclave Boot ROM. Når Secure Enclave Boot ROM har kopieret sepOS-billedet til det Secure Enclaves beskyttede hukommelse, kontrollerer Secure Enclave Boot ROM billedets kryptografiske hash-værdi og signatur for at bekræfte, at sepOS er godkendt til at køre på enheden. Hvis sepOS-billedet er signeret korrekt til at køre på enheden, overfører Secure Enclave Boot ROM kontrollen til sepOS. Hvis signaturen ikke er gyldig, er Secure Enclave Boot ROM indstillet til at forhindre yderligere brug af Secure Enclave, indtil næste gang chippen nulstilles.

På Apple A10 og nyere SoC'er låser Secure Enclave Boot ROM en hash-værdi for sepOS i et register dedikeret til dette formål. Public Key Accelerator bruger denne hash-værdi til nøgler, der er knyttet til operativsystemet.

Secure Enclave-startovervågning

På Apple A13 og nyere SoC'er omfatter Secure Enclave en startovervågning, der har til formål at sikre stærkere integritet i hash-værdien for det startede sepOS.

Ved systemstart er konfigurationen af Secure Enclave-processorens SCIP (System Coprocessor Integrity Protection) med til at forhindre, at Secure Enclave-processoren kan afvikle anden kode end Secure Enclave Boot ROM. Startovervågningen er med til at forhindre Secure Enclave i at ændre SCIP-konfigurationen direkte. For at det indlæste sepOS skal kunne afvikles, sender Secure Enclave Boot ROM en anmodning til startovervågningen med adressen og størrelsen på det indlæste sepOS. Når startovervågningen modtager anmodningen, nulstiller den Secure Enclave-processoren, og den hash-behandler det indlæste sepOS, opdaterer SCIP-indstillingerne for at tillade afvikling af det indlæste sepOS og starter afvikling i den netop indlæste kode. Mens systemet fortsat starter, bruges den samme proces, når ny kode kan afvikles. Hver gang opdaterer startovervågningen en løbende hash-værdi for startprocessen. Startovervågningen inkluderer også kritiske sikkerhedsparametre i den løbende hash-værdi.

Når starten er gennemført, færdiggør startovervågningen den løbende hash-værdi og sender den til Public Key Accelerator (PKA), hvor den skal bruges til nøgler, der er knyttet til operativsystemet. Processen er designet, så tilknytning af nøgler til operativsystemet ikke kan tilsidesættes, heller ikke hvis der er en sårbarhed i Secure Enclave Boot ROM.

Sand tilfældighedsgenerator

Den sande tilfældighedsgenerator (True Random Number Generator – TRNG) bruges til at generere sikre tilfældige data. Secure Enclave bruger TRNG, hver gang den genererer en tilfældig kryptografisk nøgle, et tilfældigt basistal for en nøgle eller anden entropi. TRNG er baseret på flere ringoscillatorer, der efterbehandles med CTR_DRBG (en algoritme baseret på blokkodeværdier med tællerfunktion).

Kryptografiske rodnøgler

Secure Enclave omfatter kryptografiske rodnøgler med UID (Unique ID). UID er unik for hver enkelt enhed, og den er ikke forbundet med andre id'er på enheden.

Et tilfældigt genereret UID brændes fast i SoC'en på fremstillingstidspunktet. Fra A9-SoC'er genereres UID af Secure Enclave TRNG under fremstillingen og skrives til sikringerne ved hjælp af en softwareproces, der udelukkende afvikles i Secure Enclave. Processen sørger for, at UID ikke kan ses uden for enheden under fremstillingen, og at hverken Apple eller nogen af Apples leverandører kan få adgang til det eller opbevare det.

sepOS benytter UID til at beskytte hemmeligheder, der er specifikke for enheden. UID gør det muligt at knytte data kryptografisk til en bestemt enhed. Det udnyttes f.eks. af det nøglehierarki, som beskytter arkivsystemet. Det omfatter UID, så der ikke er adgang til arkiverne, hvis det interne SSD-lager flyttes fysisk fra en enhed til en anden. Data til Face ID og Touch ID er en anden beskyttet hemmelighed, der er specifik for en enhed. På en Mac er det kun fuldstændig intern lagringsplads, der er knyttet til AES-modulet, der krypteres på dette niveau. F.eks. bliver hverken eksterne lagringsenheder, der er tilsluttet via USB, eller PCIe-baseret lagringsplads, der føjes til Mac Pro 2019, krypteret på denne måde.

Secure Enclave har også et enhedsgruppe-id (GID), som er fælles for alle enheder, der bruger en given SoC (så f.eks. alle enheder, der bruger Apple A15 SoC, deler det samme GID).

Der er ikke adgang til UID og GID gennem JTAG (Joint Test Action Group) eller andre fejlfindingsgrænseflader.

Secure Enclave AES-modulet

Secure Enclave AES-modulet er en hardwareblok, som bruges til at udføre symmetrisk kryptografi baseret på AES-kode. AES-modulet er designet til at undgå, at det lækker information, ved at bruge tidsmåling og Static Power Analysis (SPA). Fra og med A9-SoC'en omfatter AES-modulet også DPA-modforholdsregler (Dynamic Power Analysis).

AES-modulet understøtter hardware- og softwarenøgler. Hardwarenøgler afledes fra Secure Enclaves UID eller GID. Disse nøgler bliver ved med at være i AES-modulet og gøres ikke synlige, ikke engang for sepOS-software. Selvom software kan anmode om kryptering og dekryptering med hardwarenøgler, kan software ikke udtrække nøglerne.

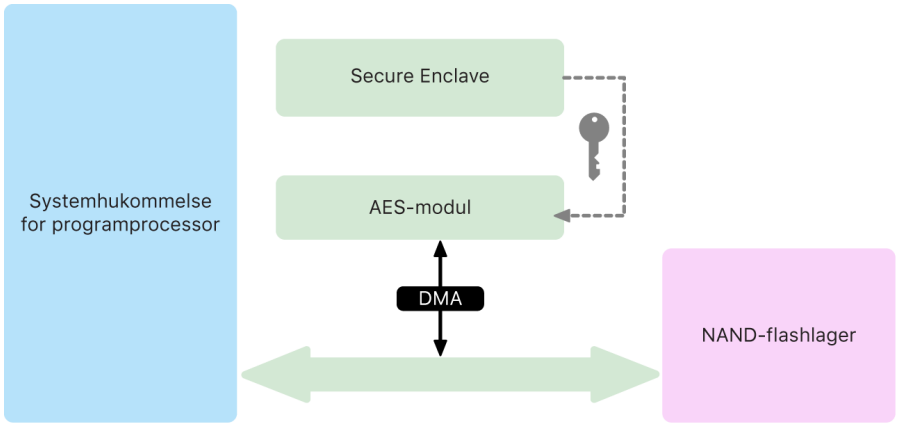
På Apple A10 og nyere SoC'er omfatter AES-modulet låsbare seed bits, som varierer de nøgler, der afledes fra UID eller GID. Dermed kan adgang til data være betinget af enhedens driftstilstand. Låsbare seed bits bruges f.eks. til at afvise adgang til adgangskodebeskyttede data, når der startes i DFU-funktion (Device Firmware Update). Du kan få flere oplysninger i Koder og adgangskoder.

AES-modul

Alle Apple-enheder med Secure Enclave har også et dedikeret modul til AES256-kryptering ("AES-modulet") , der er indbygget i DMA-stien (Direct Memory Access) mellem den ikke-flygtige NAND-flashhukommelse og den primære systemhukommelse, hvilket gør krypteringen af arkiver yderst effektiv. I A9-processorer og nyere processorer i A-serien er flashlagerets subsystem placeret i en isoleret bus, der udelukkende tildeles adgang til hukommelse med brugerdata gennem modulet til DMA-kryptering.

Ved start genererer sepOS en midlertidig nøgle til nøgleindpakning vha. TRNG. Secure Enclave overfører denne nøgle til AES-modulet vha. dedikerede ledninger, der har til formål at forhindre, at software uden for Secure Enclave får adgang til den. sepOS kan derefter bruge den midlertidige nøgle til nøgleindpakning til at pakke arkivnøgler, som app-processoren skal bruge til arkivsystemets driver. Når arkivsystemets driver læser eller skriver et arkiv, sender driveren den indpakkede nøgle til AES-modulet, som pakker nøglen ud. AES-modulet afslører aldrig den udpakkede nøgle for software.

Bemærk: AES-modulet er en anden komponent end Secure Enclave og Secure Enclaves AES-modul, men dens funktion er tæt forbundet med Secure Enclave som vist nedenfor.



Public Key Accelerator

Public Key Accelerator (PKA) er en hardwareblok, som bruges til at udføre handlinger med asymmetrisk kryptografi. PKA understøtter algoritmerne RSA og ECC (Elliptic Curve Cryptography) til signering og kryptering. PKA er designet til at undgå, at den lækker information som følge af angreb rettet mod tidsmåling og sidekanaler, f.eks. SPA og DPA.

PKA understøtter software- og hardwarenøgler. Hardwarenøgler afledes fra Secure Enclaves UID eller GID. Disse nøgler bliver ved med at være i PKA og gøres ikke synlige, ikke engang for sepOS-software.

Fra A13 SoC'er og frem har formelle godkendelsesteknikker vist, at PKA's krypteringsimplementeringer er matematisk korrekte.

På Apple A10 og nyere SoC'er understøtter PKA nøgler, der er knyttet til operativsystemet. Det kaldes også SKP (Sealed Key Protection). Disse nøgler genereres vha. en kombination af enhedens UID og hash-værdien for det sepOS, der kører på enheden. Hash-værdien leveres af Secure Enclave Boot ROM eller af Secure Enclave-startovervågningen på Apple A13 og nyere SoC'er. Nøglerne bruges også til at kontrollere sepOS-versionen, når der sendes anmodninger til visse Apple-tjenester, og til at øge sikkerheden for data, der er beskyttet med en kode, ved at bidrage til at forhindre adgang til nøglemateriale, hvis der foretages kritiske ændringer af systemet uden brugerens godkendelse.

Sikkert ikke-flygtigt lager

Secure Enclave er udstyret med en dedikeret, sikker og permanent lagringsenhed. Det sikre og permanente lager er forbundet med Secure Enclave via en dedikeret I2C bus, så det kun er Secure Enclave, der kan få adgang til det. Alle krypteringsnøgler til brugerdata er baseret på entropi, som opbevares i det permanente Secure Enclave-lagringsområde.

På enheder med A12, S4 og nyere SoC'er er Secure Enclave parret med en komponent til sikker opbevaring, så der kan opbevares entropi. Selve komponenten til sikker opbevaring er designet med uforanderlig ROM-kode, en hardwarebaseret tilfældighedsgenerator, en unik kryptografisk nøgle for hver enhed, kryptografimoduler og registrering af fysisk manipulation. Secure Enclave og komponenten til sikker opbevaring kommunikerer vha. en krypteret og godkendt protokol, der giver eneadgang til entropien.

Enheder lanceret for første gang i efteråret 2020 eller senere er udstyret med 2. generation af komponenten til sikker opbevaring. 2. generation af komponenten til sikker opbevaring tilføjer tæller-lockboxes. Hver tæller-lockbox opbevarer en 128-bit saltnøgle, en 128-bit værdi til kodekontrol, en 8-bit tæller og en 8-bit værdi for maksimalt antal forsøg. Adgang til disse lockboxes sker vha. en krypteret og godkendt protokol.

Tæller-lockboxes indeholder den entropi, der kræves for at låse brugerdata beskyttet med kode op. Adgang til brugerdata kræver, at den parrede Secure Enclave udleder entropiværdien til den rigtige kode ud fra brugerens kode og Secure Enclaves UID. Det er ikke muligt at få kendskab til brugerens kode ved hjælp af forsøg på oplåsning, der kommer fra en anden kilde end den parrede Secure Enclave. Hvis det maksimale antal kodeforsøg overskrides (f.eks. 10 forsøg på iPhone), slettes alle kodebeskyttede data af komponenten til sikker opbevaring.

Secure Enclave sender entropiværdien til koden og værdien for maksimalt antal forsøg til komponenten til sikker opbevaring for at oprette en tæller-lockbox. Komponenten til sikker opbevaring genererer saltværdien ved hjælp af sin tilfældighedsgenerator. Den udleder derefter en værdi til kontrol af koden og en lockbox-entropiværdi fra den modtagne entropiværdi til koden, den entydige kryptografiske nøgle til komponenten til sikker opbevaring og saltværdien. Komponenten til sikker opbevaring initialiserer tæller-lockboxen med antallet 0, den leverede værdi for maksimalt antal forsøg, den afledte værdi til kontrol af koden og saltværdien. Derefter returnerer komponenten til sikker opbevaring den genererede lockbox-entropiværdi til Secure Enclave.

Hvis Secure Enclave senere vil hente lockbox-entropiværdien fra en tæller-lockbox, sender Secure Enclave entropiværdien for koden til komponenten til sikker opbevaring. Komponenten til sikker opbevaring starter med at øge tælleren til lockboxen. Hvis den øgede tæller overstiger værdien for det maksimale antal forsøg, bliver tæller-lockboxen slettet af komponenten til sikker opbevaring. Hvis det maksimale antal forsøg ikke er nået, forsøger komponenten til sikker opbevaring at aflede værdien til kontrol af koden og lockbox-entropiværdien vha. samme algoritme, som blev brugt til at oprette tæller-lockboxen. Hvis den afledte værdi til kontrol af koden svarer til den lagrede værdi til kontrol af koden, returnerer komponenten til sikker opbevaring lockbox-entropiværdien til Secure Enclave og nulstiller tælleren.

De nøgler, der bruges til at få adgang til adgangskodebeskyttede data, er forankret i den entropi, der opbevares i tæller-lockboxes. Du kan få flere oplysninger i Oversigt over Databeskyttelse.

Den sikre, ikke-flygtige lagringsplads bruges til alle tjenester, der forhindrer genafspilning, i Secure Enclave. Tjenester, der forhindrer genafspilning, i Secure Enclave bruges til at tilbagekalde data i løbet af hændelser, der markerer grænserne for forhindring af genafspilning, herunder, men ikke begrænset til, følgende:

- Skift af kode
- Valg eller fravalg af Face ID og Touch ID
- Tilføjelse eller fjernelse af et Face ID-ansigt eller et Touch ID-fingeraftryk
- Nulstilling af Face ID og Touch ID
- Tilføjelse eller fjernelse af et Apple Pay-kort
- Slet alt indhold og alle indstillinger

I arkitekturer uden en komponent til sikker opbevaring sørger EEPROM (Electrically Erasable Programmable Read-Only Memory) for at levere sikre lagringstjenester til Secure Enclave. På samme måde som komponenten til sikker opbevaring er EEPROM tilsluttet og kun tilgængelig fra Secure Enclave, men den indeholder ikke dedikerede hardwaresikkerhedsfunktioner og garanterer heller ikke eneadgang til entropi (bortset fra egenskaberne ved dens fysiske tilslutning) eller funktionaliteten ved en tæller-lockbox.

Sikker Neural Engine

På enheder med Face ID konverterer Sikker Neural Engine 2D-billeder og -dybdekort til en matematisk gengivelse af en brugers ansigt.

På A11 til og med A13 SoC'er er Sikker Neural Engine integreret i Secure Enclave. Sikker Neural Engine bruger direkte hukommelsesadgang (DMA) til at opnå en høj ydeevne. En IOMMU (input-output memory management unit) under sepOS-kernens kontrol begrænser den direkte adgang til godkendte hukommelsesområder.

Fra A14 og M1-familien er Sikker Neural Engine implementeret som en sikker funktion i app-processorens neurale modul. En dedikeret kontrolenhed til hardwaresikkerhed skifter mellem opgaver fra app-processoren og Secure Enclave og nulstiller ved hvert skift status for Neural Engine for at opretholde beskyttelsen af Face ID-data. Et dedikeret modul anvender hukommelseskryptering, godkendelse og adgangskontrol. Det bruger samtidig en særskilt kryptografisk nøgle og et særskilt hukommelsesudsnit til at begrænse Sikker Neural Engine til godkendte hukommelsesområder.

Overvågning af strømforbrug og tidsmåling

Alle elektroniske produkter er designet til at arbejde inden for et begrænset spændings- og frekvensområde. Hvis de arbejder uden for dette område, kan der kan opstå fejl i elektronikken, og som følge heraf kan sikkerhedsforanstaltninger blive omgået. Secure Enclave er designet med overvågningskredsløb, der er med til at sikre, at spænding og frekvens holder sig inden for et sikkert område. Disse overvågningskredsløb er designet til at have et langt større driftsområde end resten af Secure Enclave. Hvis overvågningsfunktionerne opdager et ulovligt driftspunkt, stopper urene i Secure Enclave automatisk og starter først efter næste nulstilling af SoC.

Opsummering af Secure Enclave-funktioner

Bemærk: A12-, A13-, S4- og S5-produkter, der blev lanceret i efteråret 2020, har 2. generation af komponenten til sikker opbevaring, mens tidligere produkter baseret på disse SoC'er har 1. generation af komponenten til sikker opbevaring.

SoC	Modul til hukommelsesbeskyttelse	Sikker opbevaring	AES-modul	PKA
A8	Kryptering og godkendelse	EEPROM	Ja	Nej
A9	Kryptering og godkendelse	EEPROM	DPA-beskyttelse	Ja
A10	Kryptering og godkendelse	EEPROM	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
A11	Kryptering, godkendelse, forhindring af genafspilning	EEPROM	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
A12 (Apple-enheder lanceret inden efteråret 2020)	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 1. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
A12 (Apple-enheder lanceret efter efteråret 2020)	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 2. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
A13 (Apple-enheder lanceret inden efteråret 2020)	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 1. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystem og startovervågning
A13 (Apple-enheder lanceret efter efteråret 2020)	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 2. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystem og startovervågning
A14, A15	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 2. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystem og startovervågning
S3	Kryptering og godkendelse	EEPROM	DPA-beskyttelse og låsbare seed bits	Ja
S4	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 1. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
S5 (Apple-enheder lanceret inden efteråret 2020)	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 1. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
S5 (Apple-enheder lanceret efter efteråret 2020)	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 2. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
S6, S7	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 2. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
T2	Kryptering og godkendelse	EEPROM	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystemet
M1-familien	Kryptering, godkendelse, forhindring af genafspilning	Komponenten til sikker opbevaring 2. gen.	DPA-beskyttelse og låsbare seed bits	Nøgler knyttet til operativsystem og startovervågning

Face ID og Touch ID

Sikkerhed ved Face ID og Touch ID

Et centralt element i sikkerheden på Apple-enheder er koder og adgangskoder. Brugerne har samtidig behov for nem adgang til deres enheder, ofte mere end hundrede gange om dagen. Biometrisk godkendelse er en metode, der bevarer sikkerheden ved en stærk adgangskode – og måske endda skabe en endnu stærkere kode eller adgangskode, fordi den ikke skal indtastes manuelt – og samtidig gøre det nemt at låse op med et enkelt tryk med en finger eller med et blik. Face ID og Touch ID erstatter ikke en kode eller adgangskode, men i de fleste situationer gør de adgangen hurtigere og lettere.

Hovedprincippet for Apples biometriske sikkerhedsarkitektur er en stringent adskillelse af den biometriske sensors og Secure Enclaves ansvarsområde og en sikker forbindelse mellem de to. Sensoren registrerer det biometriske billede og sender det sikkert til Secure Enclave. Under tilmelding krypterer og opbevarer Secure Enclave-processerne data fra de tilhørende skabeloner til Face ID og Touch ID. Secure Enclave sammenligner indgående data fra den biometriske sensor med de gemte skabeloner for at afgøre, om enheden skal låses op, eller om den skal oplyse, at den har fundet et gyldigt match (ved Apple Pay, brug i apps og anden brug af Face ID og Touch ID). Arkitekturen understøtter enheder, der både har sensoren og Secure Enclave (f.eks. iPhone, iPad og mange Mac-computere), og den er i stand til fysisk at udskille sensoren til en ekstern enhed, som derefter indgår i et sikkert par med Secure Enclave i en Mac med Apple Silicon.

Face ID-sikkerhed

Vha. et enkelt blik låser Face ID understøttede Apple-enheder op på en sikker måde. Det er en intuitiv og sikker godkendelsesmetode, der styres af TrueDepth-kamerasystemet, som bruger avanceret teknologi til at kortlægge en brugers ansigtsgeometri. Face ID bruger neurale netværk til at vurdere opmærksomhed, sammenligne ansigtstræk og modvirke spoofing, så en bruger kan låse sin telefon op med et blik – selv med maske på ved brug af understøttede enheder. Face ID tilpasser sig automatisk ændringer i udseende og beskytter omhyggeligt brugerens biometriske datas anonymitet og sikkerhed.

Face ID er designet med henblik på at bekræfte, at brugerens opmærksomhed er rettet mod enheden, foretage godkendelse på en robust måde med et lavt antal forkerte genkendelser og modvirke både digital og fysisk spoofing.

TrueDepth-kameraet ser automatisk efter brugerens ansigt, når brugeren afbryder vågeblus på en Apple-enhed med Face ID ved at løfte enheden eller trykke på skærmen, og når disse enheder forsøger at godkende brugeren for at vise en indgående notifikation, eller en understøttet app anmoder om godkendelse via Face ID. Når et ansigt registreres, kontrollerer Face ID, at brugeren er opmærksom og har til hensigt at låse enheden op, ved at registrere, om brugerens øjne er åbne, og om brugerens opmærksomhed er rettet mod enheden. Af hensyn til tilgængeligheden slås kontrol af opmærksomhed fra for Face ID, når VoiceOver er slået til, og kan eventuelt slås helt fra. Registrering af opmærksomhed er altid nødvendig, når Face ID bruges med en maske.

Når TrueDepth-kameraet har bekræftet, at et ansigt har opmærksomheden rettet mod det, projicerer og læser kameraet tusindvis af infrarøde prikker og danner et dybdekort af ansigtet sammen med et infrarødt 2D-billede. Disse data bruges til at oprette en sekvens med 2D-billeder og dybdekort, som signeres digitalt og sendes til Secure Enclave. For at modvirke både digital og fysisk spoofing anbringer TrueDepth-kameraet sekvensen med registrerede 2D-billeder og dybdekort i tilfældig rækkefølge og projicerer et tilfældigt mønster, der er specifikt for enheden. Et område i Sikker Neural Engine – der er beskyttet i Secure Enclave – omformer disse data til en matematisk repræsentation og sammenligner repræsentationen med de registrerede ansigtsdata. De registrerede ansigtsdata er i sig selv en matematisk repræsentation af brugerens ansigt med forskellige udtryk og fra forskellige synsvinkler.

Touch ID-sikkerhed

Touch ID er det system til registrering af fingeraftryk, der gør sikker adgang til understøttede Apple-enheder hurtigere og nemmere. Denne teknologi læser fingeraftryksdata fra alle vinkler og lærer mere om en brugers fingeraftryk med tiden, fordi sensoren konstant udvider fingeraftrykskortet, efterhånden som flere overlappende detaljer identificeres for hver brug.

Apple-enheder med en Touch ID-sensor kan låses op med et fingeraftryk. Touch ID erstatter ikke behovet for en kode til enheden eller en brugeradgangskode. De skal stadig bruges, efter at enheden er startet eller genstartet, eller brugeren har logget ud (på en Mac). I nogle apps kan Touch ID også bruges i stedet for koden til en enhed eller brugerens adgangskode, f.eks. til at låse noter beskyttet med adgangskode op i Noter, låse websteder beskyttet med nøgleringen op og låse adgangskoder op til understøttede apps. I nogle situationer skal der dog altid bruges en kode til enheden eller brugerens adgangskode (f.eks. til at ændre en eksisterende kode eller adgangskode eller til at fjerne registrerede fingeraftryk eller oprette nye).

Når fingeraftrykssensoren registrerer en finger, får den det avancerede billedbehandlingsarray til at scanne fingeren og sender scanningen til Secure Enclave. Hvilken kanal, der bruges til at sikre forbindelsen, afhænger af om Touch ID-sensoren er indbygget i enheden med Secure Enclave eller er placeret i en separat ekstern enhed.

Mens scanningen af fingeraftryk vektoriseres forud for analysen, opbevares rasterscanningen midlertidigt i et krypteret hukommelsesområde i Secure Enclave, hvorefter den kasseres. Under analysen sammenlignes kortlægningen af rillers vinkel og forløb i underhuden. Under denne proces kasseres data om meget "små detaljer om fingrene", der ellers kunne bruges til at rekonstruere brugerens ægte fingeraftryk. Resultatet af processen er et kort med detaljer, der under tilmelding opbevares i krypteret format, der kun kan læses af Secure Enclave som en skabelon til senere sammenligninger, men uden identitetsoplysninger. Disse data forlader aldrig enheden. De sendes ikke til Apple, og de indgår ikke i sikkerhedskopieringer af enheden.

Sikkerhed i indbygget Touch ID-kanal

Kommunikationen mellem Secure Enclave og den indbyggede Touch ID-sensor sker via en seriel busgrænseflade til eksterne enheder. Processoren sender dataene videre til Secure Enclave, men kan ikke selv læse dem. De krypteres og godkendes med en sessionsnøgle, der forhandles med en delte nøgle, som blev tilknyttet hver Touch ID-sensor og dens tilhørende Secure Enclave på fabrikken. Den delte nøgle til de enkelte Touch ID-sensorer er stærk, tilfældig og entydig. Ved udveksling af sessionsnøglen bruges AES-nøgleindpakning, hvor begge parter leverer en tilfældig nøgle, der fastlægger sessionsnøglen og bruger en transportkryptering, som både leverer godkendelse og datafortrolighed (ved hjælp af AES-CCM).

Magic Keyboard med Touch ID

Magic Keyboard med Touch ID (og Magic Keyboard med Touch ID og numerisk blok) stiller en Touch ID-sensor til rådighed i et eksternt tastatur, der kan bruges til alle Mac-computere med Apple Silicon. Magic Keyboard med Touch ID har rollen som biometrisk sensor – det opbevarer ikke biometriske skabeloner, udfører ikke biometriske sammenligninger og håndhæver ikke sikkerhedspolitikker (som at stille krav om indtastning af adgangskode efter 48 timer uden en oplåsning). Touch ID-sensoren i Magic Keyboard med Touch ID skal danne et sikkert par med Secure Enclave på Mac, før den kan bruges, hvorefter Secure Enclave foretager tilmeldinger og sammenligninger og håndhæver sikkerhedspolitikker på samme måde, som den ville gøre med en indbygget Touch ID-sensor. Apple foretager pardannelsen under produktionen af et Magic Keyboard med Touch ID, som følger med en Mac. Pardannelsen kan også udføres af brugeren, hvis der er behov for det. Et Magic Keyboard med Touch ID kun indgå i et sikkert par med en Mac ad gangen, men en Mac kan indgå i sikre par med op til fem forskellige Magic Keyboard med Touch ID-tastaturer.

Magic Keyboard med Touch ID og indbyggede Touch ID-sensorer er kompatible. Hvis en finger, der er blevet tilmeldt på en indbygget Touch ID-sensor på en Mac, bruges på et Magic Keyboard med Touch ID, foretager Secure Enclave sammen ligningen og finder et match – og omvendt.

Sikker pardannelse og dermed kommunikation mellem Secure Enclave i Mac og Magic Keyboard med Touch ID understøttes ved, at tastaturet er udstyret med en Public Key Accelerator-hardwareblok (PKA), der sørger for bemyndigelse, og med hardwarebaserede nøgler, som skal udføre de nødvendige kryptografiske processer.

Sikker pardannelse

Inden et Magic Keyboard med Touch ID kan bruges til Touch ID-funktioner, skal det indgå i et sikkert par med Mac. Pardannelsen foregår ved, at Secure Enclave i Mac og PKA-blokken i Magic Keyboard med Touch ID udveksler offentlige nøgler, der er forankret i den godkendte Apple CA, og bruger hardwareindbyggede attesteringsnøgler og midlertidige ECDH-nøgler til at bevidne deres identitet. På Mac beskyttes disse data af Secure Enclave, og på Magic Keyboard med Touch ID beskyttes de af PKA-blokken. Efter sikker pardannelse krypteres alle Touch ID-data, der udveksles mellem Mac og Magic Keyboard med Touch ID, med AES-GCM med en nøglelængde på 256 bit og med midlertidige ECDH-nøgler, som bruger NIST P-256-kurven, baseret på de gemte identiteter. (Almindelige tastetryk udveksles ved brug af Bluetooth-sikkerhed på samme måde som et Bluetooth-tastatur).

Sikker pardannelseshensigt

Før brugeren kan foretage visse Touch ID-funktioner første gang, f.eks. tilmelde et nyt fingeraftryk, skal brugeren fysisk bekræfte sin hensigt til at bruge et Magic Keyboard med Touch ID sammen med Mac. Fysisk hensigt bekræftes, ved at brugeren trykker to gange på afbryderknappen på Mac, når brugeren bliver bedt om det, eller ved at brugeren benytter et fingeraftryk, som tidligere er tilmeldt i Mac. Du kan få flere oplysninger i Sikker hensigt og sikre forbindelser til Secure Enclave.

Apple Pay-transaktioner kan godkendes med Touch ID eller ved indtastning af macOS-brugerens adgangskode og to tryk på Touch ID-knappen på Magic Keyboard med Touch ID. Sidstnævnte giver brugeren mulighed for at bekræfte sin fysiske hensigt uden et Touch ID-match.

Sikkerhed i Magic Keyboard med Touch ID-kanal

En sikker kommunikationskanal mellem Touch ID-sensoren i Magic Keyboard med Touch ID og Secure Enclave på den parrede Mac kræver følgende:

- Sikker pardannelse mellem PKA-blokken i Magic Keyboard med Touch ID og Secure Enclave som beskrevet ovenfor.
- En sikker kanal mellem Magic Keyboard med Touch ID-sensoren og tastaturets PKA-blok

Den sikre kanal mellem Magic Keyboard med Touch ID-sensoren og tastaturets PKA-blok etableres under produktionen ved hjælp af en delt unik nøgle. (Det er den samme teknik, som bruges til at skabe den sikre kanal mellem Secure Enclave på Mac-computere med Touch ID og dens indbyggede sensor).

Face ID, Touch ID, koder og adgangskoder

Brug af Face ID eller Touch ID forudsætter, at brugeren indstiller sin enhed, så der skal bruges en kode eller adgangskode til at låse den op. Når Face ID eller Touch ID finder et match, låses enheden op, uden at brugeren skal indtaste koden eller adgangskoden til enheden. Det betyder, at det er langt nemmere at benytte mere komplekse koder eller adgangskoder, fordi brugeren ikke behøver at indtaste dem så tit. Face ID og Touch ID erstatter ikke brugerens kode eller adgangskode, men giver nem adgang til enheden, hvis nøje fastlagte begrænsninger i forhold til tid og andre faktorer tillader det. Det er vigtigt, eftersom en stærk kode eller adgangskode udgør grundlaget for, hvordan en brugers iPhone, iPad, Mac eller Apple Watch beskytter brugerens data kryptografisk.

Behov for indtastning af kode eller adgangskode til enheden

Brugere kan altid bruge deres kode eller adgangskode i stedet for Face ID eller Touch ID, men der er situationer, hvor biometrisk godkendelse ikke kan bruges. Følgende sikkerhedskritiske handlinger kræver altid indtastning af en kode eller adgangskode:

- Opdatering af software
- Sletning af enheden
- Visning eller sletning af indstillinger til kode
- Installering af konfigurationsprofiler
- Oplåsning af vinduet Sikkerhed & anonymitet i Systemindstillinger på Mac
- Oplåsning af vinduet Brugere & grupper i Systemindstillinger på Mac (hvis FileVault er slået til)

Der kræves også en kode eller adgangskode i følgende situationer:

- Enheden er lige blevet tændt eller genstartet.
- Brugeren har logget ud af sin Mac-konto (eller har ikke logget ind endnu).
- Brugeren har ikke låst sin enhed op i mere end 48 timer.
- Brugeren har ikke brugt sin kode eller adgangskode til at låse enheden op i 156 timer (seks og en halv dag), og brugeren har ikke brugt biometrik til at låse enheden op i 4 timer.
- Enheden har modtaget en ekstern kommando til låsning.
- Brugeren sluttede slukning/Nødopkald SOS ved at holde enten lydstyrkeknappen eller knappen Vågeblus til/fra nede i 2 sekunder og derefter trykke på Annuller.
- Der var fem forgæves forsøg på at finde et biometrisk match (af hensyn til brugervenligheden vil enheden måske foreslå, at brugeren indtaster en kode eller adgangskode i stedet for at bruge biometri, efter et mindre antal forgæves forsøg).

Når Face ID med en maske er slået til på en iPhone, kan det bruges i 6,5 time efter en af følgende brugerhandlinger:

- Gennemført forsøg med Face ID-match (med eller uden maske)
- Kontrol af koden til enheden
- Oplåsning af enheden med Apple Watch

Når en af disse handlinger udføres, forlænges tidsrummet med yderligere 6,5 time.

Når Face ID eller Touch ID slås til på en iPhone eller iPad, låses enheden straks, når der trykkes på Vågeblus til/fra, og hver gang enheden går på vågeblus. Face ID og Touch ID kræver et biometrisk match – eller brug af koden – hver gang vågeblus afbrydes.

Sandsynligheden for, at en tilfældig person i befolkningen kan låse en brugers iPhone eller iPad op, er mindre end 1 ud af 1.000.000 med Face ID, også når brug af Face ID med maske er slået til. For en brugers iPhone, iPad, Mac-modeller med Touch ID og dem, der er parret med et Magic Keyboard, er det mindre end 1 ud af 50.000. Denne sandsynlighed stiger, hvis der er flere registrerede fingeraftryk (op til 1 ud af 10.000 ved fem fingeraftryk) eller udseender (op til 1 ud af 500.000 ved to udseender). Både Face ID og Touch ID tillader kun fem forgæves matchforsøg, før brugeren skal indtaste koden eller adgangskoden for at få adgang til sin enhed eller konto. Det giver ekstra beskyttelse. Med Face ID er sandsynligheden for et falsk match højere for:

- Tvillinger eller søskende, der ligner brugeren
- Børn under 13 år (fordi deres særlige ansigtstræk måske ikke er fuldt udviklet endnu)

Sandsynligheden øges desuden i disse to tilfælde, når Face ID bruges med en maske. Hvis en bruger er bekymret for et forkert match, anbefaler Apple at bruge en kode til godkendelse.

Sikkerhed ved sammenligning af ansigter

Sammenligning af ansigter udføres i Secure Enclave ved hjælp af neurale netværk, der er trænet med netop det formål for øje. Apple har udviklet de neurale netværk til sammenligning af ansigter ud fra en milliard billeder, herunder infrarøde billeder og dybdebilleder, der er indsamlet i undersøgelser, som deltagerne har givet deres samtykke til. Apple har derefter arbejdet med deltagere over hele verden for at opnå en repræsentativ gruppe personer med hensyn til køn, alder, etnicitet og andre faktorer. Undersøgelserne blev udvidet efter behov for at opnå stor nøjagtighed for forskelligartede brugere. Face ID er designet til at fungere med hatte, tørklæder, briller, kontaktlinser og mange typer solbriller. Face ID understøtter også oplåsning med en maske på iPhone 12 og nyere iPhone-modeller og iOS 15.4 eller en nyere version. Funktionen er desuden designet til at fungere indendørs og udendørs – selv når det er helt mørkt. Et ekstra neuralt netværk – der er trænet til at identificere og modvirke spoofing – beskytter mod forsøg på at låse enheden op med fotos eller masker. Face ID-data, inklusive matematiske repræsentationer af brugerens ansigt, krypteres og er kun tilgængelige for Secure Enclave. Disse data forlader aldrig enheden. De sendes ikke til Apple, og de indgår ikke i sikkerhedskopieringer af enheden. Under normal brug gemmes og krypteres følgende Face ID-data kun til brug for Secure Enclave:

- De matematiske repræsentationer af en brugers ansigt, der beregnes under registreringen.
- De matematiske repræsentationer af en brugers ansigt, der beregnes under visse forsøg på oplåsning, hvis Face ID vurderer, at de er nyttige tilføjelser til fremtidige sammenligninger.

Ansigtsbilleder, der registreres under normal brug, gemmes ikke, men slettes, så snart den matematiske repræsentation er beregnet, enten til registrering eller sammenligning med de registrerede Face ID-data.

Forbedring af genkendelse med Face ID

Face ID udvider sin gemte matematiske repræsentation over tid for at øge genkendelsesgraden og holde trit med de naturlige ændringer af ansigt og udseende. Når et ansigt er genkendt, kan Face ID bruge den netop beregnede matematiske repræsentation – hvis kvaliteten af den er god nok – til et begrænset antal yderligere genkendelser, før disse data kasseres. Hvis Face ID derimod ikke genkender et ansigt, men kvaliteten af sammenligningen er højere end en bestemt grænseværdi, og brugeren straks efter den manglende genkendelse indtaster sin kode, foretager Face ID en ny registrering og føjer den netop beregnede matematiske repræsentation til de registrerede Face ID-data. Disse nye Face ID-data kasseres, hvis brugeren ikke længere genkendes med dem, eller efter et bestemt antal genkendelser. De nye data kasseres også, når muligheden for at nulstille Face ID vælges. Med disse udvidelser kan Face ID holde trit med større ændringer af en brugers skæg eller makeup og samtidig mindske antallet af forkerte genkendelser.

Anvendelsesmuligheder for Face ID og Touch ID

Oplåsning af en enhed eller brugerkonto

Hvis Face ID eller Touch ID er slået fra, når en enhed eller konto låses, kasseres nøglerne til den højeste databeskyttelsesklasse, som opbevares i Secure Enclave. Der er ikke adgang til arkiverne og emnerne i nøgleringen i denne klasse, før brugeren låser enheden eller kontoen op ved at indtaste sin kode eller adgangskode.

Når Face ID eller Touch ID er slået til, kasseres nøglerne ikke, når enheden eller kontoen låses. De pakkes i stedet med en nøgle, der overføres til Face ID- eller Touch ID-subsystemet i Secure Enclave. Hvis enheden finder et match, når brugeren forsøger at låse enheden eller kontoen op, leverer enheden nøglen til udpakning af databeskyttelsesnøglerne, og enheden eller kontoen låses op. Processen giver ekstra beskyttelse, fordi subsystemerne til databeskyttelse og Face ID eller Touch ID skal samarbejde om at låse enheden op.

Når enheden starter igen, går de nøgler, som Face ID eller Touch ID skal bruge til at låse enheden eller kontoen op, tabt. De kasseres af Secure Enclave, når en betingelse, der kræver indtastning af kode eller adgangskode, er opfyldt.

Beskyttelse af køb med Apple Pay

Brugeren kan også bruge Face ID og Touch ID med Apple Pay til at foretage køb på en nem og sikker måde i butikker og apps og på internettet:

- *Brug af Face ID i butikker:* Før brugeren kan godkende en betaling i en butik med Face ID, skal brugeren bekræfte sin betalingshensigt ved at trykke to gange på sideknappen. Disse to tryk opfanger brugerens hensigt vha. en fysisk bevægelse, der er direkte knyttet til Secure Enclave og er modstandsdygtig over for svindel via en ondsindet proces. Brugeren godkender derefter vha. Face ID, før enheden placeres tæt på den kontaktløse betalingslæser. Brugeren kan vælge en anden Apple Pay-betalingsmetode efter godkendelse med Face ID og skal derefter godkendes igen, men behøver ikke at trykke to gange på sideknappen.

- *Brug af Face ID i apps og på internettet:* Før brugeren kan foretage en betaling fra apps og på internettet, bekræfter brugeren sin betalingshensigt ved at trykke to gange på sideknappen og godkender derefter betalingen med Face ID-genkendelse. Hvis Apple Pay-transaktionen ikke er gennemført senest 60 sekunder efter, at brugeren har trykket to gange på sideknappen, skal brugeren bekræfte sin betalingshensigt ved at trykke to gange igen.
- *Brug af Touch ID:* Brug af Touch ID bekræfter brugerens betalingshensigt med den bevægelse, der bruges til at aktivere Touch ID-sensoren, kombineret med genkendelse af brugerens fingeraftryk.

Brug af system-API'er

Apps fra tredjeparter kan bruge system-API'er til at bede brugeren om at legitimere sig vha. Face ID eller Touch ID eller en kode eller adgangskode. Apps, der understøtter Touch ID, understøtter automatisk Face ID uden nogen ændringer. Ved brug af Face ID eller Touch ID informeres appen kun om, hvorvidt godkendelsen lykkedes. Den kan ikke få adgang til Face ID, Touch ID eller de data, der er knyttet til den registrerede bruger.

Beskyttelse af emner i nøgleringen

Emner i nøgleringen kan også beskyttes med Face ID eller Touch ID, så de kun frigives af Secure Enclave, hvis der bliver fundet et match, eller hvis koden til enheden eller adgangskoden til kontoen indtastes. App-udviklere har API'er til kontrol af, om en bruger har indstillet en kode eller adgangskode, før de kræver, at Face ID, Touch ID eller en kode eller adgangskode bruges til at låse emner i nøgleringen op. App-udviklere kan gøre følgende:

- Bestemme, at handlinger, der er udført ved hjælp af godkendelses-API'et, ikke kan benytte en app-adgangskode eller enhedens kode. De kan sende en forespørgsel om, hvorvidt en bruger er registreret, og tillade, at Face ID eller Touch ID bruges som en ekstra faktor i sikkerhedsfølsomme apps.
- Generere og bruge ECC-nøgler (Elliptic Curve Cryptography) i Secure Enclave, som kan beskyttes med Face ID eller Touch ID. Handlinger med disse nøgler foretages altid i Secure Enclave, efter at Secure Enclave har godkendt brugen af dem.

Godkendelse af køb

Brugerne kan også konfigurere Face ID eller Touch ID til at godkende køb i iTunes Store, App Store, Apple Books og andre steder, så brugerne ikke behøver at indtaste adgangskoden til deres Apple-id. Når der foretages køb, kontrollerer Secure Enclave, at der har fundet en biometrisk godkendelse sted, og frigiver derefter ECC-nøgler, der bruges til at signere butiksanmodningen.

Sikker hensigt og sikre forbindelser til Secure Enclave

Sikker hensigt er en måde at bekræfte en brugers hensigt på uden at involvere operativsystemet eller app-processoren. Forbindelsen er et fysisk link – fra en fysisk knap til Secure Enclave – som findes i følgende enheder:

- iPhone X og nyere modeller
- Apple Watch Series 1 og nyere modeller
- iPad Pro (alle modeller)
- iPad Air (2020)
- Mac-computere med Apple Silicon

Med dette link kan brugerne bekræfte deres hensigt om at gennemføre en handling på en sådan måde, at selv ikke software, der afvikles med rettigheder som rod eller i kernen, kan foretage spoofing.

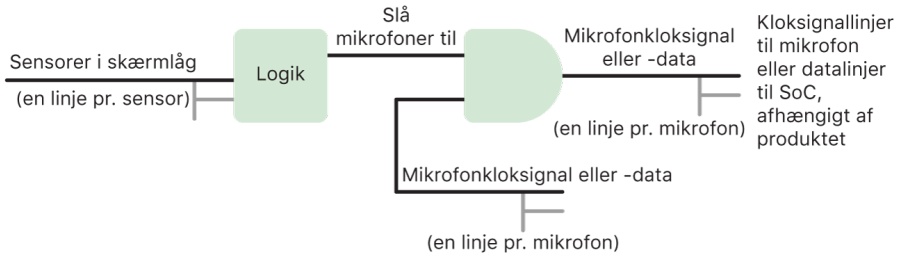
Funktionen bruges til at bekræfte brugerens hensigt under Apple Pay-transaktioner og under afslutning af pardannelse mellem et Magic Keyboard med Touch ID og en Mac med Apple Silicon. Bekræftelsen af brugerens hensigt består i to tryk på den relevante knap (Face ID) eller scanning af et fingeraftryk (Touch ID), når brugeren bliver bedt om det. Du kan få flere oplysninger i Beskyttelse af køb med Apple Pay. En lignende mekanisme – der er baseret på Secure Enclave og T2-firmwaren – understøttes på MacBook-modeller med Apple T2-sikkerhedschippen og uden Touch Bar.

Slå mikrofon fra via hardware

Alle bærbare Apple Silicon-baserede Mac-computere og bærbare Intel-baserede Mac-computere med Apple T2-sikkerhedschippen har en afbrydelsesfunktion i hardwaren, der slår mikrofonen fra, når låget lukkes. På 13" MacBook Pro- og MacBook Air-computere med T2-chippen, alle bærbare MacBook-computere med en T2-chip fra 2019 eller senere og alle bærbare Mac-computere med Apple Silicon er afbrydelsesfunktionen kun implementeret i hardwaren. Afbrydelsesfunktionen har til formål at forhindre software – selv software med rod- eller kernerettigheder i macOS og softwaren på T2-chippen eller anden firmware – i at gøre mikrofonen aktiv, når skærmen er slået ned. (Kameraet afbrydes ikke i hardwaren, fordi dets synsfelt er helt blokeret, når skærmen er slået ned).

Muligheden for at slå mikrofonen fra via hardware findes også på iPad-modeller fra starten af 2020 og frem. Når et MFi-kompatibelt etui (inklusive dem, der sælges af Apple) monteres på iPad og lukkes, slås mikrofonen fra via hardware. Det har til formål at forhindre, at mikrofonlyddata bliver tilgængelige for software – selv for software med rod- eller kernerettigheder i iPadOS og firmware på enheden.

Beskyttelsesfunktionerne i dette afsnit implementeres direkte med hardwarens logik i henhold til følgende kredsløbsdiagram:



I hvert produkt, hvor mikrofonen slås fra via hardware, registrerer en eller flere sensorer i låget, at låget eller etuiet lukkes fysisk. Det gør de ud fra en fysisk egenskab (f.eks. sensorer, der bruger Hall-effekt eller følger hængslets vinkel) i ændringen af lågets position. For sensorer, der kræver kalibrering, indstilles der parametre under produktion af enheden, og kalibreringsprocessen omfatter en permanent blokering via hardware af senere ændringer i sensorens følsomme parametre. Disse sensorer udsender et direkte hardwaresignal, der løber gennem et simpelt sæt hardwarelogik, som ikke kan programmeres om. Logikken leverer debounce, hysterese og/eller en forsinkelse på op til 500 ms, før mikrofonen slås fra. Afhængigt af produktet kan dette signal implementeres ved enten at deaktivere de linjer, der transporterer data mellem mikrofonen og SoC (System on Chip) eller en af de indgående linjer til mikrofonmodulet, som giver det mulighed for at være aktivt, f.eks. clock-linjen eller en lignende effektiv kontrolfunktion.

Ekspreskort og reservespænding

Hvis iOS ikke kører, fordi iPhone skal oplades, kan der stadig være nok batterispænding til at understøtte transaktioner med ekspreskort. Understøttede iPhone-enheder understøtter automatisk denne funktion med:

- Et betalings- eller rejsekort, der er valgt som ekspresrejsekort
- Studiekort med Ekspresfunktion slået til
- Bilnøgler med Ekspresfunktion slået til
- Nøgler til hjemmet med Ekspresfunktion slået til
- Kort til overnatningssteder eller adgangskort til virksomheder med Ekspresfunktion slået til

Ved tryk på sideknappen (eller på knappen Hjem på iPhone SE 2. generation) vises symbolet for lav batterispænding samt en tekst om, at ekspreskort kan bruges. NFC-kontrolenheden udfører transaktioner med ekspreskort under samme betingelser, som under afviklingen af iOS, bortset fra at transaktionerne kun vises med en haptisk notifikation (der vises ikke en tekstnotifikation). På iPhone SE 2. generation kan der gå et par sekunder, før gennemførte transaktioner vises på skærmen. Denne funktion er ikke tilgængelig, når brugeren har udført en standardnedlukning.

Systemsikkerhed

Oversigt over systemsikkerhed

Systemsikkerheden bygger på Apples unikke hardware og har til formål at styre adgangen til systemressourcer på Apple-enheder, uden at det går ud over brugervenligheden. Systemsikkerhed omfatter startprocessen, softwareopdateringer og beskyttelse af computersystemressourcer som CPU, hukommelse, disk, softwareapps og opbevarede data.

De nyeste versioner af Apples operativsystemer er de sikreste. En vigtig del af Apples sikkerhed er *Sikker start*, som beskytter systemet mod at blive inficeret med malware under starten af enheden. Den sikre startproces begynder med hardwaren og opbygger en godkendelseskæde gennem software, hvor hvert trin har til formål at sikre, at det næste fungerer korrekt, inden kontrollen gives videre. Denne sikkerhedsmodel understøtter ikke kun den almindelige startproces på Apple-enheder, men også de forskellige gendannelsesfunktioner og rettidige opdateringer på Apple-enheder. Underkomponenter som T2-chippen og Secure Enclave udfører også selv en sikker start for at sikre, at de kun starter godkendt kode fra Apple. Opdateringssystemet er udformet til at forhindre nedgraderingsangreb, så enhederne ikke kan rulles tilbage til ældre versioner af operativsystemet (som hackere ved, hvordan man kompromitterer) med henblik på at stjæle brugeroplysninger.

Apple-enheder indeholder også beskyttelsesforanstaltninger under start og drift, så deres integritet opretholdes under anvendelsen. Chippen designet af Apple i iPhone, iPad, Apple Watch, Apple TV, HomePod og Mac-computere med Apple Silicon skaber en fælles arkitektur til beskyttelse af operativsystemets integritet. macOS indeholder desuden et udvidet sæt beskyttelsesforanstaltninger, der kan konfigureres, og som understøtter de forskellige computermodeller, samt funktioner, der understøttes på alle Mac-hardwareplatforme.

Sikker start

Startprocessen for iOS- og iPadOS-enheder

Hvert trin i startprocessen indeholder komponenter, der er signeret kryptografisk af Apple for at sikre kontrol af integriteten, så startprocessen først fortsætter, når godkendelseskæden er verificeret. Disse komponenter omfatter bootloadere, kernen, kerneudvidelserne og mobilbasisbåndfirmwaren. Denne sikre startkæde har til formål at sikre, at software på laveste niveau ikke modificeres.

Når en iOS- eller iPadOS-enhed tændes, afvikler dens app-processor straks kode fra den skrivebeskyttede hukommelse, der kaldes Boot ROM. Denne uforanderlige kode, som er *tillidsroden i hardwaren*, defineres under chipfremstillingen og er implicit godkendt. Boot ROM-koden indeholder den offentlige nøgle fra Apples rodcertifikatmyndighed (CA), som bruges til at kontrollere, at bootloaderen iBoot er signeret af Apple, før indlæsningen af den tillades. Det er det første trin i den godkendelseskæde, hvor hvert trin kontrollerer, at det næste trin er signeret af Apple. Når iBoot er færdig med sine opgaver, kontrolleres og afvikles iOS- eller iPadOS-kernen af iBoot. På enheder med en A9-processor eller en tidligere processor i A-serien indlæses og godkendes et ekstra LLB-trin (Low Level Bootloader) af Boot ROM, og dette trin indlæser og godkender derefter iBoot.

Fejl under indlæsning eller godkendelse af efterfølgende trin håndteres forskelligt afhængigt af hardwaren:

- *Boot ROM kan ikke indlæse LLB (ældre enheder):* Skift til DFU-funktionen (Device Firmware Upgrade)
- *LLB eller iBoot:* Gendannelsesfunktion

I begge tilfælde skal enheden være forbundet med Finder (macOS 10.15 og nyere versioner) eller iTunes (i macOS 10.14 og tidligere versioner) via USB og være nulstillet.

BPR (Boot Progress Register) bruges af Secure Enclave til at begrænse adgangen til brugerdata i forskellige funktioner og opdateres, inden der skiftes til følgende funktioner:

- *DFU-funktion:* Indstilles af Boot ROM på enheder med en Apple A12 eller en nyere SoC
- *Gendannelsesfunktion:* Indstilles af iBoot på enheder med Apple A10, S2 eller en nyere SoC

På enheder med mobiladgang foretager mobilbasisbånd-subsystemet en ekstra, sikker startproces ved hjælp af software og nøgler, der er signeret og godkendt af basisbåndprocessoren.

Secure Enclave udfører også en sikker startproces, der kontrollerer, at dens software (sepOS) er godkendt og signeret af Apple.

Hukommelsessikker iBoot-implementering

I iOS 14 og iPadOS 14 har Apple ændret den C compiler-værktøjskæde, der bruges til at bygge bootloaderen iBoot, for at gøre det mere sikkert. Den ændrede værktøjskæde implementerer kode, der har til formål at forhindre sikkerhedsproblemer i forbindelse med hukommelse og type, som typisk ofte opstår i C-apps. Den kan f.eks. være med til at lukke de fleste af følgende typer sikkerhedshuller:

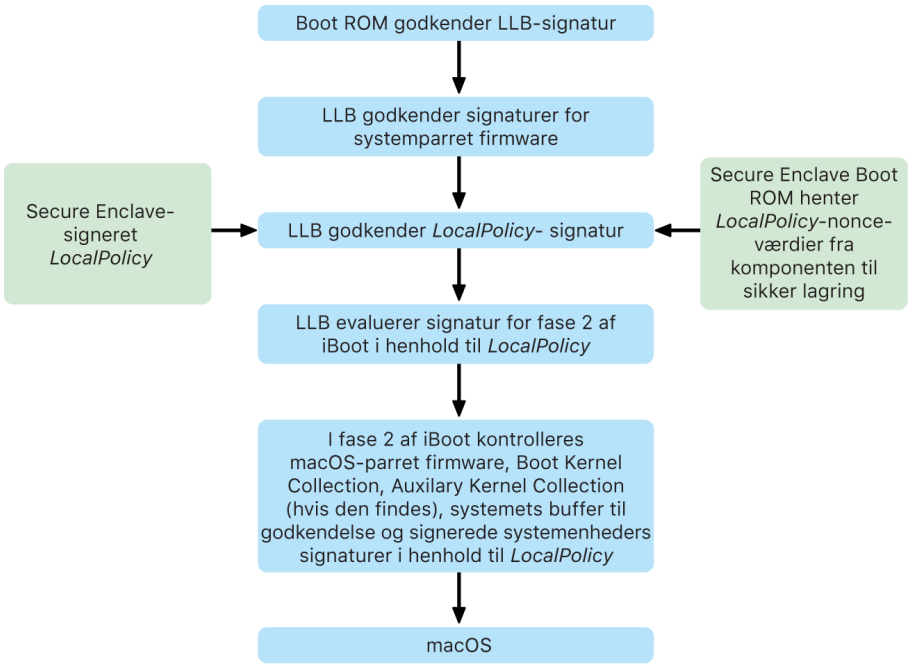
- Overløb i buffer – ved at sikre, at alle pointere overfører oplysninger om grænser, der godkendes ved adgang til hukommelsen
- Heap-udnyttelse – ved at adskille heap-data fra deres metadata og udføre nøjagtig registrering af fejltilstande såsom "double free"-fejl
- Typeforveksling – ved at sikre, at alle pointere overfører oplysninger om afviklingstype, der godkendes under pointer cast-handlinger
- Typeforveksling forårsaget af use "after free"-fejl – ved at adskille al dynamisk hukommelsesallokering efter statisk type

Teknologien findes på iPhone med Apple A13 Bionic-chippen eller en nyere chip og iPad med A14 Bionic-chippen.

Mac-computere med Apple Silicon

Startprocessen på en Mac-computer med Apple Silicon

Når en Mac med Apple Silicon tændes, foretager den en startproces, der er meget lig processen på iPhone og iPad.



Chippen afvikler kode fra Boot ROM i det første trin i godkendelseskæden. Sikker start til macOS på en Mac med Apple Silicon kontrollerer ikke kun selve koden til operativsystemet, men også sikkerhedspolitikkerne og endog kext'er (understøttes, men anbefales ikke), som er konfigureret af godkendte brugere.

Når LLB (Low Level Bootstrap) starter, godkender den derefter signaturerne og indlæser systemparret firmware til kerneelementer i intra-SoC, f.eks. styreenheder til lagringsplads, skærm, systemadministration og Thunderbolt. LLB har også ansvaret for at indlæse LocalPolicy, der er et arkiv, som er signeret af Secure Enclave-processoren. LocalPolicy-arkivet beskriver den konfiguration, som brugeren har valgt til sikkerhedspolitikker for systemstart og afvikling. LocalPolicy har samme datastrukturformat som alle andre startobjekter, men den signeres lokalt af en privat nøgle. Der er kun adgang til denne nøgle i en bestemt computers Secure Enclave, frem for at den signeres af en central Apple-server (som det sker for softwareopdateringer).

Med henblik på at forhindre genafspilning af tidligere LocalPolicy-forekomster skal LLB slå en nonce-værdi op i den komponent til sikker opbevaring, der er knyttet til Secure Enclave. Det gør den ved at bruge Secure Enclave Boot ROM og sikre, at nonce-værdien i LocalPolicy svarer til nonce-værdien i komponenten til sikker opbevaring. Det er med til at forhindre, at en tidligere LocalPolicy – som måske er konfigureret til lavere sikkerhed – bliver genanvendt i systemet efter en opgradering af sikkerheden. Det betyder, at sikker start på en Mac med Apple Silicon er med til at yde beskyttelse mod, at operativsystemversioner rulles tilbage, og at sikkerhedspolitikker nedgraderes.

LocalPolicy registrerer, om operativsystemet er konfigureret til Fuld, Reduceret eller Tolerant sikkerhed.

- *Fuld sikkerhed:* Systemet fungerer på samme måde som iOS og iPadOS og tillader kun startsoftware, som er kendt som den nyeste version, der var tilgængelig på installeringstidspunktet.
- *Reduceret sikkerhed:* LLB får anvisning om at godkende "globale" signaturer, som følger med operativsystemet. Det gør det muligt for systemet at køre ældre versioner af macOS. Det kan ikke undgås, at ældre versioner af macOS har sikkerhedshuller, som ikke er lukket, og derfor kaldes denne sikkerhedsfunktion for *Reduceret*. Det er også det politikniveau, der er nødvendigt for at understøtte start af kerneudvidelser (kext'er).
- *Tolerant sikkerhed:* Systemet fungerer på samme måde som Reduceret sikkerhed, i og med at det bruger bekræftelse med global signatur til iBoot og derudover, men det giver også iBoot besked på at acceptere, at nogle startobjekter bliver signeret af Secure Enclave med den samme nøgle, der bruges til at signere LocalPolicy. Dette politikniveau understøtter, at brugere udvikler, signerer og starter deres egne brugerdefinerede XNU-kerner.

Hvis LocalPolicy anfører over for LLB, at det valgte operativsystem afvikles med Fuld sikkerhed, evaluerer LLB den personliggjorte signatur til iBoot. Hvis det afvikles med Reduceret sikkerhed eller Tolerant sikkerhed, evalueres den globale signatur. Hvis der opstår fejl under godkendelsen af signaturen, starter systemet i macOS-gendannelse, der giver brugeren reparationsmuligheder.

Efter LLB har overdraget kontrollen til iBoot, indlæses macOS-parret firmware, f.eks. firmware til Sikker Neural Engine, Always On Processor og anden firmware. iBoot kigger også på oplysninger om den LocalPolicy, der er overdraget fra LLB. Hvis LocalPolicy anfører, at der bør være en Auxiliary Kernel Collection (AuxKC), søger iBoot efter den i arkivsystemet. Derefter kontrollerer iBoot, at den er signeret af Secure Enclave med samme nøgle som LocalPolicy, og at dens hash-værdi stemmer overens med en hash-værdi, der opbevares i LocalPolicy. Hvis AuxKC bliver godkendt, placerer iBoot den i hukommelsen med kernesamlingen til systemstart, hvorefter den låser hele det hukommelsesområde, der dækker kernesamlingen til systemstart og AuxKC med System Coprocessor Integrity Protection (SCIP). Hvis politikken anfører, at der skal være en AuxKC, og den ikke bliver fundet, går systemet videre med at starte i macOS uden en AuxKC. iBoot har også ansvaret for at godkende hash-værdien for den signerede systemenheds rod (SSV-roden). Det sker for at kontrollere, om integriteten for det arkivsystem, som kernen vil aktivere, er godkendt fuldt ud.

Startfunktioner på en Mac med Apple Silicon

En Mac med Apple Silicon har de startfunktioner, der er beskrevet nedenfor:

Tilstand	Tastkombination	Beskrivelse
macOS	Luk computeren ned, og tryk på og **slip** afbryderknappen.	1. Boot ROM overdrager kontrollen til LLB. 2. LLB indlæser systemparret firmware og LocalPolicy for det valgte macOS. 3. LLB låser en angivelse i Boot Progress Register (BPR) om, at den starter i macOS, og overdrager kontrollen til iBoot. 4. iBoot indlæser den macOS-parrede firmware, den statiske buffer til godkendelse, enhedsstrukturen og kernesamlingen til systemstart. 5. Hvis LocalPolicy tillader det, indlæser iBoot Aux KC (den sekundære kernesamling) i kext'er fra tredjeparter. 6. Hvis LocalPolicy ikke slog hash-værdien for rodsignaturen til den signerede systemenhed (SSV) fra, godkender iBoot den.
Parret macOS-gendannelse (Paired recoveryOS)	Luk computeren ned, tryk på afbryderknappen, og **hold den nede**.	1. Boot ROM overdrager kontrollen til LLB. 2. LLB indlæser systemparret firmware og LocalPolicy for det valgte macOS-gendannelsessystem. 3. LLB låser en angivelse i Boot Progress Register om, at den starter i parret macOS-gendannelse, og overdrager kontrollen til iBoot til parret macOS-gendannelse. 4. iBoot indlæser den macOS-parrede firmware, bufferen til godkendelse, enhedsstrukturen og kernesamlingen til systemstart. 5. Hvis det ikke lykkes at starte i parret macOS-gendannelse, forsøges start i macOS-gendannelse med fallback. *Bemærk:* Nedgraderinger af sikkerhed er ikke tilladt i LocalPolicy til parret macOS-gendannelse.

Tilstand	Tastkombination	Beskrivelse
Fallback for macOS-gendannelse	Luk computeren ned, **tryk to gange på afbryderknappen, og hold den nede**.	1. Boot ROM overdrager kontrollen til LLB. 2. LLB indlæser systemparret firmware og LocalPolicy for det valgte macOS-gendannelsessystem. 3. LLB låser en angivelse i Boot Progress Register om, at den starter i parret macOS-gendannelse, og overdrager kontrollen til iBoot til macOS-gendannelse. 4. iBoot indlæser den macOS-parrede firmware, bufferen til godkendelse, enhedsstrukturen og kernesamlingen til systemstart. *Bemærk:* Nedgraderinger af sikkerhed er ikke tilladt i LocalPolicy til parret macOS-gendannelse.
Sikker funktion	Start i macOS-gendannelse som anført ovenfor, og vælg derefter startenheden, mens **Skiftetasten** holdes nede.	1. Starter i macOS-gendannelse som anført ovenfor. 2. Når Skiftetasten holdes nede, mens der vælges en startenhed, bevirker det, at BootPicker-appen godkender det pågældende macOS til start som normalt, og appen indstiller desuden variablen `nvram`, der giver iBoot besked på ikke at indlæse AuxKC ved næste start. 3. Systemet lukker ned og starter igen på den valgte startenhed, men iBoot indlæser ikke AuxKC.

Begrænsninger for parret macOS-gendannelse

I macOS 12.0.1 og nyere versioner installeres ved hver ny macOS-installering også en parret version af macOS-gendannelsessystemet i den tilhørende APFS-enhedsgruppe. Designet kendes af brugere af Intel-baserede Mac-computere, men på en Mac med Apple Silicon giver det ekstra garanti for sikkerhed og kompatibilitet. Da hver macOS-installering nu har sit eget parrede macOS-gendannelsessystem, er det med til at sikre, at kun det specifikke parrede macOS-gendannelsessystem kan foretage handlinger, der nedgraderer sikkerheden. Det bidrager til at beskytte installeringer af nyere versioner af macOS mod manipulering, der igangsættes fra ældre versioner af macOS og omvendt.

Begrænsningerne for pardannelse håndhæves på følgende måde:

- Alle installeringer af macOS 11 danner par med macOS-gendannelsessystemet. Hvis en macOS 11-installering vælges til at starte som standard, kan macOS-gendannelse startes ved at holde afbryderknappen nede på starttidspunktet på en Mac med Apple Silicon. macOS-gendannelsessystemet kan nedgradere sikkerhedsindstillingerne i alle macOS 11-installeringer, men ikke i nogen installeringer af macOS 12.0.1.
- Hvis en installering af macOS 12.0.1 eller en nyere version vælges til at starte som standard, kan dens parrede macOS-gendannelsessystem startes ved at holde afbryderknappen nede, når Mac startes. Det parrede macOS-gendannelsessystem kan nedgradere sikkerhedsindstillingerne til den parrede macOS-installering, men ikke til nogen anden macOS-installering.

Hvis et macOS-gendannelsessystem, der er parret med en macOS-installering, skal startes, skal macOS-installeringen være valgt som standard. Det gøres med Startdisk i Systemindstillinger eller ved at starte en macOS-gendannelse og holde Alternativtasten nede, mens der vælges en enhed.

Bemærk: macOS-gendannelse med fallback kan ikke foretage nedgraderinger af nogen macOS-installeringer.

Styring af sikkerhedspolitik for Startdisk på en Mac med Apple Silicon

Oversigt

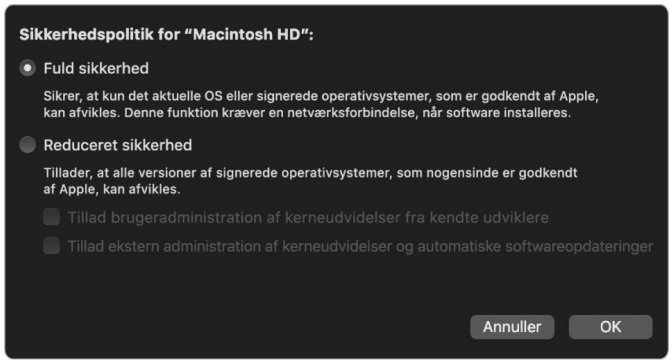
I modsætning til sikkerhedspolitikker på en Intel-baseret Mac har de installerede operativsystemer på en Mac med Apple Silicon hver sin sikkerhedspolitik. Det betyder, at flere installerede forekomster af macOS med forskellige versioner og sikkerhedspolitikker understøttes på samme Mac. Det er årsagen til, at der er føjet en *operativsystemvælger* til Startsikkerhedsværktøj.

På en Mac med Apple Silicon viser Startsikkerhedsværktøj den overordnede brugerkonfigurerede sikkerhedstilstand for macOS som f.eks. starten af en kext eller konfigurationen af System Integrity Protection (SIP). Hvis ændring af en sikkerhedsindstilling vil nedsætte sikkerheden væsentligt eller gøre det lettere at kompromittere systemet, skal brugerne starte macOS-gendannelse ved at holde afbryderknappen nede (så signalet ikke kan udløses af malware, kun af en person med fysisk adgang) for at foretage ændringen. Det betyder, at en Apple Silicon-baseret Mac ikke har behov for (eller understøtter) en firmwareadgangskode, da alle kritiske ændringer allerede er beskyttet af brugerens godkendelse. Du kan få flere oplysninger om SIP i Beskyttelse af systemets integritet.

Fuld sikkerhed og Reduceret sikkerhed kan indstilles via Startsikkerhedsværktøj fra macOS-gendannelse. Tolerant sikkerhed kan derimod kun tilgås fra kommandolinjeværktøjer af brugere, som accepterer risikoen ved at gøre deres Mac-computer langt mindre sikker.

Politik for Fuld sikkerhed

Fuld sikkerhed er standard, og det fungerer som ved iOS og iPadOS. Når softwaren hentes og gøres klar til installering, kommunikerer macOS med den samme Apple-signeringsserver, som bruges til iOS og iPadOS, og anmoder om en ny "personliggjort" signatur frem for at bruge den globale signatur, som leveres sammen med softwaren. En signatur er personliggjort, når den indeholder ECID (Exclusive Chip Identification) – et unikt id, der er specifikt for Apple CPU'en i dette tilfælde – som en del af signeringsanmodningen. Signaturen, der leveres tilbage af signeringsserveren, er derfor unik og kan kun bruges af den pågældende Apple CPU. Når politikken for Fuld sikkerhed er slået til, er Boot ROM og LLB med til at sikre, at en given signatur ikke kun er signeret af Apple, men er signeret til netop den pågældende Mac-computer, så denne version af macOS bliver knyttet til præcis denne Mac.



Brug af en onlinesigneringsserver giver også bedre beskyttelse mod rollback-angreb end typiske globale signeringsstrategier. I et globalt signeringssystem kan sikkerhedsepoken have kørt mange gange, men det ved et system, som ikke har den seneste firmware, ikke. Eksempelvis kan en computer, som nu tror, at den befinder sig i sikkerhedsepoke 1, acceptere software fra sikkerhedsepoke 2, selvom den faktiske nuværende sikkerhedsepoke er 5. Med et Apple Silicon-baseret onlinesigneringssystem kan signeringsserveren afvise at oprette signaturer til software, der befinder sig i en anden sikkerhedsepoke end den nyeste.

Ligeledes kan en hacker, der har opdaget en sikkerhedsrisiko efter en sikkerhedsepokeændring, ikke bare tage den sårbare software fra en tidligere epoke fra system A og benytte den i system B til at indlede et angreb. Da den sårbare software fra en tidligere epoke er blevet personliggjort til system A, kan den ikke overføres og dermed bruges til at angribe system B. Alle disse funktionaliteter arbejder sammen for at tilbyde meget stærkere garantier for, at personer med ondsindede hensigter ikke med vilje kan lægge sårbar software på en Mac for at omgå den sikkerhed, som den seneste software giver. Men en bruger, som er i besiddelse af et administratorbrugernavn og en adgangskode til Mac, kan altid vælge den sikkerhedspolitik, som passer bedst til vedkommendes situation.

Politik for Reduceret sikkerhed

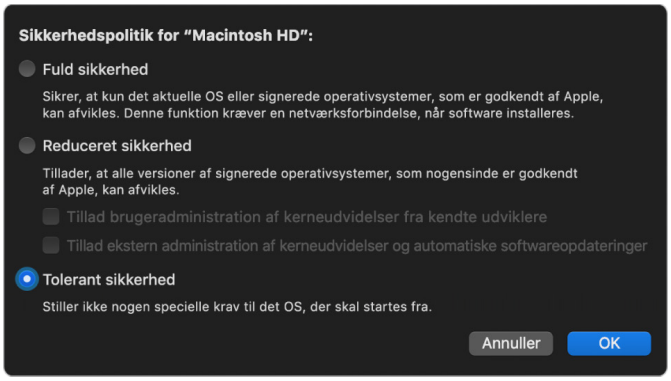
Reduceret sikkerhed svarer nogenlunde til Middel sikkerhed på en Intel-baseret Mac med en T2-chip, hvor en producent (i dette tilfælde Apple) genererer en digital signatur til koden for at fastslå, at den kommer fra producenten. Dette design er med til at forhindre hackere i at introducere kode, der ikke er signeret. Apple kalder denne type signatur en "global" signatur, fordi den kan bruges på enhver Mac, lige så længe det skal være, hvis den er konfigureret med Reduceret sikkerhed. Reduceret sikkerhed beskytter ikke i sig selv mod rollback-angreb (selvom ikke-godkendte ændringer af operativsystemet kan medføre, at der ikke længere kan fås adgang til brugerdata). Du kan få flere oplysninger i Kerneudvidelser på en Mac med Apple Silicon.

Reduceret sikkerhed giver brugerne mulighed for at afvikle ældre versioner af macOS, men Reduceret sikkerhed er også nødvendig for andre handlinger, som udsætter brugerens systemsikkerhed for risiko. Det gælder bl.a. introduktion af kerneudvidelser (kext'er) fra tredjeparter. Kext'er har samme rettigheder som kernen, og dermed kan eventuelle sikkerhedshuller i kext'er fra tredjeparter føre til kompromittering af hele operativsystemet. Derfor opfordres udviklere på det kraftigste til at benytte systemudvidelser, inden understøttelse af kext fjernes fra macOS til fremtidige Mac-computere med Apple Silicon. Selvom kext'er fra tredjeparter er slået til, kan de ikke indlæses i kernen efter behov. Kext'erne lægges i stedet i en sekundær kernesamling (AuxKC), hvis hash-værdi opbevares i LocalPolicy, og de kræver derfor en genstart. Du kan få flere oplysninger om generering af AuxKC i Kerneudvidelser i macOS.

Politik for Tolerant sikkerhed

Tolerant sikkerhed er til brugere, som accepterer risikoen ved at indstille deres Mac til en langt mere usikker tilstand. Denne funktion er forskellig fra funktionen Ingen sikkerhed på en Intel-baseret Mac med en T2-chip. Med Tolerant sikkerhed udføres godkendelse med signatur stadig i hele den sikre startkæde, men når politikken indstilles til Tolerant, er det et signal til iBoot om, at den skal acceptere lokalt Secure Enclave-signerede startobjekter, f.eks. en brugergenereret kernesamling til systemstart, der er bygget ud fra en speciel XNU-kerne. På den måde giver Tolerant sikkerhed også mulighed i arkitekturen for at afvikle en vilkårlig "operativsystem helt uden godkendelse"-kerne. Når en speciel kernesamling til systemstart eller et operativsystem helt uden godkendelse indlæses i systemet, fjernes adgangen til visse krypteringsnøgler. Det har til formål at forhindre, at et operativsystem helt uden godkendelse får adgang til data fra godkendte operativsystemer.

Vigtigt: Apple leverer og understøtter ikke specielle XNU-kerner.



Der er en anden forskel på Tolerant sikkerhed og Ingen sikkerhed på en Intel-baseret Mac med en T2-chip: Tolerant sikkerhed er en forudsætning for visse nedgraderinger af sikkerheden, som tidligere kunne håndteres særskilt. Bemærk især, at deaktivering af beskyttelsen af systemets integritet (SIP) på en Mac med Apple Silicon kræver, at brugeren bekræfter sin hensigt til at indstille systemet til Tolerant sikkerhed. Det er et krav, fordi deaktivering af SIP altid har sat systemet i en tilstand, som gør kernen meget lettere at kompromittere. Deaktivering af SIP på en Mac med Apple Silicon medfører, at håndhævelse af kext-signaturer slås fra under genereringen af AuxKC, og dermed kan enhver vilkårlig kext indlæses i kernehukommelsen. En anden forbedring af SIP, der er foretaget på en Mac med Apple Silicon, er, at lageret til politikker er flyttet fra NVRAM til LocalPolicy. Det betyder, at deaktivering af SIP nu kræver, at en bruger, som har adgang til signeringsnøglen til LocalPolicy, godkender deaktiveringen fra macOS-gendannelse (som brugeren starter ved at trykke på afbryderknappen og holde den nede). Det gør det betydeligt sværere for en softwarehacker eller endda en fysisk tilstedeværende hacker at slå SIP fra.

Det er ikke muligt at nedgradere til Tolerant sikkerhed fra appen Startsikkerhedsværktøj. Brugerne kan kun nedgradere ved at bruge kommandolinjeværktøjer fra Terminal i macOS-gendannelse, f.eks. `csrutil` (til at slå SIP fra). Når brugeren har nedgraderet, afspejles handlingen i Startsikkerhedsværktøj, så en bruger nemt kan indstille sikkerheden på et mere sikkert niveau.

Bemærk: En Mac med Apple Silicon har ikke behov for og understøtter ikke en særlig politik for start fra medier, fordi enhver start teknisk set foretages lokalt. Hvis en bruger vælger at starte fra et eksternt medie, skal mediets operativsystemversion først personliggøres ved hjælp af en godkendt genstart fra macOS-gendannelse. Denne genstart danner et LocalPolicy-arkiv på det interne drev, som bruges til at udføre en godkendt start fra operativsystemet på det eksterne medie. Det betyder, at konfigurationen af start fra et eksternt medie altid er slået eksplicit til for hvert operativsystem og allerede kræver brugerens godkendelse, så der ikke er behov for yderligere konfiguration af sikkerhed.

Oprettelse og administration af signeringsnøgler til LocalPolicy

Oprettelse

Når macOS installeres første gang på fabrikken, eller når der foretages sletning og installering via Internetdeling, afvikler Mac kode fra en RAM-disk til midlertidig gendannelse for at initialisere standardfunktionen. Under denne proces opretter gendannelsesmiljøet et nyt sæt offentlige og private nøgler, som opbevares i Secure Enclave. Den private nøgle kaldes ejeridentitetsnøglen (*OIK (Owner Identity Key)*). Hvis der allerede findes en OIK, slettes den som led i processen. Gendannelsesmiljøet initialiserer også den nøgle, der bruges til Aktiveringslås – brugeridentitetsnøglen *(UIK (User Identity Key))*. Når der anmodes om UIK-certificering for Aktiveringslås på en Mac med Apple Silicon, inkluderes desuden et sæt begrænsninger, der skal håndhæves på valideringstidspunktet for LocalPolicy. Hvis enheden ikke kan få en UIK-nøgle certificeret til Aktiveringslås (f.eks. fordi enheden er knyttet til en Find min Mac-konto og oplyst som mistet), kan den ikke fortsætte og oprette LocalPolicy. Hvis der udstedes et brugeridentitetscertifikat *(ucrt)* til enheden, indeholder dette certifikat politikbegrænsninger bestemt af serveren og politikbegrænsninger, som brugeren har anmodet om, i en X.509 v3-udvidelse.

Når Aktiveringslås/`ucrt` opnås, gemmes emnet i en database på serversiden og sendes også tilbage til enheden. Når enheden har fået et ucrt-certifikat, sendes en certificeringsanmodning om den offentlige nøgle, som svarer til ejeridentitetsnøglen (OIK), til *BAA-serveren (Basic Attestation Authority)*. BAA kontrollerer OIK-certificeringsanmodningen ved hjælp af den offentlige nøgle fra ucrt-certifikatet, der er gemt i den database, som BAA har adgang til. Hvis BAA kan godkende certificeringen, identificerer BAA den offentlige nøgle og returnerer det ejeridentitetscertifikat *(OIC (Owner Identity Certificate))*, som er signeret af BAA og indeholder begrænsningerne i ucrt-certifikatet. OIC sendes tilbage til Secure Enclave. Når Secure Enclave fremover signerer en ny LocalPolicy, bliver OIC vedhæftet Image4-arkivet. LLB har indbygget tillid til BAA-rodcertifikatet og har derfor også tillid til OIC og som følge heraf også til hele LocalPolicy-signaturen.

RemotePolicy-begrænsninger

Alle Image4-arkiver, ikke kun LocalPolicy-arkiver, indeholder begrænsninger for evaluering af Image4-manifester. Disse begrænsninger kodes med særlige OID'er (object identifiers) i bladcertifikatet. Biblioteket til Image4-godkendelse søger i et certifikat efter det særlige OID til certifikatbegrænsning, mens signaturen evalueres, og derefter evaluerer biblioteket mekanisk de begrænsninger, der er angivet i det. Begrænsningerne har dette format:

- X skal eksistere
- X må ikke eksistere
- X skal have en specifik værdi

Eksempel: For "personliggjorte" signaturer vil certifikatbegrænsningerne indeholde "ECID skal eksistere", og for "globale" signaturer vil de indeholde "ECID må ikke eksistere". Disse begrænsninger har til formål at sikre, at alle Image4-arkiver signeret af en given nøgle skal overholde visse krav for at undgå, at der genereres Image4-manifester, som er signeret forkert.

I forbindelse med hver LocalPolicy kaldes disse Image4-certifikatbegrænsninger for *RemotePolicy*. Forskellige startmiljøers LocalPolicy kan have hver deres RemotePolicy. RemotePolicy bruges til at begrænse LocalPolicy til macOS-gendannelse, så macOS-gendannelse til enhver tid kun kan fungere, som om det er startet med Fuld sikkerhed. Det øger tilliden til integriteten i startmiljøet for macOS-gendannelse som et sted, hvor politikker kan ændres. LocalPolicy begrænses af RemotePolicy til at indeholde ECID fra den Mac, hvor LocalPolicy blev genereret, og den Remote Policy Nonce Hash (`rpnh`), der opbevares i komponenten til sikker opbevaring på den pågældende maskine. `rpnh` og dermed RemotePolicy ændres kun, når der foretages handlinger i forbindelse med Find min Mac og Aktiveringslås, f.eks. tilmelding, framelding, ekstern låsning og ekstern sletning. RemotePolicy-begrænsninger fastlægges og anføres på certificeringstidspunktet for brugeridentitetsnøglen (UIK) og er logget ind på det udstedte brugeridentitetscertifikat (ucrt). Nogle Remote Policy-begrænsninger, f.eks. ECID, ChipID og BoardID, fastlægges af serveren. Formålet er at forhindre en enhed i at signere LocalPolicy-arkiver for en anden enhed. Andre RemotePolicy-begrænsninger kan defineres af enheden for at være med til at forhindre, at LocalPolicy-sikkerheden nedgraderes uden anførelse af både den lokale godkendelse, der kræves for at få adgang til den aktuelle OIK-nøgle, og den eksterne godkendelse af den konto, som enhedens Aktiveringslås er knyttet til.

Indholdet i et LocalPolicy-arkiv på en Mac med Apple Silicon

LocalPolicy er et Image4-arkiv, der er signeret af Secure Enclave. Image4 er et ASN.1 (Abstract Syntax Notation One) DER-kodet datastrukturformat, der bruges til at beskrive oplysninger om objekter i den sikre startkæde på Apples platforme. I en Image4-baseret model til sikker start anmodes der om sikkerhedspolitikker, når der installeres software, og det sker gennem en signeringsanmodning til en central Apple-signeringsserver. Hvis politikken kan accepteres, returnerer signeringsserveren et signeret Image4-arkiv, som indeholder forskellige sekvenser af 4-tegnskoder (4CC). Disse signerede Image4-arkiver og 4CC'er evalueres under starten af software som Boot ROM eller LLB.

Overdragelse af ejerskab mellem operativsystemer

Adgang til ejeridentitetsnøglen OIK kaldes "Ejerskab". Der kræves ejerskab for at give brugerne tilladelse til at signere LocalPolicy igen efter at have foretaget politik- eller softwareændringer. OIK beskyttes af samme nøglehierarki, som er beskrevet i Sealed Key Protection (SKP), hvor OIK beskyttes af samme nøglekrypteringsnøgle (KEK) som enhedskrypteringsnøglen (VEK). Det betyder, at den normalt beskyttes af både brugeradgangskoder og målinger af operativsystem og politik. Alle operativsystemer på en Mac har samme OIK. Det betyder, at hvis der installeres et operativsystem mere efter det første operativsystem, skal brugerne på det første operativsystem give deres udtrykkelige samtykke til at overdrage ejerskabet til brugerne på det nye operativsystem. Brugerne til det nye operativsystem findes imidlertid ikke endnu, når installeringsappen afvikles fra det første operativsystem. Brugerne oprettes normalt først i et operativsystem, når operativsystemet er startet, og Indstillingsassistent er åbnet. Der er derfor behov for to nye handlinger, når der installeres et operativsystem mere på en Mac med Apple Silicon:

- Oprettelse af LocalPolicy til det nye operativsystem
- Oprettelse af en "installeringsbruger" til overdragelse af ejerskab

Under afvikling af installeringsassistenten og udpegning af en tom diskenhed som modtager for installeringen bliver brugeren spurgt, om der skal oprettes en kopi af en bruger fra den aktuelle diskenhed, som skal blive den første bruger på den anden diskenhed. Hvis brugeren svarer ja, bliver den "installeringsbruger", som oprettes, i realiteten til en KEK, der afledes af den valgte brugers adgangskode og hardwarenøgler, og som derefter bruges til at kryptere OIK under overdragelsen til det nye operativsystem. I installeringsassistenten til det nye operativsystem bliver der derefter bedt om den valgte brugers adgangskode, så der kan fås adgang til Secure Enclave til det nye operativsystem. Hvis brugeren vælger ikke at oprette en kopi af en bruger, oprettes installeringsbrugeren på samme måde, men der bruges en tom adgangskode i stedet for en brugers adgangskode. Dette andet forløb bruges til visse systemadministrationssituationer. Brugere, der vil have installeringer på flere diskenheder, og som vil overdrage ejerskab på den mest sikre måde, bør altid vælge at kopiere en bruger fra det første operativsystem til det andet operativsystem.

LocalPolicy på en Mac med Apple Silicon

På en Mac med Apple Silicon er kontrollen over den lokale sikkerhedspolitik delegeret til en app, der afvikles i Secure Enclave. Denne software kan benytte brugerens godkendelsesoplysninger og startfunktionen i den primære CPU til at fastlægge, hvem der kan ændre sikkerhedspolitikken, og fra hvilket startmiljø det kan ske. Det bidrager til at forhindre, at ondsindet software bruger sikkerhedspolitikkerne mod brugeren ved at nedgradere dem og dermed opnå flere rettigheder.

Egenskaber i LocalPolicy-manifest

LocalPolicy-arkivet indeholder nogle arkitektoniske 4CC'er, som findes i næste alle Image4-arkiver, f.eks. et board-id eller model-id (BORD), som angiver en bestemt Apple-chip (CHIP) eller et ECID (Exclusive Chip Identification). De 4CC'er, der er anført nedenfor, fokuserer kun på de sikkerhedspolitikker, som brugerne kan konfigurere.

Bemærk: Apple bruger termen *Paired One True recoveryOS (1TR)* til at beskrive en start i det parrede macOS-gendannelsessystem, som opnås ved, at en bruger fysisk trykker en gang på afbryderknappen og holder den nede. Det er anderledes end en normal start i macOS-gendannelse, som sker ved hjælp af NVRAM, ved at der trykkes to gange på knappen, og den holdes nede, eller hvis der opstår fejl under starten. Det specifikke fysiske tryk på knappen øger tilliden til, at startmiljøet ikke kan tilgås af en softwarehacker, som har skaffet sig uretmæssig adgang til macOS.

LocalPolicy Nonce Hash (lpnh)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS

- *Beskrivelse:* `lpnh` bruges til at forhindre genafspilning af LocalPolicy. Det er en SHA384 hash-værdi for LPN (LocalPolicy Nonce), der opbevares i komponenten til sikker opbevaring, og som er tilgængelig via Secure Enclave Boot ROM eller Secure Enclave. Den ubearbejdede nonce-værdi er aldrig synlig for app-processoren, kun for sepOS. En hacker, som har indhentet en tidligere LocalPolicy og vil overbevise LLB om, at denne tidligere politik er gyldig, er nødt til at placere en værdi i komponenten til sikker opbevaring, som opretter hash-værdier med samme `lpnh`-værdi som i den LocalPolicy, personen vil genafspille. Normalt er der kun en enkelt LPN, som er gyldig i systemet, undtagen ved softwareopdateringer, hvor to er gyldige samtidig. Det giver mulighed for at starte den gamle software, hvis der sker fejl under opdateringen. Når LocalPolicy for et hvilket som helst operativsystem ændres, bliver alle politikker signeret igen med den nye *lpnh*-værdi, som svarer til den nye LPN, der findes i komponenten til sikker opbevaring. Ændringen sker, når brugeren ændrer sikkerhedsindstillinger eller opretter nye operativsystemer med en ny LocalPolicy til hvert af dem.

Remote Policy Nonce Hash (rpnh)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse:* `rpnh` fungerer på samme måde som `lpnh`, men den opdateres kun, når den eksterne politik opdateres, f.eks. ved ændring af tilmeldingen til Find. Ændringen sker, når brugeren ændrer indstillingen af Find på sin Mac.

recoveryOS Nonce Hash (ronh)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse:* `ronh` fungerer på samme måde som lpnh, men den findes udelukkende i LocalPolicy til macOS-gendannelse af systemet. Den opdateres, når macOS-gendannelse af systemet opdateres, f.eks. i forbindelse med softwareopdateringer. Der bruges en anden nonce-værdi end til `lpnh` og `rpnh`. Dermed sikres det, når en enhed gøres passiv via Find, at eksisterende operativsystemer kan deaktiveres (ved at fjerne deres LPN og RPN fra komponenten til sikker opbevaring), mens det stadig er muligt at starte macOS-gendannelse af systemet. Det betyder, at operativsystemerne kan genaktiveres, når systemets ejer beviser sin kontrol over systemet ved at indtaste den iCloud-adgangskode, der bruges til Find-kontoen. Ændringen sker, når brugeren opdaterer macOS-gendannelse af systemet eller opretter nye operativsystemer.

Next Stage Image4 Manifest Hash (nsih)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse: nsih*-feltet repræsenterer en SHA384 hash-værdi for Image4-manifestets datastruktur, som beskriver det macOS, der startes. Image4-manifestet i macOS indeholder målinger af alle startobjekterne, f.eks. iBoot, den statiske buffer til godkendelse, enhedsstrukturen, kernesamlingen til systemstart og hash-værdien for den signerede systemenheds rod (SSV). Når LLB får besked om at starte et givent macOS, er den indstillet til at sikre, at hash-værdien for det macOS Image4-manifest, der er knyttet til iBoot, stemmer overens med den værdi, der er indeholdt i `nsih`-feltet i LocalPolicy. På den måde registrerer `nsih` brugerens hensigt angående, hvilket operativsystem brugeren har oprettet en LocalPolicy til. Brugerne ændrer implicit `nsih`-værdien, når de udfører en softwareopdatering.

Auxiliary Kernel Collection (AuxKC) Policy Hash (auxp)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* macOS
- *Beskrivelse:* auxp er en SHA384 hash-værdi til politikken for den brugergodkendte kext-liste (UAKL). Den bidrager ved generering af AuxKC til at sikre, at kun brugergodkendte kext'er inkluderes i AuxKC. smb2 er en forudsætning for at indstille dette felt. Brugere ændrer auxp-værdien implicit, når de ændrer UAKL ved at godkende en kext i vinduet Sikkerhed & anonymitet i Systemindstillinger.

Auxiliary Kernel Collection (AuxKC) Image4 Manifest Hash (auxi)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* macOS
- *Beskrivelse:* Når systemet har bekræftet, at hash-værdien til UAKL stemmer overens med det, der findes i auxp-feltet i LocalPolicy, anmoder det om at få AuxKC signeret af Secure Enclave-processoren, som er ansvarlig for signering af LocalPolicy. Derefter bliver en SHA384 hash-værdi for signaturen til AuxKC Image4-manifestet placeret i LocalPolicy. Det sker for at undgå, at tidligere signerede AuxKC'er blandes sammen og matches med et operativsystem under starten. Hvis iBoot finder auxi-feltet i LocalPolicy, forsøger det at indlæse AuxKC fra lagringspladsen og godkende dens signatur. Det kontrollerer også, om hash-værdien for det Image4-manifest, der er knyttet til AuxKC, stemmer overens med værdien i auxi-feltet. Hvis AuxKC ikke kan indlæses, bliver systemet ved med at starte uden dette startobjekt og (dermed) uden at indlæse nogen kext'er fra tredjeparter. auxp-feltet er en forudsætning for at indstille auxi-feltet i LocalPolicy. Brugere ændrer auxi-værdien implicit, når de ændrer UAKL ved at godkende en kext i vinduet Sikkerhed & anonymitet i Systemindstillinger.

Auxiliary Kernel Collection (AuxKC) Receipt Hash (auxr)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* macOS
- *Beskrivelse:* auxr er en SHA384 hash-værdi for modtagelse af AuxKC, som indikerer det præcise sæt kext'er, som blev inkluderet i AuxKC. AuxKC-kvitteringen kan være en delmængde af UAKL, fordi kext'er kan ekskluderes fra AuxKC – også selvom de er brugergodkendte – hvis de er kendt for at blive brugt til angreb. Desuden vil nogle kext'er, som kan bruges til at bryde brugerkernens grænse, måske føre til nedsat funktionalitet, så det f.eks. ikke er muligt at bruge Apple Pay eller afspille 4K- og HDR-indhold. Brugere, som ønsker disse funktioner, tilvælger en mere restriktiv AuxKC-inklusion. auxp-feltet er en forudsætning for at indstille auxr-feltet i LocalPolicy. Brugere ændrer auxr-værdien implicit, når de opbygger en ny AuxKC i vinduet Sikkerhed & anonymitet i Systemindstillinger.

CustomOS Image4 Manifest Hash (coih)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* coih er en SHA384-hash-værdi for CustomOS Image4-manifestet. Dataene til manifestet bruges af iBoot (i stedet for XNU-kernen) til at overdrage kontrollen. Brugerne ændrer implicit coih-værdien, når de bruger kommandolinjeværktøjet `kmutil configure-boot` i 1TR.

APFS Volume Group UUID (vuid)

- *Type:* OktetStreng (16)
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse:* `vuid` angiver den enhedsgruppe, som kernen skal bruge som rod. Dette felt er primært til information og bruges ikke til sikkerhedsbegrænsninger. Brugeren indstiller `vuid` implicit ved at oprette en ny installering af et operativsystem.

Key Encryption Key (KEK) Group UUID (kuid)

- *Type:* OktetStreng (16)
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse:* `kuid` angiver den enhed, der blev startet. Nøglekrypteringsnøglen (KEK) er typisk blevet brugt til Databeskyttelse. Den bruges til at beskytte signeringsnøglen til hver LocalPolicy. Brugeren indstiller implicit `kuid` ved at oprette en ny installering af et operativsystem.

Paired recoveryOS Trusted Boot Policy Measurement (prot)

- *Type:* OktetStreng (48)
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse:* Paired recoveryOS Trusted Boot Policy Measurement (TBPM) er en særlig gentaget SHA384 hash-værdiberegning for Image4-manifestet for en LocalPolicy, som ikke medtager nonce-værdier, så den kan give en konsistent måling over tid (fordi nonce-værdier som `lpnh` opdateres jævnligt). Feltet `prot`, der kun findes i LocalPolicy til hvert macOS, skaber en pardannelse for at indikere den LocalPolicy til macOS-gendannelse, som svarer til LocalPolicy til macOS.

Has Secure Enclave Signed recoveryOS Local Policy (hrlp)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse:* `hrlp` indikerer, om ovenstående `prot`-værdi er udtryk for en LocalPolicy til macOS-gendannelse signeret af Secure Enclave. Hvis det ikke er tilfældet, signeres LocalPolicy til macOS-gendannelse af Apples onlinesigneringsserver, som signerer ting som Image4-arkiver i macOS.

Local Operating System Version (love)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse, macOS
- *Beskrivelse:* The `love` angiver den operativversion, som LocalPolicy er oprettet til. Versionen hentes fra Next stage-manifestet under oprettelse af LocalPolicy og bruges til at håndhæve begrænsninger for parring af macOS-gendannelse.

Secure Multi-Boot (smb0)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR, macOS-gendannelse
- *Beskrivelse:* Hvis `smb0` er "present and true", tillader LLB, at Next stage Image4-manifestet bliver globalt signeret frem for at kræve en personliggjort signatur. Brugerne kan ændre feltet med Startsikkerhedsværktøj eller `bputil` for at nedgradere til Reduceret sikkerhed.

Secure Multi-Boot (smb1)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* Hvis `smb1` er "present and true", tillader iBoot, at objekter som f.eks. en speciel kernesamling kan signeres af Secure Enclave med samme nøgle som LocalPolicy. Tilstedeværelsen af `smb0` er en forudsætning for tilstedeværelsen af `smb1`. Brugerne kan ændre feltet via kommandolinjeværktøjer som `csrutil` eller `bputil` for at nedgradere til Tolerant sikkerhed.

Secure Multi-Boot (smb2)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* Hvis `smb2` er "present and true", tillader iBoot, at den sekundære kernesamling kan signeres af Secure Enclave med samme nøgle som LocalPolicy. Tilstedeværelsen af `smb0` er en forudsætning for tilstedeværelsen af `smb2`. Brugerne kan ændre feltet via Startsikkerhedsværktøj eller `bputil` for at nedgradere til Reduceret sikkerhed og tillade kext'er fra tredjeparter.

Secure Multi-Boot (smb3)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* Hvis `smb3` er "present and true", har en bruger af enheden tilmeldt den til en løsning til administration af mobile enheder (MDM) for at give MDM kontrol over systemet. Tilstedeværelsen af dette felt medfører, at Secure Enclave-processoren til styring af LocalPolicy accepterer MDM-godkendelse i stedet for at kræve lokal brugergodkendelse. Brugerne kan ændre feltet via Startsikkerhedsværktøj eller `bputil` for at tillade administreret kontrol over kext'er fra tredjeparter og softwareopdateringer. (I macOS 11.2 og nyere versioner kan MDM også starte en opdatering til den nyeste version af macOS, hvis den aktuelle sikkerhedsfunktion er Fuld sikkerhed).

Secure Multi-Boot (smb4)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* macOS
- *Beskrivelse:* Hvis `smb4` er "present and true", er enheden tilmeldt en MDM-løsning via Apple School Manager, Apple Business Manager eller Apple Business Essentials for at give MDM kontrol over operativsystemet . Tilstedeværelsen af dette felt medfører, at Secure Enclave-appen til styring af LocalPolicy accepterer MDM-godkendelse i stedet for at kræve lokal brugergodkendelse. Dette felt ændres af MDM-løsningen, når den registrerer, at enhedens serienummer forekommer i en af disse tre tjenester.

System Integrity Protection (sip0)

- *Type:* 64-bit heltal uden fortegn
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* `sip0` indeholder de bits til den eksisterende politik for Beskyttelse af systemets integritet (System Integrity Protection – SIP), som tidligere blev opbevaret i NVRAM. Nye bits til SIP-politikken tilføjes her (i stedet for at bruge felter i LocalPolicy som vist nedenfor), hvis de kun bruges i macOS og ikke af LLB. Brugerne kan ændre feltet via `csrutil` fra 1TR for at slå SIP fra og nedgradere til Tolerant sikkerhed.

System Integrity Protection (sip1)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* Hvis `sip1` er "present and true", tillader iBoot, at mislykkede forsøg bekræfter hash-værdien for SSV-enhedens rod. Brugerne kan ændre feltet via `csrutil` eller `bputil` fra 1TR.

System Integrity Protection (sip2)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* Hvis sip2 er "present and true", låser iBoot ikke hardwareregistrene til *Configurable Text Read-only Region (CTRR)*, som markerer, at der ikke kan skrives til kernehukommelsen. Brugerne kan ændre feltet via `csrutil` eller `bputil` fra 1TR.

System Integrity Protection (sip3)

- *Type:* Boolesk
- *Miljøer, der kan ændres:* 1TR
- *Beskrivelse:* Hvis `sip3` er "present and true", håndhæver iBoot ikke sin indbyggede liste over tilladte indstillinger for NVRAM-variablen boot-args, som ellers ville filtrere de indstillinger, der sendes til kernen. Brugerne kan ændre feltet via `csrutil` eller `bputil` fra 1TR.

Certifikater og RemotePolicy

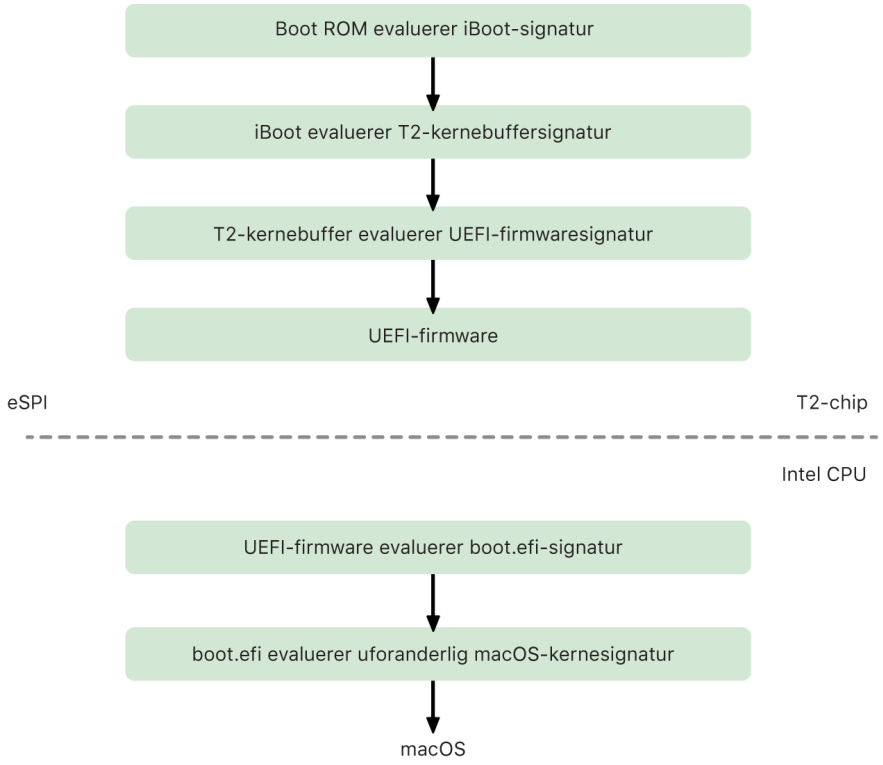
Som beskrevet i Oprettelse og administration af signeringsnøgler til LocalPolicy indeholder Image4-arkivet til LocalPolicy også ejeridentitetscertifikatet OIC og den indlejrede RemotePolicy.

Intel-baserede Mac-computere

Startproces på en Intel-baseret Mac

Intel-baseret Mac med en Apple T2-sikkerhedschip

Når en Intel-baseret Mac-computer med Apple T2-sikkerhedschippen tændes, udfører chippen en sikker start fra sin Boot ROM på samme måde som på iPhone, iPad og en Mac med Apple Silicon. Dette kontrollerer bootloaderen i iBoot og er det første trin i godkendelseskæden. iBoot kontrollerer kerne- og kerneudvidelseskoden på T2-chippen, som derefter kontrollerer Intel UEFI-firmwaren. UEFI-firmwaren og den tilhørende signatur er fra start kun tilgængelige på T2-chippen.



Efter godkendelse bliver UEFI-firmwaren tilknyttet en del af T2-chippens hukommelse. Denne hukommelse bliver gjort tilgængelig for Intel-CPU'en via eSPI (enhanced Serial Peripheral Interface). Når Intel-CPU'en starter, henter den UEFI-firmwaren via eSPI fra den integritetskontrollerede, hukommelsestilknyttede kopi af firmwaren, der ligger på T2-chippen.

Kontrollen af godkendelseskæden fortsætter i Intel-CPU'en, hvor UEFI-firmwaren evaluerer signaturen for boot.efi, der er bootloader i macOS. Signaturerne til sikker start af macOS ligger på Intel-chippen i samme Image4-format, der bruges på iOS, iPadOS og T2-chips til sikker start, og den kode, der fortolker Image4-arkiverne, er den samme hardwarekode som på den eksisterende implementering af sikker start i iOS og iPadOS. Boot.efi godkender signaturen til et nyt arkiv kaldet immutablekernel. Når sikker start er slået til, repræsenterer immutablekernel-arkivet alle de Apple-kerneudvidelser, der skal bruges til at starte macOS. Politikken til sikker start afvikles ved overdragelse til immutablekernel, hvorefter macOS-sikkerhedspolitikker (som f.eks. beskyttelse af systemets integritet og signerede kerneudvidelser) træder i kraft.

Hvis der er fejl eller nedbrud i denne proces, skifter Mac til macOS-gendannelsestilstand, gendannelsestilstand for Apple T2-sikkerhedschip eller DFU-tilstand (Device Firmware Upgrade) for Apple T2-sikkerhedschip.

Microsoft Windows på en Intel-baseret Mac med en T2-chip

Som standard har en Intel-baseret Mac, der understøtter sikker start, kun tillid til indhold, der er signeret af Apple. Men for at forbedre sikkerheden af Bootcamp-installeringer understøtter Apple også sikker start af Windows. UEFI-firmwaren (Unified Extensible Firmware Interface) indeholder en kopi af Microsoft Windows Production CA 2011-certifikatet, der bruges til at godkende bootloadere fra Microsoft.

Bemærk: Der er i øjeblikket ikke nogen godkendelse af Microsoft Corporation UEFI CA 2011, som tillader godkendelse af kode signeret af Microsoft-partnere. UEFI CA bliver normalt anvendt til at verificere ægtheden af bootloadere til andre operativsystemer som f.eks. Linux-varianter.

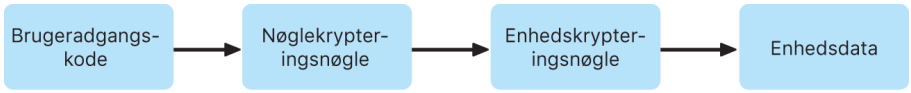
Understøttelse af sikker start af Windows er ikke slået til som standard, men slås til ved brug af Boot Camp-assistent (BCA). Når en bruger afvikler BCA, bliver macOS omkonfigureret til at godkende Microsofts førstepartssignerede kode under opstarten. Når BCA er færdig, og hvis macOS ikke kan godkende Apples førstepartstillidsevaluering i endnu en start, forsøger UEFI-firmwaren at evaluere tilliden til objektet i overensstemmelse med UEFI-formatering til sikker start. Hvis tillidsevalueringen lykkes, fortsætter Mac med at starte Windows. Hvis det ikke lykkes, skifter Mac til macOS-gendannelse, og brugeren får besked om, at tillidsevalueringen ikke blev gennemført.

Intel-baserede Mac-computere uden en T2-chip

En Intel-baseret Mac uden en T2-chip understøtter ikke sikker start. Derfor indlæser UEFI-firmwaren (Unified Extensible Firmware Interface) macOS-starteren (boot.efi) fra arkivsystemet uden kontrol, og starteren indlæser kernen (prelinkedkernel) fra arkivsystemet uden kontrol. For at beskytte integriteten i startkæden bør brugeren slå alle disse sikkerhedsmekanismer til:

- *System Integrity Protection (SIP):* Dette er slået til som standard og beskytter starteren og kernen mod skadelig kode fra et fungerende macOS.
- *FileVault:* Dette kan slås til på to måder: enten af brugeren eller af en MDM-administrator (Mobile Device Management). Dette beskytter mod, at en person med onde hensigter, der har fysisk adgang, kan benytte funktionen Computer som ekstern harddisk (TDM) til at overskrive starteren.

- *Firmwareadgangskode:* Denne kan slås til på to måder: Af brugeren eller af en MDM-administrator. Det er med til at beskytte computeren mod, at en person med onde hensigter, der har fysisk adgang, kan starte alternative startfunktioner, såsom macOS-gendannelse, Enkeltbrugerfunktion eller Computer som ekstern harddisk, hvorfra starteren kan overskrives. Det er også med til at forhindre start fra alternative medier, som en person med onde hensigter eventuelt ville kunne bruge til at afvikle kode, der overskriver starteren.



Startfunktioner på en Intel-baseret Mac med en Apple T2-sikkerhedschip

En Intel-baseret Mac med en Apple T2-sikkerhedschip har en række startfunktioner, der kan tilgås i forbindelse med starten vha. tastkombinationer, der genkendes af UEFI-firmwaren eller starteren. Nogle startfunktioner, f.eks. Enkeltbrugerfunktion, fungerer kun, hvis sikkerhedspolitikken ændres til Ingen sikkerhed i Startsikkerhedsværktøj.

Tilstand	Tastkombination	Beskrivelse
macOS-start	Ingen	UEFI-firmwaren giver besked til macOS-booteren (en UEFI-app), som giver besked til kernen i macOS. Ved standardstart af en Mac med FileVault slået til viser macOS-booteren login-vinduet, hvor brugeren indtaster den adgangskode, der dekrypterer arkivdata.
Startdisk	Alt (⌥)	UEFI-firmwaren starter den indbyggede UEFI-app, som viser brugeren et skærmbillede med en liste over de startenheder, der kan vælges imellem.
Computer som ekstern harddisk (TDM)	T	UEFI-firmwaren starter den indbyggede UEFI-app, som viser den interne lagringsenhed som en rå, blokbaseret enhed via FireWire, Thunderbolt, USB eller en kombination af disse tre (afhængigt af Mac-modellen).
Enkeltbrugerfunktion	Kommando (⌘)-S	macOS-kernen fortolker flaget –s i launchd-vektorargumentet, hvorefter launchd opretter en enkeltbruger-shell i Konsols tty. *Bemærk:* Hvis brugeren forlader denne shell, fortsætter macOS frem til login-vinduet.
macOS-gendannelse	Kommando (⌘)-R	UEFI-firmwaren starter en minimal version af macOS fra et signeret diskbilledarkiv (.dmg) på den interne lagringsenhed.
macOS-internetgendannelse	Alt (⌥)-Kommando (⌘)-R	Det signerede diskbillede bliver hentet fra internettet via HTTP.
Diagnosticering	D	UEFI-firmwaren starter en minimal version af UEFI-diagnosticeringsmiljøet fra et signeret diskbilledarkiv på den interne lagringsenhed.
Diagnosticering over internettet	Alt (⌥)-D	Det signerede diskbillede bliver hentet fra internettet via HTTP.
Start af Windows	Ingen	Hvis Windows er blevet installeret med Boot Camp, overdrager UEFI-firmwaren kontrollen til Windows Boot Manager, som overdrager til Windows-kernen.

Startsikkerhedsværktøj til en Mac med en Apple T2-sikkerhedschip

Oversigt

På en Intel-baseret Mac med en Apple T2-sikkerhedschip håndterer Startsikkerhedsværktøj et antal indstillinger til sikkerhedspolitikker. Værktøjet kan bruges, hvis man starter i macOS-gendannelse og vælger Startsikkerhedsværktøj på menuen Hjælpeapps. Det beskytter mod, at en hacker nemt kan ændre understøttede sikkerhedsindstillinger.

Vigtige ændringer i politikken kræver godkendelse – selv i macOS-gendannelsestilstand. Første gang Startsikkerhedsværktøj åbnes, bliver brugeren bedt om at indtaste en administratoradgangskode fra den primære macOS-installering, der er knyttet til den macOS-gendannelse, der er startet fra. Hvis der ikke er nogen administratorkonto, skal der oprettes en, før politikken kan ændres. T2-chippen kræver, at Mac-computeren i øjeblikket er startet i macOS-gendannelse, og at der er foretaget godkendelse med Secure Enclave-godkendelsesoplysninger, før der kan foretages ændringer i politikken. Der er to implicitte krav ved ændringer af sikkerhedspolitikken. macOS-gendannelse skal:

- Startes fra en lagringsenhed, der er direkte forbundet til T2-chippen, fordi partitioner på andre enheder ikke har Secure Enclave-sikkerhedsoplysninger, der er knyttet til den interne lagringsenhed.
- Være placeret på en APFS-baseret enhed, fordi den kun understøtter opbevaring af godkendelsesoplysninger til Godkendelse i gendannelse sendt til Secure Enclave på et drevs “Preboot” APFS-enhed. HFS plus-formaterede enheder kan ikke bruge sikker start.

Denne politik vises kun i Startsikkerhedsværktøj på en Intel-baseret Mac med en T2-chip. Selvom de fleste brugssituationer ikke burde kræve, at der foretages ændringer i politikken til sikker start, har brugere i sidste ende kontrol over indstillingerne på deres enhed og kan efter behov vælge at slå funktionen sikker start fra eller nedgradere den på deres Mac.

Ændringer i politikken til sikker start, der foretages fra denne app, gælder kun for evaluering af godkendelseskæden på Intel-processoren. Muligheden "Sikker start: T2-chip" er altid i funktion.

Politikken til sikker start kan konfigureres til en af disse tre indstillinger: Fuld sikkerhed, Middel sikkerhed og Ingen sikkerhed. Ingen sikkerhed slår sikker start-evalueringen fuldstændigt fra på Intel-processoren og lader brugeren starte hvad som helst.

Sikker start med Fuld sikkerhed

Fuld sikkerhed er standardstartpolitikken, og det fungerer stort set som i iOS og iPadOS og på en Mac med Apple Silicon. På det tidspunkt, hvor software hentes og klargøres til installering, bliver den personliggjort med en signatur, der indeholder ECID (Exclusive Chip Identification) – et unikt id, der er specifikt for T2-chippen i dette tilfælde – som en del af signeringsanmodningen. Signaturen, der leveres tilbage af signeringsserveren, er derfor unik og kan kun bruges af den pågældende T2-chip. UEFI-firmwaren (Unified Extensible Firmware Interface) har til formål at sikre, at en given signatur ikke kun er signeret af Apple, når politikken Fuld sikkerhed er slået til, men er signeret til netop den pågældende Mac-computer, så denne version af macOS bliver knyttet til præcis denne Mac. Det bidrager til at forhindre rollback-angreb som beskrevet i Fuld sikkerhed på en Mac med Apple Silicon.

Sikker start med Middel sikkerhed

Startpolitikken Middel sikkerhed svarer nogenlunde til en traditionel sikker start med UEFI, hvor en producent (i dette tilfælde Apple) genererer en digital signatur til koden for at fastslå, at den kommer fra producenten. På den måde kan hackere ikke introducere kode, der ikke er signeret. Vi kalder denne type signatur en "global" signatur, fordi den kan bruges på enhver Mac, lige så længe det skal være, hvis den er konfigureret med Reduceret sikkerhed. Hverken iOS, iPadOS eller selve T2-chippen understøtter globale signaturer. Denne indstilling gør intet forsøg på at forhindre rollback-angreb.

Politik for start fra medier

Politikken for start fra medier findes kun på en Intel-baseret Mac med en T2-chip og har intet at gøre med politikken for sikker start. Det betyder, at selvom en bruger slår sikker start fra, ændrer det ikke på standardvirkemåden, som kun tillader, at Mac-computeren startes fra den lagringsenhed, der er sluttet direkte til T2-chippen. (Der er ikke behov for en politik for start fra medier på en Mac med Apple Silicon. Du kan få flere oplysninger i Styring af sikkerhedspolitik for Startdisk).

Beskyttelse med firmwareadgangskode på en Intel-baseret Mac

macOS på Intel-baserede Mac-computere med en Apple T2-sikkerhedschip understøtter brugen af en firmwareadgangskode for at bidrage til at forhindre utilsigtede ændringer af firmwareindstillinger på en Mac-computer. Firmwareadgangskoden har til formål at forhindre valg af andre starttilstande såsom macOS-gendannelse, Enkeltbrugerfunktion, Computer som ekstern harddisk eller start fra en ikke-godkendt systemenhed.

Bemærk: Der er ikke behov for firmwareadgangskoden på en Mac med Apple Silicon, fordi den kritiske firmwarefunktionalitet, den beskyttede, er flyttet til macOS-gendannelse, og macOS-gendannelse kræver brugerens godkendelse (når FileVault er slået til), før der gives adgang til kritisk funktionalitet.

Den enkleste version af firmwareadgangskoder findes i Hjælpeprogram til firmwareadgangskode i macOS-gendannelsestilstand på en Intel-baseret Mac *uden* en T2-chip og i Startsikkerhedsværktøj på en Intel-baseret Mac *med* en T2-chip. Avancerede indstillinger (såsom mulighed for at bede om adgangskode, hver gang Mac-computeren starter) findes i kommandoen `firmwarepasswd` i macOS.

Det er særlig vigtigt at indstille en firmwareadgangskode for at nedbringe risikoen for angreb på Intel-baserede Mac-computere uden en T2-chip, hvor en hacker har fysisk adgang til computeren. Firmwareadgangskoden er med til at forhindre en person med onde hensigter i at starte computeren fra macOS-gendannelsestilstand, hvorfra Beskyttelse af systemets integritet kan slås fra. Når muligheden for at starte Mac-computeren fra alternative medier begrænses, kan en hacker ikke afvikle priviligeret kode fra et andet operativsystem med henblik på at angribe firmware i eksterne enheder.

Der findes en funktion til nulstilling af firmwareadgangskoden, hvis brugeren har glemt sin adgangskode. Brugeren benytter en tastkombination ved start og får en modelafhængig streng, der skal oplyses til AppleCare. AppleCare signerer en ressource digitalt, hvorefter den bliver signaturkontrolleret af Uniform Resource Identifier (URI). Hvis signaturen bliver godkendt, og indholdet er beregnet til den pågældende Mac, fjerner UEFI-firmwaren firmwareadgangskoden.

Af hensyn til brugere, som ikke ønsker, at andre end de selv skal kunne fjerne firmwareadgangskoden med software, blev parameteren `–disable–reset–capability` føjet til kommandoen `firmwarepasswd` i macOS 10.15. Inden denne mulighed indstilles, skal brugeren bekræfte, at det påhviler vedkommende at afholde udgifterne til et nyt hovedkort, hvis adgangskoden glemmes og skal fjernes. Organisationer, der vil beskytte deres Mac-computere mod eksterne personer med onde hensigter og mod medarbejdere, skal indstille en firmwareadgangskode på systemer, der ejes af organisationen. Det kan gøres på enheden på følgende måder:

- På klargøringstidspunktet ved hjælp af kommandoen `firmwarepasswd` på kommandolinjen
- Ved hjælp af administrationsværktøjer fra tredjeparter, der bruger kommandoen `firmwarepasswd` på kommandolinjen
- Ved hjælp af administration af mobile enheder (MDM)

macOS-gendannelse og diagnosticeringsmiljøer til en Intel-baseret Mac

macOS-gendannelse

macOS-gendannelse ligger helt separat fra macOS-hoveddelen, og alt indhold bliver opbevaret i et diskbilledarkiv kaldet BaseSystem.dmg. Der findes også en tilknyttet BaseSystem.chunklist, som bruges til at kontrollere integriteten af BaseSystem.dmg. Chunklist er en række hash-værdier til 10 MB-segmenter i BaseSystem.dmg. UEFI-firmwaren (Unified Extensible Firmware Interface) evaluerer signaturen på chunklist-arkivet og derefter hash-værdien for et segment ad gangen i BaseSystem.dmg. Det er med til at sikre, at det stemmer overens med det signerede indhold, der ligger i chunklist. Hvis en af disse hash-værdier ikke stemmer overens, afbrydes starten fra den lokale macOS-gendannelse, og UEFI-firmwaren forsøger at starte fra macOS-internetgendannelse i stedet for.

Hvis godkendelsen går igennem, starter UEFI-firmwaren BaseSystem.dmg som en RAM-disk og initierer det boot.efi-arkiv, der ligger på disken. Det er ikke nødvendigt for UEFI-firmwaren at udføre en specifik kontrol af boot.efi eller for boot.efi at kontrollere kernen, fordi integriteten af det fulde indhold af operativsystemet (som disse elementer kun er en delmængde af) allerede er blevet kontrolleret.

Apple-diagnosticering

Proceduren for start af det lokale diagnosticeringsmiljø er næsten den samme som for start af macOS-gendannelse. Der bliver brugt separate AppleDiagnostics.dmg- og AppleDiagnostics.chunklist-arkiver, men de bliver godkendt på samme måde som BaseSystem-arkiverne. I stedet for at starte boot.efi starter UEFI-firmwaren et arkiv i diskbilledet (.dmg-arkivet) med navnet diagss.efi, som kalder en række andre UEFI-drivere, der kan kommunikere med hardwaren og kontrollere den for fejl.

macOS-internetgendannelse og diagnosticeringsmiljøer

Hvis der sker en fejl under starten af de lokale gendannelses- eller diagnosticeringsmiljøer, forsøger UEFI-firmwaren at hente billederne fra internettet i stedet for. (En bruger kan desuden specifikt anmode om, at billederne bliver hentet fra internettet ved hjælp af en særlig tastesekvens under starten). Integritetsevalueringen af diskbilleder og segmentlister hentet fra macOS-gendannelsesserveren bliver udført på samme måde, som når billeder hentes fra en lagringsenhed.

Forbindelsen til macOS-gendannelsesserveren oprettes via HTTP, men alt hentet indhold bliver alligevel integritetsevalueret som beskrevet tidligere og er dermed beskyttet mod manipulation af personer med ondsindede hensigter, som har skaffet sig kontrol over netværket. I tilfælde af, at et enkelt segment ikke bliver integritetsgodkendt, bliver der anmodet om det igen fra macOS-gendannelsesserveren 11 gange, inden handlingen indstilles, og der vises en fejlmeddelelse.

Da funktionerne til internetgendannelse og diagnosticering blev føjet til Mac-computere i 2011, besluttede man, at det var bedre at bruge den enklere HTTP-transport og håndtere godkendelse af indhold vha. chunklist-mekanismen frem for at implementere den mere komplicerede HTTPS-funktion i UEFI-firmwaren, som ville have udvidet firmwarens angrebsflade.

Sikkerhed på den signerede systemenhed i iOS, iPadOS og macOS

Apple lancerede i macOS 10.15 den skrivebeskyttede systemenhed, som er en dedikeret, isoleret enhed til systemindhold. macOS 11 og nyere versioner føjer stærk kryptografisk beskyttelse til systemindhold med en *signeret systemenhed (SSV)*. SSV omfatter en mekanisme i kernen, som bekræfter systemindholdets integritet under afviklingen og afviser alle data – kode og ikke-kode – uden en gyldig kryptografisk signatur fra Apple. Fra iOS 15 og iPadOS 15 blev systemenheden på en iOS- og iPadOS-enhed signeret og opnåede dermed også den kryptografiske beskyttelse.

SSV er med til at forhindre manipulation af den Apple-software, som er en del af operativsystemet, og gør macOS-softwareopdateringer mere pålidelige og langt mere sikre. SSV bruger snapshots af APFS (Apple File System), så hvis en opdatering ikke kan gennemføres, er det muligt at gendanne den tidligere systemversion uden geninstallering.

Siden APFS blev lanceret, har det givet arkivsystemets metadata integritet vha. ikke-kryptografiske kontrolsummer på den interne lagringsenhed. SSV styrker integritetsmekanismen ved at tilføje kryptografiske hash-værdier, og udvider den dermed til at omfatte hver eneste byte i arkivdata. Data fra den interne lagringsenhed (inklusive arkivsystemets metadata) bliver kryptografisk hash-behandlet i læsestien, og hash-værdien sammenlignes derefter med en forventet værdi i arkivsystemets metadata. I tilfælde af, at de ikke stemmer overens, formoder systemet, at der er manipuleret med dataene, og det vil så ikke returnere dem til den software, der anmoder om dem.

Hver SSV SHA256 hash-værdi opbevares i hovedarkivsystemets metadatastruktur, som i sig selv er hash-behandlet. Da hver node i strukturen rekursivt bekræfter integriteten af sine underordnede elementers hash-værdi på samme måde som i en binær hash-værdistruktur (Merkle), omfatter rodnodens hash-værdi – som kaldes en *forsegling* – derfor hver eneste byte data i SSV. Det betyder, at den kryptografiske signatur dækker hele systemenheden.

Under installering og opdatering af macOS genberegnes forseglingen fra arkivsystemet på enheden, og denne måling sammenlignes med den måling, som Apple signerede. På en Mac med Apple Silicon kontrollerer bootloaderen forseglingen, inden kontrollen overføres til kernen. På en Intel-baseret Mac med en Apple T2-sikkerhedschip sender bootloaderen målingen og signaturen videre til kernen, som derefter godkender forseglingen direkte, inden rodarkivsystemet aktiveres. I begge tilfælde stopper startprocessen, hvis godkendelsen ikke lykkes, og brugeren får besked om at installere macOS igen. Denne procedure gentages ved hver start, medmindre brugeren har valgt en indstilling med lavere sikkerhed og separat har valgt at slå den signerede systemenhed fra.

Under opdatering af iOS- og iPadOS-software bliver systemenheden klargjort og genberegnet på lignende vis. Bootloaderne til iOS og iPadOS kontrollerer, at forseglingen er intakt, og at værdien er signeret af Apple, før enheden får tilladelse til at starte kernen. Hvis der er uoverensstemmelser under starten, får brugeren besked på at opdatere enhedens systemsoftware. Brugerne har ikke tilladelse til at slå beskyttelsen af en signeret systemenhed fra i iOS og iPadOS.

SSV og kodesignering

Kodesignering findes stadig og håndhæves af kernen. Den signerede systemenhed yder beskyttelse, hver eneste gang der læses bytes fra den interne lagringsenhed. Derimod giver kodesignering beskyttelse, når Mach-objekter knyttes til hukommelsen på en måde, så de kan afvikles. Både SSV og kodesignering beskytter app-kode på alle stier til læsning og afvikling.

SSV og FileVault

I macOS 11 giver SSV lignende beskyttelse af inaktivt systemindhold, og systemenheden behøver derfor ikke længere blive krypteret. Alle ændringer foretaget i arkivsystemet, når det er inaktivt, registreres af arkivsystemet, når de læses. Hvis brugeren har slået FileVault til, bliver brugerens indhold i dataenheden stadig krypteret med en brugerangivet hemmelighed.

Hvis brugeren vælger at slå SSV fra, bliver systemet sårbart over for manipulation, når det er inaktivt, og denne manipulation kan sætte en hacker i stand til at udtrække krypterede brugerdata, næste gang systemet starter. Systemet vil derfor ikke give brugeren tilladelse til at slå SSV fra, hvis FileVault er slået til. Beskyttelse af det inaktive system skal slås til for begge enheder på en ensartet måde.

I macOS 10.15 og tidligere versioner beskytter FileVault operativsystemets software, når det er inaktivt, ved at kryptere bruger- og systemindholdet med en nøgle, der er beskyttet med en brugerangivet hemmelighed. Det yder beskyttelse mod, at en person med ondsindede hensigter, der har fysisk adgang til enheden, kan få adgang til eller ændre det arkivsystem, der indeholder systemsoftware.

SSV og en Mac med en Apple T2-sikkerhedschip

På en Mac med en Apple T2-sikkerhedschip er det kun selve macOS, der beskyttes af SSV. Den software, der afvikles på T2-chippen og godkender macOS, beskyttes af sikker start.

Sikre softwareopdateringer

Sikkerhed er en løbende proces. Det er ikke nok at starte det operativsystem, der blev installeret på fabrikken – der skal også være en mekanisme, der hurtigt og sikkert kan hente de nyeste sikkerhedsopdateringer. Apple frigiver regelmæssigt softwareopdateringer for at imødegå potentielle sikkerhedsproblemer. Brugere af iOS- og iPadOS-enheder modtager opdateringsnotifikationer på enheden. Mac-brugere finder de tilgængelige opdateringer i Systemindstillinger. Opdateringer leveres trådløst, hvilket sikrer hurtig implementering af de seneste sikkerhedsopdateringer.

Opdateringsprocessen

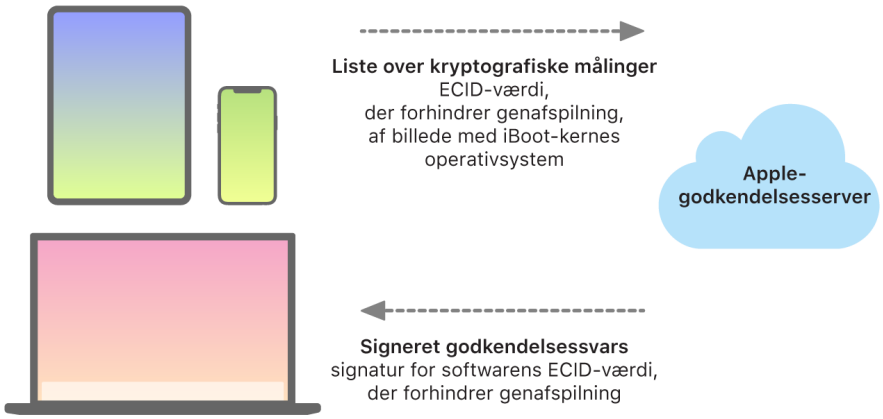
Opdateringsprocessen bruger den samme hardwarebaserede tillidsrod, der bruges af Sikker start, og som sikrer, at kun kode signeret af Apple installeres. Opdateringsprocessen bruger også godkendelse af systemsoftware til at sørge for, at kun ægte kopier af de operativsystemversioner, der er aktivt signeret af Apple, kan installeres på iOS- og iPadOS-enheder og på Mac-computere med indstillingen Fuld sikkerhed slået til som sikker start-politik i Startsikkerhedsværktøj. Disse sikre processer betyder, at Apple kan ophøre med at signere ældre operativsystemversioner med kendte sikkerhedshuller, og gør det svært at gennemføre nedgraderingsangreb.

Sikkerheden ved softwareopdateringer øges, ved at en fuld kopi af iOS eller iPadOS hentes og installeres, når en enhed er sluttet fysisk til en Mac. Ved OTA-softwareopdateringer (Over The Air) *hentes kun de komponenter, der kræves for at gennemføre en opdatering*, i stedet for hele operativsystemet. Det sker af hensyn til netværkseffektiviteten. Desuden kan softwareopdateringer opbevares i bufferen på en Mac med macOS 10.13 eller en nyere version, hvor Indlæsning af indhold i buffer er slået til, så iOS- og iPadOS-enheder ikke behøver at hente den nødvendige opdatering igen fra internettet. (De skal stadig kontakte Apple-servere for at gennemføre opdateringen).

Personliggjort opdateringsproces

Under en opgradering eller opdatering oprettes der forbindelse til Apples godkendelsesserver til installering, som sender en liste med kryptografiske målinger for hvert af de elementer i installeringspakken, der skal installeres (f.eks. iBoot, kernen og operativsystembilledet), en tilfældig værdi, der forhindrer genafspilning (nonce-værdien), og enhedens unikke ECID (Exclusive Chip Identification).

Godkendelsesserveren holder den modtagne liste med målinger op mod de versioner, det er tilladt at installere, og hvis den finder et match, føjer den ECID til målingen og signerer resultatet. Serveren overfører et komplet sæt signerede data til enheden som led i opgraderingen. Tilføjelsen af ECID "personliggør" godkendelsen af den enhed, der sender anmodningen. Da godkendelse og signering kun sker for kendte målinger, er serveren med til at sikre, at opdateringerne foretages præcis, som Apple har fastlagt.



Evalueringen i godkendelseskæden på starttidspunktet kontrollerer, at signaturen stammer fra Apple, og at målingen for det emne, der indlæses fra lagerenheden, sammen med enhedens ECID modsvarer det, som signaturen dækker. Disse trin har til formål at sikre, at godkendelsen på enheder, der understøtter personlig indstilling, er til en bestemt enhed, og at et ældre operativsystem eller en ældre firmwareversion fra en enhed ikke kan kopieres til en anden. Nonce-værdien er med til at forhindre en person med ondsindede hensigter i at opsnappe serverens svar og bruge det til at modificere en enhed eller ændre systemsoftwaren.

Den personlige indstilling er årsagen til, at der altid kræves netværksforbindelse til Apple, før en enhed med en chip designet af Apple, herunder en Intel-baseret Mac med Apple T2-sikkerhedschippen, kan opdateres.

Som en ekstra foranstaltning aktiveres brugerens dataenhed på disken aldrig under en softwareopdatering for at forhindre læsning fra eller skrivning til enheden under opdateringer.

På enheder med Secure Enclave benytter denne hardware på lignende vis godkendelse af systemsoftware til at kontrollere integriteten af systemets software og være med til at forhindre nedgraderinger.

Operativsystemets integritet

Apples operativsystemer er designet med sikkerhed som et centralt element. Designet omfatter en tillidsrod i hardwaren, der bruges til at gøre sikker start mulig, og en hurtig og sikker softwareopdateringsproces. Apples operativsystemer bruger også deres specielle chipbaserede hardwarefunktioner til at mindske risikoen for udnyttelse under operativsystemets afvikling. Under afvikling af godkendt kode beskytter disse funktioner den godkendte kodes integritet. Apples operativsystemer er med andre ord med til at danne et bolværk mod angrebs- og udnyttelsesteknikker, uanset om de kommer fra en skadelig app, fra internettet eller en anden kanal. De beskyttelsesforanstaltninger, der er beskrevet her, findes på enheder med SoC'er designet af Apple, herunder iOS, iPadOS, tvOS, watchOS og nu også macOS på en Mac med Apple Silicon.

Funktion	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	M1-familien
Beskyttelse af kernens integritet	✓	✓	✓	✓	✓	✓
Hurtige begrænsninger i adgangen		✓	✓	✓	✓	✓
Beskyttelse af systemhjælpeprocessorers integritet			✓	✓	✓	✓
Koder til markørgodkendelse			✓	✓	✓	✓
Sidebeskyttelseslag		✓	✓	✓	✓	Se bemærkning nedenfor.

Bemærk: PPL (Page Protection Layer) kræver, at platformen *kun* afvikler signeret og godkendt kode. Det er en sikkerhedsmodel, der ikke er relevant for macOS.

Beskyttelse af kernens integritet

Når initialiseringen af operativsystemets kerne er færdig, aktiveres beskyttelsen af kernens integritet (KIP – Kernel Integrity Protection) for at bidrage til at forhindre modificering af kerne- og driverkode. Styreenheden til hukommelse tilvejebringer et beskyttet område i den fysiske hukommelse, som iBoot bruger til at indlæse kernen og kerneudvidelser. Når starten er gennemført, afviser styreenheden til hukommelse forsøg på at skrive til det beskyttede område af den fysiske hukommelse. App-processorens MMU (Memory Management Unit) konfigureres, så den bidrager til at forhindre overførsel af privilegeret kode fra fysisk hukommelse uden for det beskyttede hukommelsesområde og er med til at forhindre overførsel af fysisk hukommelse med skrivemulighed inden for kernehukommelsesområdet.

Ændring af konfigurationen forhindres, ved at den hardware, der bruges til at aktivere KIP, låses, når startprocessen er færdig.

Hurtige begrænsninger i adgangen

Med Apple A11 Bionic og S3 SoC'er som de første blev der indført en ny basal hardwarefunktion. Denne basale funktion, Hurtige begrænsninger i adgangen, omfatter et CPU-register, der hurtigt begrænser adgangen pr. tråd. Disse hurtige begrænsninger i adgangen (kaldes også APRR-registre) gør det muligt for understøttede operativsystemer at fjerne afviklingstilladelser fra hukommelsen uden at bruge ressourcer på et systemkald og gennemgang eller tømning af sidetabellen. Disse registre danner et ekstra bolværk mod angreb fra internettet, især mod kode, der kompileres på afviklingstidspunktet (JIT-kompileres), da hukommelsen i praksis ikke kan afvikles, samtidig med at der læses fra den eller skrives til den.

Beskyttelse af systemhjælpeprocessorers integritet

Hjælpeprocessorfirmware håndterer mange kritiske systemopgaver, f.eks. Secure Enclave, billedsensorprocessoren og bevægelseshjælpeprocessoren. Dens sikkerhed er derfor et vigtigt element i hele systemets sikkerhed. Apple bruger mekanismen *Beskyttelse af systemhjælpeprocessorers integritet (SCIP – System Coprocessor Integrity Protection)* til at forhindre modificering af hjælpeprocessorfirmwaren.

SCIP fungerer stort set på samme måde som beskyttelsen af kernens integritet (KIP – Kernel Integrity Protection): Under starten indlæser iBoot hver enkelt hjælpeprocessors firmware i et beskyttet hukommelsesområde, der er reserveret hertil og adskilt fra KIP-området. iBoot konfigurerer hver enkelt hjælpeprocessors hukommelsesenhed for at være med til at forhindre:

- Eksekverbare mapninger uden for dens del af det beskyttede hukommelsesområde
- Overførsel med skrivemulighed inden for dens del af det beskyttede hukommelsesområde

Under starten bruges Secure Enclave-operativsystemet til at konfigurere SCIP til Secure Enclave. Når startprocessen er færdig, låses den hardware, der bruges til at aktivere SCIP. Det har til formål at forhindre ændring af konfigurationen.

Koder til markørgodkendelse

Koder til markørgodkendelse (PAC) bruges til at beskytte mod udnyttelse af fejl, der ødelægger hukommelsen. Systemsoftware og indbyggede apps bruger PAC til at bidrage til at forhindre modificering af funktionsmarkører og returadresser (kodemarkører). PAC benytter fem hemmelige 128-bit værdier til at signere kerneinstruktioner og data, og hver brugerområdeproces har sine egne B-nøgler. Emner bliver tilføjet og signeret som vist nedenfor.

Emne	Nøgle	Salt
Funktionsreturadresse	IB	Lagringsadresse
Funktionsmarkører	IA	0
Blokaktiveringsfunktion	IA	Lagringsadresse
Objective-C Method Cache	IB	Lagringsadresse + Klasse + Vælger

Emne	Nøgle	Salt
C++ V-tabelværdier	IA	Lagringsadresse + Hash (name mangling-metode)
Beregnet Goto-label	IA	Hash (funktionsnavn)
Kerne-trådtilstand	GA	•
Registre over brugertråde	IA	Lagringsadresse
C++ V-tabelmarkører	DA	0

Signaturværdien opbevares i de ubrugte padding-bits øverst i 64-bit markøren. Signaturen bliver godkendt inden brug, og paddingen bliver gendannet for at være med til at sikre, at markøradressen fungerer. Manglende godkendelse resulterer i en afbrydelse. Denne godkendelse forhindrer mange angreb, som f.eks. ROP-angreb (Return Oriented Programming), der forsøger at narre enheden til at afvikle eksisterende kode på en ondsindet måde ved at manipulere funktionsreturadresser, der opbevares i stakken.

Sidebeskyttelseslag

Sidebeskyttelseslag (Page Protection Layer, PPL) i iOS, iPadOS og watchOS har til formål at forhindre, at kode i brugerområdet modificeres, efter godkendelsen af kodesignaturen er gennemført. PPL, der bygger på KIP (Kernel Integrity Protection) og hurtige begrænsninger i adgangen, administrerer tilsidesættelser af sidetabeltilladelser for at sikre, at kun PPL kan ændre beskyttede sider, der indeholder brugerkode og sidetabeller. Systemet reducerer angrebsfladen betydeligt, fordi det understøtter håndhævelse af kodeintegritet i hele systemet, selv hvis en kerne bliver kompromitteret. Denne beskyttelse findes ikke i macOS, fordi PPL kun kan anvendes på systemer, hvor al kode, der afvikles, skal være signeret.

Ekstra systemsikkerhedsfunktioner i macOS

Ekstra systemsikkerhedsfunktioner i macOS

macOS bruges på et bredt udvalg af hardware (f.eks. Intel-baserede CPU'er, Intel-baserede CPU'er kombineret med Apple T2-sikkerhedschip og Apple Silicon-baserede SoC'er) og understøtter en række almindelige anvendelsesområder. Nogle brugere anvender kun de apps, der var installeret på forhånd, og dem, der kan hentes fra App Store, mens andre er kernehackere, som har behov for at slå stort set alle platformens beskyttelsesforanstaltninger fra, så de kan afvikle og teste deres app-kode på det højeste godkendelsesniveau.
De fleste befinder sig et sted midt imellem, og mange af dem har ydre enheder og software, der kræver forskellige adgangsniveauer. Apple designede macOS-platformen med en integreret tilgang til hardware, software og tjenester. Platformen har indbygget databeskyttelse (security by design), og den er nem at konfigurere, implementere og administrere, samtidig med at den kan konfigureres på den måde, brugerne forventer. macOS indeholder også de nøglesikkerhedsteknologier, som en it-medarbejder har brug for til at hjælpe med at beskytte virksomhedens data og integrere sikre netværksmiljøer i hele virksomheden.

Følgende funktioner understøtter og bidrager til sikkerheden for macOS-brugernes forskellige behov. De omfatter:

- Sikkerhed på den signerede systemenhed
- Beskyttelse af systemets integritet
- Buffere til godkendelse
- Beskyttelse af ydre enheder
- Understøttelse af og sikkerhed i Rosetta 2 (automatisk oversættelse) på en Mac med Apple Silicon
- DMA-understøttelse og -beskyttelsesforanstaltninger
- Understøttelse af og sikkerhed i kerneudvidelser (kext'er)
- Understøttelse af og sikkerhed i Option ROM
- UEFI-firmwaresikkerhed på Intel-baserede Mac-computere

Beskyttelse af systemets integritet

macOS bruger kernetilladelser og en funktion, der beskytter systemets integritet (*SIP – System Integrity Protection*), til at begrænse skrivning i kritiske systemarkiver. SIP er en særskilt funktion, der supplerer den hardwarebaserede beskyttelse af kernens integritet (KIP – Kernel Integrity Protection), der findes på en Mac med Apple Silicon og beskytter mod ændring af kernen i hukommelsen. Obligatorisk adgangskontrolteknologi udnyttes til at levere denne og et antal andre beskyttelsesforanstaltninger på kerneniveau, herunder brug af et isoleret miljø ("sandbox") og Data Vault.

Obligatorisk adgangskontrol

macOS bruger obligatorisk adgangskontrol – politikker, der indstiller sikkerhedsbegrænsninger, som udvikleren har oprettet, og som ikke kan tilsidesættes. Fremgangsmåden afviger fra valgfri adgangskontrol, der giver brugerne mulighed for at tilsidesætte sikkerhedspolitikker efter eget valg.

Obligatorisk adgangskontrol er ikke synlig for brugerne, men det er den underliggende teknologi, der er med til at slå flere vigtige funktioner til, herunder brug af et isoleret miljø ("sandbox"), børnesikring, administrerede indstillinger, udvidelser og beskyttelse af systemets integritet.

Beskyttelse af systemets integritet

Beskyttelse af systemets integritet indstiller komponenter på bestemte, vigtige placeringer i arkivsystemet som skrivebeskyttede for at være med til at forhindre, at de ændres af skadelig kode. Beskyttelse af systemets integritet er en computerspecifik indstilling, der slås til som standard, når en bruger opgraderer til OS X 10.11 eller en nyere version. Hvis den slås fra på en Intel-baseret Mac, fjernes beskyttelsen af alle partitioner på den fysiske lagerenhed. macOS anvender denne sikkerhedspolitik på alle processer, som afvikles på systemet, uanset om de afvikles i et isoleret miljø ("sandbox") eller med administratorrettigheder.

Buffere til godkendelse

Et af de objekter, der er indeholdt i den sikre startkæde, er den statiske buffer til godkendelse, som er en godkendt fortegnelse over alle de binære Mach-O-arkiver, der er inkorporeret i den signerede systemenhed. Hvert Mach-O-arkiv repræsenteres af en hash-værdi i kodebiblioteket. Disse hash-værdier sorteres, inden de indsættes i bufferen til godkendelse, for at gøre søgning mere effektiv. Kodebiblioteket er resultatet af den signeringsproces, der foretages af `codesign(1)`. Håndhævelse af bufferen til godkendelse kræver, at SIP er slået til. Hvis håndhævelse af bufferen til godkendelse skal slås fra på en Mac med Apple Silicon, skal sikker start indstilles til Tolerant sikkerhed.

Når et binært arkiv afvikles (enten som led i oprettelsen af en ny proces eller i overførslen af app-kode til en eksisterende proces), uddrages og hash-behandles dets kodebibliotek. Hvis den hash-værdi, der er et resultat af behandlingen, findes i bufferen til godkendelse, tildeles de afviklingsoverførsler, der er oprettet til det binære arkiv, platformrettigheder. Det betyder, at de kan have enhver rettighed og afvikles uden yderligere kontrol med hensyn til signaturens ægthed. Det er anderledes end på en Intel-baseret Mac, hvor platformrettigheder overdrages til indhold i operativsystemet af det Apple-certifikat, som signerer de binære arkiver. (Certifikatet begrænser ikke de rettigheder, det binære arkiv kan have).

Binære arkiver, som ikke er platformarkiver (f.eks. notarielt bekræftet tredjepartskode), skal have gyldige certifikatkæder for at blive afviklet, og deres rettigheder begrænses af den signeringsprofil, som er udstedt til udvikleren af Apple Developer Program.

Alle de binære arkiver, der leveres med macOS, er signeret med et *platform-id*. På en Mac med Apple Silicon bruges dette id til at anføre, at selvom det binære arkiv er signeret af Apple, skal dets hash-værdi i kodebiblioteket være til stede i bufferen til godkendelse, før arkivet kan afvikles. På en Intel-baseret Mac-computer bruges platform-id'et til at foretage målrettet tilbagekaldelse af binære arkiver fra en ældre version af macOS. Denne målrettede tilbagekaldelse er med til at forhindre, at de binære arkiver afvikles på nyere versioner.

Den statiske buffer til godkendelse knytter et sæt binære arkiver til en givet version af macOS. Denne virkemåde er med til at forhindre, at binære arkiver signeret af Apple fra ældre operativsystemer indføres i nyere operativsystemer for at give en hacker en fordel.

Platformkode leveret uden for operativsystemet

Apple leverer visse binære arkiver, f.eks. Xcode og stakken med udviklingsværktøjer, der ikke er signeret med et platform-id. De har dog stadig tilladelse til at blive afviklet med platformrettigheder på en Mac med Apple Silicon og Mac-computere med en T2-chip. Da denne platformsoftware leveres uafhængigt af macOS, er den ikke underlagt de tilbagekaldelsesmekanismer, der håndhæves af den statiske buffer til godkendelse.

Buffere til godkendelse, der kan indlæses

Apple leverer visse softwarepakker med *buffere til godkendelse, som kan indlæses*. Disse buffere har samme datastruktur som den statiske buffer til godkendelse. Der er kun en enkelt statisk buffer til godkendelse, hvis indhold altid er låst i skrivebeskyttede områder, efter at kernen er blevet initialiseret på et tidligt tidspunkt, men under app-afvikling føjes buffere til godkendelse, som kan indlæses, til systemet.

Disse buffere til godkendelse bliver enten godkendt ved hjælp af den samme mekanisme, som godkender startfirmware (personliggjort med Apples godkendte signeringstjeneste), eller som globalt signerede objekter (hvis signaturer ikke binder dem til en bestemt enhed).

Der følger for eksempel en personliggjort buffer til godkendelse med det diskbillede, der bruges til at foretage feltdiagnosticering på en Mac med Apple Silicon. Bufferen til godkendelse personliggøres sammen med diskbilledet og indlæses i den pågældende Mac-computers kerne, mens den startes i et diagnosticeringsmiljø. Bufferen til godkendelse gør det muligt at afvikle softwaren i diskbilledet med platformrettighed.

Der følger for eksempel en globalt signeret buffer til godkendelse med softwareopdateringer til macOS. Denne buffer til godkendelse gør det muligt at afvikle et kodestykke i softwareopdateringen – *opdateringshjernen* – med platformrettighed. Opdateringshjernen foretager det arbejde, der planlægger softwareopdateringen tidsmæssig, og som værtssystemet ikke har mulighed for at udføre på ensartet vis mellem versioner.

Sikkerhed i eksterne processorer på Mac-computere

Alle moderne computersystemer har mange indbyggede eksterne processorer, der bruges til opgaver som netværk, grafik, strømstyring mv. Disse eksterne processorer tjener ofte kun ét formål og er meget svagere end den primære CPU. Indbyggede eksterne processorer, der ikke benytter tilstrækkelige sikkerhedsforanstaltninger, kan lettere udnyttes af hackere, som kan foretage en vedvarende infektion af operativsystemet via processorerne. En hacker, der har inficeret firmwaren i en ekstern processor, kan gå efter software på den primære CPU eller direkte opsnappe følsomme data (en Ethernet-enhed vil f.eks. kunne se indholdet i pakker, der ikke er krypteret).

Apple arbejder på så vidt muligt at reducere antallet af nødvendige eksterne processorer og på at undgå design, der kræver firmware. Men når separate processorer med deres egen firmware er påkrævet, bliver der gjort bestræbelser på at være med til at sikre, at en hacker ikke kan skaffe sig permanent adgang til disse processorer. Det kan gøres ved at kontrollere processoren på en af disse to måder:

- Få processoren til at hente godkendt firmware fra den primære CPU ved start
- Få den eksterne processor til at implementere sin egen sikre startkæde, så den eksterne processors firmware kontrolleres, hver gang Mac-computeren starter

Apple samarbejder med producenter for at evaluere deres implementeringer og forbedre deres design, så de omfatter ønskede egenskaber som f.eks.:

- Minimumskrav til kryptografisk styrke
- Ubetinget tilbagekaldelse af kendt skadelig firmware
- Deaktivering af grænseflader til fejlfinding
- Signering af firmwaren med kryptografiske nøgler, der opbevares på Apple-kontrollerede hardwaresikkerhedsmoduler (HSM'er)

I de senere år har Apple arbejdet sammen med eksterne producenter om at bruge den samme "Image4"-datastruktur, godkendelseskode og infrastruktur til signering, som Apple Silicon bruger.

Når der hverken er mulighed for at arbejde uden lagring eller med lagring og sikker start, kræver designet, at firmwareopdateringerne bliver kryptografisk signeret og godkendt, før det vedvarende lager kan opdateres.

Rosetta 2 på en Mac med Apple Silicon

En Mac med Apple Silicon er i stand til at afvikle kode, der er kompileret til x86_64-instruktionssættet, ved at bruge en oversættelsesmekanisme med navnet *Rosetta 2*. Der er mulighed for to typer oversættelse: enten samtidig med (JIT – Just In Time) eller forud for (AOT – Ahead Of Time) afviklingen.

JIT-oversættelse

I JIT-oversættelsesprocessen identificeres et x86_64 Mach-objekt tidligt i billedafviklingen. Når disse billeder forekommer, overdrager kernen kontrollen til et særligt ankerpunkt for Rosetta-oversættelse i stedet for det dynamiske redigeringsværktøj til links, `dyld(1)`. Ankerpunktet oversætter derefter x86_64-siderne under afvikling af billedet. Oversættelsen foregår udelukkende i processen. Kernen kontrollerer stadig hash-værdierne for koderne på hver x86_64-side i forhold til den kodesignatur, der blev knyttet til det binære arkiv, da siden blev inkorporeret. Hvis hash-værdierne ikke stemmer overens, håndhæver kernen den udbedringspolitik, der er relevant for den pågældende proces.

AOT-oversættelse

I AOT-oversættelsesprocessen læses binære x86_64-arkiver fra lagringspladsen på det tidspunkt, som systemet bedømmer til at være optimalt for den pågældende kodes reaktionsevne. De oversatte artefakter skrives til lagringspladsen som en særlig type Mach-objektarkiv. Arkivet ligner et billede, der kan afvikles, men det mærkes for at vise, at det er det oversatte produkt af et andet billede.

Med denne model henter AOT-artefakten alle sine identitetsoplysninger fra det oprindelige x86_64-app-billede. Håndhævelsen af denne binding sker ved, at en priviligeret entitet i brugerområdet signerer oversættelsesartefakten ved hjælp af en enhedsspecifik nøgle, der administreres af Secure Enclave. Nøglen frigives kun til den priviligerede entitet i brugerområdet, som identificeres ved hjælp af en begrænset berettigelse. Det kodebibliotek, der oprettes til oversættelsesartefakten, indeholder hash-værdien i kodebiblioteket til det oprindelige x86_64-app-billede. Signaturen på selve oversættelsesartefakten kaldes en *supplerende signatur*.

AOT-processen begynder i lighed med JIT-processen med, at kernen overdrager kontrollen til Rosetta-afviklingsfunktionen i stedet for det dynamiske redigeringsværktøj til links, `dyld(1)`. Men derefter sender Rosetta-afviklingsfunktionen en proces til proces-forespørgsel (IPC) til Rosetta-systemtjenesten om, hvorvidt der er en tilgængelig AOT-oversættelse til det aktuelle app-billede. Hvis der findes en, oplyser Rosetta-tjenesten en reference til oversættelsen, og den inkorporeres i processen og afvikles. Under afviklingen håndhæver kernen hash-værdierne i kodebiblioteket for oversættelsesartefakten, som godkendes af den signatur, der er afledt af den enhedsspecifikke signeringsnøgle. Hash-værdierne i kodebiblioteket for det oprindelige x86_64-billede er ikke involveret i denne proces.

Oversatte artefakter opbevares i en Data Vault, som ingen entiteter bortset fra Rosetta-tjenesten har adgang til under afviklingen. Rosetta-tjenesten administrerer adgangen til sin buffer ved at distribuere skrivebeskyttede arkivbeskrivelser til de enkelte oversættelsesartefakter. Det begrænser adgangen til AOT-artefaktbufferen. Tjenestens proces til proces-kommunikation og tilhørende fodaftryk holdes med vilje smalt for at begrænse dens angrebsflade.

Hvis det oprindelige x86_64-billedes hash-værdi i kodebiblioteket ikke stemmer overens med den værdi, der er kodet ind i AOT-oversættelsesartefaktens signatur, betragtes kodesignaturen som ugyldig, og der træffes en passende foranstaltning.

Hvis en ekstern proces sender en forespørgsel til kernen for at få oplyst berettigelser eller andre kodeidentitetsegenskaber for et AOT-oversat app-arkiv, returneres egenskaberne for det oprindelige x86_64-billede til den.

Indhold i statisk buffer til godkendelse

macOS 11 og nyere versioner leveres med "fede" binære arkiver, som indeholder stykker af x86_64- og arm64-computerkode. På en Mac med Apple Silicon kan brugeren vælge at afvikle x86_64-stykket i et binært systemarkiv via Rosetta-processen, f.eks. for at indlæse et tilbehør, som ikke har en indbygget arm64-variant. Fremgangsmåden understøttes ved, at den statiske buffer til godkendelse, der leveres med macOS, som hovedregel indeholder tre hash-værdier i kodebiblioteket pr. Mach-objektarkiv.

- En hash-værdi i kodebiblioteket til arm64-stykket
- En hash-værdi i kodebiblioteket til x86_64-stykket
- En hash-værdi i kodebiblioteket til AOT-oversættelsen af x86_64-stykket

Rosetta AOT-oversættelsesproceduren er deterministisk, ved at den genskaber identisk output for et givet input, uanset hvornår eller på hvilken enhed oversættelsen blev foretaget.

Når macOS bygges, gennemgår alle Mach-objektarkiver den Rosetta AOT-oversættelsesproces, der hører til den version af macOS, der bygges, og den hash-værdi i kodebiblioteket, der genereres, anføres i bufferen til godkendelse. Af hensyn til effektiviteten leveres de faktiske oversatte produkter ikke med operativsystemet, men etableres igen ved behov, når brugeren anmoder om dem.

Når et x86_64-billede afvikles på en Mac med Apple Silicon, og billedets hash-værdi i kodebiblioteket findes i den statiske buffer til godkendelse, forventes den genererede AOT-artefakts hash-værdi i kodebiblioteket *også* at være i den statiske buffer til godkendelse. Sådanne produkter signeres ikke med den enhedsspecifikke nøgle, da signeringsmyndigheden er forankret i Apples sikre startkæde.

Ikke-signeret x86_64-kode

En Mac med Apple Silicon tillader ikke, at indbygget arm64-kode afvikles, hvis den ikke har en gyldig kodesignatur. Signaturen kan blot være en ad hoc-kodesignatur (jf. `codesign(1)`), som ikke indeholder en faktisk identitet fra den hemmelige halvdel af et asymmetrisk nøglepar (den er blot en ikke-godkendt måling af det binære arkiv).

Af hensyn til den binære kompatibilitet tillades afvikling af x86_64-kode via Rosetta helt uden signaturoplysninger. Koden tildeles ingen særlig identitet i den enhedsspecifikke signeringsprocedure i Secure Enclave, og den afvikles med præcis de samme begrænsninger som indbygget ikke-signeret kode, der afvikles på en Intel-baseret Mac.

Direct Memory Access-beskyttelse på Mac-computere

For at opnå høj dataoverførselshastighed på højhastighedsforbindelser som PCIe, FireWire, Thunderbolt og USB skal computere understøtte direkte hukommelsesadgang (DMA) fra eksterne enheder. Dvs. at de skal kunne læse og skrive til RAM, uden at CPU'en er involveret hele tiden. Siden 2012 er Mac-computere blevet forsynet med adskillige teknologier, der beskytter DMA, og har nu de bedste og mest omfattende DMA-beskyttelsesforanstaltninger på nogen pc.

Foranstaltninger til beskyttelse af DMA på en Mac med Apple Silicon

Apple SoC'er (System on Chip) indeholder en Input/Output Memory Management Unit (IOMMU) for hver DMA-agent i systemet, herunder PCIe- og Thunderbolt-porte. Da hver IOMMU har sit eget sæt tabeller til adresseoversættelse, som oversætter DMA-anmodninger, kan eksterne enheder tilsluttet via PCIe eller Thunderbolt kun få adgang til hukommelse, der er knyttet eksplicit til deres brug. Eksterne enheder kan ikke få adgang til hukommelse, der tilhører andre dele af systemet, f.eks. kernen eller firmware, eller hukommelse tildelt til andre eksterne enheder. Hvis en IOMMU registrerer, at en ekstern enhed forsøger at få adgang til hukommelse, der ikke er knyttet til den pågældende enheds brug, udløser den en "kernel panic".

Foranstaltninger til beskyttelse af DMA på en Intel-baseret Mac

Intel-baserede Mac-computere med Intel Virtualization Technology for Directed I/O (VT-d) initialiserer IOMMU, så DMA-gentilknytning og afbrydelse af gentilknytning aktiveres meget tidligt i startprocessen for at modvirke forskellige klasser af sikkerhedshuller. Apples IOMMU-hardware starter handlingen med en politik, der som standard afviser ekstern start. I det øjeblik der tændes for systemet, begynder det derfor automatisk at blokere DMA-anmodninger fra eksterne enheder. Efter IOMMU'erne er initialiseret af software, begynder de at tillade DMA-anmodninger fra ydre enheder til hukommelsesområder, der er knyttet eksplicit til deres brug.

Bemærk: Afbrydelse af gentilknytning til PCIe er ikke nødvendig på en Mac med Apple Silicon, da hver IOMMU håndterer MSI'er for sine egne eksterne enheder.

Fra macOS 11 afvikler alle Mac-computere med en Apple T2-sikkerhedschip UEFI-drivere, der tilvejebringer DMA i et begrænset ring 3-miljø, når driverne danner par med eksterne enheder. Denne egenskab bidrager til at mindske de sikkerhedshuller, der kan opstå, når en enhed med skadeligt indhold interagerer med en UEFI-driver på en uventet måde under starten af systemet. Den mindsker især effekten af sikkerhedshuller i en drivers håndtering af DMA-buffere.

Kerneudvidelser i macOS

Fra macOS 11 gælder, at hvis kerneudvidelser fra tredjeparter (kext'er) er slået til, kan de ikke indlæses i kernen efter behov. De lægges i stedet i en *sekundær kernesamling (AuxKC – Auxiliary Kernel Collection)*, som indlæses under starten. På en Mac med Apple Silicon er AuxKC-målingen indsat i LocalPolicy (på Mac-computere med tidligere hardware er AuxKC placeret på dataenheden). Genopbyggelse af AuxKC kræver brugerens godkendelse og genstart af macOS for at indlæse ændringerne i kernen. Genopbyggelse kræver også, at sikker start er indstillet til Reduceret sikkerhed.

Vigtigt: Kext'er anbefales ikke længere til macOS. Kext'er udgør en sikkerhedsrisiko for operativsystemets integritet og stabilitet, og Apple anbefaler, at brugerne vælger løsninger, der ikke indebærer kerneudvidelser.

Kerneudvidelser på en Mac med Apple Silicon

Kext'er skal slås til manuelt på en Mac med Apple Silicon, ved at brugeren holder afbryderknappen nede under starten, så 1TR-funktionen (One True Recovery) aktiveres, nedgraderer sikkerheden til Reduceret sikkerhed og vælger afkrydsningsfeltet, der slår kerneudvidelser til. Under processen skal brugeren skrive en administrators adgangskode for at godkende nedgraderingen. Kombinationen af 1TR og kravet om adgangskode gør det svært for softwarehackere, der begynder inde fra macOS, at skyde kext'er ind i macOS, som de derefter kan udnytte til at opnå kernerettigheder.

Når en bruger har godkendt, at kext'er må indlæses, bruges processen Indlæsning af brugergodkendte kerneudvidelser, der er beskrevet ovenfor, til at godkende installeringen af kext'er. Den godkendelse, som bruges til ovennævnte forløb, bruges også til at registrere en SHA384 hash-værdi til den brugergodkendte kext-liste (UAKL) i LocalPolicy. Kerneadministrationsdæmonen (`kmd`) er derefter ansvarlig for at kontrollere de kext'er, som findes i UAKL, med henblik på at inkludere dem i AuxKC.

- Hvis Beskyttelse af systemets integritet (SIP) er slået til, kontrolleres hver kexts signatur, før den inkluderes i AuxKC.
- Hvis SIP er slået fra, håndhæves kext-signaturen ikke.

Denne fremgangsmåde giver udviklere eller kunder, som ikke deltager i Apple Developer Program, mulighed for at bruge forløb med Tolerant sikkerhed til at teste kext'er, før de signeres.

Når AuxKC er oprettet, sendes dens måling til Secure Enclave til signering, og den inkluderes i en Image4-datastruktur, som kan evalueres af iBoot under starten. Under opbygningen af AuxKC genereres der også en kext-kvittering. Kvitteringen indeholder den liste med kext'er, som ender med at blive inkluderet i AuxKC, hvilket kan være en delmængde af UAKL, hvis der blev opdaget sortlistede kext'er. En SHA384 hash-værdi for AuxKC Image4-datastrukturen og kext-kvitteringen inkluderes i LocalPolicy. Hash-værdien for AuxKC Image4-arkivet bruges til, at iBoot kan foretage en udvidet godkendelse under starten for at bidrage til at sikre, at det ikke er muligt at starte et ældre Secure Enclave-signeret AuxKC Image4-arkiv med en nyere LocalPolicy. Kext-kvitteringen bruges af subsystemer som Apple Pay til at afgøre, om der er nogen kext'er, der er indlæst i øjeblikket, som kan underminere tilliden til macOS. Hvis det er tilfældet, kan Apple Pay-funktionerne blive slået fra.

Alternativer til kext'er (macOS 10.15 og nyere versioner)

macOS 10.15 sætter udviklerne i stand til at udvide funktionerne i macOS ved at installere og administrere systemudvidelser, der afvikles i brugerområdet i stedet for på kerneniveau. Når systemudvidelserne afvikles i brugerområdet, øges macOS-systemets stabilitet og sikkerhed. Selvom fuld adgang til hele operativsystemet er indbygget i kext'er, får udvidelser, der afvikles i brugerområdet, kun de rettigheder, der er nødvendige, for at de kan udføre deres specifikke funktion.

Udviklere kan bruge frameworks som DriverKit, EndpointSecurity og NetworkExtension til at skrive USB-drivere og drivere til brugergrænsefladen, slutpunktssikkerhedsværktøjer (f.eks. agenter, der kan forhindre datatab, og andre slutpunktsagenter), VPN- og netværksværktøjer – alt sammen uden at skulle skrive kext'er. Sikkerhedsagenter fra tredjeparter bør kun bruges, hvis de udnytter disse API'er eller har faste planer for, hvordan de vil gå over til dem og væk fra kerneudvidelser.

Indlæsning af brugergodkendte kerneudvidelser

For at forbedre sikkerheden kræver det brugerens samtykke at indlæse kerneudvidelser, der er installeret sammen med eller efter installering af macOS 10.13. Denne proces kaldes *indlæsning af brugergodkendte kerneudvidelser*. Det kræver administratorrettigheder at godkende en kerneudvidelse. Kerneudvidelser kræver ikke tilladelse, hvis de:

- Var installeret på en Mac med macOS 10.12 eller en tidligere version
- Erstatter tidligere godkendte udvidelser
- Har tilladelse til at blive indlæst uden brugersamtykke ved brug af kommandolinjeværktøjet `spctl`, der er tilgængeligt, når en Mac startes fra macOS-gendannelse.
- Har tilladelse til at blive indlæst ved brug af MDM-konfigurationen (Mobile Device Management)

  Fra og med macOS 10.13.2 kan brugere benytte MDM til at danne en liste med kerneudvidelser, der må indlæses uden brugerens samtykke. Denne mulighed kræver en Mac-computer med macOS 10.13.2, som er tilmeldt MDM – enten via Apple School Manager, Apple Business Manager eller brugerens egen tilmelding til MDM.

Sikkerhed med Option ROM i macOS

Bemærk: Option ROM understøttes i øjeblikket ikke på en Mac med Apple Silicon.

Sikkerhed med Option ROM på en Mac med Apple T2-sikkerhedschippen

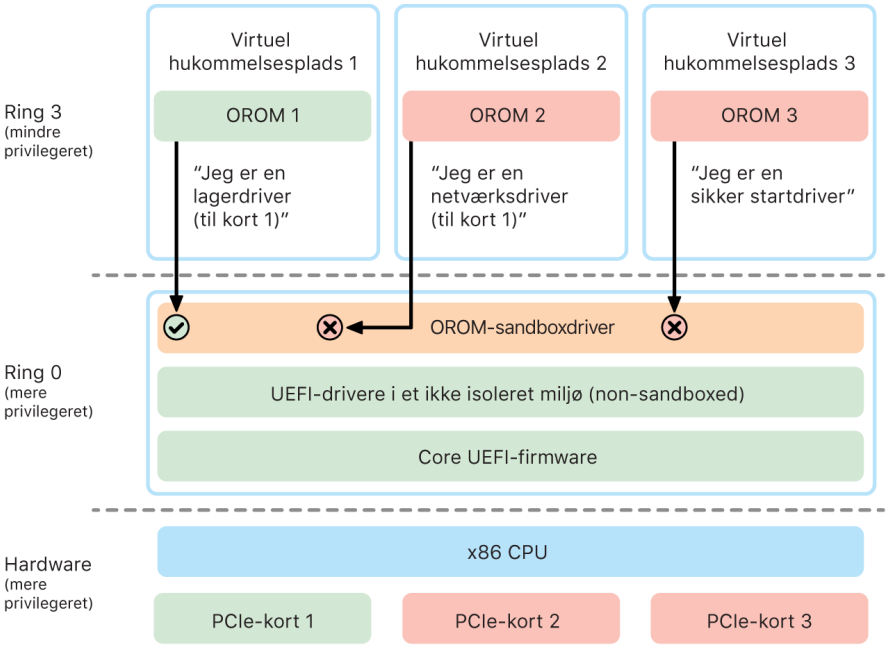
Både Thunderbolt og PCIe-enheder kan have en "Option ROM (OROM)", som er sluttet fysisk til enheden. (Det er som regel ikke ægte ROM, men en chip, der kan overskrives, og som firmwaren opbevares på). På UEFI-baserede systemer er denne firmware typisk en UEFI-driver, der indlæses af UEFI-firmwaren og afvikles. Den afviklede kode skal initialisere og konfigurere den hardware, den blev hentet fra, så hardwaren kan bruges af resten af firmwaren. Denne funktion er påkrævet, så specialiseret tredjepartshardware kan indlæses og fungere i de tidligste faser af starten, f.eks. i forbindelse med start fra eksterne RAID-matrixer.

Men da OROM generelt kan overskrives, afvikles en hackers kode tidligt i startprocessen, hvis vedkommende overskriver OROM i en godkendt ekstern enhed, og koden bliver dermed i stand til at påvirke afviklingsmiljøet og kompromittere integriteten af den software, der indlæses senere. På samme måde kan en hacker afvikle skadelig kode, hvis vedkommende slutter sin egen enhed med skadeligt indhold til systemet.

I macOS 10.12.3 blev virkemåden for Mac-computere solgt efter 2011 ændret til ikke at eksekvere OROM som standard, når Mac-computeren blev startet, medmindre der blev trykket på en bestemt tastkombination. Denne tastkombination beskyttede mod, at OROM med skadeligt indhold utilsigtet kunne introduceres i macOS-startprocessen. Standardindstillingen i Hjælpeprogram til firmwareadgangskode blev også ændret, så OROM ikke kunne afvikles, når en bruger havde indstillet en firmwareadgangskode, heller ikke selvom der blev trykket på tastkombinationen. Det forhindrede en hacker med fysisk adgang til systemet i med vilje at introducere OROM med skadeligt indhold. Brugere, der stadig har behov for at bruge OROM, når de har indstillet en firmwareadgangskode, kan konfigurere en anden indstilling end standardindstillingen ved hjælp af kommandolinjeværktøjet `firmwarepasswd` i macOS.

Sikkerhed med OROM-sandbox

I macOS 10.15 blev UEFI-firmwaren opdateret til at indeholde en mekanisme til at afvikle OROM i et isoleret miljø (“sandbox”) og til at fjerne OROMs rettigheder. UEFI-firmware afvikler typisk al kode, herunder OROM, på højeste rettighedsniveau i CPU’en (ring 0) og har et enkelt delt virtuelt hukommelsesområde til al kode og alle data. Ring 0 er det rettighedsniveau, som macOS-kernen afvikles med, mens apps afvikles på det lavere rettighedsniveau ring 3. OROM-sandbox nedgraderede OROM-rettighederne ved at benytte samme opdeling af den virtuelle hukommelse, som kernen bruger, og lade OROM blive afviklet i ring 3.



Sandboxing begrænser desuden i betydelig grad de grænseflader, som OROM kan kalde (stort set som filtrering af systemkald i kerner), og den type enheder, som en OROM kan registreres som (stort set som godkendelse af apps). Fordelene ved denne arkitektur er, at OROM med skadeligt indhold ikke længere kan skrive direkte inden for ring 0-hukommelse. De er i stedet begrænset til en meget snæver og veldefineret sandboxgrænseflade. Denne begrænsede grænseflade reducerer angrebsfladen betydeligt og tvinger hackere til først at omgå det isolerede miljø (sandbox) og eskalere rettigheder.

UEFI-firmwaresikkerhed på en Intel-baseret Mac

En Intel-baseret Mac med en Apple T2-sikkerhedschip bruger UEFI-firmware (Intel) til at sørge for sikkerheden.

Oversigt

Siden 2006 har Mac-computere med en Intel-baseret CPU benyttet Intel-firmware baseret på Extensible Firmware Interface (EFI) Development Kit (EDK), version 1 eller 2. EDK2-baseret kode er i overensstemmelse med specifikationerne i Unified Extensible Firmware Interface (UEFI). Dette afsnit refererer til firmwaren fra Intel som *UEFI-firmware*. UEFI-firmwaren var den første kode, der blev afviklet på Intel-chippen.

På en Intel-baseret Mac uden Apple T2-sikkerhedschippen er tillidsroden for UEFI-firmwaren den chip, som firmwaren opbevares på. UEFI-firmwareopdateringer bliver digitalt signeret af Apple og godkendt af firmwaren, inden lagringsenheden opdateres. Opdateringer skal altid have en nyere version end den eksisterende for at bidrage til at forhindre rollback-angreb. En hacker med fysisk adgang til Mac-computeren vil dog kunne bruge hardware til at oprette forbindelse til den chip, firmwaren opbevares på, og opdatere chippen med skadeligt indhold. På samme måde kan sikkerhedshuller i begyndelsen af UEFI-firmwarens startproces (inden den skrivebeskytter opbevaringschippen) også føre til vedvarende infektion af UEFI-firmwaren. Det er en hardwarearkitektonisk begrænsning, som findes på de fleste Intel-baserede pc'er og på alle Intel-baserede Mac-computere uden T2-chippen.

Mac-computernes arkitektur blev ændret, så tillidsroden for UEFI-firmwaren nu ligger i Apple T2-chippen, for at forhindre fysiske angreb, der manipulerer UEFI-firmwaren. På disse Mac-computere ligger tillidsroden for UEFI-firmwaren i T2-firmwaren som beskrevet i Startproces på en Intel-baseret Mac.

Intel Management Engine (ME) – underkomponent

Firmware til *Intel Management Engine (ME)* er en underkomponent, som opbevares i UEFI-firmwaren. ME er en separat processor og et separat subsystem med Intel-chips og bruges primært til copyrightbeskyttelse af lyd og video på en Mac, der kun har Intel-baserede grafikkort. En Intel-baseret Mac anvender speciel ME-firmware, hvorfra de fleste komponenter er blevet fjernet, til at reducere denne underkomponents angrebsflade. Eftersom ME-firmwaren på Mac er mindre end den minimale standardfirmware, som Intel stiller til rådighed, er mange komponenter, der tidligere har givet anledning til kritik fra sikkerhedseksperter, ikke længere til stede.

System Management Mode (SMM)

Intel-processorer har en særlig afviklingstilstand, som er forskellig fra den almindelige driftstilstand. Den kaldes *System Management Mode (SMM)* og blev oprindeligt indført for at håndtere tidsfølsomme handlinger som strømstyring. Historisk set har Mac-computere dog brugt en separat mikrostyreenhed kaldet *System Management Controller (SMC)* til at udføre den type handlinger. SMC er ikke længere en separat mikrostyreenhed, men er blevet integreret i T2-chippen.

Systemsikkerhed til watchOS

Apple Watch bruger mange af de samme hardwarebaserede funktioner i platformsikkerheden som iOS og iPadOS. Apple Watch gør f.eks. følgende:

- Udfører sikker start og sikre softwareopdateringer
- Opretholder operativsystemets integritet
- Bidrager til at beskytte data, både på enheden og under kommunikation med en iPhone, den har dannet par med, eller internettet

De understøttede teknologier er anført under Systemsikkerhed (f.eks. KIP, SKP og SCIP) samt teknologier inden for Databeskyttelse, Nøglering og netværk.

Opdatering af watchOS

watchOS kan konfigureres til at blive opdateret i løbet af natten. Der er flere oplysninger om, hvordan Apple Watch-koden opbevares og bruges under opdateringen, i Nøglesamlinger.

Registrering af håndled

Hvis Registrering af håndled er slået til, låses enheden automatisk, kort efter at den er blevet fjernet fra brugerens håndled. Hvis Registrering af håndled er slået fra, kan Apple Watch låses ved hjælp af låsemuligheden i Kontrolcenter. Når Apple Watch er låst, kan Apple Pay kun bruges, hvis koden indtastes på Apple Watch. Registrering af håndled slås fra med appen Apple Watch på iPhone. Denne indstilling kan også håndhæves vha. en MDM-løsning (Mobile Device Management).

Aktiveringslås

Når Find er slået til på iPhone, kan det Apple Watch, den er parret med, bruge Aktiveringslås. Aktiveringslås gør det sværere for personer at bruge eller sælge et Apple Watch, som mistes eller bliver stjålet. Aktiveringslås kræver brugerens Apple-id og den tilhørende adgangskode for at ophæve pardannelsen eller slette eller genaktivere et Apple Watch.

Sikker pardannelse med iPhone

Apple Watch kan kun danne par med en iPhone ad gangen. Når pardannelsen med Apple Watch ophæves, sender iPhone instruktioner om, at alt indhold og alle data skal slettes fra Apple Watch.

Pardannelse mellem Apple Watch og iPhone sikres vha. en OOB-proces (Out-Of-Band) til udveksling af offentlige nøgler efterfulgt af BLE-forbindelsens “shared secret”. Apple Watch viser et animeret mønster, som optages af kameraet på iPhone. Mønsteret indeholder en kodet nøgle, som bruges til BLE 4.1 OOB-pardannelse. Der bruges en almindelig BLE-kodeoptegnelse som reservemetode til pardannelse, hvis det viser sig nødvendigt.

Når BLE-sessionen er etableret og krypteret vha. den protokol med størst sikkerhed, der er tilgængelig i BLE Core Specification, udveksler iPhone og Apple Watch nøgler på en af følgende måder:

- Med en proces, der er tilpasset fra Apple Identity Service (IDS) som beskrevet i Oversigt over iMessage-sikkerhed.
- Med en nøgleudveksling ved hjælp af IKEv2/IPsec. Den første udveksling af nøgler godkendes enten ved hjælp af Bluetooth-sessionsnøglen (i situationer med pardannelse) eller IDS-nøglerne (i situationer, hvor operativsystemet skal opdateres). Hver enhed genererer et par med en offentlig og privat Ed25519-nøgle på 256 bit, og de offentlige nøgler udveksles under den første nøgleudveksling.

Bemærk: Der bruges forskellige mekanismer til nøgleudveksling og kryptering, afhængigt af hvilke operativsystemversioner der findes på iPhone og Apple Watch. iPhone-enheder med iOS 13 eller en nyere version bruger kun IKEv2/IPsec til nøgleudveksling og kryptering, når de danner par med et Apple Watch med watchOS 6 eller en nyere version.

Efter udvekslingen af nøgler:

- Bluetooth-sessionsnøglen kasseres, og al kommunikation mellem iPhone og Apple Watch krypteres med en af de metoder, der er anført ovenfor. De krypterede forbindelser via Bluetooth, Wi-Fi og mobilnetværk udgør et sekundært krypteringslag.
- (Kun IKEv2/IPsec) Nøglerne opbevares i systemnøgleringen og bruges til at godkende efterfølgende IKEv2/IPsec-sessioner mellem enhederne. Videre kommunikation mellem enhederne krypteres og integritetsbeskyttes ved hjælp af AES-256-GCM eller ChaCha20-Poly1305 (256-bit nøgler) på iPhone-enheder med iOS 15 eller en nyere version, som er parret med et Apple Watch Series 4 eller en nyere model med watchOS 8 eller en nyere version.

Bluetooth Low Energy-enhedsadressen bliver udskiftet med intervaller på 15 minutter for at mindske risikoen for, at enheden spores lokalt, hvis nogen udsender en vedholdende identifikator.

For at understøtte apps, der kræver streamingdata, leveres kryptering med metoder, der er beskrevet under FaceTime-sikkerhed, ved brug af den Apple Identity Service-tjeneste (IDS), som leveres af den iPhone, der er dannet par med, eller af en direkte internetforbindelse.

Apple Watch implementerer hardwarekrypteret lagringsplads og klassebaseret beskyttelse af arkiver og nøgleringsemner. Der bruges også nøglesamlinger med adgangskontrol til nøgleringsemner. De nøgler, der bruges til at kommunikere mellem Apple Watch og iPhone, sikres også vha. klassebaseret beskyttelse. Du kan få flere oplysninger i Nøglesamlinger til Databeskyttelse.

Lås automatisk op og Apple Watch

For at gøre det nemmere at bruge flere Apple-enheder kan nogle enheder i visse situationer automatisk låse andre enheder op. Automatisk oplåsning har tre anvendelsesområder:

- Et Apple Watch kan låses op af en iPhone.
- En Mac kan låses op af et Apple Watch.
- En iPhone kan låses op af et Apple Watch, når der registreres en bruger med tildækket næse og mund.

Alle tre anvendelsesområder bygger på samme grundlag: En STS-protokol (Station-to-Station) med gensidig godkendelse, hvor der udveksles langtidsholdbare nøgler, når funktionen slås til, og unikke midlertidige sessionsnøgler for hver anmodning. Uanset den underliggende kommunikationskanal forhandles STS-tunnelen direkte mellem Secure Enclave i begge enheder, og alt kryptografisk materiale holdes inden for dette sikre domæne (bortset fra Mac-computere uden Secure Enclave, som afbryder STS-tunnelen i kernen).

Oplåsning

Hele oplåsningsprocessen kan inddeles i to faser: Først danner den enhed, der skal låses op (“modtageren”), en kryptografisk hemmelighed til oplåsning og sender den til den enhed, der skal foretage oplåsningen (“iværksætteren”). Derefter foretager iværksætteren oplåsningen ved hjælp af den hemmelighed, der blev dannet tidligere.

Enhederne forbereder automatisk oplåsning ved at oprette en BLE-forbindelse til hinanden. Derefter sendes en tilfældigt genereret hemmelighed på 32 byte til oplåsning til iværksætteren via STS-tunnelen. Under den næste oplåsning med biometrik eller adgangskode kombinerer målenheden sin nøgle afledt af kode (PDK) med hemmeligheden til oplåsning fra sin hukommelse.

Oplåsningen foretages, ved at enhederne opretter en ny BLE-forbindelse og derefter bruger Peer-to-Peer Wi-Fi til at anslå afstanden mellem dem på en sikker måde. Hvis enhederne er inden for den fastlagte rækkevidde, og de nødvendige sikkerhedspolitikker er overholdt, sender iværksætteren sin hemmelighed til oplåsning til modtageren via STS-tunnelen. Modtageren danner derefter en ny hemmelighed til oplåsning på 32 byte og sender til den iværksætteren. Hvis den aktuelle hemmelighed til oplåsning, der er sendt af iværksætteren, kan dekryptere oplåsningsposten, låses modtagerenheden, og PDK kombineres med en ny hemmelighed til oplåsning. Til sidst slettes den nye hemmelighed til oplåsning og PDK fra modtagerens hukommelse.

Sikkerhedspolitikker for automatisk oplåsning af Apple Watch

Af praktiske hensyn kan Apple Watch låses op af en iPhone lige efter den første start, uden at brugeren først skal skrive koden på Apple Watch. Det opnås ved, at den tilfældige hemmelighed til oplåsning (der blev genereret under den allerførste oplåsningsproces, efter at funktionen blev slået til) bruges til at oprette en langtidsholdbar deponeringspost, som opbevares i nøglesamlingen Apple Watch. Hemmeligheden i deponeringsposten opbevares i nøgleringen på iPhone og bruges til at igangsætte en ny session efter hver genstart af Apple Watch.

Sikkerhedspolitikker for automatisk oplåsning af iPhone

Der gælder ekstra sikkerhedspolitikker for automatisk oplåsning af iPhone med Apple Watch. Apple Watch kan ikke bruges i stedet for Face ID på iPhone til andre funktioner som Apple Pay eller app-godkendelser. Når Apple Watch låser en parret iPhone op, vises en notifikation på uret, og der afspilles en tilhørende haptisk feedback. Hvis brugeren trykker på knappen Lås iPhone i notifikationen, sender uret en låsekommando til iPhone via BLE. Når iPhone modtager låsekommandoen, låser den og slår både Face ID og oplåsning ved hjælp af Apple Watch fra. Den næste oplåsning af iPhone skal foretages med koden til iPhone.

Oplåsning af en parret iPhone fra Apple Watch (når funktionen er slået til), forudsætter, at følgende kriterier er opfyldt:

- iPhone skal være blevet låst op med en anden metode, mindst en gang efter at det tilknyttede Apple Watch blev sat på håndleddet og låst op.
- Sensorer skal kunne registrere, at næse og mund er tildækket.
- Den målte afstand må højst være 2–3 meter
- Funktionen Sengetid må ikke være slået til på Apple Watch.
- Apple Watch eller iPhone skal have været låst op for nylig, eller Apple Watch skal have registreret fysisk bevægelse, der viser, at brugeren er aktiv (og ikke sover for eksempel).
- iPhone skal være blevet låst op mindst en gang i løbet af de sidste 6,5 timer.
- iPhone skal være i en tilstand, hvor Face ID har tilladelse til at foretage en oplåsning af enheden. (Du kan få flere oplysninger i Face ID, Touch ID, koder og adgangskoder).

Godkend i macOS med Apple Watch

Når automatisk oplåsning med Apple Watch er slået til, kan Apple Watch bruges i stedet for eller sammen med Touch ID til at godkende adgang og beskeder om godkendelse fra:

- macOS og Apple-apps, der beder om godkendelse
- Tredjepartsapps, der beder om godkendelse
- Gemte Safari-adgangskoder
- Sikre noter

Sikker brug af Wi-Fi, mobilforbindelse, iCloud og Gmail

Når Apple Watch ikke er inden for Bluetooth-rækkevidde, kan Wi-Fi- eller mobilnetværk bruges i stedet. Apple Watch opretter automatisk forbindelse til Wi-Fi-netværk, der allerede har været forbindelse til på den parrede iPhone, og hvis godkendelsesoplysninger er blevet synkroniseret til Apple Watch, mens begge enheder var inden for rækkevidde. Denne funktion til automatisk forbindelse kan derefter konfigureres pr. netværk under Wi-Fi i appen Indstillinger på Apple Watch. Hvis ingen af enhederne tidligere har oprettet forbindelse til Wi-Fi-netværket, kan der manuelt oprettes forbindelse til netværket under Wi-Fi i Indstillinger på Apple Watch.

Når Apple Watch og iPhone er uden for rækkevidde, opretter Apple Watch direkte forbindelse til iCloud- og Gmail-servere for at hente e-mail, i stedet for at synkronisere Mail-data med den parrede iPhone via internettet. Når det gælder Gmail-konti, skal brugeren legitimere sig over for Google i Mail-delen af appen Watch på iPhone. Det OAuth-token, der modtages fra Google, sendes til Apple Watch i krypteret format via IDS (Apple Identity Service), så det kan bruges til at hente e-mail. Dette OAuth-token bruges aldrig til forbindelse med Gmail-serveren fra den parrede iPhone.

Generering af tilfældige tal

Kryptografiske pseudotilfældige talgeneratorer (CPRNG'er) er en vigtig byggesten i sikker software. Til det formål benytter Apple et betroet stykke CPRNG-software, der kører på kernerne i iOS, iPadOS, macOS, tvOS og watchOS. CPRNG-softwaren er ansvarlig for at akkumulere rå entropi fra systemet og tilvejebringe sikre tilfældige tal til brugerne både i kernen og i brugerområdet.

Entropikilder

CPRNG'en i kernen forsynes af flere entropikilder både i startprocessen og i løbet af enhedens levetid. Disse omfatter (afhængigt af om de er til rådighed):

- Hardware-TRNG i Secure Enclave
- Tidsafhængig jitter indsamlet under start
- Entropi indsamlet fra hardwareafbrydelser
- En skabelon, der bruges til at sikre entropi ved start
- Tilfældige Intel-instruktioner, f.eks. RDSEED og RDRAND (kun på en Intel-baseret Mac)

CPRNG i kernen

CPRNG i kernen er et Fortuna-baseret design beregnet på et 256-bit sikkerhedsniveau. Den tilvejebringer tilfældige tal af høj kvalitet til brugerområdet ved hjælp af følgende API'er:

- Systemkaldet `getentropy`(2)
- Den tilfældige enhed (/dev/random)

CPRNG i kernen accepterer brugerleveret entropi via skrivning til den tilfældige enhed.

Apples enhed til sikkerhedsforskning

Apples enhed til sikkerhedsforskning er en specialudstyret iPhone, som sikkerhedsforskere kan bruge til at udføre forskning i iOS uden at omgå funktionerne i platformsikkerheden på iPhone eller slå funktionerne fra. Med denne enhed kan en forsker sideindlæse indhold, som kører med samme tilladelser som på platformen, og dermed udføre forskning på en platform, der er tættere på produktionsenheders platform.

For at bidrage til at sikre at brugerenheder ikke påvirkes af afviklingspolitikken på enheden til sikkerhedsforskning, bliver ændringer af politikken implementeret i en variant af iBoot og i kernesamlingen til systemstart. De vil ikke starte på brugerens hardware. Forskningsenhedens iBoot kontrollerer, om der er en ny specialtilstand, og starter en panic-sløjfe, hvis den afvikles på specialudstyret hardware, der ikke bruges til forskning.

Subsystemet cryptex giver en forsker mulighed for at indlæse en personliggjort buffer til godkendelse og et diskbillede med tilsvarende indhold. Der er implementeret en række dybdegående forsvarsforanstaltninger, der har til formål at sikre, at dette subsystem ikke tillader afvikling på brugernes enheder:

- `launchd` indlæser ikke launchd-egenskabslisten `cryptexd`, hvis den registrerer en almindelig kundeenhed.
- `cryptexd` afbrydes, hvis den registrerer en almindelig kundeenhed.
- `AppleImage4` stiller ikke den nonce-værdi, som bruges til at kontrollere en forsknings-cryptex på en almindelig kundeenhed, til rådighed.
- Signeringsserveren afviser at personliggøre et cryptex-diskbillede til en enhed, som ikke står på en liste med kun de tilladte enheder.

For at respektere sikkerhedsforskerens anonymitet er det kun målinger (f.eks. hash-værdier) for app-arkiverne eller kernebufferen og id'er til enheden til sikkerhedsforskning, der sendes til Apple ved personliggørelse. Apple modtager ikke indholdet i den cryptex, der indlæses på enheden.

For at undgå at en hacker forsøger at få en forskningsenhed til at ligne en brugerenhed, så andre kan narres til at bruge den til almindelige ting, afviger enheden til sikkerhedsforskning på følgende måder:

- Enheden til sikkerhedsforskning kan kun starte, mens den oplades. Den kan oplades med et Lightning-kabel eller en Qi-kompatibel oplader. Hvis enheden ikke oplades under starten, skifter den til gendannelsesfunktion. Hvis en bruger begynder at oplade enheden og genstarter den, starter den på normal vis. Så snart XNU er startet, behøver enheden ikke længere at være under opladning for at kunne bruges.
- Teksten *Security Research Device* vises under Apple-logoet, når iBoot starter.
- XNU-kernen starter i detaljeret tilstand.
- På siden af enheden er følgende tekst indgraveret: "Property of Apple. Confidential and Proprietary. Call +1 877 595 1125."

Følgende ekstra foranstaltninger er implementeret i software, der vises efter enhedens start:

- Teksten *Security Research Device* vises under indstilling af enheden.
- Teksten *Security Research Device* vises på den låste skærm og i appen Indstillinger.

Enheden til sikkerhedsforskning giver forskerne muligheder, som de ikke har på en brugerenhed. De kan gøre følgende:

- Sideindlæse app-kode på enheden med vilkårlige berettigelser på samme tilladelsesniveau som komponenter i Apple-operativsystemet
- Starte tjenester under systemstarten
- Bevare indhold fra en genstart til den næste
- Bruge rettigheden `research.com.apple.license-to-operate` til at give en proces tilladelse til at foretage fejlfinding af en anden proces på systemet, herunder systemprocesser.

  Navneområdet `research.` respekteres kun af varianten RESEARCH af kerneudvidelsen AppleMobileFileIntegrity. Enhver proces med denne rettighed på en kundeenhed afbrydes under signaturkontrollen.
- Personliggør og gendan en speciel kernebuffer

Kryptering og databeskyttelse

Oversigt over kryptering og databeskyttelse

Både den sikre startkæde, systemsikkerheden og mulighederne for app-sikkerhed bidrager til at kontrollere, at kun godkendt kode og godkendte apps afvikles på en enhed. Apple-enheder har yderligere krypteringsfunktioner, der har til formål at beskytte brugerdata, også i situationer, hvor andre dele af sikkerhedsinfrastrukturen er blevet svækket (f.eks. hvis en enhed er blevet væk eller afvikler kode, der ikke er godkendt). Alle disse funktioner indebærer store fordele for både brugere og it-administratorer. Personlige oplysninger og virksomhedsdata beskyttes, og hvis en enhed bliver stjålet eller bliver væk, kan den øjeblikkeligt slettes fuldstændigt eksternt.

iOS- og iPadOS-enheder bruger en metode til kryptering af arkiver, der kaldes *Databeskyttelse*, mens data på en Intel-baseret Mac beskyttes med en teknologi til kryptering af diskenheder, som kaldes *FileVault*. En Mac med Apple Silicon bruger en hybridmodel, der understøtter Databeskyttelse med to undtagelser: Det laveste beskyttelsesniveau (D) understøttes ikke, og standardniveauet (klasse C) bruger en diskenhedsnøgle og fungerer lige som FileVault på en Intel-baseret Mac. Hierarkier til nøgleadministration er i alle tilfælde forankret i et dedikeret område af Secure Enclave, og et dedikeret AES-modul understøtter kryptering med linjehastighed og bidrager til at sikre, at krypteringsnøgler med lang levetid ikke kan ses af kerneoperativsystemet eller CPU'en (hvor de kan blive kompromitteret). (En Intel-baseret Mac med en T1-chip eller uden Secure Enclave bruger ikke et dedikeret område til at beskytte sine krypteringsnøgler til FileVault).

Ud over Databeskyttelse og FileVault bruger Apple *operativsystemkerner* som led i håndhævelsen af beskyttelse og sikkerhed. Kernen bruger adgangskontrol til at anbringe apps i et isoleret miljø (hvor apps har adgang til begrænsede data) og en mekanisme ved navn *Data Vault* (som i stedet for at begrænse de kald, en app kan foretage, begrænser adgangen fra andre apps til appens data).

Koder og adgangskoder

Apple bruger koder i iOS og iPadOS og adgangskoder i macOS til at beskytte brugerdata mod ondsindede angreb. Jo længer en kode eller adgangskode er, des stærkere er den – og jo lettere er det at modvirke brute-force-angreb. Apple gør angreb endnu mere besværlige ved at benytte tidsforsinkelser (til iOS og iPadOS) og fastlægge et begrænset antal adgangskodeforsøg (til Mac).

Når en bruger i iOS og iPadOS indstiller en kode eller en adgangskode til enheden, slås databeskyttelse automatisk til. Databeskyttelse slås også til på andre enheder, der indeholder en Apple SoC (System on Chip), f.eks. en Mac med Apple Silicon, Apple TV og Apple Watch. I macOS bruger Apple *FileVault*, som er en indbygget app til kryptering af enheder.

Sådan øger stærke koder og adgangskoder sikkerheden

iOS og iPadOS understøtter koder på seks eller fire cifre og alfanumeriske koder med en vilkårlig længde. Ud over at låse enheden op sørger koden eller adgangskoden for entropi til visse krypteringsnøgler. Det betyder, at en person med ondsindede hensigter, som er i besiddelse af enheden, ikke kan få adgang til data i bestemte beskyttelsesklasser uden koden.

Koden eller adgangskoden er kombineret med enhedens UID, så det er nødvendigt at udføre såkaldte brute force-forsøg ved angreb på enheden. Et stort antal gentagelser bruges til at gøre hvert forsøg langsommere. Antallet af gentagelser er kalibreret, så hvert forsøg tager ca. 80 millisekunder. Det ville faktisk tage mere end fem et halvt år at prøve med alle kombinationer af en alfanumerisk kode på seks tegn bestående af små bogstaver og tal.

Jo stærkere brugerens kode er, des stærkere bliver krypteringsnøglen. Og med Face ID og Touch ID kan brugeren anvende en langt stærkere kode, end det normalt ville være praktisk muligt. Den stærkere kode øger det effektive omfang af entropi, som beskytter de krypteringsnøgler, der bruges til Databeskyttelse, uden at det bliver besværligt for brugeren at låse en enhed op flere gange om dagen.

Hvis der skal indtastes en lang adgangskode, der kun består af tal, vises en numerisk blok på den låste skærm i stedet for hele tastaturet. Det kan være nemmere at indtaste en lang numerisk kode i stedet for en kortere alfanumerisk kode og samtidig opnå stort set samme sikkerhed.

Brugerne kan angive en længere alfanumerisk kode ved at vælge Speciel alfanumerisk kode under Indstillinger til kode i Indstillinger > Touch ID & kode eller Face ID & kode.

Brug af trinvis forøgelse af tidsforsinkelse mod brute-force-angreb (iOS, iPadOS)

I iOS og iPadOS gøres brute-force-angreb på koder endnu mere besværlige vha. en trinvis forøgelse af tidsforsinkelsen, når der er indtastet en ugyldig kode på den låste skærm. Det er vist i tabellen herunder.

Forsøg	Forsinkelse
1-4	Ingen
5	1 minut
6	5 minutter
7-8	15 minutter
9	1 time

Hvis indstillingen Slet data er slået til (i Indstillinger > Touch ID & kode), fjernes alt indhold og alle indstillinger fra disken efter 10 forgæves forsøg i træk på at indtaste koden. Flere på hinanden følgende forsøg med den samme forkerte kode tæller kun som et forgæves forsøg. Denne indstilling er også tilgængelig som en administrativ politik via en løsning til administration af mobile enheder (MDM), der understøtter denne funktion, og via Microsoft Exchange ActiveSync, og den kan indstilles til en lavere grænse.

På enheder med Secure Enclave håndhæves forsinkelserne af Secure Enclave. Hvis enheden genstartes under en tidsforsinkelse, gennemtvinges forsinkelsen stadig, og timeren starter forfra med den aktuelle periode.

Brug af trinvis forøgelse af tidsforsinkelse mod brute-force-angreb (macOS)

Med henblik på at forhindre brute force-angreb er højst 10 adgangskodeforsøg tilladt i login-vinduet eller ved brug af Computer som ekstern harddisk, når Mac startes. Desuden øges tiden fra et vist antal forkerte forsøg, til næste forsøg er muligt, gradvist. Tidsforsinkelserne styres af Secure Enclave. Hvis Mac genstartes under en tidsforsinkelse, gennemtvinges forsinkelsen stadig, og timeren starter forfra med den aktuelle periode.

I tabellen herunder vises forsinkelser mellem kodeforsøg på en Mac med Apple Silicon og en Mac med en T2-chip.

Forsøg	Forsinkelse
5	1 minut
6	5 minutter
7	15 minutter
8	15 minutter
9	1 time
10	Slået fra

Med henblik på at forhindre malware i at skabe permanent datatab som følge af angreb på brugerens adgangskode håndhæves disse tidsgrænser ikke, når brugeren har logget ind på Mac, men de gælder igen, når Mac startes igen. Hvis de 10 forsøg er blevet brugt, er det muligt at få 10 forsøg mere ved at starte i macOS-gendannelse. Hvis disse forsøg heller ikke lykkes, er der mulighed for yderligere 10 forsøg for hver FileVault-gendannelsesfunktion (iCloud-gendannelse, FileVault-gendannelsesnøgle og organisationens nøgle) – i alt 30 forsøg mere. Når disse ekstra forsøg er brugt, behandler Secure Enclave ikke længere anmodninger om at dekryptere enheden eller godkende adgangskoden, og det er ikke længere muligt at gendanne enhedens data.

Som led i beskyttelsen af data i et virksomhedsmiljø skal it-afdelingen definere og håndhæve konfigureringspolitikker til FileVault ved hjælp af en MDM-løsning. Virksomheder har adskillige muligheder til administration af krypterede enheder, bl.a. gendannelsesnøgler fra organisationen (som valgfrit kan deponeres hos MDM), eller en kombination af begge. Rotation af nøgler kan også indstilles som en politik i MDM.

På en Mac med Apple T2-sikkerhedschippen fungerer adgangskoder på stort set samme måde, bortset fra at den genererede nøgle bruges til FileVault-kryptering i stedet for Databeskyttelse. macOS har desuden flere muligheder for at gendanne adgangskoder:

- iCloud-gendannelse
- FileVault-gendannelse
- Institutionens nøgle til FileVault

Databeskyttelse

Oversigt over Databeskyttelse

Apple bruger en teknologi kaldet Databeskyttelse til at beskytte data, der opbevares i flashlageret på enheder med en Apple SoC, f.eks. iPhone, iPad, Apple Watch, Apple TV og Mac-computere med Apple Silicon. Med Databeskyttelse kan en enhed reagere på almindelige begivenheder som indgående telefonopkald, samtidig med at funktionen sørger for kryptering af brugerdata på højt niveau. Visse systemapps (f.eks. Beskeder, Mail, Kalender, Kontakter og Fotos) og data fra Sundhed bruger som standard Databeskyttelse. Apps fra tredjeparter får automatisk denne beskyttelse.

Implementering

Databeskyttelse implementeres ved, at et hierarki med nøgler opbygges og administreres, og bygger på de teknologier til hardwarekryptering, der er integreret i Apple-enheder. Databeskyttelse styres pr. arkiv. Hvert arkiv tildeles en klasse, og adgangen til arkivet bestemmes af, om klassenøglerne er blevet låst op. APFS (Apple File System) gør, at nøgler i arkivsystemet kan underinddeles yderligere inden for områder (hvor dele af et arkiv kan have forskellige nøgler).

Hver gang der oprettes et arkiv på dataenheden, opretter Databeskyttelse en ny 256-bit nøgle (*arkivnøglen*). Nøglen overdrages til AES-modulet i hardwaren, som bruger nøglen til at kryptere arkivet, når det skrives til flashlageret. På enheder med en A14-chip, A15-chip eller en chip i M1-familien bruger krypteringen AES-256 i XTS-funktion, hvor 256-bit arkivnøglen behandles med en funktion til nøgleafledning (NIST Special Publication 800-108) for at aflede en 256-bit "tweak"-nøgle og en 256-bit ciffernøgle. I hardwaregenerationerne A9 til og med A13, S5, S6 og S7 bruges AES-128 i XTS-funktion, hvor 256-bit arkivnøglen deles til en 128-bit "tweak"-nøgle og en 128-bit ciffernøgle.

På en Mac med Apple Silicon bruger Databeskyttelse som standard klasse C (se Databeskyttelsesklasser), men benytter en diskenhedsnøgle i stedet for en nøgle pr. område eller pr. arkiv og genskaber dermed FileVaults sikkerhedsmodel til brugerdata. Brugerne skal stadig tilvælge FileVault for at få den fulde beskyttelse, der opnås ved at kombinere hierarkiet med krypteringsnøgler med deres adgangskode. Udviklere kan også tilvælge en højere beskyttelsesklasse, hvor der benyttes en nøgle pr. arkiv eller pr. område.

Databeskyttelse på Apple-enheder

På Apple-enheder med Databeskyttelse er hvert arkiv beskyttet af en unik nøgle pr. arkiv (eller pr. område). Nøglen, der er pakket med nøgleindpakningsalgoritmen NIST AED, pakkes derudover med en af flere mulige klassenøgler, afhængigt af hvordan der skal være adgang til arkivet. Den indpakkede nøgle pr. arkiv opbevares derefter i arkivets metadata.

Enheder med APFS-format understøtter måske kloning af arkiver (kopier uden omkostninger ved hjælp af teknologien kopier ved skrivning). Hvis et arkiv kopieres, får hver halvdel af kopien en ny nøgle til accept af indgående skrivninger, så der skrives nye data til mediet med en ny nøgle. Over tid kan arkivet komme til at bestå af forskellige områder (eller fragmenter), der hver knyttes til forskellige nøgler. Alle de områder, der udgør et arkiv, beskyttes imidlertid af samme klassenøgle.

Når et arkiv åbnes, dekrypteres dets metadata med arkivsystemnøglen, og den indpakkede arkivnøgle og en notation til den klasse, der beskytter arkivet, vises. Arkivnøglen (eller områdenøglen) pakkes ud med klassenøglen og overdrages derefter til AES-modulet til hardware, som dekrypterer arkivet, mens det læses fra flashlageret. Al håndtering af den indpakkede arkivnøgle finder sted i Secure Enclave. Arkivnøglen vises aldrig direkte til app-processoren. Når enheden startes, afhandler Secure Enclave en midlertidig nøgle med AES-modulet. Når Secure Enclave udpakker et arkivs nøgler, pakkes de igen med den midlertidige nøgle og sendes tilbage til app-processoren.

Metadata til alle arkiver i dataenhedens arkivsystem krypteres med en tilfældig enhedsnøgle, som oprettes, når operativsystemet installeres første gang, eller når enheden slettes af en bruger. Nøglen krypteres og indpakkes af en nøgle til nøgleindpakning, som kun kendes af Secure Enclave, med henblik på langvarig opbevaring. Nøglen til nøgleindpakning skifter, hver gang en bruger sletter sin enhed. I A9 (og nyere) SoC'er benytter Secure Enclave entropi suppleret med systemer, der forhindrer genafspilning (nonce), til at opnå sletbarhed og til at beskytte sin nøgle til nøgleindpakning og andre aktiver. Du kan få flere oplysninger i Sikkert ikke-flygtigt lager.

Ligesom arkivnøgler eller områdenøgler vises metadatanøglen til dataenheden aldrig direkte for app-processoren. Secure Enclave leverer i stedet en midlertidig version til hver start. Under opbevaring er den krypterede arkivsystemnøgle desuden pakket med en sletbar nøgle ("effaceable key"), der opbevares i Effaceable Storage, eller med en medienøgle til nøgleindpakning, som beskyttes af den Secure Enclave-mekanisme, der forhindrer genafspilning. Denne nøgle øger ikke datafortroligheden yderligere. Dens formål er derimod, at den hurtigt kan slettes ved behov (af brugeren med indstillingen Slet alt indhold og alle indstillinger eller af en bruger eller administrator, der afsender en ekstern slettekommando fra en løsning til administration af mobile enheder (MDM), Microsoft Exchange ActiveSync eller iCloud). Når nøglen slettes på denne måde, ophæves al kryptografisk adgang til alle arkiver.

Indholdet af et arkiv kan krypteres med en eller flere nøgler pr. arkiv (eller pr. område), der pakkes med en klassenøgle og opbevares i et arkivs metadata, som på sin side krypteres med arkivsystemnøglen. Klassenøglen beskyttes med hardwarens UID og for nogle klasser også med brugerens kode. Dette hierarki er både fleksibelt og effektivt. Således skal arkivnøglen blot pakkes om, hvis et arkivs klasse ændres, mens en ændring af koden kun kræver, at klassenøglen pakkes om.

Databeskyttelsesklasser

Når der oprettes et nyt arkiv på enheder, der understøtter Databeskyttelse, tildeles det en klasse af den app, som opretter det. Hver klasse benytter forskellige strategier til at afgøre, hvornår der er adgang til dataene. De grundlæggende klasser og strategier er beskrevet i følgende afsnit. Apple Silicon-baserede Mac-computere understøtter ikke klasse D: Klassen Ingen beskyttelse og en sikkerhedsafgrænsning etableres, når der logges ind og ud (ikke ved låsning og oplåsning som på iPhone, iPad og iPod touch).

Klasse	Beskyttelsestype
Klasse A: Fuldstændig beskyttelse	NSFileProtectionComplete
Klasse B: Beskyttet, hvis ikke åben	NSFileProtectionCompleteUnlessOpen
Klasse C: Beskyttet indtil første brugergodkendelse *Bemærk:* macOS bruger en diskenhedsnøgle til at genskabe FileVaults beskyttelsesegenskaber.	NSFileProtectionCompleteUntilFirstUserAuthentication
Klasse D: Ingen beskyttelse *Bemærk:* Understøttes ikke i macOS.	NSFileProtectionNone

Fuldstændig beskyttelse

NSFileProtectionComplete: Klassenøglen beskyttes med en nøgle, der er afledt af brugerens kode eller adgangskode og enhedens UID. Kort efter at brugeren har låst en enhed (10 sekunder, hvis Bed om adgangskode er indstillet til Straks), kasseres den krypterede klassenøgle, hvorved adgangen til alle data i klassen fjernes, indtil brugeren indtaster koden igen eller låser enheden op (eller logger ind på enheden) ved hjælp af Face ID eller Touch ID.

I macOS kasseres den dekrypterede klassenøgle, kort tid efter at den sidste bruger er logget ud, hvorved adgangen til alle data i klassen fjernes, indtil en bruger indtaster koden igen eller logger ind på enheden ved hjælp af Touch ID.

Beskyttet, hvis ikke åben

NSFileProtectionCompleteUnlessOpen: Det kan være nødvendigt at skrive visse arkiver, mens enheden er låst, eller brugeren er logget ud. Et godt eksempel er et e-mailbilag, der hentes i baggrunden. Denne funktionsmåde opnås ved at bruge asymmetrisk elliptisk kurvekryptografi (ECDH over Curve25519). Den sædvanlige arkivnøgle beskyttes af en nøgle, der er dannet ved hjælp af en One-Pass Diffie-Hellman-nøgleaftale, som er beskrevet i NIST SP 800-56A.

Den midlertidige offentlige nøgle til aftalen opbevares sammen med den indpakkede arkivnøgle. KDF er Concatenation Key Derivation Function (godkendt alternativ 1) som beskrevet under 5.8.1 i NIST SP 800-56A. AlgorithmID er udeladt. PartyUInfo og PartyVInfo er henholdsvis den midlertidige og den statiske offentlige nøgle. SHA256 bruges som hashing-funktion. Så snart arkivet lukkes, slettes arkivnøglen fra hukommelsen. Når arkivet skal åbnes igen, oprettes nøglen (“shared secret”) igen ved hjælp af den private nøgle til klassen NSFileProtectionCompleteUnlessOpen (Beskyttet, hvis ikke åben) og arkivets midlertidige offentlige nøgle, som bruges til at pakke arkivnøglen ud. Derefter dekrypteres arkivet med arkivnøglen.

I macOS er den private del af NSFileProtectionCompleteUnlessOpen tilgængelig, så længe alle brugere i systemet er logget ind eller godkendt.

Beskyttet indtil første brugergodkendelse

NSFileProtectionCompleteUntilFirstUserAuthentication: Denne klasse fungerer på samme måde som NSFileProtectionComplete (Fuldstændig beskyttelse), bortset fra at den dekrypterede klassenøgle ikke fjernes fra hukommelsen, når enheden låses, eller brugeren logger ud. Beskyttelsen i denne klasse har stort set samme egenskaber som fuld diskbeskyttelse på skrivebordscomputere og beskytter data mod angreb, der omfatter genstart af enheden. Det er standardklassen til alle data i apps fra tredjeparter, som ikke er tildelt en anden databeskyttelsesklasse.

I macOS benytter denne klasse en diskenhedsnøgle, der er tilgængelig, så længe enheden er aktiveret, og fungerer præcis som FileVault.

Ingen beskyttelse

NSFileProtectionNone: Denne klassenøgle er kun beskyttet med UID og opbevares i Effaceable Storage. Eftersom alle de nøgler, der skal bruges til at dekryptere arkiver i denne klasse, opbevares på enheden, er den eneste fordel ved krypteringen, at enheden hurtigt kan slettes eksternt. Selvom et arkiv ikke tildeles en databeskyttelsesklasse, opbevares det stadig i krypteret format (det gælder alle data på iOS- og iPadOS-enheder).

Det understøttes ikke i macOS.

Bemærk: i macOS gælder, at for enheder, der ikke svarer til et startet operativsystem, er alle databeskyttelsesklasser tilgængelige, så længe enheden er aktiveret. Databeskyttelsesklassen NSFileProtectionCompleteUntilFirstUserAuthentication er standard. Funktioner til nøgler pr. område findes til både Rosetta 2 og lokale apps.

Nøglesamlinger til Databeskyttelse

Nøglerne til klasserne i Databeskyttelse til både arkiver og nøglering er samlet i og administreres i nøglesamlinger i iOS, iPadOS, watchOS og tvOS. Disse operativsystemer bruger følgende nøglesamlinger: bruger, enhed, sikkerhedskopi, depot og iCloud-sikkerhedskopi.

Nøglesamlingen Bruger

Nøglesamlingen Bruger er det sted, hvor de indpakkede klassenøgler, som bruges under den normale drift af enheden, opbevares. Når der f.eks. indtastes en kode, indlæses *NSFileProtectionComplete* fra nøglesamlingen Bruger og pakkes ud. Det er et binært egenskabslistearkiv (.plist), der opbevares i klassen Ingen beskyttelse.

På enheder med en SoC-processor før A9 krypteres indholdet af .plist-arkivet med en nøgle i Effaceable Storage. Fremadrettet sikkerhed til nøglesamlinger sikres ved, at denne nøgle slettes og dannes igen, hver gang en bruger skifter kode.

På enheder med A9- eller nyere SoC-processorer indeholder .plist-arkivet en nøgle, som viser, at nøglesamlingen opbevares i et skab beskyttet af en nonce-værdi, der forhindrer genafspilning, og som styres af Secure Enclave.

Secure Enclave administrerer nøglesamlingen Bruger og kan besvare forespørgsler om en enheds låsestatus. Den meddeler kun, at enheden er låst op, hvis der er adgang til alle klassenøglerne i nøglesamlingen Bruger, og de er pakket ud uden fejl.

Nøglesamlingen Enhed

Nøglesamlingen Enhed bruges til at opbevare de indpakkede klassenøgler, der bruges til funktioner i forbindelse med enhedsspecifikke data. iPadOS-enheder, der er konfigureret til delt brug, har sommetider brug for adgang til godkendelsesoplysninger, før en bruger er logget på. Der er derfor behov for en nøglesamling, der ikke er beskyttet med brugerens kode.

iOS og iPadOS understøtter ikke kryptografisk adskillelse af arkivsystemindhold pr. bruger, hvilket betyder, at systemet bruger klassenøgler fra nøglesamlingen Enhed til at indpakke arkivnøgler. Nøgleringen bruger derimod klassenøgler fra nøglesamlingen Bruger til at beskytte emner i brugerens nøglering. På iOS- og iPadOS-enheder, der er konfigureret til en enkelt bruger (standardkonfigurationen), er nøglesamlingen Enhed og nøglesamlingen Bruger ens og er beskyttet af brugerens kode.

Nøglesamlingen Sikkerhedskopi

Nøglesamlingen Sikkerhedskopi oprettes, når Finder (macOS 10.15 og nyere versioner) eller iTunes (macOS 10.14 og tidligere versioner) opretter en krypteret sikkerhedskopi og gemmer den på den computer, som enheden blev sikkerhedskopieret til. Der oprettes en ny nøglesamling med et nyt sæt nøgler, og de sikkerhedskopierede data omkrypteres med de nye nøgler. Som beskrevet tidligere er ikke-flytbare emner i nøgleringen pakket med den nøgle, der er afledt af UID. Det betyder, at de kan gendannes på den enhed, de oprindeligt blev sikkerhedskopieret fra, og at der ikke kan opnås adgang til dem på en anden enhed.

Nøglesamlingen – der beskyttes af den indstillede adgangskode – behandles med 10 millioner gennemløb af funktionen PBKDF2 til nøgleafledning. På trods af dette store antal gentagelser er der ingen sammenkædning med en specifik enhed, og der er derfor i teorien risiko for et brute-force-angreb på nøglesamlingen Sikkerhedskopi parallelt på mange computere. Denne trussel kan mindskes med en tilstrækkelig stærk adgangskode.

Hvis en bruger vælger ikke at kryptere sikkerhedskopien, bliver arkiverne ikke krypteret uanset deres databeskyttelsesklasse, men nøgleringen er fortsat beskyttet med en nøgle afledt af UID. Det er årsagen til, at emner i nøgleringen kun kan flyttes til en ny enhed, hvis der er indstillet en adgangskode til sikkerhedskopien.

Nøglesamlingen Depot

Nøglesamlingen Depot bruges til at synkronisere med Finder (macOS 10.15 og nyere versioner) eller iTunes (i macOS 10.14 og tidligere versioner) via USB og administration af mobile enheder (MDM). Denne nøglesamling giver Finder eller iTunes mulighed for at sikkerhedskopiere og synkronisere, uden at brugeren skal indtaste en adgangskode, og den gør det muligt for en MDM-løsning at slette en brugers adgangskode eksternt. Den opbevares på den computer, der bruges til at synkronisere med Finder eller iTunes, eller i den MDM-løsning, som fjernadministrerer enheden.

Nøglesamlingen Depot giver en bedre brugeroplevelse under synkronisering af enheden, hvor der kan være behov for at få adgang til alle typer data. Første gang en kodebeskyttet enhed opretter forbindelse til Finder eller iTunes, bliver brugeren bedt om at indtaste en kode. Enheden opretter derefter en nøglesamling af typen Depot, der indeholder de samme klassenøgler, som bruges på enheden. Nøglesamlingen beskyttes med en ny, genereret nøgle. Nøglesamlingen Depot og den nøgle, der beskytter den, fordeles mellem enheden og værten eller serveren, mens dataene opbevares på enheden i klassen Beskyttet indtil første brugergodkendelse. Det er derfor, at koden til enheden skal indtastes, før brugeren kan sikkerhedskopiere med Finder eller iTunes første gang efter en genstart.

Hvis softwareopdateringen sker via en trådløs forbindelse, bliver brugeren bedt om at indtaste sin kode, når opdateringen startes. Dette bruges til sikker oprettelse af et engangstoken til oplåsning, som låser nøglesamlingen Bruger op efter opdateringen. Dette token kan ikke genereres, uden at brugerens kode indtastes, og alle tidligere genererede tokens gøres ugyldige, hvis brugerens kode ændres.

Engangstokens til oplåsning er beregnet til enten overvåget eller uovervåget installering af en softwareopdatering. De krypteres med en nøgle, der er afledt af den aktuelle værdi for en monoton tæller i Secure Enclave, nøglesamlingens UUID og Secure Enclaves UID.

På A9 (og nyere SoC'er) bruger engangstokenet til oplåsning ikke længere tællere eller Effaceable Storage. Det beskyttes i stedet af en værdi, der forhindrer genafspilning (nonce), og som styres af Secure Enclave.

Engangstokenet til oplåsning til overvågede softwareopdateringer udløber efter 20 minutter. I iOS 13 og iPadOS 13.1 og nyere versioner opbevares tokenet i et skab beskyttet af Secure Enclave. I versioner før iOS 13 blev dette token eksporteret fra Secure Enclave og skrevet til Effaceable Storage eller blev beskyttet af den Secure Enclave-mekanisme, der forhindrer genafspilning. En politiktimer øgede tælleren med 1, hvis enheden ikke blev genstartet inden for 20 minutter.

Uovervågede softwareopdateringer foretages, når systemet opdager en tilgængelig opdatering, og hvis et af følgende er sandt:

- Automatiske opdateringer er konfigureret i iOS 12 og nyere versioner.
- Brugeren vælger Installer senere, når der kommer en meddelelse om opdateringen.

Når brugeren har indtastet koden, genereres et engangstoken til oplåsning, og dette kan bevare sin gyldighed i Secure Enclave i op til 8 timer. Hvis opdateringen endnu ikke har fundet sted, ødelægges engangstokenet til oplåsning, hver gang enheden låses, og oprettes igen ved hver efterfølgende oplåsning. Hver oplåsning genstarter gyldighedsperioden på 8 timer. Efter 8 timer gør en politiktimer engangstokenet til oplåsning ugyldigt.

Nøglesamlingen iCloud-sikkerhedskopi

Nøglesamlingen iCloud-sikkerhedskopi ligner nøglesamlingen Sikkerhedskopi. Alle klassenøglerne i denne nøglesamling er asymmetriske (vha. Curve25519 ligesom databeskyttelsesklassen Beskyttet, hvis ikke åben). Der bruges også en asymmetrisk nøglesamling til sikkerhedskopien i forbindelse med gendannelse af iCloud-nøgleringen.

Beskyttelse af nøgler ved andre startfunktioner

Databeskyttelse er beregnet til kun at give adgang til brugerdata efter godkendelse og kun til den godkendte bruger. Klasser i Databeskyttelse understøtter en række forskellige anvendelsesområder, f.eks. muligheden for at læse og skrive visse data, også når en enhed er låst (men efter at enheden er låst op første gang). Der træffes flere foranstaltninger for at beskytte brugerdata ved andre startfunktioner, f.eks. DFU-funktion (Device Firmware Update), gendannelsesfunktion og Apple-diagnosticering, og også under softwareopdatering. Disse foranstaltninger er baseret på en kombination af hardware- og softwarefunktioner og er blevet udvidet i takt med udviklingen af chips designet af Apple.

Funktion	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1-familien
Gendannelse: Alle klasser i Databeskyttelse er beskyttet	✓	✓	✓	✓	✓
Start med DFU-funktion, Gendannelse og under softwareopdateringer: Data i klasse A, B og C er beskyttet		✓	✓	✓	✓

AES-modulet i Secure Enclave er udstyret med låsbare software seed bits. Når der oprettes nøgler fra UID, inkluderes disse seed bits i funktionen til nøgleafledning for at oprette yderligere nøglehierarkier. Den måde, en seed bit bruges på, afhænger af SoC'en:

- Seed bits startede på Apple A10- og S3 SoC-processorer og er dedikeret til at skelne nøgler, der er beskyttet af brugerens kode. En seed bit indstilles til nøgler, der kræver brugerens kode (herunder nøgler til databeskyttelsesklasse A, B og C), og slettes til nøgler, der ikke kræver brugerens kode (herunder nøglen til arkivsystemmetadata og nøgler til klasse D).
- På enheder med A10 eller nyere og iOS 13 eller en nyere version eller iPadOS 13.1 eller en nyere version gælder, at kryptografisk adgang til alle brugerdata ophæves, når enhederne startes i Diagnosticeringsfunktion. Det opnås ved hjælp af en ekstra seed bit, hvis indstilling styrer muligheden for at få adgang til medienøglen, som er nødvendig for at få adgang til metadata (og dermed indholdet af alle arkiver) på dataenheden, der er krypteret med databeskyttelse. Denne beskyttelse omfatter arkiver, der er beskyttet i alle klasser (A, B, C og D), og ikke kun dem, der kræver brugerens kode.
- På A12 SoC'er låser Secure Enclave Boot ROM kodens seed bit, hvis app-processoren er i DFU-funktion eller Gendannelsesfunktion. Når kode-seed bit'en er låst, tillades ændringer af den ikke. Det har til formål at forhindre adgang til data, der er beskyttet af brugerens kode.

Når en enhed gendannes, efter den er skiftet til DFU-funktionen, går den tilbage til en kendt, gyldig status, hvor der er sikkerhed for, at kun umodificeret kode signeret af Apple er til stede. Det er muligt at skifte manuelt til DFU-funktionen.

Følgende Apple-supportartikler beskriver, hvordan der skiftes til DFU-funktion på en enhed:

Enhed	Artikel
iPhone, iPad, iPod touch	Hvis du har glemt koden til din iPhone
Apple TV	Hvis du ser et advarselssymbol på Apple TV
En Mac med Apple Silicon	Revive or restore a Mac with Apple silicon (Genopliv eller gendan en Mac med Apple Silicon)

Beskyttelse af brugerdata mod angreb

Hackere, der vil have fat i brugerdata, prøver ofte med et antal forskellige teknikker som f.eks. at overføre de krypterede data til et andet medie i forbindelse med brute force-angreb, modificere operativsystemversionen eller på anden vis ændre eller svække enhedens sikkerhedspolitik for at åbne vej for angrebet. Angreb på data på en enhed kræver ofte kommunikation med enheden via fysiske grænseflader som Lightning eller USB. Apple-enheder indeholder funktioner, der kan være med til at forhindre disse angreb.

Apple-enheder understøtter teknologien *SKP (Sealed Key Protection)*, der har til formål at sikre, at kryptografisk materiale gøres utilgængeligt, når det befinder sig uden for enheden, eller som bruges, hvis der foretages modificering af operativsystemversion eller af sikkerhedsindstillinger uden den nødvendige brugergodkendelse. Funktionen leveres *ikke* af Secure Enclave, men understøttes af hardwareregistre på et lavere lag for at tilvejebringe et ekstra lag af beskyttelse af de nøgler, der skal bruges til at dekryptere brugerdata uafhængigt af Secure Enclave.

Bemærk: SKP findes kun på enheder med en SoC designet af Apple.

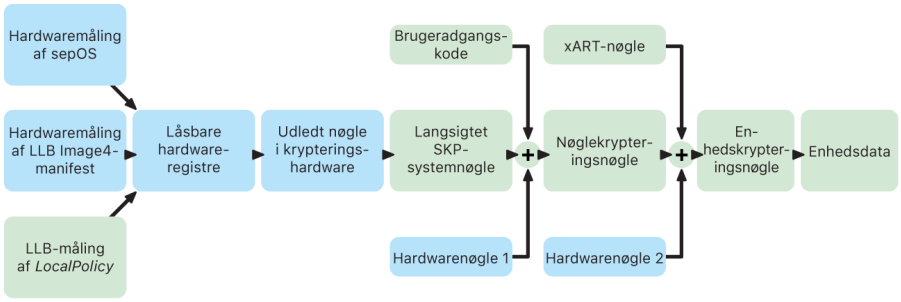
Funktion	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1-familien
Sealed Key Protection	✓	✓	✓	✓	✓

iPhone og iPad kan indstilles, så de kun gør dataforbindelser aktive i situationer, hvor det er mest sandsynligt, at enheden stadig er under den godkendte brugers kontrol.

Sealed Key Protection (SKP)

På Apple-enheder, der understøtter Databeskyttelse, beskyttes (forsegles) nøglekrypteringsnøglen (KEK) med foranstaltninger i softwaren på systemet, og den er desuden knyttet til det UID, der kun er tilgængeligt fra Secure Enclave. På en Mac med Apple Silicon gøres beskyttelsen af KEK endnu stærkere, ved at den inkorporerer oplysninger om sikkerhedspolitikken på systemet, fordi macOS understøtter kritiske ændringer af sikkerhedspolitikken (f.eks. slå sikker start eller SIP fra), som ikke understøttes på andre platforme. På en Mac med Apple Silicon omfatter denne beskyttelse nøgler i FileVault, fordi FileVault er implementeret med brug af Databeskyttelse (klasse C).

Den nøgle, der dannes som en kombination af brugeradgangskoden, den langtidsholdbare SKP-nøgle og Hardwarenøgle 1 (UID fra Secure Enclave), kaldes *nøglen afledt af kode*. Nøglen bruges til at beskytte nøglesamlingen Bruger (på alle understøttede platforme) og KEK (kun macOS) og derefter slå oplåsning eller automatisk oplåsning til på andre enheder, f.eks. Apple Watch.



Secure Enclaves startovervågning indhenter målingen af det Secure Enclave-operativsystem, der indlæses. Når app-processorens Boot ROM måler det Image4-manifest, der er knyttet til LLB, indeholder dette manifest en måling af al den anden systemparrede firmware, der også indlæses. LocalPolicy (den lokale politik) indeholder de centrale sikkerhedskonfigurationer for det macOS, der indlæses. LocalPolicy indeholder også feltet `nsih`, som er en hash-værdi af Image4-manifestet i macOS. Image4-manifestet i macOS indeholder målinger af al macOS-parret firmware og alle parrede centrale macOS-startobjekter, f.eks. kernesamlingen til systemstart og hash-værdien for den signerede systemenheds rod.

Hvis det mod forventning sker, at en person med onde hensigter kan ændre noget af den firmware, software eller de komponenter til sikkerhedskonfiguration, der er nævnt ovenfor som målt, ændrer det de målinger, der opbevares i hardwareregistrene. Ændringen af målingerne får *rodnøglen til systemmåling (SMRK)*, som er afledt af krypteringshardware, til at aflede til en anden værdi, hvorved forseglingen af nøglehierarkiet brydes. Det medfører, at der ikke er adgang til *enhedsnøglen til systemmåling (SMDK)*, og dette medfører videre, at der ikke kan fås adgang til KEK og dermed heller ikke til dataene.

Når systemet ikke er under angreb, skal det dog være i stand til at tage højde for gyldige softwareopdateringer, som ændrer firmware-målingerne og `nsih`-feltet i LocalPolicy for at pege på nye macOS-målinger. I andre systemer, som forsøger at inkorporere firmwaremålinger, men ikke har en kendt fungerende sandhedskilde, skal brugeren slå sikkerheden fra, opdatere firmwaren og slå funktionerne til igen, så der kan indhentes et nyt grundlag for målingerne. Det giver en betydeligt større risiko for, at en person med ondsindede hensigter kan manipulere med firmwaren under en softwareopdatering. Systemet har gavn af, at Image4-manifestet indeholder alle de nødvendige målinger. Den hardware, som dekrypterer SMDK med SMRK, når målingerne stemmer overens under en normal start, kan også kryptere SMDK til en foreslået fremtidig SMRK. Ved at angive de målinger, som forventes efter en softwareopdatering, kan hardwaren kryptere en SMDK, som der er adgang til i et aktuelt operativsystem, så der fortsat er adgang til det i et kommende operativsystem. Noget tilsvarende sker, når en kunde legitimt ændrer sine sikkerhedsindstillinger i LocalPolicy, idet SMDK så skal krypteres til den fremtidige SMRK ud fra den måling til LocalPolicy, som LLB vil beregne ved næste genstart.

Sikker aktivering af dataforbindelser i iOS og iPadOS

Hvis der på iOS- og iPadOS-enheder ikke har været oprettet dataforbindelser for nylig, skal brugerne benytte Face ID, Touch ID eller en kode til at gøre dataforbindelser aktive via en Lightning-, USB- eller Smart Connector-grænseflade. Dette begrænser angrebsoverfladen for fysisk tilsluttede enheder, f.eks. skadelige opladere, mens der stadig kan bruges andet tilbehør inden for rimelige tidsmæssige begrænsninger. Hvis der er gået mere end en time, siden iOS- eller iPadOS-enheden blev låst, eller siden et tilbehørs dataforbindelse blev afbrudt, tillader enheden ikke, at der etableres nye dataforbindelser, før enheden låses op. I denne periode på en time tillades der kun dataforbindelser fra tilbehør, som tidligere er blevet forbundet til enheden, mens den var i oplåst tilstand. Sådant tilbehør huskes i 30 dage fra sidste gang, der var forbindelse. Hvis et ukendt tilbehør forsøger at åbne en dataforbindelse i denne periode, vil alle tilbehørs dataforbindelser gennem Lightning, USB og Smart Connector blive deaktiveret, indtil enheden låses op igen. Denne periode på en time:

- Er med til at sikre, at brugere, der ofte bruger tilslutninger til en Mac eller pc, til tilbehør eller til CarPlay med ledning, ikke skal indtaste deres kode, hver gang de tilslutter deres enhed
- Er nødvendig, fordi tilbehørsøkosystemet ikke tilbyder en kryptografisk pålidelig metode til identificering af tilbehør, før der oprettes dataforbindelse

Der er yderligere sikkerhed, idet enheden ikke tillader nye dataforbindelser, lige efter at den er blevet låst, hvis der er gået mere end 3 dage, siden en dataforbindelse blev etableret med et tilbehør. Formålet er at øge beskyttelsen af brugere, der ikke bruger denne type tilbehør særlig ofte. Dataforbindelser via Lightning, USB og Smart Connector slås også fra, når enheden er i en tilstand, hvor der kræves en kode for at slå biometrisk godkendelse til igen.

Brugeren kan vælge at slå Altid-til-dataforbindelser til igen i Indstillinger (det sker automatisk ved indstilling af visse hjælpemiddelenheder).

Apples arkivsystems rolle

Apple File System (APFS) er Apples eget arkivsystem, der er udviklet med fokus på kryptering. APFS kan bruges på alle Apples platforme – til iPhone, iPad, iPod Touch, Mac, Apple TV og Apple Watch. Det er optimeret til Flash/SSD-lager og har stærk kryptering, copy-on-write metadata, deling af områder, kloning for arkiver og biblioteker, snapshots, hurtig størrelsesændring af biblioteker, primitiver til atomisk sikker lagring og forbedringer i det grundlæggende arkivsystem samt et unikt copy-on-write design, som benytter I/O-samling til at levere maksimal ydelse, mens datapålidelighed sikres.

Deling af plads

APFS tildeler lagringsplads efter behov. Når en enkelt APFS-beholder har flere enheder, er beholderens ledige plads delt og kan tildeles de individuelle enheder efter behov. Hver enhed bruger kun en del af den samlede beholder, så den ledige plads er beholderens samlede størrelse minus den plads, som bruges på alle enheder i beholderen.

Flere enheder

I macOS 10.15 og nyere versioner skal en APFS-beholder, der bruges til at starte Mac, indeholde mindst fem diskenheder, hvoraf de tre første er skjult for brugeren:

- *Preboot-enhed:* Enheden er ikke krypteret og indeholder data, der kræves for at starte hver af systemenhederne i beholderen
- *VM-enhed:* Enheden er ikke krypteret og bruges af macOS til opbevaring af krypterede swap-arkiver.
- *Gendannelsesenhed:* Enheden er ikke krypteret og skal være tilgængelig uden oplåsning af en systemenhed for at kunne starte i macOS-gendannelse.
- *Systemenhed:* Indeholder følgende:
  - Alle de arkiver, der er nødvendige for at starte Mac
  - Alle apps, som er installeret uden ændringer af macOS (apps, der plejede at være i mappen /Apps, findes nu i /System/Apps)

  Bemærk: Som standard er der ingen proces, der kan skrive til systemenheden – heller ikke Apple-systemprocesser.
- *Dataenhed:* Indeholder data, der sandsynligvis vil blive ændret, f.eks.:
  - Alle data i brugerens mappe, herunder fotos, musik, videoer og dokumenter
  - Apps, brugeren har installeret, herunder AppleScript og Automator-apps
  - Specielle frameworks og dæmoner, der er installeret af brugeren, organisationen eller apps fra tredjeparter
  - Andre placeringer, som brugeren ejer og kan skrive til, f.eks. /Apps, /Bibliotek, /Brugere, /Enheder, /usr/local, /private, /var og /tmp

Der oprettes en dataenhed for hver ekstra systemenhed. Både Preboot-enheden, VM-enheden og gendannelsesenheden er fælles og dubleres ikke.

I macOS 11 og nyere versioner bliver der taget et snapshot af systemenheden. Operativsystemet starter fra et snapshot af systemenheden og ikke bare et skrivebeskyttet diskbillede af den systemenhed, der kan ændres.

I iOS og iPadOS er lagringspladsen fordelt på mindst to APFS-enheder:

- Systemenhed
- Dataenhed

Databeskyttelse af nøglering

Mange apps skal kunne håndtere adgangskoder og andre korte, men følsomme, datasekvenser, f.eks. nøgler og login-tokens. Med nøgleringen kan disse emner opbevares på en sikker måde. Apples operativsystemer bruger forskellige mekanismer til at håndhæve de garantier, der er knyttet til de forskellige klasser til beskyttelse af nøgleringen. I macOS (også på en Mac med Apple Silicon) bruges Databeskyttelse ikke direkte til at håndhæve disse garantier.

Oversigt

Emner i nøgleringen krypteres vha. to forskellige AES-256-GCM-nøgler: en tabelnøgle (metadata) og en rækkenøgle (hemmelig nøgle). Nøgleringsmetadata (alle attributter undtagen kSecValue) krypteres med metadatanøglen for at øge hastigheden ved søgninger, og den hemmelige værdi (kSecValueData) krypteres med den hemmelige nøgle. Metadatanøglen beskyttes af Secure Enclave, men indlæses i app-processorens buffer for at tillade hurtige nøgleringsforespørgsler. Den hemmelige nøgle kræver altid en rundtur gennem Secure Enclave.

Nøgleringen implementeres som en SQLite-database, der opbevares i arkivsystemet. Der er kun én database, og `securityd`-dæmonen bestemmer, hvilke emner i nøgleringen hver proces eller app har adgang til. API'er til nøgleringsadgang afsender kald til dæmonen, som sender forespørgsler om appens værdi for berettigelserne "Keychain-access-groups", "application-identifier" og "application-group". Adgangsgrupper gør det muligt at dele emner i nøgleringen mellem apps, i stedet for at adgangen begrænses til en enkelt proces.

Emner i nøgleringen kan kun deles mellem apps fra samme udvikler. For at kunne dele emner i nøgleringen bruger apps fra tredjeparter adgangsgrupper med et præfiks, de har fået tildelt via Apple Developer Program i deres app-grupper. Præfikskravet og app-gruppernes forskellighed opretholdes ved hjælp af kodesignering, programprofiler og Apple Developer Program.

Data i nøgleringe beskyttes med en klassestruktur, som ligner den, der bruges til databeskyttelse af arkiver. Disse klassers funktionsmåde ligner den for klasserne til beskyttelse af arkivdata, men de bruger særlige nøgler og funktioner.

Tilgængelighed	Databeskyttelse af arkiver	Databeskyttelse af nøglering
Når låst op	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Når låst	NSFileProtectionCompleteUnlessOpen	Ikke aktuelt
Efter enheden er låst op første gang	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Altid	NSFileProtectionNone	kSecAttrAccessibleAlways
Kode slået til	Ikke aktuelt	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

Apps, som bruger opdateringstjenester i baggrunden, kan bruge *kSecAttrAccessibleAfterFirstUnlock* til emner i nøgleringen, der skal være adgang til under opdateringer i baggrunden.

Klassen *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* opfører sig på samme måde som *kSecAttrAccessibleWhenUnlocked*, men den er kun tilgængelig, når enheden er konfigureret med en kode. Denne klasse eksisterer kun i systemnøglesamlingen. Den:

- Synkroniserer ikke til iCloud-nøgleringen
- Sikkerhedskopieres ikke
- Er ikke omfattet af depotnøglesamlinger

Hvis koden fjernes eller nulstilles, bliver emnerne ubrugelige, fordi klassenøglerne kasseres.

Andre nøgleringsklasser har en modpart af typen "Kun denne enhed", hvor et emne altid beskyttes med UID, når det kopieres fra enheden under en sikkerhedskopiering, så det er ubrugeligt, hvis det gendannes på en anden enhed. Apple har nøje afvejet sikkerhed og anvendelighed og valgt nøgleringsklasser, som afhænger af den type oplysninger, der skal sikres, og det tidspunkt, hvor iOS og iPadOS har brug for dem. Et VPN-certifikat skal f.eks. altid være tilgængeligt, så enhedens forbindelse ikke afbrydes, men det er klassificeret som "ikke-flytbart", så det ikke kan flyttes til en anden enhed.

Klassebeskyttelse til data i nøglering

De klassebeskyttelsesforanstaltninger, der er anført nedenfor, håndhæves for emner i nøgleringen:

Emne	Tilgængeligt
Wi-Fi-adgangskoder	Efter enheden er låst op første gang
E-mailkonti	Efter enheden er låst op første gang
Microsoft Exchange ActiveSync-konti	Efter enheden er låst op første gang
VPN-adgangskoder	Efter enheden er låst op første gang
LDAP, CalDAV, CardDAV	Efter enheden er låst op første gang
Tokens til sociale netværkskonti	Efter enheden er låst op første gang
Annonceringskrypteringsnøgler til Handoff	Efter enheden er låst op første gang
iCloud-token	Efter enheden er låst op første gang
iMessage-nøgler	Efter enheden er låst op første gang
Adgangskode til deling i hjemmet	Når låst op
Safari-adgangskoder	Når låst op
Safari-bogmærker	Når låst op
Finder-/iTunes-sikkerhedskopiering	Når låst op, ikke-flytbar
Private nøgler installeret af en konfigurationsprofil	Når låst op, ikke-flytbar
VPN-certifikater	Altid, ikke-flytbar
Bluetooth®-nøgler	Altid, ikke-flytbar
Token for APNs (Apple Push Notification service)	Altid, ikke-flytbar
Certifikater og privat nøgle til iCloud	Altid, ikke-flytbar
PIN-kode til SIM	Altid, ikke-flytbar
Certifikater installeret af en konfigurationsprofil	Altid
Token til Find	Altid
Telefonsvarer	Altid

Adgangskontrol for nøglering

Nøgleringe kan bruge adgangskontrollister (ACL'er) til at indstille strategier for tilgængelighed og godkendelseskrav. Emner kan fastlægge betingelser for brugerens tilstedeværelse ved at angive, at der ikke er adgang til emnerne, medmindre brugeren legitimerer sig vha. Face ID eller Touch ID eller ved at indtaste enhedens kode eller adgangskode. Adgang til emner kan også begrænses via en angivelse af, at Face ID- eller Touch ID-registreringen ikke er ændret, siden emnet blev tilføjet. Begrænsningen bidrager til at forhindre en person med ondsindede hensigter i at tilføje sit eget fingeraftryk for at få adgang til et emne i nøgleringen. Adgangskontrollister evalueres i Secure Enclave og frigives kun til kernen, hvis deres angivne betingelser er opfyldt.

Arkitektur med nøgleringe i macOS

macOS giver også adgang til nøgleringen, så brugernavne og adgangskoder, digitale identiteter, krypteringsnøgler og sikre noter kan opbevares praktisk og sikkert. Der kan opnås adgang ved at åbne appen Hovednøglering i /Apps/Hjælpeapps/. Når der bruges en nøglering, er det ikke længere nødvendigt at skrive – og heller ikke at huske – godkendelsesoplysningerne til hver enkelt ressource. Til hver Mac-bruger oprettes i starten en standardnøglering, men brugerne kan oprette andre nøgleringe til særlige formål.

Ud over nøgleringe til brugere benytter macOS en række nøgleringe på systemniveau til at vedligeholde godkendelsesaktiver, der ikke er brugerspecifikke, f.eks. godkendelsesoplysninger til netværk og PKI-identiteter (Public Key Infrastructure). En af disse nøgleringe, System Roots, er uforanderlig og opbevarer PKI-rodcertifikater fra en certifikatmyndighed til brug på internettet til almindelige opgaver som netbank og internethandel. På tilsvarende vis kan brugeren implementere certifikater fra en intern certifikatmyndighed (CA) på administrerede Mac-computere som hjælp til godkendelse af interne websteder og tjenester.

FileVault

Kryptering af enheder med FileVault i macOS

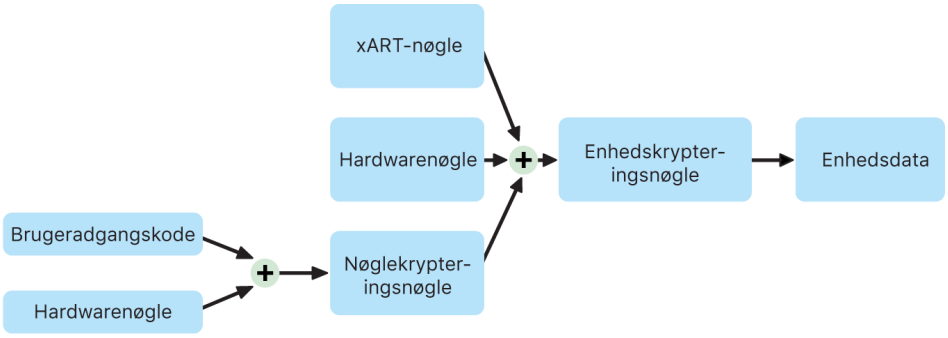
Mac-computere indeholder FileVault, som er en indbygget krypteringsfunktion, der beskytter alle data under opbevaring. FileVault bruger algoritmen AES-XTS til datakryptering til at yde fuld beskyttelse af enheder på interne og udskiftelige lagringsenheder.

FileVault på en Mac med Apple Silicon er implementeret ved hjælp af Databeskyttelsesklasse C med en enhedsnøgle. På en Mac med Apple T2-sikkerhedschippen og på en Mac med Apple Silicon udnytter de krypterede interne lagringsenheder, der er sluttet direkte til Secure Enclave, chippens sikkerhedsfunktioner til hardware og AES-modulets sikkerhedsfunktioner. Når en bruger slår FileVault til på en Mac, skal brugeren indtaste sine godkendelsesoplysninger under starten.

Intern lagring med FileVault slået til

Uden gyldige godkendelsesoplysninger til login eller en kryptografisk gendannelsesnøgle er de interne APFS-enheder krypteret og beskyttet mod uvedkommendes adgang, også selvom den fysiske lagringsenhed fjernes og sluttes til en anden computer. I macOS 10.15 er både systemenheden og dataenheden omfattet. Fra macOS 11 er systemenheden beskyttet af den signerede systemenhed (SSV), mens kryptering fortsat bruges til at beskytte dataenheden. Kryptering af en intern enhed på en Mac med Apple Silicon og Mac-computere med T2-chippen implementeres ved, at et hierarki med nøgler opbygges og administreres, og bygger på de teknologier til hardwarekryptering, der er integreret i chippen. Dette hierarki med nøgler er udviklet til at opnå fire målsætninger på samme tid:

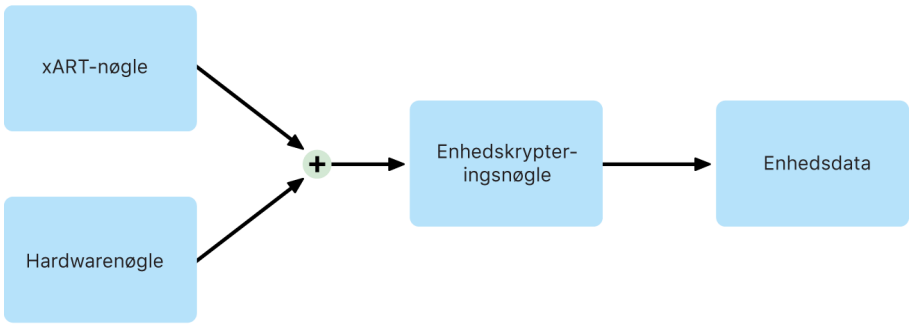
- Kræve brugerens adgangskode til dekryptering
- Beskytte systemet mod brute force-angreb rettet direkte mod et lagringsmedie, der er fjernet fra Mac
- Udgøre en hurtig og sikker metode til sletning af indhold, ved at nødvendigt kryptografisk materiale slettes
- Give brugerne mulighed for at skifte adgangskode (og dermed de kryptografiske nøgler, der bruges til at beskytte deres arkiver), uden at det er nødvendigt at kryptere hele diskenheden igen



På en Mac med Apple Silicon og Mac-computere med T2-chippen finder al håndtering af FileVault-nøglerne sted i Secure Enclave. Krypteringsnøgler vises aldrig direkte til Intel-CPU'en. Alle APFS-enheder er som standard oprettet med en enhedskrypteringsnøgle. Indholdet af enhed og metadata krypteres med denne enhedskrypteringsnøgle, som er pakket sammen med klassenøglen. Klassenøglen beskyttes med en kombination af brugerens adgangskode og hardwarens UID, når FileVault slås til.

Intern lagring med FileVault slået fra

Hvis FileVault ikke slås til på en Mac med Apple Silicon eller en Mac med T2-chippen under den første Indstillingsassistent-proces, krypteres diskenheden alligevel, men enhedskrypteringsnøglen beskyttes kun af hardwarens UID i Secure Enclave.



Hvis FileVault slås til senere (processen gennemføres straks, fordi dataene allerede er krypteret), forhindrer en mekanisme, der er med til at modvirke automatisk afspilning, at den gamle nøgle, som kun er baseret på hardwarens UID, bruges til at dekryptere enheden. Enheden beskyttes herefter af en kombination af brugerens adgangskode og hardwarens UID som tidligere beskrevet.

Sletning af FileVault-enheder

Når en enhed slettes, slettes enhedskrypteringsnøglen til den på en sikker måde af Secure Enclave. Det er med til at forhindre, at der senere kan opnås adgang med nøglen, heller ikke af Secure Enclave. Desuden pakkes alle enhedskrypteringsnøgler sammen med en medienøgle. Medienøglen øger ikke datafortroligheden yderligere, men har til formål at gøre det muligt at slette data hurtigt og sikkert, eftersom dekryptering ikke ville være mulig uden medienøglen.

På en Mac med Apple Silicon og Mac-computere med T2-chippen garanteres, at medienøglen slettes af Secure Enclaves understøttede teknologi, f.eks. ved hjælp af eksterne MDM-kommandoer. Når medienøglen slettes på denne måde, ophæves al kryptografisk adgang til alle arkiver.

Udskiftelige lagringsenheder

Secure Enclaves sikkerhedsfunktioner bruges ikke til at kryptere udskiftelige lagringsenheder. De krypteres på samme måde som på en Intel-baseret Mac uden T2-chippen.

Administration af FileVault i macOS

I macOS kan organisationer administrere FileVault ved hjælp af Secure Token eller Bootstrap Token.

Brug af Secure Token

APFS (Apple File System) i macOS 10.13 og nyere versioner ændrer den måde FileVault-krypteringsnøgler genereres på. I tidligere versioner af macOS på CoreStorage-enheder blev de nøgler, der blev brugt i FileVault-krypteringsprocessen, oprettet, når en bruger eller en organisation slog FileVault til på en Mac. I macOS på APFS-enheder genereres nøglerne enten under brugeroprettelse, indstilling af den første brugers adgangskode eller første gang, en bruger logger ind på Mac. Denne implementering af krypteringsnøglerne, tidspunktet for genereringen og måden, de opbevares på, er en del af en funktion, der kaldes *Secure Token* (sikkert token). Helt specifikt er et sikkert token en indpakket version af en KEK (Key Encryption Key), der beskyttes af en brugers adgangskode.

Ved implementering af FileVault på APFS kan brugeren fortsætte med at:

- Bruge eksisterende værktøjer og processer, f.eks. en personlig gendannelsesnøgle (PRK – Personal Recovery Key), der kan deponeres i en løsning til administration af mobile enheder (MDM)
- Oprette og bruge en gendannelsesnøgle fra organisationen (IRK – Institutional Recovery Key)
- Vente med at slå FileVault til, indtil en bruger logger ind eller ud af Mac

Når den første adgangskode indstilles til den første bruger på Mac med macOS 11, får brugeren tildelt et sikkert token. I nogle arbejdsgange er denne funktionsmåde måske uønsket, da tildeling af det første sikre token tidligere ville have krævet, at brugeren skulle logge ind. Funktionsmåden kan forhindres, ved at `;DisabledTags;SecureToken` føjes til den programmæssigt oprettede brugers `AuthenticationAuthority`-attribut, inden brugerens adgangskode indstilles, som vist herunder:

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

Brug af Bootstrap Token

I macOS 10.15 blev funktionen *Bootstrap Token* lanceret. Den hjælper med at tildele et sikkert token til både mobile konti og den valgfri administratorkonto oprettet under enhedstilmelding ("administreret administrator"). I macOS 11 kan et Bootstrap Token tildele et sikkert token til enhver bruger, der logger ind på en Mac-computer, herunder lokale brugerkonti. Brug af Bootstrap Token-funktionen i macOS 10.15 og nyere versioner kræver:

- Tilmelding af Mac i MDM via Apple School Manager eller Apple Business Manager, hvilket sætter Mac under tilsyn
- MDM-leverandørens understøttelse

I macOS 10.15.4 og nyere versioner genereres et Bootstrap Token, og det deponeres i MDM, første gang en bruger med sikkert token slået til logger ind, hvis MDM-løsningen understøtter funktionen. Ved behov er det også muligt at generere et Bootstrap Token og deponere det i MDM ved hjælp af kommandolinjeværktøjet `profiles`.

I macOS 11 kan et Bootstrap Token bruges til mere end blot at tildele et sikkert token til brugerkonti. På en Mac med Apple Silicon kan et Bootstrap Token, hvis det er tilgængeligt, bruges til at godkende installeringen af kerneudvidelser og softwareopdateringer, hvis de administreres med MDM.

Sådan beskytter Apple brugernes persondata

Beskyttelse af app-adgang til brugerdata

Ud over at kryptere data under opbevaring hjælper Apple-enheder med at forhindre apps i at få adgang til en brugers personlige oplysninger uden tilladelse ved hjælp af forskellige teknologier, herunder Data Vault. I Indstillinger i iOS og iPadOS og i Systemindstillinger i macOS kan brugerne se, hvilke apps de har givet adgang til bestemte oplysninger, og tillade adgang eller tilbagekalde adgangen. Adgangskontrol håndhæves her:

- *iOS, iPadOS og macOS:* Kalender, Kamera, Kontakter, Mikrofon, Fotos, Påmindelser, Talegenkendelse
- *iOS og iPadOS:* Bluetooth, Hjem, Medier, Medie-apps og Apple Music, Bevægelse og fitness
- *iOS og watchOS:* Sundhed
- *macOS:* Overvågning af tastatur (f.eks. tastaturanslag), Spørg, Skærmoptagelse (f.eks. statiske skærmbilleder og video), Systemindstillinger

I iOS 13.4 og nyere versioner og iPadOS 13.4 og nyere versioner beskyttes alle data fra apps fra tredjeparter automatisk i en Data Vault. Data Vault øger beskyttelsen mod uautoriseret adgang til data, også fra processer, der ikke selv afvikles i et isoleret miljø. I iOS 15 og nyere versioner findes også klasserne Local Network, Nearby Interactions, Research Sensor & Usage Data og Focus.

Hvis brugeren logger ind på iCloud, får apps i iOS og iPadOS som standard adgang til iCloud Drive. Brugerne kan styre den enkelte apps adgang under iCloud i Indstillinger. iOS og iPadOS har desuden begrænsninger, der har til formål at forhindre, at data flyttes mellem apps og konti, der er installeret af en løsning til administration af mobile enheder (MDM), og dem, der er installeret af brugeren.

Beskyttelse af adgangen til brugerens sundhedsdata

HealthKit kan fungere som et centralt opbevaringssted til sundheds- og træningsdata på iPhone og Apple Watch. HealthKit arbejder også direkte sammen med sundheds- og træningsenheder, f.eks. kompatible BLE-pulsmålere (Bluetooth Low Energy) og den bevægelseshjælpeprocessor, der er indbygget i mange iOS-enheder. Brugerens samtykke kræves til al interaktion mellem HealthKit og sundheds- og træningsapps, sundhedsinstitutioner og sundheds- og træningsenheder. Disse data opbevares i klassen Beskyttet, hvis ikke åben i Databeskyttelse. Adgang til dataene ophører, 10 minutter efter at enheden låses, og der bliver adgang til dataene igen, næste gang brugeren indtaster deres kode eller bruger Face ID eller Touch ID til at låse enheden op.

Indsamling og opbevaring af sundheds- og træningsdata

HealthKit indsamler og opbevarer også administrationsdata, f.eks. adgangstilladelser til apps, navne på enheder med forbindelse til HealthKit og planlægningsoplysninger, der bruges til at starte apps, når nye data er tilgængelige. Disse data opbevares i klassen Beskyttet indtil første brugergodkendelse i Databeskyttelse. Helbredsjournaler, der genereres, når enheden er låst, f.eks. når brugeren træner, gemmes i midlertidige journalarkiver. De opbevares i klassen Beskyttet, hvis ikke åben i Databeskyttelse. Når enheden låses op, importeres de midlertidige journalarkiver i de primære sundhedsdatabaser og slettes, når fletningen er færdig.

Sundhedsdata kan gemmes i iCloud. End-to-end-kryptering af data fra Sundhed kræver iOS 12 eller en nyere version og tofaktorgodkendelse. Ellers krypteres brugerens data stadigvæk under overførsel og lagring, men de bliver ikke end-to-end-krypterede. Når brugeren har slået tofaktorgodkendelse til og opdateret til iOS 12 eller en nyere version, skifter brugerens sundhedsdata til end-to-end-kryptering.

Hvis brugeren sikkerhedskopierer sin enhed med Finder (macOS 10.15 og nyere versioner) eller iTunes (i macOS 10.14 og tidligere versioner) bliver sundhedsdata kun gemt, hvis sikkerhedskopien krypteres.

Sygejournaler

Brugerne kan logge ind på understøttede sundhedssystemer fra appen Sundhed for at få fat i en kopi af deres sygejournaler. Når en bruger får forbindelse til et sundhedssystem, legitimerer brugeren sig ved hjælp af OAuth 2-klientoplysningerne. Når der er oprettet forbindelse, hentes sygejournaldata direkte fra sundhedsinstitutionen via en forbindelse beskyttet med TLS 1.3. Når de er hentet, opbevares sygejournalerne sikkert sammen med andre sundhedsdata.

Beskyttelse af sundhedsdata

De data, der gemmes i databasen, omfatter metadata, der holder styr på, hvor hver datapost stammer fra. Metadataene inkluderer et app-id, der viser, hvilken app der gemte posten. Et valgfrit emne i metadataene kan indeholde en digitalt signeret kopi af posten. Dets formål er at skabe dataintegritet for poster, der genereres af en godkendt enhed. Den digitale signatur er i CMS-format (Cryptographic Message Syntax), som er specificeret i RFC 5652.

Tredjeparters adgang til data fra Sundhed

Adgangen til HealthKit API'et styres med berettigelser, og appsene skal overholde restriktioner med hensyn til brugen af dataene. Apps har f.eks. ikke tilladelse til at benytte sundhedsdata i reklameøjemed. Det er desuden et krav, at appsene forsyner brugerne med en anonymitetspolitik, som i detaljer beskriver appsenes brug af sundhedsdata.

Adgang til sundhedsdata fra apps styres af brugerens anonymitetsindstillinger. Brugerne bliver bedt om at give adgang, når apps anmoder om adgang til sundhedsdata, i lighed med Kontakter, Fotos og andre iOS-datakilder. I forbindelse med sundhedsdata tildeles apps imidlertid særskilt adgang til at læse og skrive data og særskilt adgang til hver type sundhedsdata. Brugerne kan se og tilbagekalde tilladelser til at få adgang til sundhedsdata under Indstillinger > Sundhed > Dataadgang og enheder.

Hvis apps får tilladelse til at skrive data, kan appsene også læse de data, de skriver. Hvis apps får tilladelse til at læse data, kan de læse data, som er skrevet af alle kilder. Apps kan dog ikke se, hvilken adgang andre apps har fået tildelt. Desuden kan apps ikke med sikkerhed afgøre, om de har fået læseadgang til sundhedsdata. Når en app ikke har læseadgang, returnerer alle forespørgsler et tomt resultat – samme svar, som en tom database vil returnere. Det har til formål at forhindre apps i at udlede brugerens sundhedstilstand ved at lære, hvilke typer data brugeren registrerer.

Nødinfo om brugere

Appen Sundhed giver brugerne mulighed for at udfylde formularen Nødinfo med oplysninger, der kan være vigtige i en helbredsmæssig nødsituation. Oplysningerne skrives og opdateres manuelt, og de synkroniseres ikke med oplysningerne i sundhedsdatabaserne.

Brugeren kan se oplysningerne i Nødinfo ved at trykke på knappen Nødopkald på den låste skærm. Oplysningerne gemmes på enheden ved hjælp af klassen Ingen beskyttelse i Databeskyttelse, så der er adgang til dem uden indtastning af koden til enheden. Nødinfo er en valgfri funktion, der giver brugerne mulighed for at afveje hensyn til sikkerhed og til anonymitet. Dataene sikkerhedskopieres i iCloud-sikkerhedskopi i iOS 13 og tidligere versioner. I iOS 14 synkroniseres Nødinfo mellem enhederne via CloudKit, og disse data krypteres på samme måde som de øvrige sundhedsdata.

Deling af sundhedsdata

I iOS 15 giver appen Sundhed brugerne mulighed for at dele deres data i Sundhed med andre brugere. Der bruges end-to-end-kryptering af iCloud til sundhedsdata, der deles mellem to brugere. Apple har ikke adgang til data, der deles via Sundhed. Både afsenderen og modtageren skal have iOS 15 eller en nyere version og have slået tofaktorgodkendelse til for at bruge funktionen.

Brugerne kan også vælge at dele deres data i Sundhed med deres leverandør af sundhedsydelser ved at bruge funktionen Del med behandler i appen Sundhed. Data, der deles med denne funktion, stilles kun til rådighed for de sundhedsinstitutioner, brugeren har valgt. De bliver end-to-end-krypterede, og Apple hverken opbevarer eller har adgang til de krypteringsnøgler, der bruges til at dekryptere, se eller på anden vis oprette adgang til data i Sundhed, der deles med funktionen Del med behandler. Du kan læse mere om, hvordan designet af denne tjeneste beskytter brugerens data i Sundhed, i afsnittet Security and Privacy i Apple Registration Guide for Healthcare Organizations.

Digital signering og kryptering

Adgangskontrollister

Data i nøgleringen adskilles og beskyttes med adgangskontrollister (Access Control Lists, ACL'er). Derfor kan der ikke opnås adgang til godkendelsesoplysninger, som er gemt af apps fra tredjeparter eller fra apps med andre identiteter, medmindre brugeren udtrykkeligt godkender dem. Denne metode beskytter godkendelsesoplysningerne på Apple-enheder på tværs af en række apps og tjenester i organisationen.

Mail

I appen Mail kan brugerne sende beskeder, der er signeret digitalt og krypteret. Mail finder automatisk de relevante e-mailadresser og alternative navne på emnet (med forskel på store og små bogstaver) i overensstemmelse med RFC 5322 på digitale signerings- og krypteringscertifikater i tilknyttede PIV-tokens (Personal Identification Verification) på kompatible Smart Cards. Hvis en konfigureret e-mailkonto svarer til en e-mailadresse på et digitalt signerings- eller krypteringscertifikat i et tilknyttet PIV-token, viser Mail automatisk knappen Signering på værktøjslinjen i en ny besked. Hvis Mail har modtagerens certifikat til kryptering af e-mail eller kan finde det i den globale adresseliste fra Microsoft Exchange, vises symbolet for ulåst på værktøjslinjen i en ny besked. Hvis symbolet er en låst hængelås, sendes beskeden krypteret med modtagerens offentlige nøgle.

S/MIME for hver besked

iOS, iPadOS og macOS understøtter S/MIME for hver besked. Det betyder, at brugerne af S/MIME kan vælge, om beskeder som standard altid skal signeres og krypteres, eller om brugerne for hver besked skal vælge, om den skal signeres og krypteres.

Identiteter, der bruges med S/MIME, kan leveres til Apple-enheder ved hjælp af en konfigurationsprofil, en løsning til administration af mobile enheder (MDM), SCEP (Simple Certificate Enrollment Protocol) eller en Microsoft Active Directory-certifikatmyndighed.

Smart Cards

macOS 10.12 og nyere versioner understøtter uden videre PIV-kort. Disse kort bruges ofte i erhvervslivet og det offentlige til tofaktorgodkendelse, digital signering og kryptering.

Smart Cards indeholder en eller flere digitale identiteter, der har et par med en offentlig og en privat nøgle og et tilhørende certifikat. Når et kort låses op med PIN-koden, gives adgang til de private nøgler, der bruges til godkendelse, kryptering og signering. Certifikatet bestemmer, hvad nøglen kan bruges til, hvilke egenskaber der er knyttet til den, og om den er godkendt (signeret) af en certifikatmyndighed (CA).

Smart Cards kan bruges til tofaktorgodkendelse. De to elementer, der kræves for at låse et kort op, er "noget, brugeren har" (kortet) og "noget, brugeren ved" (PIN-koden). macOS 10.12 og nyere versioner understøtter også uden videre godkendelse af login-vinduet til Smart Card og godkendelse af klientcertifikater over for websteder i Safari. Kerberos-godkendelse med nøglepar (PKINIT) til SSO (Single sign-on) på Kerberos-kompatible tjenester understøttes også. Du kan læse mere om Smart Cards og macOS i Introduktion til integration af Smart Card i *Implementering af Apples platforme*.

Krypterede diskbilleder

I macOS fungerer krypterede diskbilleder som sikre beholdere, hvori brugerne kan opbevare og overføre følsomme dokumenter og andre arkiver. Krypterede diskbilleder oprettes med Disk Utility i /Apps/Hjælpeapps/. Diskbilleder kan krypteres med 128-bit eller 256-bit AES-kryptering. Et aktivt diskbillede behandles som en lokal disk, der er sluttet til Mac, og brugerne kan derfor kopiere, flytte og åbne arkiver og mapper, der opbevares i det. Ligesom med FileVault krypteres og dekrypteres indholdet i et diskbillede i realtid. Med krypterede diskbilleder kan brugere udveksle dokumenter, arkiver og mapper sikkert ved at gemme det krypterede diskbillede på et udskifteligt medie, sende det som et bilag i en e-mail eller opbevare det på en ekstern server. I Brugerhåndbog til Diskværktøj er der flere oplysninger om krypterede diskbilleder.

App-sikkerhed

Oversigt over app-sikkerhed

Apps er i dag et af de mest kritiske elementer i en sikkerhedsarkitektur. Apps kan give brugerne fantastiske fordele med hensyn til produktivitet, men hvis de ikke håndteres korrekt, kan de have en negativ indflydelse på systemsikkerhed, stabilitet og brugerdata.

Apple implementerer derfor beskyttelseslag, der skal være med til at sikre, at apps er fri for kendt malware, og at de ikke er blevet manipuleret. Ekstra beskyttelse sikrer, at adgang til brugerdata fra apps styres omhyggeligt. Disse sikkerhedsforanstaltninger skaber en stabil og sikker platform til apps, så tusindvis af udviklere kan levere hundredtusindvis af apps til iOS, iPadOS og macOS uden at skade systemintegriteten. Brugerne kan benytte disse apps på deres Apple-enheder uden unødig frygt for virus, malware og angreb fra uautoriserede personer.

På iPhone, iPad og iPod touch hentes alle apps fra App Store og placeres i et isoleret miljø ("sandbox") for at give den bedste sikkerhed.

På Mac hentes mange apps fra App Store, men Mac-brugere kan også hente og bruge apps fra internettet. I macOS er der ekstra beskyttelsesforanstaltninger, der sørger for, at emner kan hentes sikkert fra internettet. Først og fremmest skal alle Mac-apps i macOS 10.15 være bekræftet notarielt af Apple for at kunne startes. Dette krav er med til at sikre, at appsene er fri for kendt malware, uden at kræve at apps skal hentes fra App Store. Desuden indeholder macOS avanceret antivirusbeskyttelse, der har til formål at blokere og om nødvendigt fjerne malware.

En ekstra sikkerhedsforanstaltning på alle platforme er placering af apps i et isoleret miljø ("sandbox"), hvilket er med til at beskytte brugerdata mod uautoriseret adgang fra apps. I macOS beskyttes data i kritiske områder også – det er med til at sikre, at brugerne styrer adgangen fra alle apps til arkiver i mapperne Skrivebord, Dokumenter, Overførsler og andre områder, uanset om de apps, der anmoder om adgang, er placeret i et isoleret miljø.

Indbygget funktionalitet	**Tilsvarende tredjepart**
Liste over ikke godkendte plug-ins, liste over ikke godkendte Safari-udvidelser	Definitioner på virus/malware
Arkivkarantæne	Definitioner på virus/malware
XProtect/YARA-signaturer	Definitioner på virus/malware; beskyttelse af slutpunkt
Gatekeeper	Beskyttelse af slutpunkt – sikrer kodesignering på apps for at bidrage til at sikre, at der kun afvikles godkendt software.
EFI-tjek (nødvendigt for en Mac uden en Apple T2-sikkerhedschip)	Beskyttelse af slutpunkt – registrering af rodpakke
App-firewall	Beskyttelse af slutpunkt – via firewall
Pakkefilter (pf)	Firewall-løsninger
Beskyttelse af systemets integritet	Indbygget i macOS
Obligatorisk adgangskontrol	Indbygget i macOS
Kext-ekskluderingsliste	Indbygget i macOS
Obligatorisk signering af app-kode	Indbygget i macOS
Notariel bekræftelse af apps	Indbygget i macOS

App-sikkerhed i iOS og iPadOS

Introduktion til app-sikkerhed til iOS og iPadOS

I modsætning til nogle andre mobile platforme tillader iOS og iPadOS ikke, at brugerne installerer potentielt ondsindede ikke-signerede apps fra websteder eller afvikler apps, der ikke er godkendt. Under app-afviklingen kontrollerer kodesignaturen, at alle sider i hukommelsen fremstilles i forbindelse med indlæsningen af dem, for at bidrage til at sikre, at en app ikke er blevet modificeret, efter den blev installeret eller sidst blev opdateret.

Efter at have bekræftet, at en app stammer fra en godkendt kilde, benytter iOS og iPadOS sikkerhedsforanstaltninger til at forhindre appen i at kompromittere andre apps eller resten af systemet.

Signeringsprocessen for app-kode i iOS og iPadOS

I iOS og iPadOS stiller Apple app-sikkerhed til rådighed i kraft af ting som obligatorisk kodesignering, stringent login for udviklere m.m.

Obligatorisk kodesignering

Efter iOS- eller iPadOS-kernen er startet, styrer den, hvilke brugerprocesser og apps der må afvikles. For at bidrage til at sikre at alle apps kommer fra en kendt og godkendt kilde og ikke er blevet modificeret, kræver iOS og iPadOS, at al app-kode skal være signeret med et certifikat udstedt af Apple. Apps, der følger med enheden, f.eks. Mail og Safari, er signeret af Apple. Apps fra tredjeparter skal også godkendes og signeres ved hjælp af et certifikat udstedt af Apple. Obligatorisk kodesignering udvider begrebet godkendelseskæde fra operativsystemet til apps og er med til at forhindre apps fra tredjeparter i at indlæse ikke-signerede koderessourcer eller benytte selvmodificerende kode.

Udvikleres signering af apps

Udviklere kan signere deres apps gennem godkendelse af certifikat (via Apple Developer Program). De kan også integrere frameworks i deres apps og få denne kode godkendt med et certifikat, som er udstedt af Apple (via en streng med team-id).

- *Godkendelse af certifikat:* For at kunne udvikle og installere apps på iOS- eller iPadOS-enheder skal udviklerne registrere sig hos Apple og tilmelde sig Apple Developer Program. Udviklerens rigtige identitet, uanset om udvikleren er en enkeltperson eller en virksomhed, kontrolleres af Apple, før de udsteder et certifikat. Med certifikatet kan udviklere signere apps og indsende dem til App Store, så de kan distribueres derfra. Det betyder, at alle apps i App Store er indsendt af en person eller organisation, der kan identificeres. Det modvirker udvikling af ondsindede apps. Appsene er også blevet gennemgået af Apple for at bidrage til at sikre, at de overordnet fungerer som beskrevet og ikke indeholder åbenlyse fejl eller andre større problemer. Ud over den teknologi, der allerede er beskrevet, giver denne kuratering brugerne tillid til kvaliteten af de apps, de køber.

- *Kodesignaturgodkendelse:* iOS og iPadOS tillader, at udviklere integrerer frameworks i deres apps, som kan bruges af appen selv eller af udvidelser, som er integreret i appen. For at beskytte systemet og andre apps mod, at der indlæses kode fra tredjeparter i deres adresseområde, foretager systemet kodesignaturgodkendelse af alle de dynamiske biblioteker, som en proces henviser til på starttidspunktet. Godkendelsen gennemføres ved hjælp af team-id'et, som udtrækkes fra certifikatet, der er udstedt af Apple. Et team-id er en alfanumerisk streng på 10 tegn – f.eks. 1A2B3C4D5F. En app kan henvise til et hvilket som helst platformbibliotek, der følger med systemet, eller til et bibliotek med samme team-id i dets kodesignatur som hovedapp-arkivet. Eftersom de app-arkiver, der følger med systemet, ikke har et team-id, kan de kun henvise til biblioteker, som følger med systemet.

Kontrol af interne virksomhedsapps

Kvalificerede virksomheder har også mulighed for at udvikle interne virksomhedsapps til brug i deres egen organisation og distribuere dem til deres medarbejdere. Virksomheder og organisationer kan ansøge om medlemskab af Apple Developer Enterprise Program (ADEP). Du kan få flere oplysninger og se kvalifikationskravene på webstedet om Apple Developer Enterprise Program. Når en organisation er blevet medlem af ADEP, kan den registrere sig for at få en programprofil, der tillader, at interne virksomhedsapps afvikles på enheder, som den godkender.

Programprofilen skal være installeret hos brugerne, før de kan afvikle disse apps. Det er med til at sikre, at kun organisationens godkendte brugere er i stand til at indlæse appsene på deres iOS- og iPadOS-enheder. Apps, der installeres via administration af mobile enheder (MDM), er implicit godkendt, fordi relationen mellem organisationen og enheden allerede er etableret. Ellers skal brugerne godkende appens programprofil under Indstillinger. Organisationer kan desuden forhindre brugere i at godkende apps fra ukendte udviklere. Første gang en intern virksomhedsapp startes, skal enheden modtage en positiv bekræftelse fra Apple af, at appen har tilladelse til at blive afviklet.

Sikkerhed under afvikling af apps i iOS og iPadOS

iOS og iPadOS bidrager til sikkerheden under afvikling af apps ved at bruge et isoleret miljø (en "sandbox"), erklærede berettigelser og ASLR (Address Space Layout Randomization).

Placering i et isoleret miljø

Alle apps fra tredjeparter afvikles i et isoleret miljø ("sandbox"), der forhindrer dem i at få adgang til arkiver, som andre apps har oprettet, og i at foretage ændringer af enheden. "Sandboxing" har til formål at forhindre apps i at indsamle eller ændre oplysninger, som andre apps har gemt. Hver app har sit eget hjemmebibliotek til sine arkiver. Det tildeles efter en tilfældighedsalgoritme, når appen installeres. Hvis en app fra en tredjepart har behov for at få adgang til andre oplysninger end sine egne, gør den det udelukkende ved hjælp af tjenester i iOS og iPadOS.

Systemarkiver og -ressourcer skærmes også mod brugernes apps. De fleste systemarkiver og -ressourcer i iOS og iPadOS afvikles som den ikke-privilegerede bruger i "mobile". Det samme gør alle apps fra tredjeparter. Hele partitionen med operativsystemet er aktiveret som skrivebeskyttet. Unødvendige værktøjer, f.eks. tjenesterne til ekstern login, indgår ikke i systemsoftwaren, og API'er tillader ikke, at apps eskalerer deres tilladelser for at ændre andre apps eller iOS og iPadOS.

Brug af berettigelse

Adgang fra apps fra tredjeparter til brugeroplysninger og funktioner som iCloud og udvidelsesmuligheder styres ved hjælp af erklærede berettigelser. Berettigelser er parvise nøgler og værdier, som indgår i appens signatur og tillader godkendelse ud over afviklingsfaktorer som f.eks. bruger-id til UNIX. Eftersom berettigelser er signeret digitalt, kan de ikke ændres. Berettigelser bruges i vidt omfang af systemapps og -dæmoner til at udføre bestemte, privilegerede funktioner, som ellers skulle udføres som root. Det giver en langt mindre risiko for, at en systemapp eller en systemdæmon, som er blevet kompromitteret, eskalerer sine tilladelser.

Apps kan desuden kun udføre opgaver i baggrunden via systemets API'er. Det gør, at apps kan blive ved med at fungere uden at forringe ydeevnen eller forkorte batteritiden voldsomt.

ASLR (Address Space Layout Randomization)

ASLR (Address Space Layout Randomization) er med til at beskytte mod udnyttelse af fejl, der ødelægger hukommelsen. Indbyggede apps bruger ASLR til at bidrage til at sikre en tilfældig placering af alle hukommelsesområder, når de startes. Ud over funktionen under start placerer ASLR hukommelsesadresserne til app-kode, systembiblioteker og relaterede programmeringskonstruktioner tilfældigt og mindsker derved sandsynligheden for mange angreb. Eksempelvis forsøger et return-to-libc-angreb at narre en enhed til at udføre en ondsindet kode ved at manipulere hukommelsesadresserne i stakken og systembibliotekerne. Når de placeres tilfældigt, er det sværere at foretage et angreb, især på flere enheder samtidig. Xcode, såvel som udviklingsmiljøerne i iOS og iPadOS, kompilerer automatisk apps fra tredjeparter med ASLR-understøttelse slået til.

Funktionen Execute Never

Yderligere beskyttelse opnås ved, at iOS og iPadOS bruger ARM-funktionen Execute Never (XN), som markerer hukommelsessider som ikke-app-sider. Hukommelsessider, der både er markeret med skriveadgang og som app-sider, kan kun bruges af apps under yderst kontrollerede betingelser: Kernen undersøger, om den Apple-mærkede berettigelse "dynamisk kodesignering" er til stede. Selv da kan der kun foretages et enkelt `mmap`-kald for at anmode om en app-side, der er skriveadgang til, og som er tildelt en tilfældig adresse. Safari bruger denne funktionalitet til sin JavaScript JIT-compiler (Just-in-Time).

Supplerende udvidelser i iOS, iPadOS og macOS

Ved hjælp af udvidelser i iOS, iPadOS og macOS kan apps stille funktionalitet til rådighed for andre apps. Udvidelser er signerede binære app-arkiver til bestemte formål, som er indpakket i en app. Under installering registrerer systemet automatisk udvidelser og gør dem tilgængelige for andre apps, der bruger et tilsvarende system.

Udvidelsespunkter

Et systemområde, der understøtter udvidelser, kaldes et *udvidelsespunkt*. Hvert udvidelsespunkt stiller API'er til rådighed og håndhæver politikker for området. Systemet afgør ud fra særlige sammenligningsregler for udvidelsespunktet, hvilke udvidelser der er tilgængelige. Systemet starter automatisk udvidelsesprocesser efter behov og administrerer deres levetid. Berettigelser kan bruges til at begrænse udvidelsernes tilgængelighed til bestemte systemapps. Den widget, der viser oversigten "I dag", findes f.eks. kun i Notifikationscenter, og en udvidelse vedrørende deling er kun tilgængelig fra vinduet Deling. Der er f.eks. følgende udvidelsespunkter: "I dag"-widgets, Del, handlinger, Fotoredigering, Arkivudbyder og Specielt tastatur.

Kommunikation mellem udvidelser

Udvidelser afvikles i deres eget adresseområde. Kommunikation mellem udvidelsen og den app, den blev aktiveret fra, bruger kommunikation mellem processer med systemets framework som mægler. De har ikke adgang til hinandens arkiver eller hukommelsesområder. Udvidelser er designet, så de er isoleret i forhold til hinanden, til de apps, de er indeholdt i, og til de apps, der bruger dem. De afvikles i et isoleret miljø ("sandbox") og har en beholder, der er adskilt fra den indeholdende apps beholder. De har imidlertid samme adgang til anonymitetsindstillinger som den app, de er indeholdt i. Det betyder, at hvis en bruger tildeler en app adgang til Kontakter, udvides tildelingen til de udvidelser, der er integreret i appen, men ikke til de udvidelser, som appen aktiverer.

Brug af specielle tastaturer

Specielle tastaturer er en særlig type udvidelse, fordi den aktiveres af brugeren til hele systemet. Når en tastaturudvidelse er aktiveret, bruges den til alle tekstfelter, undtagen indtastning af koder og sikre tekstoversigter. For at begrænse overførslen af brugerdata afvikles specielle tastaturer som standard i et meget restriktivt isoleret miljø, der blokerer adgang til netværket, til tjenester, som udfører netværksfunktioner på vegne af en proces, og til API'er, der ville give udvidelsen mulighed for at tilegne sig indtastede data. Udviklere af specielle tastaturer kan anmode om åben adgang for deres udvidelse, så systemet kan afvikle udvidelsen i det isolerede standardmiljø (standardsandbox), hvis brugeren giver sit samtykke.

MDM og udvidelser

For enheder, der er tilmeldt en løsning til administration af mobile enheder (MDM), gælder, at dokument- og tastaturudvidelser overholder administrerede "Åbn i"-regler. MDM-løsningen kan f.eks. være med til at forhindre brugere i at eksportere et dokument fra en administreret app til en ikke-administreret dokumentudbyder eller bruge et ikke-administreret tastatur til en administreret app. Derudover kan app-udviklere forhindre brugen af tastaturudvidelser fra tredjeparter i deres app.

App-beskyttelse og app-grupper i iOS og iPadOS

I iOS og iPadOS kan organisationer beskytte apps ved at bruge iOS SDK og ved at blive medlem af en app-gruppe på Apple Developer Portal.

Implementering af databeskyttelse i apps

iOS Software Development Kit (SDK) til iOS og iPadOS omfatter et komplet sæt API'er, der gør det let for tredjepartsudviklere og interne udviklere at benytte databeskyttelse og hjælpe med at sikre det højst mulige beskyttelsesniveau i deres apps. Databeskyttelse er tilgængeligt for API'er til arkiver og databaser, herunder NSFileManager, CoreData, NSData og SQLite.

Databasen til appen Mail (inkl. bilag), administrerede bøger, Safari-bogmærker, startbilleder til apps og lokalitetsdata opbevares også via kryptering med nøgler, der beskyttes af brugerens kode på enheden. Kalender (ekskl. bilag), Kontakter, Påmindelser, Noter, Beskeder og Fotos implementerer databeskyttelsesberettigelsen Beskyttet indtil første brugergodkendelse.

Brugerinstallerede apps, som ikke tilvælger en bestemt databeskyttelsesklasse, tildeles som standard Beskyttet indtil første brugergodkendelse.

Tilmelding til en app-gruppe

Apps og udvidelser, der ejes af en given udvikler, kan dele indhold, når de konfigureres som en del af en app-gruppe. Det er udviklerens ansvar at oprette de relevante grupper på Apple Developer Portal og inkludere det ønskede sæt apps og udvidelser. Når apps er konfigureret som en del af en app-gruppe, har de adgang til følgende:

- En delt beholder til arkivering på disken, som bevares på enheden, så længe mindst en app fra gruppen er installeret
- Delte indstillinger
- Delte emner i nøgleringen

Apple Developer Portal bidrager til at sikre, at alle gruppe-id'er er forskellige i hele økosystemet til apps.

Bekræftelse af tilbehør i iOS og iPadOS

MFi-licensprogrammet (Made for iPhone, iPad og iPod touch) giver godkendte producenter af tilbehør adgang til iPod Accessories Protocol (iAP) og de nødvendige hardwarekomponenter, der understøtter det.

Når MFi-tilbehør kommunikerer med en iOS- eller iPadOS-enhed via et Lightning- eller USB-C-stik eller Bluetooth, beder enheden tilbehøret om at bevise, at det er godkendt af Apple, ved at svare med et certifikat fra Apple, som enheden derefter godkender. Derefter sender enheden en udfordring, som tilbehøret skal besvare med et signeret svar. Denne proces håndteres udelukkende af et særligt integreret kredsløb, som Apple stiller til rådighed for godkendte producenter af tilbehør. Det egentlige tilbehør skal ikke foretage sig noget.

Tilbehør kan anmode om adgang til forskellige transportformer og funktioner, f.eks. adgang til digitale lydstreams via Lightning- eller USB-C-kablet eller lokalitetsoplysninger leveret via Bluetooth. Et integreret kredsløb til godkendelse har til formål at sikre, at kun godkendt tilbehør får fuld adgang til enheden. Hvis noget tilbehør ikke understøtter godkendelse, er dets adgang begrænset til analog lyd og en lille del af det serielle (UART) betjeningspanel til lydafspilning.

AirPlay bruger også det integrerede kredsløb til godkendelse til at bekræfte, at modtagerne er godkendt af Apple. AirPlay-lydstreams og CarPlay-videostreams bruger MFi-SAP (Secure Association Protocol), som krypterer kommunikationen mellem tilbehøret og enheden ved hjælp af AES128 med tællerfunktion (CTR). Midlertidige nøgler udveksles via ECDH-nøgleudveksling (Curve25519) og signeres ved hjælp af det integrerede godkendelseskredsløbs 1024-bit RSA-nøgle som en del af STS-protokollen (Station-To-Station).

App-sikkerhed i macOS

Introduktion til app-sikkerhed i macOS

App-sikkerhed i macOS består af et antal overlappende lag, hvoraf det første er muligheden for kun at afvikle signerede og godkendte apps fra App Store. Derudover indeholder macOS beskyttelseslag, som er med til at sikre, at apps, der er hentet fra internettet, er fri for kendt malware. macOS indeholder teknologier, der har til formål at finde og fjerne malware, samt ekstra beskyttelsesforanstaltninger, som skal forhindre, at ikke-godkendte apps får adgang til brugerdata. Apple-tjenester som f.eks. opdateringer til Notarization og XProtect har til formål at bidrage til at forhindre installering af malware. Ved behov finder disse tjenester malware, som måske ikke blev opdaget i første omgang, og fjerner den derefter hurtigt og effektivt. I sidste ende har macOS-brugere frihed til at arbejde inden for den sikkerhedsmodel, der giver mening for dem – også at afvikle kode, der hverken er signeret eller godkendt.

Signeringsprocessen for app-kode i macOS

Alle apps fra App Store er signeret af Apple. Signeringen har til formål at sikre, at de ikke er blevet manipuleret eller ændret. Apple signerer alle apps, som følger med Apple-enheder.

I macOS 10.15 skal alle apps, som distribueres uden for App Store, være signeret af udvikleren med et udviklercertifikat udstedt af Apple (sammen med en privat nøgle) og bekræftet notarielt for at kunne afvikles under standardindstillinger i Gatekeeper. Apps, der er udviklet internt, bør også signeres med et udviklercertifikat udstedt af Apple, så deres integritet kan kontrolleres.

I macOS fungerer kodesignering og notariel bekræftelse uafhængigt af hinanden – og kan udføres af forskellige aktører – til forskellige formål. Kodesignering foretages af udvikleren med udviklerens certifikat (udstedt af Apple), og bekræftelse af denne signatur beviser over for brugeren, at der ikke er manipuleret med udviklerens software, eftersom den er udviklet og signeret af udvikleren. Notariel bekræftelse kan udføres af enhver, der er involveret i distributionen af softwaren, og beviser, at Apple har modtaget en kopi af koden med henblik på at undersøge, om den indeholder malware, og at der ikke blev fundet kendt malware. Resultatet af den notarielle bekræftelse er en billet, der opbevares på Apple-servere og eventuelt kan hæftes sammen med appen uden at gøre udviklerens signatur ugyldig.

Obligatorisk adgangskontrol (MAC) kræver kodesignering for at aktivere rettigheder, som er beskyttet af systemet. Som eksempel skal apps, der kræver adgang via firewall, kodesigneres med den relevante MAC-rettighed.

Sikkerhed via Gatekeeper og under app-afvikling i macOS

macOS indeholder teknologien Gatekeeper og beskyttelse under app-afvikling, der er med til at sikre, at kun godkendt software afvikles på en brugers Mac.

Gatekeeper

macOS indeholder en sikkerhedsteknologi, der kaldes *Gatekeeper*, og som har til formål at sikre, at der kun afvikles godkendt software på en brugers Mac. Når en bruger henter og åbner en app, et tilbehør eller en installeringspakke fra et andet sted end App Store, kontrollerer Gatekeeper, at softwaren kommer fra en identificeret udvikler, at Apple notarielt har bekræftet, at den er fri for kendt skadeligt indhold, og at den ikke er blevet modificeret. Gatekeeper anmoder også om brugerens godkendelse, før hentet software åbnes første gang, for at sikre, at brugeren ikke er blevet narret til at afvikle app-kode, som brugeren troede var et almindeligt dataarkiv.

Gatekeeper er som standard med til at sikre, at al hentet software er blevet signeret af App Store eller signeret af en registreret udvikler og bekræftet notarielt af Apple. Både kontrolprocessen i App Store og den notarielle bekræftelsesproces har til formål at sikre, at apps ikke indeholder kendt malware. Det betyder, at *al software i macOS som standard bliver kontrolleret for, om den indeholder kendt skadeligt indhold, første gang den åbnes, uanset hvordan den er blevet installeret på Mac*.

Brugere og organisationer har mulighed for at indstille, at det kun er muligt at installere software fra App Store. Alternativt kan brugerne tilsidesætte Gatekeeper-politikker og åbne al software, medmindre en løsning til administration af mobile enheder (MDM) forhindrer det. Organisationer kan bruge MDM til at konfigurere indstillinger til Gatekeeper, herunder tillade software signeret med andre identiteter. Gatekeeper kan også deaktiveres fuldstændigt, hvis det er nødvendigt.

Gatekeeper beskytter også mod distribution af skadeligt tilbehør med godartede apps. Her udløser brugen af appen indlæsning af et skadeligt tilbehør uden brugerens viden. Hvis det er nødvendigt, åbner Gatekeeper apps fra en tilfældigt udvalgt skrivebeskyttet placering. Det har til formål at forhindre, at tilbehør, der er distribueret sammen med appen, automatisk indlæses.

Beskyttelse ved afvikling

Systemarkiver, systemressourcer og kernen er afskærmet fra brugerens app-område. Alle apps fra App Store er placeret i et isoleret miljø (“sandbox”), der begrænser adgangen til data, som andre apps har gemt. Hvis en app fra App Store har brug for adgang til data fra en anden app, kan det kun få adgang ved at bruge de API'er og tjenester, der stilles til rådighed af macOS.

Beskyttelse mod malware i macOS

Apple benytter en proces baseret på oplysninger om trusler til hurtigt at identificere og blokere malware.

Tre lag med forsvarsforanstaltninger

Forsvarsforanstaltninger mod malware er struktureret i tre lag:

1. *Sørg for, at malware ikke kan startes eller afvikles:* App Store eller Gatekeeper i kombination med Notarization

2. *Bloker afvikling af malware på kundesystemer:* Gatekeeper, Notarization og XProtect

3. *Afbød virkningerne af afviklet malware:* XProtect

Det første lag med forsvarsforanstaltninger har til formål at modvirke distribution af malware og forhindre, at malware nogensinde startes – det er formålet med App Store og Gatekeeper i kombination med Notarization.

Det næste lag med forsvarsforanstaltninger er med til at sikre, at hvis der forekommer malware på en Mac, bliver den hurtigt identificeret og blokeret, både for at stoppe udbredelsen og for at reparere de Mac-systemer, det er lykkedes at komme ind på. XProtect er med i denne forsvarsforanstaltning sammen med Gatekeeper og Notarization.

Endelig bruges XProtect til at afbøde virkningerne af malware, det er lykkedes af afvikle.

Tilsammen understøtter disse beskyttelsesforanstaltninger, som er beskrevet nærmere nedenfor, de bedste metoder til beskyttelse mod virus og malware. Der er flere beskyttelsesforanstaltninger, især på en Mac med Apple Silicon, der begrænser skadevirkningerne som følge af malware, det alligevel er lykkedes at afvikle. I Beskyttelse af app-adgang til brugerdata kan du læse, hvordan macOS kan hjælpe med at beskytte brugerdata mod malware, og i Operativsystemets integritet kan du læse, hvordan macOS kan begrænse det, som malware kan foretage sig på systemet.

Notarization

Notarization er en tjeneste fra Apple, som scanner efter malware. Udviklere, som ønsker at distribuere apps til macOS uden for App Store, sender deres apps til scanning som et led i distributionsprocessen. Apple undersøger, om softwaren indeholder kendt malware, og udsteder en Notarization-billet, hvis der ikke bliver fundet malware. Udviklere hæfter typisk billetten sammen med deres app, så Gatekeeper kan godkende og starte appen, også offline.

Apple kan også udstede en tilbagekaldelsesbillet til apps, der er kendt som skadelige – også selvom de tidligere er blevet bekræftet notarielt. macOS undersøger jævnligt, om der er nye tilbagekaldelsesbilletter, så Gatekeeper har de nyeste oplysninger og kan forhindre, at disse app-arkiver startes. Processen kan meget hurtigt blokere skadelige apps, fordi opdateringer foregår i baggrunden langt hyppigere end selv de baggrundsopdateringer, som udsender nye XProtect-signaturer. Denne beskyttelse kan desuden anvendes både til apps, der tidligere er blevet bekræftet notarielt, og dem, der ikke er.

XProtect

macOS bruger en indbygget antivirusteknologi, der kaldes *XProtect*, til at finde og fjerne malware på grundlag af signaturer. Systemet bruger YARA-signaturer, et værktøj, der bruges til at foretage signaturbaseret registrering af malware, og som opdateres jævnligt af Apple. Apple overvåger nye infektioner og belastninger fra malware og opdaterer automatisk signaturer – uafhængigt af systemopdateringer – for at hjælpe med at forsvare en Mac mod infektion fra malware. XProtect registrerer og blokerer automatisk afvikling af kendt malware. I macOS 10.15 og nyere versioner undersøger XProtect, om der er kendt skadeligt indhold, når:

- En app startes første gang
- En app er blevet ændret (i arkivsystemet)
- XProtect-signaturer opdateres

Når XProtect finder kendt malware, blokeres softwaren, og brugeren underrettes og får mulighed for at flytte softwaren til papirkurven.

Bemærk: Notarization er en effektiv foranstaltning mod kendte arkiver (eller arkivers hash-værdier) og kan bruges på apps, der tidligere er blevet startet. De signaturbaserede regler i XProtect er mere generiske end specifikke hash-værdier til arkiver, så XProtect kan finde varianter, som Apple ikke har set. XProtect undersøger kun apps, der er blevet ændret, eller som startes for første gang.

Hvis malware kommer ind på en Mac-computer, har XProtect også teknologi til at udbedre infektioner. Det indeholder f.eks. et modul, der udbedrer infektioner ved hjælp af opdateringer, der automatisk leveres af Apple (som led i automatiske opdateringer af systemdataarkiver og sikkerhedsopdateringer). Det fjerner også malware, når det modtager opdaterede oplysninger, og kontrollerer løbende, om der er infektioner. XProtect genstarter ikke automatisk Mac.

Automatiske sikkerhedsopdateringer til XProtect

Apple udsender automatisk opdateringer til XProtect på grundlag af de nyeste oplysninger om trusler. Som standard undersøger macOS hver dag, om der er opdateringer. Opdateringer til Notarization, som distribueres ved hjælp af CloudKit-synkronisering, sker langt oftere.

Apples reaktion, når der findes ny malware

Når der bliver fundet ny malware, kan der træffes forskellige foranstaltninger:

- Eventuelle tilknyttede certifikater til udvikler-id'er tilbagekaldes.
- Der udstedes notarielt bekræftede tilbagekaldelsesbilletter til alle arkiver (apps og deres tilhørende arkiver).
- XProtect-signaturer dannes og frigives.

  Disse signaturer anvendes også bagudrettet til tidligere notarielt bekræftet software, og alle nye fund kan medføre, at en af de tidligere handlinger foretages.

Opdagelse af malware udløser således en række foranstaltninger i løbet af de næste sekunder, timer og dage for at give Mac-brugere den bedst mulige beskyttelse.

Styring af app-adgang til arkiver i macOS

Apple mener, at brugerne skal give deres samtykke og have fuld indsigt i og kontrol over, hvad apps gør med deres data. I macOS 10.15 håndhæves denne model af systemet for at bidrage til at sikre, at alle apps indhenter brugerens samtykke, før de får adgang til arkiver i Dokumenter, Overførsler, Skrivebord, iCloud Drive og netværksenheder. I macOS 10.13 og nyere versioner skal apps, der kræver adgang til hele lagringsenheden, tilføjes ved navn i Systemindstillinger. Tilgængeligheds- og automatiseringsfunktioner kræver også brugertilladelse for at bidrage til at sikre, at de ikke omgår andre beskyttelsesforanstaltninger. Afhængigt af adgangspolitikken kan brugerne blive bedt om eller få besked på at ændre indstillingen i Systemindstillinger > Sikkerhed & anonymitet > Anonymitet:

Emne	Bruger spørges af app	Bruger skal redigere systemets anonymitetsindstillinger
Tilgængelighed		✅
Adgang til hele den interne lagringsplads		✅
Arkiver og mapper *Bemærk:* Omfatter Skrivebord, Dokumenter, Overførsler, netværksenheder og udskiftelige enheder	✅	
Automatisering (Apple-begivenheder)	✅	

Emner i brugerens papirkurv beskyttes mod apps, der bruger fuld diskadgang; brugeren bliver ikke bedt om at give appen adgang. Hvis brugeren ønsker, at apps skal have adgang til arkiverne, skal arkiverne flyttes fra papirkurven til en anden placering.

En bruger, der slår FileVault til på en Mac, bliver bedt om at oplyse gyldige godkendelsesoplysninger, for at startprocessen kan fortsætte, og for at få adgang til specielle startmuligheder. Uden gyldige godkendelsesoplysninger til login eller en gendannelsesnøgle er hele disken krypteret og beskyttet mod uvedkommendes adgang, også selvom den fysiske lagringsenhed fjernes og sluttes til en anden computer.

For at beskytte data i et virksomhedsmiljø skal it-afdelingen definere og håndhæve konfigureringspolitikker til FileVault ved hjælp af en løsning til administration af mobile enheder (MDM). Virksomheder har adskillige muligheder til administration af krypterede enheder, bl.a. gendannelsesnøgler fra organisationen (som valgfrit kan deponeres hos MDM), eller en kombination af begge. Rotation af nøgler kan også indstilles som en politik i MDM.

Sikkerhedsfunktioner i Noter

Appen Noter indeholder en funktion til sikre noter på iPhone, iPad og iCloud-webstedet, der sætter en bruger i stand til at beskytte indholdet af bestemte noter. Brugerne kan også dele noter med andre på en sikker måde.

Sikre noter

Sikre noter er end-to-end-krypterede med en adgangskode, som brugeren angiver, og som skal indtastes for at se noterne på iOS-, iPadOS- og macOS-enheder og på iCloud-webstedet. Hver iCloud-konto (herunder konti af typen "På min" enhed) kan have sin egen adgangskode.

Når en bruger sikrer en note, dannes en nøgle på 16 byte ud fra brugerens adgangskode ved hjælp af PBKDF2 og SHA256. Noten og alle dens bilag krypteres ved hjælp af AES med Galois-/tællerfunktion (AES-GCM). Der oprettes nye poster i Core Data og CloudKit til opbevaring af den krypterede note, krypterede bilag, krypteret mærke og krypteret initialiseringsvektor. Når de nye poster er oprettet, slettes de oprindelige ukrypterede data. Følgende bilag kan krypteres: billeder, skitser, tabeller, kort og websteder. Noter, der indeholder andre typer bilag, kan ikke krypteres, og bilag, der ikke understøttes, kan ikke føjes til sikre noter.

En bruger, der vil se en sikker note, skal skrive sin adgangskode eller godkendes med sit Face ID eller Touch ID. Når brugeren er godkendt – til at se eller oprette en sikker note – åbner Noter en sikker session. Mens den sikre session er åben, kan brugeren se eller gøre andre noter sikre uden yderligere godkendelse. Den sikre session kan dog kun anvendes til noter, der er beskyttet med den anførte adgangskode. Brugeren skal stadig godkendes til noter, der er beskyttet med en anden adgangskode. Den sikre session lukkes, når:

- Brugeren trykker på knappen Lås nu i Noter
- Noter anbringes i baggrunden i mere end 3 minutter (8 minutter i macOS)
- iOS- eller iPadOS-enheden låses

Hvis brugeren vil skifte kode til en sikker note, skal brugeren skrive den nuværende kode, da Face ID og Touch ID ikke kan bruges til at skifte kode. Når der er valgt en ny adgangskode, ompakker Noter i samme konto nøglerne til alle eksisterende noter, som er krypteret med den gamle adgangskode.

Hvis en bruger skriver adgangskoden forkert tre gange i træk, viser Noter et stikord, hvis brugeren oplyste et stikord under indstillingen. Hvis brugeren stadig ikke kan huske sin adgangskode, kan adgangskoden nulstilles i indstillingerne til Noter. Denne funktion sikrer, at brugerne kan oprette nye sikre noter med en ny adgangskode, men giver dem ikke mulighed for at se tidligere sikrede noter. De tidligere sikrede noter kan ses, hvis brugeren kommer i tanke om den gamle adgangskode. Adgangskoden til brugerens iCloud-konto skal bruges, hvis adgangskoden skal nulstilles.

Delte noter

Noter, der ikke er end-to-end-krypterede med en adgangskode, kan deles med andre. Delte noter bruger stadig den krypterede datatype i CloudKit til tekst eller bilag, som brugeren anbringer i en note. Aktiver krypteres altid med en nøgle, der er krypteret i CKRecord. Metadata, f.eks. oprettelses- og ændringsdatoer, krypteres ikke. CloudKit håndterer den proces, hvormed deltagere kan kryptere eller dekryptere hinandens data.

Sikkerhedsfunktioner i Genveje

Det er muligt at synkronisere genvejene i appen Genveje mellem Apple-enheder vha. iCloud. Genveje kan også deles med andre brugere via iCloud. Genveje opbevares lokalt i krypteret format.

Specielle genveje er alsidige – de ligner instrukser eller apps. Når en bruger henter genveje fra internettet, får brugeren en advarsel om, at genvejen ikke er blevet kontrolleret af Apple, og får mulighed for at undersøge genvejen. Der hentes opdaterede definitioner af malware for at identificere skadelige genveje under afvikling og beskytte brugerne mod dem.

Specielle genveje kan også afvikle JavaScript anført af brugeren på websteder i Safari, når dette startes fra siden til delinger. De førnævnte definitioner af malware bruges til at kontrollere JavaScript-kode og beskytte brugerne mod skadelig kode, der f.eks. prøver at narre dem til at afvikle en instruks på websteder til sociale medier, som indsamler deres data. Første gang en bruger afvikler JavaScript på et domæne, bliver brugeren bedt om at give tilladelse til, at genveje, der indeholder JavaScript, kan afvikles på den aktuelle webside for domænet.

Sikkerhedstjenester

Oversigt over sikkerhedstjenester

Apple har skabt nogle gedigne tjenester for at hjælpe brugerne med at få en bedre brugeroplevelse og større produktivitet med deres enheder. Tjenesterne giver brugerne mulighed for effektiv opbevaring i skyen, synkronisering, opbevaring af adgangskoder, godkendelse, betaling, chat, kommunikation m.m., samtidig med at brugernes anonymitet og data beskyttes.

Dette kapitel beskriver de sikkerhedsteknologier, der bruges i iCloud, Log ind med Apple, Apple Pay, iMessage, Apple Messages for Business, FaceTime, Find og Kontinuitet.

Bemærk: Nogle Apple-tjenester og noget indhold er ikke tilgængeligt i alle lande eller områder.

Apple-id og administreret Apple-id

Oversigt over Apple-id-sikkerhed

Et Apple-id er den konto, der bruges til at logge ind på Apples tjenester. Det er vigtigt, at brugerne beskytter deres Apple-id for at forhindre uautoriseret adgang til deres konti. Derfor kræves der til Apple-id'er stærke adgangskoder, som:

- Er på mindst otte tegn
- Indeholder både bogstaver og tal
- Højst indeholder tre ens tegn efter hinanden
- Ikke er almindeligt anvendte adgangskoder

Det er en god idé, hvis brugerne gør deres adgangskode endnu stærkere ved at bruge symboler og skilletegn.

Apple giver desuden brugerne besked via e-mails, push-notifikationer eller begge dele, hvis der sker noget vigtigt i forbindelse med deres konto, f.eks. hvis adgangskoden eller faktureringsoplysningerne er ændret, eller hvis deres Apple-id er blevet brugt til at logge ind på en ny enhed. Hvis noget ser mistænkeligt ud, får brugerne besked på straks at skifte adgangskode til deres Apple-id.

Apple benytter desuden en række strategier og procedurer, der har til formål at beskytte brugerkonti. De omfatter blandt andet begrænsning af antal forsøg på at logge ind og på at nulstille adgangskoder, aktiv overvågning af forsøg på bedrag for at identificere angreb, mens de foretages, og regelmæssig gennemgang af politikker, der hjælper Apple med at indpasse nye oplysninger, der kan påvirke brugerens sikkerhed.

Bemærk: Adgangskodepolitikken for Administreret Apple-id indstilles af en administrator i Apple School Manager eller Apple Business Manager.

Tofaktorgodkendelse

Apple bruger *tofaktorgodkendelse*, som er et ekstra sikkerhedslag til Apple-id'er, der hjælper brugerne med at beskytte deres konti yderligere. Formålet er at sikre, at kun kontoejeren kan få adgang til kontoen, selvom en anden kender adgangskoden. Med tofaktorgodkendelse kan der kun opnås adgang til en brugers konto på godkendte enheder, som f.eks. brugerens iPhone, iPad, iPod touch, Mac-computer eller andre enheder, efter at der er sket en bekræftelse via en af disse godkendte enheder eller et godkendt telefonnummer. Første gang der logges ind på en ny enhed, skal der bruges to oplysninger – adgangskoden til Apple-id'et og en bekræftelseskode på seks cifre, der automatisk vises på brugerens godkendte enheder eller sendes til et godkendt telefonnummer. Når brugeren indtaster koden, bekræfter brugeren, at den nye enhed er godkendt, og at det er sikkert at logge ind. Adgangskoden er ikke længere nok til at få adgang til en brugers konto, og tofaktorgodkendelse forbedrer dermed sikkerheden for brugerens Apple-id og alle de personlige oplysninger, som brugeren opbevarer hos Apple. Funktionen er integreret i iOS, iPadOS, macOS, tvOS, watchOS og de godkendelsessystemer, som bruges af Apples websteder.

Når en bruger logger ind på et af Apples websteder i en browser, sendes der en anden faktoranmodning til alle godkendte enheder, der er forbundet med brugerens iCloud-konto, med en anmodning om godkendelse af browsersessionen. Hvis brugeren logger ind på et Apple-websted fra en browser på en godkendt enhed, vises bekræftelseskoden lokalt på den enhed, der er i brug. Når brugeren indtaster koden på enheden, bliver websessionen godkendt.

Nulstilling af adgangskode og kontogendannelse

Hvis en bruger glemmer adgangskoden til sin Apple-id-konto, kan brugeren nulstille den på en godkendt enhed. Hvis adgangskoden er kendt, og der ikke er nogen tilgængelig godkendt enhed, kan brugeren benytte et godkendt telefonnummer til at foretage godkendelsen via en sms-bekræftelse. Desuden kan en tidligere anvendt kode sammen med en sms bruges til at gendanne et Apple-id. Hvis det ikke er muligt at gøre brug af disse metoder, skal kontogendannelsesprocessen følges. Du kan få flere oplysninger i Apple-supportartiklen Sådan bruger du kontogendannelse, når du ikke kan nulstille adgangskoden til dit Apple-id.

Sikkerhed i Administreret Apple-id

Administrerede Apple-id'er fungerer på næsten samme måde som Apple-id'er, men de ejes og administreres af virksomheder eller uddannelsesinstitutioner. Institutionen kan nulstille adgangskoder, begrænse køb og kommunikation som FaceTime og Beskeder og indstille tilladelser baseret på roller for administrative medarbejdere, lærere og studerende.

For administrerede Apple-id'er er nogle tjenester slået fra (f.eks. Apple Pay, iCloud-nøglering, HomeKit og Find).

Inspektion af administrerede Apple-id'er

Administrerede Apple-id'er understøtter desuden *inspektion*, så institutioner kan overholde lovkrav og regulering vedrørende privatlivsbeskyttelse. En Apple School Manager-administrator, -manager eller -lærer kan inspicere visse administrerede Apple-id-konti.

Inspektører kan kun overvåge konti, der rangerer lavere end deres egen i skolens hierarki. Det vil sige, at lærere kan overvåge studerende, managers kan inspicere lærere og studerende, mens administratorer kan inspicere managers, lærere og studerende.

Når der anmodes om tilladelse til inspektion af godkendelsesoplysninger ved brug af Apple School Manager, oprettes en særlig konto, som kun har adgang til det administrerede Apple-id, der blev anmodet om inspektion af. Inspektøren kan herefter læse og ændre brugerens indhold, som er gemt i iCloud eller i apps, der kan arbejde med CloudKit. Alle anmodninger om revisionsadgang logges i Apple School Manager. Logarkiverne viser inspektørens identitet, det administrerede Apple-id, som inspektøren har anmodet om adgang til, tidspunktet for anmodningen og en oplysning om, hvorvidt inspektionen blev foretaget.

Administrerede Apple-id'er og personlige enheder

Administrerede Apple-id'er kan også bruges til personligt ejede iOS- og iPadOS-enheder og Mac-computere. Studerende kan logge ind på iCloud med det administrerede Apple-id, som institutionen har udstedt, og en ekstra adgangskode til hjemmebrug, der fungerer som den anden faktor i tofaktorgodkendelsen af det administrerede Apple-id. iCloud-nøglering er ikke tilgængelig, når elever bruger et administreret Apple-id på en personlig enhed, og institutionen har mulighed for at begrænse andre funktioner som FaceTime og Beskeder. Der kan foretages revision som beskrevet tidligere i dette afsnit af iCloud-dokumenter, som oprettes af studerende, mens de er logget ind.

iCloud

Oversigt over iCloud-sikkerhed

iCloud opbevarer en brugers kontakter, kalendere, fotos, dokumenter m.m. og holder automatisk oplysningerne ajour på alle brugerens enheder. iCloud kan også bruges af apps fra tredjeparter til opbevaring og synkronisering af dokumenter samt nøgleværdier til app-data, som udvikleren har defineret. Brugere indstiller iCloud ved at logge ind med et Apple-id og vælge, hvilke tjenester de vil bruge. Nogle iCloud-funktioner, f.eks. iCloud Drive og iCloud-sikkerhedskopiering kan slås fra af it-administratorer vha. MDM-konfigurationsprofiler.

iCloud bruger stærke sikkerhedsmetoder og strenge politikker til at beskytte brugerdata. De fleste iCloud-data krypteres først på brugerens enhed vha. enhedsgenererede iCloud-nøgler, før de overføres til iCloud-servere. For data der ikke er end-to-end-krypteret, overfører brugerens enhed på sikker vis disse iCloud-nøgler til iCloud-hardwaresikkerhedsmoduler i Apples datacentre. Dette gør det muligt for Apple at hjælpe brugeren med datagendannelse og dekryptering af data på vegne af brugeren, når vedkommende har brug for det (f.eks. når der logges ind på en ny enhed, gendannes fra sikkerhedskopi, eller brugeren vil have adgang til sine iCloud-data på internettet). Data, der flyttes mellem brugerens enheder og iCloud-servere, krypteres hver for sig med TLS under overførsel, og iCloud-servere opbevarer brugerdata med et yderligere lag af kryptering.

Krypteringsnøgler beskyttes i Apples datacentre, når de er tilgængelige for Apple. Ved behandling af data, der opbevares i et datacenter ejet af en tredjepart, har kun Apple-software, der afvikles på sikre servere, adgang til disse krypteringsnøgler og kun, mens den nødvendige behandling foretages. Mange Apple-tjenester bruger end-to-end-kryptering for at opnå yderligere anonymitet og sikkerhed. Det betyder, at kun brugerne har adgang til deres iCloud-data og kun på godkendte enheder, hvor de er logget ind med deres Apple-id.

Apple tilbyder brugere to muligheder for at kryptere og beskytte data, de opbevarer i iCloud:

- **Standard databeskyttelse (standardindstilling):** Brugerens iCloud-data krypteres, krypteringsnøglerne beskyttes i Apples datacentre, og Apple kan hjælpe med data- og kontogendannelse. Det er kun visse iCloud-data – 14 datakategorier, herunder Sundhedsdata og adgangskoder i iCloud-nøglering – der er end-to-end-krypteret.
- **Avanceret databeskyttelse til iCloud:** En valgfri indstilling, der tilbyder Apples højeste sikkerhedsniveau til data i netskyen. Hvis en bruger vælger, at slå Avanceret databeskyttelse til, er det kun brugerens godkendte enheder, der har adgang til krypteringsnøglerne til størstedelen af brugerens iCloud-data, hvilket betyder, at dataene beskyttes vha. end-to-end-kryptering. Når Avanceret databeskyttelse slås til, øges antallet af datakategorier, der bruger end-to-end-kryptering, til 23, og de inkluderer din iCloud-sikkerhedskopi, Fotos, Noter m.m.

De specifikke kategorier af iCloud-data, der beskyttes med end-to-end-kryptering, vises i Apple-supportartiklen Oversigt over sikkerheden for iCloud-data.

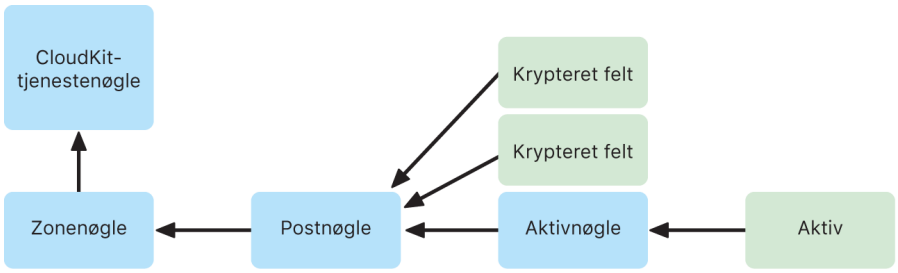
iCloud-kryptering

Kryptering af data i iCloud er tæt knyttet til datalagringsmodellen, startende med CloudKit-frameworks og API'er, der gør det muligt for apps og systemsoftware at opbevare data i iCloud på vegne af brugeren og holde alt ajour på tværs af enheder og på internettet.

CloudKit-kryptering

CloudKit er et framework, der gør det muligt for app-udviklere at opbevare nøgle-værdidata, strukturerede data og aktiver (store mængder data, der opbevares adskilt fra databasen, f.eks. billeder eller videoer) i iCloud. CloudKit understøtter både offentlige og private databaser grupperet i beholdere. Offentlige databaser deles globalt, bruges typisk til generelle aktiver og er ikke krypterede. Hver brugers iCloud-data gemmes i private databaser.

CloudKit bruger et hierarki med nøgler, der matcher datastrukturen. Hver beholders private database er beskyttet af et nøglehieraki, der er forankret i en asymmetrisk nøgle, som kaldes en *CloudKit-tjenestenøgle*. Disse nøgler er unikke for hver iCloud-bruger og genereres på deres godkendte enhed. Når data skrives til CloudKit, bliver alle postnøgler genereret på brugerens godkendte enhed og pakket til det relevante nøglehieraki, før der overføres nogen data.



Mange Apple-tjenester, som er anført i Apple-supportartiklen Oversigt over sikkerheden for iCloud-data, bruger end-to-end-kryptering med en CloudKit-tjenestenøgle, der beskyttes af synkroniseringen af iCloud-nøglering. Tjenestenøglerne til disse CloudKit-beholdere opbevares i brugerens iCloud-nøglering og deler iCloud-nøgleringens sikkerhedsegenskaber. Tjenestenøglerne er kun tilgængelige på brugerens godkendte enheder. Hverken Apple eller nogen tredjepart har adgang til dem. Hvis enheden mistes, kan brugere gendanne deres data i iCloud-nøglering ved at bruge Sikker gendannelse af iCloud-nøglering, Kontakter til kontogendannelse eller en nøgle til kontogendannelse.

Administration af krypteringsnøgler

Sikkerheden af krypterede data i CloudKit afhænger af sikkerheden af de tilsvarende krypteringsnøgler. CloudKit-tjenestenøgler er opdelt i to kategorier: end-to-end-krypterede og tilgængelige efter godkendelse.

- **Tjenestenøgler med end-to-end-kryptering:** For iCloud-tjenester med end-to-end-kryptering bliver de private nøgler til den relevante CloudKit-tjeneste aldrig tilgængelige for Apples servere. Tjenestenøglepar, herunder de private nøgler, oprettes lokalt på en brugers godkendte enhed og overføres til brugerens anden enhed vha. Sikkerhed i iCloud-nøglering. Selvom forløbene til gendannelse og synkronisering i iCloud-nøglering styres af Apples servere, er disse servere kryptografisk forhindret i at få adgang til brugerens data i nøgleringen. Hvis det værst tænkelige skulle ske, og brugeren mister adgangen til iCloud-nøglering og alle mekanismer til gendannelse, mister brugeren også de end-to-end-krypterede data i CloudKit. Apple kan ikke gendanne disse data.
- **Tjenestenøgler tilgængelige efter godkendelse:** For andre tjenester, f.eks. Fotos og iCloud Drive, opbevares tjenestenøglerne i iCloud-hardwaresikkerhedsmoduler i Apples datacentre, og det er muligt at få adgang til dem vha. visse Apple-tjenester. Når en bruger logger ind på iCloud på en ny enhed og bekræfter sit Apple-id, kan Apples servere få adgang til disse nøgler uden yderligere brugerinteraktion eller -input. Brugeren kan f.eks. se sine fotos online med det samme, når der logges ind på iCloud.com. Disse tjenestenøgler er nøgler, der er *tilgængelige efter godkendelse*.

Avanceret databeskyttelse til iCloud

Avanceret databeskyttelse til iCloud er en valgfri indstilling, der tilbyder Apples højeste sikkerhedsniveau til data i netskyen. Når en bruger slår Avanceret databeskyttelse til, er det kun brugerens godkendte enheder, der har adgang til krypteringsnøglerne til størstedelen af brugerens iCloud-data, hvilket betyder, at dataene beskyttes vha. *end-to-end-kryptering*. Hvis brugere slår Avanceret databeskyttelse til, øges det samlede antal af datakategorier, der beskyttes vha. end-to-end-kryptering, fra 14 til 23, og de inkluderer iCloud-sikkerhedskopiering, Fotos, Noter m.m.

Avanceret databeskyttelse til iCloud vil være tilgængelig i USA ved udgangen af 2022 og bliver tilgængelig i resten af verden i starten af 2023.

Princippet bag avanceret databeskyttelse er enkelt: Alle CloudKit-tjenestenøgler, der blev genereret på enheden og senere overført til iCloud-hardwaresikkerhedsmoduler (HSM) (der er *tilgængelige efter godkendelse*) i Apples datacentre, bliver slettet fra hardwaresikkerhedsmodulerne og bliver i stedet opbevaret i kontoens beskyttelsesdomæne til iCloud-nøglering. De håndteres som de eksisterende tjenestenøgler med *end-to-end-kryptering*, hvilket betyder, at Apple ikke længere kan læse eller få adgang til disse nøgler.

Avanceret databeskyttelse beskytter også automatisk CloudKit-felter, som tredjepartsudviklere valgte at markere som krypterede, og alle CloudKit-aktiver.

Aktivering af Avanceret databeskyttelse

Når brugeren slår Avanceret databeskyttelse til, udfører brugerens godkendte enhed to handlinger: Den kommunikerer først brugerens intention om at slå Avanceret databeskyttelse til til brugerens andre enheder, der bruger end-to-end-kryptering. Det gør den ved at skrive en ny værdi, der er signeret af lokale nøgler på enheden, i enhedens metadata til iCloud-nøglering. Apples servere kan ikke fjerne eller ændre denne attestering, mens den synkroniseres med brugerens andre enheder.

Dernæst igangsætter enheden fjernelsen af tjenestenøglerne, der er *tilgængelige efter godkendelse*, fra Apples datacentre. Eftersom disse nøgler er beskyttet af iCloud-hardwaresikkerhedsmoduler, bliver de slettet med det samme og permanent, og handlingen kan ikke fortrydes. Når nøglerne er slettet, kan Apple ikke længere få adgang til *nogen* data, der er beskyttet af brugerens tjenestenøgler. På dette tidspunkt starter enheden en asynkron nøglerotationshandling, som opretter en ny tjenestenøgle til hver tjeneste, hvis nøgle tidligere var tilgængelig for Apples servere. Hvis nøglerotationen mislykkes pga. netværksafbrydelser eller andre fejl, forsøger enheden at udføre nøglerotationen igen, indtil den gennemføres.

Når tjenestenøglerotationen lykkes, kan nye data, der skrives til tjenesten, ikke dekrypteres med den gamle tjenestenøgle. De beskyttes med den nye nøgle, der udelukkende styres af brugerens godkendte enheder, og som aldrig var tilgængelig for Apple.

Avanceret databeskyttelse og internetadgang på iCloud.com

Når en bruger slår Avanceret databeskyttelse til første gang, bliver internetadgang til brugerens data på iCloud.com automatisk slået fra. Det sker, fordi iCloud-webservere ikke længere har adgang til nøglerne, der kræves til at dekryptere og vise brugerens data. Brugeren kan vælge at slå internetadgang til igen og bruge deltagelsen af sin godkendte enhed til at få adgang til sine krypterede iCloud-data på internettet.

Når internetadgang er blevet slået til, skal brugeren godkende login på internettet på en af sine godkendte enheder, hver gang brugeren går ind på iCloud.com. Godkendelsen klargør enheden til internetadgang. I en time accepterer enheden anmodninger fra specifikke Apple-servere til at overføre individuelle tjenestenøgler, men kun dem der svarer til en tilladt liste med tjenester, der normalt er tilgængelige på iCloud.com. Så selvom brugeren godkender login på internettet, kan en serveranmodning ikke få brugerens enhed til at overføre tjenestenøgler til data, der ikke bør kunne ses på iCloud.com (f.eks. Sundhedsdata eller adgangskoder i iCloud-nøglering). Apples servere anmoder kun om de tjenestenøgler, der er nødvendige for at dekryptere de specifikke data, som brugeren anmoder om at få adgang til på internettet. Hver gang en tjenestenøgle overføres, er den krypteret vha. en midlertidig nøgle, der er knyttet til websessionen, som brugeren godkendte, og der vises en notifikation på brugerens enhed om den iCloud-tjeneste, hvis data midlertidigt bliver tilgængelige for Apples servere.

Bevarelse af brugerens valg

Indstillingerne til Avanceret databeskyttelse og internetadgang på iCloud.com kan kun ændres af brugeren. Disse værdier opbevares i brugerens enhedsmetadata til iCloud-nøglering og kan kun ændres på en af brugerens godkendte enheder. Apples servere kan ikke ændre disse indstillinger på vegne af brugeren og kan heller ikke tilbageføre dem til en tidligere konfiguration.

Betydning for sikkerheden ved deling og samarbejde

Når brugere deler indhold for at samarbejde – f.eks. delte noter, delte påmindelser, delte mapper i iCloud Drive eller Delt iCloud-fotobibliotek – og alle brugere har slået Avanceret databeskyttelse til, bruges Apples servere i de fleste tilfælde kun til at etablere deling, men de har ikke adgang til krypteringsnøglerne til de delte data. Indholdet er stadig end-to-end-krypteret og er kun tilgængeligt på deltagernes godkendte enheder. Apple gemmer muligvis en titel og repræsentativ miniature med standard databeskyttelse for hver handling til deling for at vise et eksempel til modtagerne.

Hvis indstillingen "alle med linket" vælges, når samarbejde slås til, bliver indholdet tilgængeligt for Apples servere med standard databeskyttelse, fordi serverne skal kunne give adgang til alle, der åbner URL-adressen.

iWork-samarbejde og funktionen Delte album i Fotos understøtter ikke Avanceret databeskyttelse, Når brugere samarbejder i et iWork-dokument eller åbner et iWork-dokument fra en delt mappe i iCloud Drive, bliver krypteringsnøglerne til dokumentet på sikker vis overført til iWork-servere i Apples datacentre. Det sker, fordi samarbejde i realtid i iWork kræver formidling på serversiden for at koordinere dokumentændringer mellem deltagere. Fotos, der føjes til Delte album, gemmes med standard databeskyttelse, fordi funktionen tillader, at album kan deles offentligt på internettet.

Deaktivering af Avanceret databeskyttelse

Brugeren kan altid slå Avanceret databeskyttelse fra. Hvis brugeren vælger at gøre dette:

1. Brugerens enhed registrerer først det nye valg i metadata for deltagelse til iCloud-nøglering, og denne indstilling synkroniseres på sikker vis på alle brugerens enheder.

2. Brugerens enhed overfører på sikker vis tjenestenøglerne til alle tjenester, der er *tilgængelige efter godkendelse*, til iCloud-hardwaresikkerhedsmodulerne i Apples datacentre. Dette inkluderer aldrig nøgler til tjenester, der er end-to-end-krypterede under standard databeskyttelse, f.eks. iCloud-nøglering og Sundhed.

Enheden overfører både de originale tjenestenøgler, der blev genereret, før Avanceret databeskyttelse blev slået til, og de nye tjenestenøgler, der blev genereret, efter brugeren slog funktionen til. Dette gør alle data i disse tjenester tilgængelige efter godkendelse og tilbagefører kontoen til standard databeskyttelse, hvor det igen er muligt for Apple at hjælpe brugeren med at gendanne de fleste data, hvis brugeren mister adgangen til sin konto.

iCloud-data, der ikke er inkluderet i Avanceret databeskyttelse

iCloud-mail, Kontakter og Kalender er ikke end-to-end-krypterede, fordi de skal kunne samarbejde med de globale systemer til e-mail, kontakter og kalendere.

iCloud opbevarer nogle data uden beskyttelse fra brugerspecifikke CloudKit-tjenestenøgler, også selvom Avanceret brugerbeskyttelse er slået til. CloudKit-postfelter skal udtrykkeligt deklareres som "krypteret" i beholderens skema for at være beskyttet, og mulighed for at læse og skrive krypterede felter kræver brug af dedikerede API'er. Datoer og tidspunkter, hvor et arkiv eller et objekt blev ændret, bruges til at sortere en brugers oplysninger, og kontrolsummer af arkiv- og fotodata bruges til at hjælpe Apple med deduplikering og optimering af brugerens lagringsplads på iCloud og enheden – alt sammen uden at have adgang til selve arkiverne og fotoene. Oplysninger om, hvordan kryptering brugers til specifikke datakategorier, kan findes i Apple-supportartiklen Oversigt over sikkerheden for iCloud-data.

Beslutninger, f.eks. brug af kontrolsummer til deduplikering af data – en anerkendt metode kaldet *konvergent kryptering* – var en del af det originale design i iCloud-tjenester, da de blev lanceret. Disse metadata er altid krypterede, men krypteringsnøglerne opbevares af Apple med standard databeskyttelse. For at fortsætte med at forbedre sikkerhedsbeskyttelsen for alle brugere lægger Apple vægt på at sikre, at flere data, herunder denne type metadata, bliver end-to-end-krypteret, når Avanceret databeskyttelse er slået til.

Krav til Avanceret databeskyttelse

Kravene til at slå Avanceret databeskyttelse til iCloud til inkluderer følgende:

- Brugerens konto skal understøtte end-to-end-kryptering. End-to-end-kryptering kræver tofaktorgodkendelse til brugerens Apple-id og en kode eller adgangskode, der er indstillet på brugerens godkendte enheder. Du kan få flere oplysninger i Apple-supportartiklen Tofaktorgodkendelse til Apple-id.
- Enheder, hvor brugeren er logget ind med sit Apple-id, skal være opdateret til iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 og have den nyeste version af iCloud til Windows. Dette krav forhindrer, at en tidligere version af iOS, iPadOS, macOS, tvOS eller watchOS håndterer de nyligt oprettede tjenestenøgler forkert ved at overføre dem igen til hardwaresikkerhedsmoduler, der er *tilgængelige efter godkendelse*, i et forsøg på at reparere kontoens status.
- Brugeren skal indstille mindst en alternativ gendannelsesmetode – en eller flere gendannelseskontakter eller en gendannelsesnøgle – som kan bruges til at gendanne iCloud-data, hvis brugeren mister adgangen til sin konto.

Hvis gendannelsesmetoden mislykkes, f.eks. hvis gendannelseskontaktens oplysninger er forældede eller brugeren glemmer dem, kan Apple ikke hjælpe med at gendanne brugerens end-to-end-krypterede iCloud-data.

Avanceret databeskyttelse til iCloud kan slås til for kun Apple-id'er. Administrerede Apple-id'er og børnekonti (afhænger af land og område) understøttes ikke.

Sikkerheden i iCloud-sikkerhedskopiering

iCloud sikkerhedskopierer oplysninger – herunder enhedsindstillinger, appdata, fotos og videoer i Kamerarulle og samtaler i appen Beskeder – dagligt via Wi-Fi. Der foretages kun iCloud-sikkerhedskopiering, når enheden er låst, er sluttet til en strømkilde og har Wi-Fi-adgang til internettet. Takket være den kryptering, der bruges i iOS og iPadOS, er iCloud-sikkerhedskopiering designet, så den beskytter data og samtidig tillader trinvis, uovervåget sikkerhedskopiering og gendannelse. Tjenestenøglen til iCloud-sikkerhedskopiering er som standard sikkerhedskopieret på sikker vis til iCloud-hardwaresikkerhedsmoduler i Apple-datacentre og er en del af datakategorien "tilgængelig efter godkendelse". Hvis brugere slår Avanceret databeskyttelse til iCloud til, er tjenestenøglen til iCloud-sikkerhedskopiering beskyttet med end-to-end-kryptering og kun tilgængelig for brugere på deres godkendte enheder.

Når der oprettes arkiver i klasser i Databeskyttelse, der ikke er adgang til, når enheden er låst, krypteres deres arkivnøgler med klassenøglerne fra nøglesamlingen iCloud-sikkerhedskopiering og sikkerhedskopieres til iCloud i deres oprindelige, krypterede form. Alle arkiver krypteres under transport, og ved opbevaring krypteres de med kontobaserede nøgler som beskrevet i CloudKit-kryptering.

Nøglesamlingen iCloud-sikkerhedskopiering indeholder asymmetriske (Curve25519) nøgler til databeskyttelsesklasser, der ikke er tilgængelige, når enheden låses. Sikkerhedskopisættet gemmes i brugerens iCloud-konto og består af en kopi af brugerens arkiver og nøglesamlingen iCloud-sikkerhedskopiering. Nøglesamlingen iCloud-sikkerhedskopiering beskyttes med en tilfældig nøgle, som også gemmes sammen med sikkerhedskopisættet. Brugerens iCloud-adgangskode benyttes ikke til kryptering, så eksisterende sikkerhedskopier bliver ikke ugyldige, selvom iCloud-adgangskoden ændres.

Under en gendannelse hentes de sikkerhedskopierede arkiver, nøglesamlingen iCloud-sikkerhedskopiering og nøglen til nøglesamlingen fra brugerens iCloud-konto. Nøglesamlingen iCloud-sikkerhedskopiering dekrypteres med dens nøgle, og arkivnøglerne i nøglesamlingen bruges til at dekryptere arkiverne i sikkerhedskopisættet, før de skrives som nye arkiver i arkivsystemet, hvorved de krypteres igen i henhold til deres databeskyttelsesklasse.

Følgende indhold sikkerhedskopieres ved brug af iCloud-sikkerhedskopiering:

- Poster til købte film, tv-udsendelser, apps og bøger og købt musik. En brugers iCloud-sikkerhedskopi indeholder oplysninger om købt indhold, som findes på brugerens enhed, men ikke selve det købte indhold. Når brugeren gendanner data fra en iCloud-sikkerhedskopi, hentes brugerens købte indhold automatisk fra iTunes Store, App Store, Apple TV eller Apple Books. Nogle typer indhold hentes ikke automatisk i alle lande og områder, og tidligere køb er muligvis ikke tilgængelige, hvis beløbet, der er betalt for dem, er blevet refunderet, eller hvis de pågældende emner ikke længere er tilgængelige i den pågældende butik. En komplet købshistorik er knyttet til en brugers Apple-id.
- Fotos og videoer på en brugers enheder. Bemærk, at hvis en bruger slår iCloud-fotos til i iOS 8.1, iPadOS 13.1 eller OS X 10.10.3 eller en nyere version, medtages brugerens fotos og videoer ikke i iCloud-sikkerhedskopien, fordi emnerne allerede opbevares i iCloud.
- Kontakter, kalenderbegivenheder, påmindelser og noter
- Enhedsindstillinger
- App-data

- Organisering af hjemmeskærm og apps
- HomeKit-konfiguration
- Data om Nødinfo
- Adgangskode til Memoer (kræver om nødvendigt det fysiske SIM-kort, der var i brug under sikkerhedskopieringen)
- Beskeder, Apple Messages for Business, sms'er og mms'er (kræver om nødvendigt det fysiske SIM-kort, der var i brug under sikkerhedskopieringen)

iCloud-sikkerhedskopiering bruges også til at sikkerhedskopiere den lokale enheds nøglering, der krypteres med en nøgle, som afledes af enhedens kryptografiske rodnøgle i Secure Enclave UID. Denne nøgle er unik for enheden og kendes ikke af Apple. Det betyder, at databasen kun kan gendannes på den enhed, den stammer fra, og at ingen andre, heller ikke Apple, kan læse den. Du kan få flere oplysninger i Secure Enclave.

Beskeder i iCloud

Beskeder i iCloud holder hele brugerens beskedhistorik ajour og tilgængelig på alle enheder.

Beskeder i iCloud er end-to-end-krypteret vha. standard databeskyttelse, når iCloud-sikkerhedskopiering er slået fra. Når iCloud-sikkerhedskopiering er slået til, inkluderer sikkerhedskopien en kopi af krypteringsnøglen til Beskeder i iCloud, så Apple kan hjælpe brugeren med at gendanne sine beskeder, også selvom brugeren har mistet adgangen til iCloud-nøglering og sine godkendte enheder. Hvis brugeren slår iCloud-sikkerhedskopiering fra, genereres en ny nøgle på enheden for at beskytte fremtidige beskeder i iCloud. Den nye nøgle lagres kun i iCloud-nøglering, er kun tilgængelig for brugeren på godkendte enheder, og nye data, der skrives til beholderen, kan ikke dekrypteres med den gamle beholdernøgle.

Beskeder i iCloud er altid end-to-end-krypteret vha. Avanceret databeskyttelse. Når iCloud-sikkerhedskopiering er slået til er alt i kopien end-to-end-krypteret, inklusive krypteringsnøglen til Beskeder i iCloud. Både tjenestenøglen til iCloud-sikkerhedskopiering og beholdernøglen til Beskeder i iCloud udskiftes, når brugeren slår Avanceret databeskyttelse til. Du kan få flere oplysninger i Apple-supportartiklen Oversigt over sikkerheden for iCloud-data.

Sikkerhed i forbindelse med kontakter til kontogendannelse

Brugere kan tilføje op til fem personer, de stoler på, som kontakt til kontogendannelse og få hjælp fra dem til at gendanne deres iCloud-konto og data, herunder alle end-to-end-krypterede data, uanset om brugeren har slået Avanceret databeskyttelse til. Hverken Apple eller gendannelseskontakten har de oplysninger, der kræves for at gendanne brugerens end-to-end-krypterede data i iCloud.

Gendannelseskontakt er designet med brugerens anonymitet for øje. En brugers valgte gendannelseskontakter kendes ikke af Apple. Apples servere kan kun få oplysninger om en gendannelseskontakt sent i forløbet med et forsøg på gendannelse, når brugeren beder kontakten om hjælp, og kontakten begynder at hjælpe med gendannelsen. Oplysningerne opbevares ikke, efter gendannelsen er gennemført.

Sikkerhedsproces i forbindelse med gendannelseskontakter

Når en bruger indstiller en kontakt til kontogendannelse, bliver nøglen, der giver adgang til brugerens iCloud-data (herunder end-to-end-krypterede CloudKit-data), krypteret med en tilfældig nøgle. Den tilfældige nøgle deles derefter mellem gendannelseskontakten og Apple. På gendannelsestidspunktet er det først muligt at få adgang til brugerens iCloud-data, når de to dele af nøglen kombineres igen, og den originale nøgle gendannes.

Når en kontakt til kontogendannelse skal indstilles, kommunikerer brugerens enhed med Apples servere for at overføre den del af nøgleoplysningerne, som Apple opbevarer. Derefter etableres en CloudKit-beholder med end-to-end-kryptering sammen med gendannelseskontakten, så den del, gendannelseskontakten har brug for, kan deles. Både Apple og gendannelseskontakten modtager den samme hemmelige godkendelsesoplysning fra brugeren, som senere skal bruges til gendannelse. Kommunikation om at invitere og acceptere gendannelseskontakter sker gennem en gensidigt godkendt IDS-kanal. Gendannelseskontakten opbevarer automatisk de modtagne oplysninger i sin iCloud-nøglering. Apple kan ikke få adgang til indholdet i CloudKit-beholderen eller iCloud-nøgleringen, der opbevarer disse oplysninger. Når delingen sker, ser Apples servere kun et anonymt id til gendannelseskontakten.

Hvis en bruger senere har behov for at gendanne sin konto og sine iCloud-data, kan brugeren anmode sin gendannelseskontakt om hjælp. På det tidspunkt genererer gendannelseskontaktens enhed en kode, som gendannelseskontakten oplyser til brugeren med en analog metode (f.eks. personligt eller i et telefonopkald). Brugeren indtaster koden på sin enhed for at etablere en sikker forbindelse mellem enheder ved brug af SPAKE2+-protokollen, hvis indhold Apple ikke har adgang til. Interaktionen gennemføres ved hjælp af Apple-servere, men Apple kan ikke igangsætte gendannelsesprocessen.

Når den sikre forbindelse er etableret, og alle de nødvendige sikkerhedskontroller er gennemført, sender gendannelseskontaktens enhed sin del af nøgleoplysningerne og den hemmelige godkendelsesoplysning tilbage til brugeren, der anmoder om gendannelse. Brugeren angiver denne hemmelige godkendelsesoplysning til en Apple-server, hvilket giver adgang til nøgleoplysningerne, som Apple opbevarer. Når den hemmelige godkendelsesoplysning angives, er det også en godkendelse af, at nulstilling af adgangskoden til kontoen kan bruges til at retablere adgangen til kontoen.

Til sidst kombinerer brugerens enhed nøgleoplysningerne fra Apple og kontakten til kontogendannelse og bruger dem til at dekryptere og gendanne brugerens iCloud-data.

Der findes sikkerhedsforanstaltninger, som skal forhindre en gendannelseskontakt i at starte gendannelse uden brugerens samtykke, hvilket inkluderer en aktivitetskontrol af brugerens konto. Hvis kontoen er i brug, kræver gendannelse med en gendannelseskontakt også oplysninger om en nylig kode til enheden eller iCloud-sikkerhedskoden.

Sikkerhed i forbindelse med arvekontakter

Hvis brugere ønsker, at deres iCloud-data skal være tilgængelige for udpegede begunstigede efter brugernes død, kan de indstille arvekontakter til deres konto. En begunstiget arvekontakt får adgang til alle den afdødes iCloud-data, herunder næsten alle end-to-end-krypterede data, men ikke data i iCloud-nøglering, f.eks. adgangskoder til konti. Teknologien bag Arvekontakt fungerer på samme måde som i Gendannelseskontakt – en stærk tilfældig nøgle, der opdeles mellem Apple og arvekontakten, så ingen parter kan dekryptere dataene alene. En begunstiget modtager de samme typer data, uanset om brugeren har slået Avanceret databeskyttelse til.

Nøgleoplysningerne, en begunstiget modtager, kaldes en adgangsnøgle i dokumentationen til brugere og gemmes automatisk på understøttede enheder, men kan også udskrives og gemmes offline til senere brug. Du kan få flere oplysninger i Apple-supportartiklen Sådan føjer du en arvekontakt til dit Apple-id.

Efter brugerens død logger arvekontakten ind på Apples websted til anmodninger for at anmode om adgang. Dette kræver en dødsattest og godkendes til dels vha. den hemmelige godkendelsesoplysning nævnt i forrige afsnit. Når alle sikkerhedskontroller er gennemført, udsteder Apple et brugernavn og en adgangskode til den nye konto og frigiver de nødvendige nøgleoplysninger til arvekontakten.

Som hjælp til indsættelse af adgangsnøglen, når der er behov for det, vises den som en alfanumerisk kode med en tilhørende QR-kode. Når den er indsat, gendannes adgangen til den afdødes iCloud-data. Det kan foretages på en enhed eller på internettet. Du kan få flere oplysninger i Apple-supportartiklen Anmod om adgang til en Apple-konto som arvekontakt.

Sikkerhed i Privat datatrafik med iCloud

Privat datatrafik med iCloud er med til at beskytte brugerne, især når de surfer på internettet med Safari, men det bruges også til anmodninger om opløsning af DNS-navne. Det er med til at sikre, at ingen enkeltpart, heller ikke Apple, kan forbinde brugerens IP-adresse og browseraktiviteter. Det gøres ved, at der bruges forskellige proxyer: En indgangsproxy, der administreres af Apple, og en udgangsproxy, som administreres af en indholdsudbyder. Brugeren skal have iOS 15, iPadOS 15 eller macOS 12.0.1 eller en nyere version og skal være logget ind på sin iCloud+ konto med sit Apple-id for at bruge Privat datatrafik med iCloud. Privat datatrafik med iCloud slås til i Indstillinger > iCloud eller Systemindstillinger > iCloud.

Du kan få flere oplysninger i dette dokument: iCloud Private Relay Overview.

Administrationer af koder og adgangskoder

Oversigt over adgangskodesikkerhed

iOS, iPadOS og macOS gør det nemt for brugerne at godkende apps fra tredjeparter og websteder, der bruger adgangskoder. Den bedste måde at administrere adgangskoder på er at undgå at indtaste adgangskoder. Log ind med Apple gør det muligt for brugere at logge ind på tredjeparters apps og websteder uden at skulle oprette og administrere endnu en konto eller adgangskode og beskytter samtidig login-processen med brugernes tofaktorgodkendelse til Apple-id. Til websteder, der ikke understøtter Log ind med Apple, findes funktionen til automatiske stærke adgangskoder på brugerens enheder, så de automatisk kan oprette, synkronisere og indtaste unikke, stærke adgangskoder til websteder og apps. I iOS og iPadOS gemmes adgangskoder i den særlige nøglering Autoudfyld adgangskode, som styres af brugeren og kan administreres i Indstillinger > Adgangskoder.

I macOS kan gemte adgangskoder administreres i indstillingerne til Safari-adgangskoder. Dette system til synkronisering kan også benyttes til at synkronisere adgangskoder, der oprettes manuelt af brugeren.

Sikkerhed ved Log ind med Apple

Log ind med Apple er et anonymitetsvenligt alternativ til andre SSO-systemer. Teknologien gør det nemt og effektivt at logge ind med et klik, samtidig med at brugeren opnår større gennemsigtighed og kontrol med sine personlige oplysninger.

Med Log ind med Apple kan brugerne oprette en konto og logge ind på apps og websteder ved hjælp af det Apple-id, de allerede har, og det giver dem bedre kontrol over deres personlige oplysninger. Apps kan kun bede om brugerens navn og e-mailadresse, når der oprettes en konto, og brugeren har altid et valg: Brugeren kan dele sin private e-mailadresse med en app eller vælge at holde den hemmelig og i stedet benytte den nye private Apple-tjeneste til videresendelse af e-mails. Denne tjeneste til videresendelse af e-mails deler en unik, anonymiseret e-mailadresse, der videresender til brugerens personlige adresse, så vedkommende stadig kan modtage nyttige informationer fra udvikleren, men samtidig bibeholde en grad af anonymitet og kontrol med sine personlige oplysninger.

Log ind med Apple er udviklet med sikkerhed for øje. Alle brugere af Log ind med Apple skal benytte tofaktorgodkendelse for deres Apple-id. Tofaktorgodkendelse hjælper ikke blot med at sikre brugernes Apple-id, men også de konti, de opretter med deres apps. Apple har desuden udviklet et signal, der skal bekæmpe svindel og beskytte brugerens anonymitet, og indbygget signalet i Log ind med Apple. Signalet giver udviklerne tillid til, at deres nye brugere er rigtige mennesker og ikke robotter eller instruksbaserede konti.

Automatiske stærke adgangskoder

Når iCloud-nøglering er slået til, opretter iOS, iPadOS og macOS stærke, tilfældige og unikke adgangskoder, når brugere tilmelder sig eller ændrer adgangskoder i en app eller på et websted i Safari. I iOS og iPadOS er generering af automatiske stærke adgangskoder også tilgængelige i apps. Brugerne skal fravælge at bruge stærke adgangskoder. Genererede adgangskoder gemmes i nøgleringen og holdes opdateret på tværs af enheder med iCloud-nøglering, når den er slået til.

Adgangskoder, der genereres af iOS og iPadOS, er som standard på 20 tegn. De indeholder et tal, et stort bogstav, to bindestreger og 16 små bogstaver. Disse genererede adgangskoder er stærke, da de indeholder 71 bit entropi.

Adgangskoder er baseret på heuristik, der bestemmer, om en indtastning i et adgangskodefelt skal bruges til oprettelse af en adgangskode. Hvis heuristikken ikke genkender en kontekstafhængig adgangskode som passende til adgangskodeoprettelse, kan app-udviklere bruge `UITextContentType.newPassword` i deres tekstfelt, og webudviklere kan bruge `autocomplete= "new-password"` i deres <input>-elementer.

Apps og websteder kan oprette regler for at sikre, at de oprettede adgangskoder overholder de relevante tjenesters krav. Udviklere angiver disse regler ved at bruge `UITextInputPasswordRules` eller attributten `passwordrules` i deres inputelementer. Enhederne opretter derefter de stærkeste adgangskoder, de kan, som opfylder disse regler.

Sikkerheden ved Autoudfyld adgangskode

Funktionen Autoudfyld adgangskode udfylder automatisk godkendelsesoplysninger, der opbevares i nøgleringen. Adgangskodeadministratoren til iCloud-nøglering og Autoudfyld adgangskode indeholder følgende funktioner:

- Udfyldelse af godkendelsesoplysninger i apps og på websteder
- Generering af stærke adgangskoder
- Arkivering af adgangskoder i apps og på websteder i Safari
- Sikker deling af adgangskoder til en brugers kontakter
- Levering af adgangskoder til et Apple TV i nærheden, som anmoder om godkendelsesoplysninger

Det er kun muligt at oprette og gemme adgangskoder i apps samt oprette adgangskoder til Apple TV i iOS og iPadOS.

Autoudfyld adgangskode i apps

iOS og iPadOS gør det muligt for brugere at udfylde adgangskodefelter med gemte brugernavne og adgangskoder i apps svarende til den måde, som Autoudfyld adgangskode fungerer på i Safari. I iOS og iPadOS trykker brugerne på et nøgleforslag på softwaretastaturets QuickType-linje. I macOS-apps, der er udviklet i Mac Catalyst, fremkommer rullemenuen Adgangskoder under felterne til godkendelsesoplysninger.

Når en app er stærkt forbundet med et websted, der bruger samme app-website-tilknytningsmekanisme, og som er drevet af samme apple-app-site-association-arkiv, foreslår QuickType-linjen i iOS og iPadOS samt rullemenuen i macOS direkte godkendelsesoplysninger til appen, hvis de er gemt i nøgleringen til Autoudfyld adgangskode. Det giver brugerne mulighed for at vælge at vise godkendelsesoplysninger, der er gemt i Safari, til apps med samme sikkerhedsegenskaber, uden at disse apps skal anvende et API.

Autoudfyld adgangskode viser ingen godkendelsesoplysninger til appen, før en bruger giver sit samtykke til at frigive godkendelsesoplysninger. Listerne med godkendelsesoplysninger bliver dannet eller vist ud fra appens proces.

Når en app og et websted har en godkendt relation, og en bruger skriver godkendelsesoplysninger i en app, kan iOS og iPadOS foreslå brugeren at gemme godkendelsesoplysningerne i nøgleringen til Autoudfyld adgangskode til senere brug.

App-adgang til gemte adgangskoder

Apps i iOS, iPadOS og macOS kan anmode om hjælp fra nøgleringen til Autoudfyld adgangskode til at logge en bruger ind ved hjælp af `ASAuthorizationPasswordProvider` og `SecAddSharedWebCredential`. Adgangskodegeneratoren og dens anmodning kan bruges sammen med Log ind med Apple, så det samme API kaldes for at hjælpe brugerne med at logge ind i en app, uanset om brugerens konto er adgangskodebaseret eller er oprettet ved hjælp af Log ind med Apple.

Apps kan kun få adgang til gemte adgangskoder, hvis app-udvikleren og webstedsadministratoren har godkendt det, og brugeren har givet sit samtykke. Udviklere af apps viser deres intention om at få adgang til adgangskoder, som er gemt af Safari, ved at indsætte en berettigelse i deres app. Berettigelsen angiver de tilknyttede websteders fuldstændige domænenavn, og webstederne skal placere et arkiv på deres server, som indeholder en liste med de entydige app-id'er til de apps, der er blevet godkendt af Apple.

Når en app med berettigelsen com.apple.developer.associated-domains installeres, sender iOS og iPadOS en TLS-anmodning til hvert af webstederne på listen med en anmodning om et af følgende arkiver:

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

Hvis arkivet indeholder id'et på den app, der skal installeres, definerer iOS og iPadOS en godkendt relation mellem webstedet og appen. Der kræves en godkendt relation, før kald til disse to API'er medfører, at brugeren bliver bedt om at give sit samtykke, før adgangskoder frigives til appen, opdateres eller slettes.

Sikkerhedsanbefalinger for adgangskoder

Listen med adgangskoder til Autoudfyld adgangskode i iOS, iPadOS og macOS viser, hvilke af en brugers gemte adgangskoder der bliver *genbrugt* på andre websteder, hvilke adgangskoder der anses for at være *svage*, og adgangskoder, der er kompromitteret på grund af *lækkede data*.

Oversigt

Hvis man bruger samme adgangskode til flere tjenester, kan disse konti blive sårbare ved et såkaldt "credential stuffing"-angreb. Hvis en tjeneste bliver kompromitteret, og adgangskoder lækkes, kan hackere prøve de samme godkendelsesoplysninger på andre tjenester for at få adgang til flere konti.

- Adgangskoder markeres som *genbrugt*, hvis det registreres, at den samme adgangskode bruges til mere end en gemt adgangskode på tværs af forskellige domæner.
- Adgangskoder bliver markeret som *svage*, hvis de nemt kan gættes af en hacker. iOS, iPadOS og macOS registrerer fælles mønstre i oprettelsen af adgangskoder, der er nemme at huske, f.eks. ord i et opslagsværk, almindelige bogstaverstatninger (som f.eks. "p4ssw0rd" i stedet for "password"), mønstre på tastaturet (som f.eks. "q12we34r" på et QWERTY-tastatur) eller gentagne sekvenser (som f.eks. "123123"). Disse mønstre bruges ofte til at oprette adgangskoder, der opfylder minimumskravene på forskellige tjenester, men de bruges også ofte af personer med onde hensigter, der forsøger at få fat i en adgangskode gennem brute force.

  Eftersom mange tjenester specifikt kræver en PIN-kode på fire eller seks cifre, bliver disse korte koder vurderet efter andre regler. PIN-koder anses for at være svage, hvis de er blandt de oftest anvendte, hvis de er en stigende eller faldende sekvens såsom "1234" eller "8765", eller hvis de følger et gentagelsesmønster som f.eks. "123123" eller "123321".
- Adgangskoder markeres som *lækkede*, hvis funktionen til overvågning af adgangskoder kan hævde, at de indgik i en datalækage. Du kan få flere oplysninger i Overvågning af adgangskoder.

Svage, genbrugte og lækkede adgangskoder vises enten på listen med adgangskoder (macOS) eller på den særlige brugerflade til sikkerhedsanbefalinger (iOS og iPadOS). Hvis brugeren logger ind på et websted i Safari vha. en tidligere gemt adgangskode, der er meget svag, eller som er blevet kompromitteret på grund af datalækage, vises der en advarsel, som kraftigt opfordrer brugeren til at opgradere til en automatisk stærk adgangskode.

Opgradering af sikkerhed ved kontogodkendelse i iOS og iPadOS

Apps, der implementerer en udvidelse til ændring af kontogodkendelse (i Authentication Services-framework), kan tilbyde nemme opgraderinger for adgangskodebaserede konti, så brugerne kan skifte til at bruge Log ind med Apple eller en automatisk stærk adgangskode ved at trykke på en knap. Udvidelsespunktet findes i iOS og iPadOS.

Hvis en app har implementeret udvidelsespunktet og er installeret på enheden, får brugeren vist muligheder for at opgradere gennem udvidelsen. De vises, når brugeren ser på sikkerhedsanbefalingerne for de godkendelsesoplysninger, der er knyttet til appen i adgangskodeadministratoren til iCloud-nøglering under Indstillinger. Opgraderingerne tilbydes også, når brugerne logger på appen med de godkendelsesoplysninger, der er udsat for risiko. Apps er i stand til at fortælle systemet, at det ikke skal vise brugerne muligheder for opgradering, når de har logget ind. Vha. det nye API AuthenticationServices kan apps også starte deres udvidelser og udføre opgraderinger selv. Det er bedst, hvis det sker via skærmen til kontoindstillinger eller kontoadministration i selve appen.

Apps kan vælge at understøtte opgradering til stærke adgangskoder, opgradering til Log ind med Apple eller begge dele. Ved opgradering til stærke adgangskoder genererer systemet en automatisk stærk adgangskode til brugeren. Hvis det er nødvendigt, kan appen opstille særlige regler for adgangskoder, som skal følges ved generering af den nye adgangskode. Når en bruger vælger, at en konto skal skifte fra brug af adgangskode til brug af Log ind med Apple, leverer systemet nye godkendelsesoplysninger til Log ind med Apple, som udvidelsen knytter til denne konto. E-mailadressen til brugerens Apple-id indgår ikke i godkendelsesoplysningerne. Når opgraderingen til Log ind med Apple er gennemført, sletter systemet godkendelsesoplysningerne for den tidligere adgangskode fra brugerens nøglering, hvis de er gemt i den.

Udvidelser til ændring af kontogodkendelse kan også udføre yderligere brugergodkendelse, inden der udføres en opgradering. Når en opgradering starter i adgangskodeadministratoren eller efter, at brugeren har logget på en app, angiver udvidelsen brugernavnet og adgangskoden til den konto, der skal opgraderes. Når opgraderingen sker direkte i appen, oplyses kun brugernavnet. Hvis udvidelsen kræver yderligere brugergodkendelse, kan den anmode om at vise en speciel brugerflade, inden opgraderingen fortsætter. Formålet med at vise denne brugerflade er, at brugeren her skal anføre en ekstra godkendelsesfaktor for at godkende opgraderingen.

Overvågning af adgangskoder

Overvågning af adgangskoder er en funktion, der sammenligner adgangskoder gemt i brugerens nøglering til Autoudfyld adgangskode med en liste over adgangskoder, som har vist sig at være synlige ved datalækage fra forskellige organisationer på internettet. Denne liste opdateres og kurateres løbende. Hvis funktionen er slået til, vil overvågningsprotokollen løbende sammenligne brugerens adgangskoder i nøgleringen til Autoudfyld adgangskode med den kurateredе liste.

Sådan fungerer overvågning

Brugerens enhed udfører løbende "round robin"-kontrol af en brugers adgangskoder og sender forespørgsler i et interval, der er uafhængigt af brugerens adgangskoder og mønster for brug af adgangskodeadministration. Det er med til at sikre, at godkendelsestilstandene holdes ajour med den aktuelle kurateredе liste over lækkede adgangskoder. Forespørgsler samles i batches og udføres parallelt for at bidrage til at forhindre, at der lækkes oplysninger om, hvor mange unikke adgangskoder en bruger har. Et fast antal adgangskoder kontrolleres parallelt ved hver kontrol, og hvis brugeren har færre end dette antal, genereres der tilfældige adgangskoder, som føjes til forespørgslerne for at udligne forskellen.

Sammenligning af adgangskoder

Sammenligningen af adgangskoder udføres i en totrinsproces. De adgangskoder, der hyppigst er lækket, er opført på en lokal liste på brugerens enhed. Hvis brugerens adgangskode står på denne liste, får brugeren straks besked uden nogen ekstern interaktion. Det har til formål at sikre, at der ikke lækkes nogen oplysninger om de adgangskoder, brugeren har, og som er mest udsat for risiko pga. et brud på sikkerheden omkring adgangskoder.

Hvis adgangskoden ikke er opført på listen med hyppigst lækkede adgangskoder, sammenlignes den med adgangskoder, der ikke lækkes så tit.

Sammenligning af brugeres adgangskoder med en kurateret liste

Kontrol af, om en adgangskode, der ikke står på den lokale liste, har et match, indebærer en vis interaktion med Apples servere. Som led i sikringen af, at en brugers gyldige adgangskoder ikke bliver sendt til Apple, anvendes der en form for kryptografisk *privat skæringspunkt mellem sæt*, som sammenligner brugerens adgangskoder med et omfattende sæt af lækkede adgangskoder. Det har til formål at sikre, at der kun deles ganske få oplysninger med Apple om de adgangskoder, som er mindre udsat for brud på datasikkerheden. Til en brugers adgangskode er oplysningerne begrænset til et 15-bit præfiks til en kryptografisk hash-værdi. Fjernelsen af de hyppigst lækkede adgangskoder fra denne interaktive proces vha. den lokale liste med de hyppigst lækkede adgangskoder reducerer delta for den relative hyppighed af adgangskoder i webtjenestens buckets, så det i praksis ikke er muligt at udlede adgangskoder ved hjælp af opslag.

Den underliggende protokol opdeler listen over kuraterede adgangskoder, som i skrivende stund omfattede ca. 1,5 milliarder adgangskoder, i 2^{15} forskellige buckets. Den bucket, en adgangskode hører til i, er baseret på de første 15 bits i adgangskodens SHA256 hash-værdi. Desuden bliver hvert lækket adgangskode – pw – knyttet til et elliptisk kurvepunkt på NIST P256-kurven: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, hvor α er en hemmelig, tilfældig nøgle, som kun kendes af Apple, og H_{SWU} er en Oracle-tilfældighedsfunktion, som knytter adgangskoder til kurvepunkter ud fra Shallue-van de Woestijne-Ulas-metoden. Denne transformation er designet til beregningsmæssigt at skjule adgangskoders værdier, og den er med til at forhindre afsløring af nyligt lækkede adgangskoder gennem overvågning af adgangskoder.

For at beregne det private skæringspunkt mellem sæt fastslår brugerens enhed, hvilken bucket brugerens adgangskode hører til i, ved at bruge λ, som er 15-bit præfikset til SHA256(upw), hvor upw er en af brugerens adgangskoder. Enheden genererer sin egen tilfældige konstant, β, og sender punktet $P_c = \beta \cdot H_{SWU}(upw)$ til serveren sammen med en anmodning til den bucket, der svarer til λ. Her sørger β for at skjule oplysninger om brugerens adgangskode og for, at de oplysninger fra adgangskoden, som Apple kan se, er begrænset til λ. Til sidst tager serveren det punkt, der er sendt af brugerens enhed, beregner $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$ og returnerer den sammen med den relevante bucket med punkter, $B\lambda = \{ P_{pw} \mid SHA256(pw)$ begynder med præfiks $\lambda\}$ til enheden.

Ved hjælp af de returnerede oplysninger kan enheden beregne $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$ og fastslå, at brugerens adgangskode er lækket, hvis $\alpha P_c \in B'_\lambda$.

Afsendelse af adgangskoder til andre brugere eller Apple-enheder

Apple sender adgangskoder på en sikker måde til andre brugere eller Apple-enheder med AirDrop og på Apple TV.

Brug af AirDrop til at gemme godkendelsesoplysninger på en anden enhed

Når iCloud er slået til, kan brugerne benytte AirDrop til at sende gemte godkendelsesoplysninger til en anden enhed. Godkendelsesoplysningerne inkluderer brugerens navn og adgangskode og de websteder, de er gemt til. Når der sendes godkendelsesoplysninger via AirDrop, bruges funktionen Kun kontakter altid uanset brugerens indstillinger. Når brugeren har givet sit samtykke, gemmes godkendelsesoplysningerne på modtagerens enhed i nøgleringen til Autoudfyld adgangskode.

Udfyldelse af godkendelsesoplysninger i apps på Apple TV

Autoudfyld adgangskode kan bruges til at udfylde godkendelsesoplysninger i apps på Apple TV. Når brugeren fokuserer på et tekstfelt til brugernavn eller adgangskode i tvOS, begynder Apple TV at vise en anmodning om Autoudfyld adgangskode over Bluetooth Low Energy (BLE).

Enhver iPhone, iPad eller iPod touch i nærheden viser en besked, der inviterer brugeren til at dele godkendelsesoplysninger med Apple TV. Sådan fastlægges krypteringsmetoden:

- Hvis enheden og Apple TV bruger den samme iCloud-konto, foretages kryptering mellem enhederne automatisk.
- Hvis enheden er logget ind på en anden iCloud-konto end den, der bruges af Apple TV, bliver brugeren bedt om at oprette en krypteret forbindelse ved at bruge en PIN-kode. Brugerens iPhone skal være låst op og tæt på den Siri Remote, der er parret med den pågældende Apple TV-enhed, for at modtage beskeden.

Når den krypterede forbindelse er oprettet vha. BLE-kryptering, sendes godkendelsesoplysningerne til Apple TV og udfyldes automatisk i de relevante tekstfelter i appen.

Udvidelser til levering af godkendelsesoplysninger

I iOS, iPadOS og macOS kan brugere angive, at en understøttet tredjepartsapp skal levere godkendelsesoplysninger til Autoudfyld adgangskode, i indstillingerne til Adgangskoder (iOS og iPadOS) eller i vinduet Udvidelser i Systemindstillinger (macOS). Denne mekanisme bygger på app-udvidelser. Udvidelsen til levering af godkendelsesoplysninger skal vise en mulighed for at vælge godkendelsesoplysninger og kan eventuelt levere metadata om gemte godkendelsesoplysninger, så de kan vises direkte på QuickType-linjen (iOS og iPadOS) eller i et forslag til automatisk udfyldning (macOS). Disse metadata inkluderer webstedet, hvor godkendelsesoplysningerne bruges, og det tilknyttede brugernavn, men ikke adgangskoden. iOS, iPadOS og macOS kommunikerer med udvidelsen for at få adgangskoden, når brugeren vælger at udfylde godkendelsesoplysninger i en app eller på et websted i Safari. Metadata til godkendelsesoplysninger lagres i beholderen i den app, der leverer godkendelsesoplysninger, og fjernes automatisk, når en app fjernes.

iCloud-nøglering

Oversigt over sikkerhed i iCloud-nøglering

Med iCloud-nøglering kan brugerne synkronisere deres adgangskoder sikkert mellem iOS- og iPadOS-enheder samt Mac-computere, uden at Apple kan se oplysningerne. Ud over effektiv anonymitet og sikkerhed er brugervenlighed og muligheden for at gendanne en nøglering nogle af de mål, der har påvirket iCloud-nøgleringens design og arkitektur mest. iCloud-nøglering består af to tjenester: Synkronisering af nøgleringen og gendannelse af nøgleringen.

Apple designede iCloud-nøglering og gendannelse af nøgleringen, så en brugers adgangskoder stadig er beskyttet i følgende situationer:

- En brugers iCloud-konto er blevet kompromitteret.
- iCloud er blevet kompromitteret af en udefrakommende person med ondsindede hensigter eller en medarbejder.
- En tredjepart skaffer sig adgang til brugerkonti.

Integration mellem adgangskodeadministratoren og iCloud-nøglering

iOS, iPadOS og macOS kan automatisk generere kryptografisk stærke tilfældige strenge, der kan bruges som adgangskoder til konti i Safari. iOS og iPadOS kan også generere stærke adgangskoder til apps. Genererede adgangskoder gemmes i nøgleringen og synkroniseres til andre enheder. Emner i nøgleringen overføres fra enhed til enhed via Apple-servere, men de er krypteret på en sådan måde, at Apple og andre enheder ikke kan læse deres indhold.

Sikker synkronisering af nøglering

Når en bruger slår iCloud-nøglering til for første gang, etablerer enheden en godkendelseskæde og opretter en synkroniseringsidentitet til sig selv. Synkroniseringsidentiteten består af en privat nøgle og en offentlig nøgle og opbevares i enhedens nøglering. Synkroniseringsidentitetens offentlige nøgle placeres i kæden, og kæden signeres to gange. Først med synkroniseringsidentitetens private nøgle og derefter igen med en asymmetrisk elliptisk nøgle (der bruger P-256) afledt af adgangskoden til brugerens iCloud-konto. I kæden gemmes også de parametre (tilfældig saltnøgle og gentagelser), som bruges til at danne den nøgle, der er baseret på brugerens adgangskode til iCloud.

Til konti med tofaktorgodkendelse oprettes en ekstra lignende kæde, som opbevares i CloudKit. Enhedsidentiteter i dette system består af to par asymmetriske elliptiske nøgler (der bruger P-384), som også opbevares i nøgleringen. De enkelte enheder danner deres egen liste med de identiteter, de stoler på, og signerer listen med en af deres identitetsnøgler.

Lagring af synkroniseringskæden i iCloud

Den signerede synkroniseringskæde opbevares i brugerens iCloud-lagringsområde til nøgleværdier. Den kan ikke læses uden kendskab til brugerens iCloud-adgangskode og kan ikke ændres på en gyldig måde uden den private nøgle til medlemmets synkroniseringsidentitet.

Til konti med tofaktorgodkendelse opbevares hver enheds synkroniseringsliste i CloudKit. Listerne kan ikke læses uden kendskab til brugerens iCloud-adgangskode og kan ikke ændres uden private nøgler på ejerenheden.

Sådan føjes en brugers andre enheder til synkroniseringskæden

Når der logges ind på iCloud på nye enheder, indlemmes enhederne i synkroniseringskæden i iCloud-nøglering på en af to måder: Enten ved at danne par med og blive sponsoreret af en eksisterende enhed i iCloud-nøglering eller ved at bruge gendannelse af iCloud-nøglering.

Under pardannelsen opretter ansøgerenheden nye synkroniseringsidentiteter til såvel synkroniseringskæden som synkroniseringslisterne (til konti med tofaktorgodkendelse) og præsenterer dem for sponsoren. Sponsoren føjer det nye medlems offentlige nøgle til synkroniseringskæden og signerer den igen med både dets synkroniseringsidentitet og den nøgle, der er afledt af brugerens iCloud-adgangskode. Den nye synkroniseringskæde placeres i iCloud, hvor den ligeledes signeres af det nye medlem af kæden. Ved konti med tofaktorgodkendelse forsyner sponsorenheden også den enhed, der skal indlemmes, med en *kupon*, der er signeret med dens identitetsnøgler, og som viser, at ansøgerenheden er godkendt. Den opdaterer derefter sin egen liste med godkendte synkroniseringsidentiteter ved at tilføje ansøgeren.

Der er nu to medlemmer af signeringskæden, og hvert medlem har det andet medlems offentlige nøgle. De kan nu begynde at udveksle de enkelte emner i nøgleringen via iCloud-lagringsområdet til nøgleværdier, eller de gemmer dem i CloudKit, alt efter situationen. Hvis begge medlemmer af kæden har opdateringer til samme emne, vælges en af dem, så emnerne efterhånden bliver ens. Hvert emne, der synkroniseres, bliver krypteret, så det kun kan dekrypteres af en enhed i brugerens godkendelseskæde. Det kan ikke dekrypteres af nogen anden enhed eller af Apple.

Denne "indlemmelsesproces" gentages, når nye enheder indlemmes i synkroniseringskæden. Når en tredje enhed indlemmes, kan den danne par med en af de to eksisterende enheder. Når der tilføjes nye enheder, synkroniseres hver enhed med de nye. Det har til formål at sikre, at alle medlemmer har samme emner i nøgleringen.

Kun visse emner synkroniseres

Nogle emner i nøgleringen gælder kun en enhed, iMessage-nøgler, og må ikke forlade enheden. Det betyder, at alle de emner, der skal synkroniseres, eksplicit skal mærkes med attributten `kSecAttrSynchronizable`.

Apple indstiller denne attribut til brugerdata i Safari (herunder brugernavne, adgangskoder og kreditkortnumre) samt til Wi-Fi-adgangskoder, HomeKit-krypteringsnøgler og andre emner i nøgleringen, der understøtter end-to-end-kryptering af iCloud.

Desuden gælder, at emner i nøgleringen, som er tilføjet af apps fra tredjeparter, ikke synkroniseres. Udviklerne skal indstille attributten `kSecAttrSynchronizable`, når de føjer emner til nøgleringen.

Sikker gendannelse af iCloud-nøglering

iCloud-nøgleringen deponerer brugernes data i nøgleringen hos Apple *uden* at tillade, at Apple læser de adgangskoder og andre data, den indeholder. Selvom brugeren kun har en enkelt enhed, er gendannelse af nøgleringen et sikkerhedsnet for at undgå datatab. Det er især vigtigt, når Safari bruges til at generere tilfældige, stærke adgangskoder til webkonti, eftersom disse adgangskoder kun er registreret i nøgleringen.

Hjørnestenen i gendannelse af nøgleringen er sekundær godkendelse og en sikker deponeringstjeneste, som Apple har oprettet med henblik på at understøtte denne funktion. Brugerens nøglering krypteres med en stærk kode, og deponeringstjenesten udleverer kun en kopi af nøgleringen, hvis nogle strenge betingelser er opfyldt.

Brug af sekundær godkendelse

Der kan oprettes en stærk kode på flere måder:

- Hvis tofaktorgodkendelse er slået til for brugerens konto, bruges enhedens kode til at gendanne en deponeret nøglering.
- Hvis tofaktorgodkendelse ikke er indstillet, bliver brugeren bedt om at oprette en iCloud-sikkerhedskode bestående af seks cifre. Uden tofaktorgodkendelse kan brugerne i stedet selv opgive en lang kode, eller de kan lade deres enheder oprette en kryptografisk tilfældig kode, som de selv kan registrere og opbevare.

Deponeringsprocessen for nøgleringe

Når koden er etableret, deponeres nøgleringen hos Apple. iOS-, iPadOS- eller macOS-enheden eksporterer først en kopi af brugerens nøglering, krypterer den pakket med nøgler i en asymmetrisk nøglesamling og placerer den i brugerens iCloud-lagringsområde til nøgleværdier. Nøglesamlingen pakkes med brugerens iCloud-sikkerhedskode og med den offentlige nøgle til den klynge i hardwaresikkerhedsmodulet (HSM), hvor deponeringsposten skal opbevares. Det bliver brugerens *iCloud-deponeringspost*. Til konti med tofaktorgodkendelse gemmes nøgleringen også i CloudKit og pakkes med mellemliggende nøgler, som kun kan gendannes med indholdet i iCloud-deponeringsposten, og det giver dermed samme beskyttelsesniveau.

Indholdet af deponeringsposten giver også den enhed, der gendanner data, tilladelse til at blive indlemmet i iCloud-nøgleringen igen, hvilket viser over for eksisterende enheder, at denne enhed har gennemført deponeringsprocessen og dermed har opnået kontoejerens tilladelse.

Bemærk: Hvis brugeren beslutter at acceptere en kryptografisk tilfældig sikkerhedskode i stedet for at angive sin egen eller bruge en værdi på fire cifre, er der ikke behov for en deponeringspost. I stedet bruges iCloud-sikkerhedskoden til at indpakke den tilfældige nøgle direkte.

Ud over en sikkerhedskode skal brugerne også registrere et telefonnummer. Det giver et sekundært godkendelsesniveau under gendannelse af nøgleringen. Brugeren modtager en sms-besked og skal svare på den, før gendannelsen kan fortsætte.

Deponeringssikkerhed i iCloud-nøglering

iCloud har en sikker infrastruktur til nøgleringsdeponering, der er med til at sikre, at kun godkendte brugere og enheder kan udføre en gendannelse. Klynger af hardwaresikkerhedsmoduler (HSM'er) er topografisk set placeret bag iCloud og vogter deponeringsposterne. Som beskrevet tidligere har hver af dem en nøgle, der bruges til at kryptere de deponeringsposter, som de vogter over.

Når brugerne vil gendanne en nøglering, skal de legitimere sig med deres iCloud-konto og adgangskode og svare på en sms, der er sendt til deres registrerede telefonnummer. Når det er gjort, skal brugerne indtaste deres iCloud-sikkerhedskode. HSM-klyngen bekræfter ved hjælp af SRP-protokollen (Secure Remote Password), at en bruger kender sin iCloud-sikkerhedskode. Koden selv sendes ikke til Apple. Medlemmerne af klyngen bekræfter uafhængigt af hinanden, at brugeren ikke har overskredet det maksimale antal forsøg på at hente sine data, som beskrevet nedenfor. Hvis flertallet bekræfter det, pakker klyngen deponeringsposten ud og sender den til brugerens enhed.

Derefter bruger enheden iCloud-sikkerhedskoden til at pakke de tilfældige nøgler ud, som er brugt til at kryptere brugerens nøglering. Med den nøgle bliver nøgleringen, der er hentet fra iCloud-lagringsområdet til nøgleværdier og CloudKit, dekrypteret og gendannet på enheden. I iOS, iPadOS og macOS må der højst bruges 10 forsøg på at godkende og hente en deponeringspost. Efter flere mislykkede forsøg låses posten, og brugeren skal kontakte Apple-support for at få tildelt flere forsøg. Efter det 10. mislykkede forsøg ødelægger HSM-klyngen deponeringsposten, og nøgleringen går tabt for altid. Det beskytter mod brute-force-forsøg på at hente posten. Til gengæld ofres dataene i nøgleringen.

Disse politikker er kodet i HSM-firmwaren. De kort til administrativ adgang, der tillader, at firmwaren ændres, er blevet ødelagt. Forsøg på at ændre firmwaren eller få adgang til den private nøgle får HSM-klyngen til at slette den private nøgle. Hvis det sker, modtager ejeren af hver nøglering, der beskyttes af klyngen, en besked om, at vedkommendes deponeringspost er gået tabt. Personen kan derefter vælge at tilmelde sig igen.

Apple Pay

Oversigt over sikkerhed i Apple Pay

Med Apple Pay kan brugere benytte understøttede iPhone-, iPad-, Mac- og Apple Watch-enheder til at betale på en nem, sikker og privat måde i butikker, apps og på internettet i Safari. Brugerne kan også føje Apple Pay-kompatible rejsekort, studiekort og adgangskort til Apple Wallet. Det er enkelt for brugerne, og der er indbygget sikkerhed i både hardware og software.

Apple Pay er også designet, så det beskytter brugerens personlige oplysninger. Apple Pay indsamler ingen transaktionsoplysninger, der kan spores tilbage til brugeren. Betalingstransaktionerne foregår mellem brugeren, butikken og kortudstederen.

Komponentsikkerhed i Apple Pay

Apple Pay bruger flere hardware- og softwarefunktioner til at tilbyde sikre og pålidelige køb.

Secure Element

Secure Element (det sikre element) er en certificeret chip, der er standard i branchen og afvikles på Java Card-platformen, som overholder finanssektorens krav til elektroniske betalinger. Secure Element IC og Java Card-platformen er certificeret i henhold til EMVCo Security Evaluation-processen. Når sikkerhedsevalueringen er gennemført, udsteder EMVCo unikke IC- og platformscertifikater.

Secure Element IC er blevet certificeret i henhold til Common Criteria-standarden. Du kan få flere oplysninger under Sikkerhedscertificeringer til Secure Enclave Processor i Certificeringer af Apples platforme.

NFC-kontrolenhed

NFC-kontrolenheden håndterer NFC-protokoller (Near Field Communication) og dirigerer kommunikationen mellem app-processoren og Secure Element og mellem Secure Element og betalingsterminalen.

Apple Wallet

Appen Apple Wallet bruges til at tilføje og administrere kredit-, debet- og butikskort og til at foretage betalinger med Apple Pay. Brugerne kan se deres kort og kan muligvis se yderligere oplysninger, deres kortudsteder har oplyst, f.eks. kortudstederens anonymitetspolitik, og de seneste transaktioner m.m. i Apple Wallet. Brugerne kan også føje kort til Apple Pay i:

- Indstillingsassistent og Indstillinger i iOS og iPadOS
- Appen Watch til Apple Watch
- Wallet & Apple Pay i Systemindstillinger til Mac-computere med Touch ID

Med Apple Wallet kan brugerne også tilføje og administrere rejsekort, fordelskort, boardingkort, billetter, gavekort, studiekort, adgangskort m.m.

Secure Enclave

Secure Enclave på iPhone, iPad, Apple Watch, Mac-computere med Touch ID og Mac-computere med Apple Silicon, der bruger Magic Keyboard med Touch ID, administrerer godkendelsesprocessen og gør det muligt at gå videre med en betalingstransaktion.

På Apple Watch skal enheden være låst op, og brugeren skal trykke to gange på sideknappen. De to tryk registreres og overføres direkte til Secure Element eller Secure Enclave, hvis den er tilgængelig, uden at passere gennem app-processoren.

Apple Pay-servere

Apple Pay-servere administrerer indstilling og tilknytning af kredit-, debet-, rejse-, studie- og adgangskort i Apple Wallet. Serverne administrerer også de kontonumre til enheden, der opbevares i Secure Element. De kommunikerer både med enheden og betalingsnetværkets eller kortudstederens servere. Apple Pay-serverne har også ansvaret for at kryptere godkendelsesoplysninger igen til betalinger i apps eller på nettet.

Sådan beskytter Apple brugernes køb

Secure Element

Secure Element indeholder en miniapp, der er specifikt designet til at administrere Apple Pay. Det inkluderer også miniapps, der er certificeret af betalingsnetværk eller kortudstedere. Data til kreditkort, debetkort og forudbetalte kort, der sendes fra betalingsnetværket eller kortudstederen til disse miniapps, er krypteret ved hjælp af nøgler, der kun kendes af betalingsnetværket eller kortudstederen og miniappsenes sikkerhedsdomæne. Dataene gemmes i disse miniapps og beskyttes af sikkerhedsfunktionerne i Secure Element. Under en transaktion kommunikerer terminalen direkte med Secure Element via NFC-kontrolenheden (near-field-communication) gennem en dedikeret hardwarebus.

NFC-kontrolenhed

Som indgangsport til Secure Element er NFC-kontrolenheden med til at sikre, at alle kontaktløse transaktioner gennemføres med en betalingsterminal, der er i umiddelbar nærhed af enheden. Kun betalingsanmodninger, der kommer fra en terminal i NFC-feltet, markeres af NFC-kontrolenheden som kontaktløse transaktioner.

Når en betaling med kredit- eller debetkort eller forudbetalte kort (inklusive butikskort) er godkendt af kortindehaveren vha. Face ID, Touch ID eller en kode eller via to tryk på sideknappen på et oplåst Apple Watch, sendes de kontaktløse svar, som betalingsminiappsene i Secure Element har udarbejdet, udelukkende til NFC-feltet af kontrolenheden. Detaljer om godkendte betalinger i kontaktløse betalingstransaktioner holdes således inden for det lokale NFC-felt og kan aldrig ses af app-processoren. Derimod sendes detaljer om godkendte betalinger, der er foretaget fra en app eller internettet, til app-processoren, men først efter de er blevet krypteret af Secure Element og overført til Apple Pay-serveren.

Kreditkort, debetkort og forudbetalte kort

Oversigt over sikkerheden ved tilknytning af kort

Når en bruger føjer et kreditkort, et debetkort eller et forudbetalt kort (herunder butikskort) til Apple Wallet, sender Apple kortoplysningerne sammen med andre oplysninger om brugerens konto og enhed i sikkert format til kortudstederen eller kortudstederens autoriserede serviceudbyder. Ud fra oplysningerne afgør kortudstederen, om kortet kan godkendes og føjes til Apple Wallet. Under tilknytningen af kort bruger Apple Pay tre kald på serversiden til at sende og modtage kommunikation til/fra kortudstederen eller netværket:

- Felter, der skal udfyldes
- Kontroller kort
- Forbind og tilknyt

Kortudstederen eller netværket bruger kaldene til at bekræfte og godkende kort og føje kort til Apple Wallet. Disse klient-serversessioner bruger TLS 1.2 til at overføre dataene.

De fuldstændige kortnumre opbevares ikke på enheden eller Apple Pay-serverne. I stedet oprettes et entydigt kontonummer for enheden, der krypteres og derefter gemmes i Secure Element. Det entydige kontonummer for enheden er krypteret på en måde, så Apple ikke kan få adgang til det. Dette kontonummer for enheden er unikt og forskelligt fra de fleste kredit- eller debetkortnumre. Kortudstederen eller betalingsnetværket kan forhindre brugen af det på kort med magnetstribe, telefonisk eller på websteder. Kontonummeret til enheden i Secure Element bliver aldrig opbevaret på Apple Pay-serverne eller sikkerhedskopieret til iCloud, og det er isoleret fra iOS-, iPadOS- og watchOS-enheder og fra Mac-computere med Touch ID.

Kort til brug sammen med Apple Watch knyttes til Apple Pay vha. Apple Watch-appen på iPhone eller kortudstederens iPhone-app. Hvis et kort skal føjes til Apple Watch, kræver det, at uret er inden for Bluetooth-rækkevidde. Kort tilmeldes specifikt til brug sammen med Apple Watch og har deres egne enhedskontonumre, som opbevares i Secure Element på Apple Watch.

Når der tilføjes kreditkort, debetkort eller forudbetalte kort (herunder butikskort), vises de på en liste med kort i Indstillingsassistent på enheder, der er logget ind på den samme iCloud-konto. Disse kort forbliver på denne liste, så længe de er aktive på mindst en enhed. Kort fjernes fra denne liste, når de har været fjernet fra alle enheder i 7 dage. Denne funktion kræver tofaktorgodkendelse for at blive slået til i den pågældende iCloud-konto.

Tilføjelse af kredit- eller debetkort til Apple Pay

Kreditkort kan manuelt føjes til Apple Pay på Apple-enheder.

Manuel tilføjelse af kredit- eller debetkort

Når et kort tilføjes manuelt, bruges navnet, kortnummeret, udløbsdatoen og sikkerhedskoden til tilknytningsprocessen. Brugerne kan via Indstillinger, Apple Wallet eller appen Apple Watch indsætte disse oplysninger ved at skrive dem eller ved at bruge enhedens kamera. Når kameraet har registreret kortoplysningerne, forsøger Apple at udfylde navnet, kortnummeret og udløbsdatoen. Fotoet gemmes aldrig på enheden og opbevares ikke i fotobiblioteket. Når alle felterne er udfyldt, kontrollerer processen Kontroller kort alle felterne bortset fra sikkerhedskoden. Oplysningerne krypteres derefter og sendes til Apple Pay-serveren.

Hvis der returneres et id for vilkår og betingelser i processen Kontroller kort, henter Apple den respektive kortudsteders vilkår og betingelser og viser dem for brugeren. Hvis brugeren accepterer vilkårene og betingelserne, sender Apple id'et for de accepterede vilkår samt sikkerhedskoden til processen Forbind og tilknyt. Som led i processen Forbind og tilknyt deler Apple desuden oplysninger fra enheden med kortudstederen eller netværket. Det gælder oplysninger om (a) brugerens aktiviteter i iTunes og App Store (f.eks. om brugeren har foretaget køb i iTunes igennem længere tid), (b) oplysninger om brugerens enhed (f.eks. enhedens telefonnummer, navn og model samt en evt. tilhørende Apple-enhed, der kræves til indstilling af Apple Pay) og (c) brugerens omtrentlige lokalitet på det tidspunkt, hvor vedkommende tilføjer kortet (hvis Lokalitetstjenester er slået til). Ud fra oplysningerne afgør kortudstederen, om kortet kan godkendes og føjes til Apple Pay.

Der sker to ting som følge af processen Forbind og tilknyt:

- Enheden begynder at hente det arkiv med kortet til Apple Wallet, der repræsenterer kredit- eller debetkortet.
- Enheden begynder at binde kortet til Secure Element.

Kortarkivet indeholder URL-adresser til overførsel af kortillustrationer, metadata om kortet, f.eks. kontaktoplysninger, den relaterede app fra udstederen og understøttede funktioner. Det indeholder også kortets status, som bl.a. omfatter oplysninger om, hvorvidt individualiseringen af Secure Element er færdig, hvorvidt kortet i øjeblikket er spærret af kortudstederen, og om der kræves yderligere bekræftelse, før kortet kan bruges til at foretage betalinger med Apple Pay.

Tilføjelse af kredit- eller debetkort fra en iTunes Store-konto

Hvis et kredit- eller debetkort er registreret i iTunes, skal brugeren måske indtaste adgangskoden til sit Apple-id igen. Kortnummeret hentes fra iTunes, og processen Kontroller kort startes. Hvis kortet kan bruges til Apple Pay, henter og viser enheden vilkår og betingelser og sender derefter vilkårenes id og kortets sikkerhedskode til processen Forbind og tilknyt. Der kræves måske yderligere godkendelse af kort, der er registreret under iTunes-konti.

Tilføjelse af kredit- eller debetkort fra en kortudsteders app

Når en app registreres til brug sammen med Apple Pay, oprettes nøgler til appen og til kortudstederens server. Disse nøgler bruges til at kryptere de kortoplysninger, der sendes til kortudstederen. Det har til formål at forhindre, at oplysningerne bliver læst af Apple-enheden. Tilknytningsflowet svarer til det, som er beskrevet tidligere for kort, der tilføjes manuelt, bortset fra at der bruges engangsadgangskoder i stedet for sikkerhedskoden.

Tilføjelse af kredit- eller debetkort fra en kortudsteders websted

Nogle kortudstedere giver mulighed for at indlede processen, der knytter kortet til Apple Wallet, direkte fra deres websted. I det tilfælde starter brugeren opgaven ved at vælge et kort, der skal tilknyttes, på kortudstederens websted. Brugeren dirigeres derefter til et isoleret login-sted hos Apple (på Apples domæne) og bliver bedt om at logge ind med sit Apple-id. Når brugeren er logget ind, vælger brugeren en eller flere enheder, som kortet skal tilknyttes, og skal derefter bekræfte tilknytningen på hver af de valgte modtagerenheder.

Tilføjelse af yderligere godkendelse

En kortudsteder kan beslutte, at et kredit- eller debetkort kræver yderligere godkendelse. Brugeren kan vælge mellem de muligheder for yderligere godkendelse, som kortudstederen tilbyder. Det kan f.eks. være en sms, en e-mail, et opkald fra kundeservice eller en metode i en godkendt app fra tredjepart, der fuldfører godkendelsen. I tilfælde af sms eller e-mail vælger brugeren blandt de kontaktoplysninger, der er registreret hos kortudstederen. Der sendes en kode, som skal skrives i Apple Wallet, Indstillinger eller appen Apple Watch. I tilfælde af brug af kundeservice eller godkendelse via en app benytter udstederen sin egen kommunikationsproces.

Betalingsgodkendelse i Apple Pay

På enheder med Secure Enclave kan der først foretages betaling, når betalingen har modtaget en godkendelse fra Secure Enclave. På iPhone og iPad kræver det en bekræftelse af, at brugeren har legitimeret sig med Face ID, Touch ID eller koden til enheden. Hvis Face ID eller Touch ID er tilgængelig, er det standardmetoden, men koden kan altid bruges i stedet. Efter tre forgæves forsøg på at genkende et fingeraftryk eller to forgæves forsøg på at genkende et ansigt får brugeren mulighed for at indtaste koden. Efter fem forgæves forsøg kræves, at koden indtastes. Der skal også bruges en kode, hvis Face ID eller Touch ID ikke er konfigureret eller ikke er indstillet til Apple Pay. Før en betaling kan gennemføres på Apple Watch, skal enheden låses op med koden eller med to tryk på sideknappen.

Brug af delt pardannelsesnøgle

Kommunikationen mellem Secure Enclave og Secure Element foregår via en seriel grænseflade, hvor Secure Element er forbundet med NFC-kontrolenheden, som på sin side er forbundet med app-processoren. Selvom Secure Enclave og Secure Element ikke er forbundet direkte, kan de kommunikere sikkert ved at bruge en delt pardannelsesnøgle, som blev tilknyttet under fremstillingen. Krypteringen og godkendelsen af kommunikationen bygger på AES, hvor kryptografiske nonce-værdier bruges af begge parter som beskyttelse mod genafspilningsangreb. Pardannelsesnøglen genereres i Secure Enclave ud fra dens UID-nøgle og det entydige Secure Element-id. På fabrikken overføres pardannelsesnøglen sikkert fra Secure Enclave til et hardwaresikkerhedsmodul (HSM), som har det nøglemateriale, der kræves for derefter at skyde pardannelsesnøglen ind i det sikre element.

Godkendelse af en sikker transaktion

Når brugeren godkender en transaktion, som omfatter en fysisk bevægelse, der kommunikeres direkte til Secure Enclave, sender Secure Enclave signerede data om transaktionens type (kontaktløs eller fra en app) til Secure Element sammen med en tilfældig godkendelsesværdi (AR – Authorization Random). AR-værdien genereres i Secure Enclave, første gang en bruger tilknytter et kreditkort. Den bevares, så længe Apple Pay er aktiveret, og beskyttes af Secure Enclave-krypteringen og -forsvarsmekanismen mod rollback-angreb. Den overføres på en sikker måde til Secure Element ved brug af pardannelsesnøglen. Når Secure Element modtager en ny AR-værdi, markerer elementet tidligere tilføjede kort som slettet.

Brug af betalingskryptogram til dynamisk sikkerhed

Betalingstransaktioner fra betalingsminiappsene indeholder et betalingskryptogram sammen med kontonummeret for en enhed. Dette kryptogram – en engangskode – beregnes ved hjælp af en transaktionstæller og en nøgle. Transaktionstælleren øges med 1 for hver ny transaktion. Nøglen dannes i betalingsminiappen under individualiseringen og kendes af betalingsnetværket eller kortudstederen eller begge dele. Afhængigt af betalingsmåden kan der indgå andre data i beregningen, f.eks.:

- Et Terminal Unpredicable Number i forbindelse med NFC-transaktioner (near-field-communication)
- En Apple Pay-servers nonce-værdi i forbindelse med transaktioner fra apps

Disse sikkerhedskoder videregives til betalingsnetværket og kortudstederen, så udstederen kan godkende de enkelte transaktioner. Sikkerhedskodernes længde kan variere afhængigt af transaktionens type.

Betaling med kort og Apple Pay

Apple Pay kan bruges til at betale for køb i butikker, i apps og på websteder.

Betaling med kort i butikker

Hvis iPhone eller Apple Watch er tændt og registrerer et NFC-felt, får brugeren vist det kort, der blev anmodet om (hvis automatisk valg er slået til for kortet) eller det standardkort, som administreres i Indstillinger. Brugeren kan også gå til Apple Wallet og vælge et kort eller gøre et af følgende, hvis enheden er låst:

- Tryk to gange på sideknappen på enheder med Face ID
- Tryk to gange på knappen Hjem på enheder med Touch ID
- Brug Tilgængelighedsfunktioner, der giver mulighed for at bruge Apple Pay fra den låste skærm.

Næste skridt, inden oplysningerne sendes, er, at brugeren godkendes ved hjælp af Face, Touch ID eller sin kode. Når Apple Watch er låst op, aktiveres standardkortet til betaling, når der trykkes to gange på sideknappen. Der sendes ingen betalingsoplysninger uden brugergodkendelse.

Når brugeren er godkendt, bruges enhedens kontonummer og en transaktionsspecifik dynamisk sikkerhedskode til at behandle betalingen. Hverken Apple eller brugerens enhed sender hele kredit- eller debetkortets nummer til butikkerne. Apple vil måske modtage anonyme transaktionsoplysninger, f.eks. transaktionens omtrentlige tidspunkt og lokalitet, som kan hjælpe med at forbedre Apple Pay og andre produkter og tjenester fra Apple.

Betaling med kort i apps

Apple Pay kan også bruges til at foretage betalinger fra apps på iPhone, iPad, Mac og Apple Watch. Når brugerne betaler med Apple Pay fra apps, modtager Apple de krypterede transaktionsoplysninger. Inden oplysningerne sendes til udvikleren eller butikken, krypterer Apple transaktionen igen med en særlig udviklernøgle. Apple Pay gemmer anonyme transaktionsoplysninger, f.eks. det omtrentlige købsbeløb. Oplysningerne kan ikke spores til brugeren og omfatter aldrig det, som brugeren har købt.

Når en app starter en Apple Pay-betalingstransaktion, modtager Apple Pay-serverne den krypterede transaktion fra enheden, før butikken modtager den. Derefter krypterer Apple Pay-serverne transaktionen igen med en særlig nøgle til butikken, før den sendes videre til butikken.

Når en app anmoder om betaling, kalder den et API for at afgøre, om enheden understøtter Apple Pay, og om brugeren har kredit- eller debetkort, der kan foretage betalinger på et betalingsnetværk, som butikken accepterer. Appen anmoder om de oplysninger, den skal bruge for at behandle og gennemføre transaktionen, f.eks. faktureringsadressen, leveringsadressen og kontaktoplysninger. Appen anmoder derefter iOS, iPadOS eller watchOS om at vise Apple Pay-arket, der anmoder om oplysninger til appen og andre nødvendige oplysninger, f.eks. hvilket kort der skal bruges.

På dette tidspunkt modtager appen oplysninger om by og postnummer, så den kan beregne de endelige leveringsomkostninger. Alle de oplysninger, appen har anmodet om, videregives først til appen, når brugeren har godkendt betalingen med Face ID, Touch ID eller koden til enheden. Når betalingen er godkendt, overføres de oplysninger, der vises i Apple Pay-arket, til butikken.

Betalingsgodkendelse i app

Når brugeren godkender betalingen, foretages der et kald til Apple Pay-serverne for at rekvirere en kryptografisk nonce-værdi, som ligner den værdi, der returneres af NFC-terminalen i forbindelse med transaktioner i butikker. Sammen med andre transaktionsdata overføres nonce-værdien til Secure Element for at få beregnet godkendelsesoplysninger til betalingen, som krypteres med en Apple-nøgle. De krypterede godkendelsesoplysninger til betalingen sendes tilbage til Apple Pay-serverne, som dekrypterer godkendelsesoplysningerne, kontrollerer nonce-værdien i godkendelsesoplysningerne i forhold til den nonce-værdi, som Apple Pay-serverne oprindeligt sendte, og krypterer godkendelsesoplysningerne igen med den nøgle, som er knyttet til butikkens id. Betalingen returneres derefter til enheden, som sender den tilbage til appen via API'et. Appen sender dem derefter til behandling i butikkens system. Butikken kan nu dekryptere godkendelsesoplysningerne til betalingen med sin private nøgle før behandling. Sammen med signaturen fra Apples servere betyder denne proces, at butikken nu kan bekræfte, at transaktionen hører til vedkommende.

API'erne kræver en berettigelse, hvori id'erne for de understøttede butikker indgår. En app kan medsende flere data (f.eks. et ordrenummer eller et kunde-id) til signering i Secure Element, hvilket sikrer, at transaktionen ikke kan omdirigeres til en anden kunde. Det gøres af app-udvikleren, som kan angive app-data (applicationData) i betalingsanmodningen PKPaymentRequest. I de krypterede betalingsdata indgår en hash-værdi for disse data. Butikken har nu ansvaret for at bekræfte, at butikkens hash-værdi til applicationData matcher værdien i betalingsdataene.

Betaling med kort på websteder

Apple Pay kan bruges til at foretage betalinger på websteder med iPhone, iPad, Apple Watch og Mac-computere med Touch ID. Apple Pay-transaktioner kan også startes på en Mac og fuldføres på en iPhone eller et Apple Watch, hvor Apple Pay er slået til, og som bruger samme iCloud-konto.

Brug af Apple Pay på internettet forudsætter, at alle de deltagende websteder tilmelder sig hos Apple. Når domænet er registreret, udføres der ikke godkendelse af domænenavnet, før Apple har udstedt et TLS-klientcertifikat. Websteder, der understøtter Apple Pay, skal levere deres indhold via HTTPS. Til hver betalingstransaktion skal webstederne oprette en sikker og specifik session mellem butikken og en Apple-server ved hjælp af det TLS-klientcertifikat, som er udstedt af Apple. Data i butikkens session signeres af Apple. Når signaturen til en butikssession er bekræftet, kan webstedet spørge, om brugeren har en enhed med Apple Pay, og om brugeren har slået et kreditkort, debetkort eller forudbetalt kort til på enheden. Ingen andre oplysninger deles. Hvis brugerne ikke ønsker at dele disse oplysninger, kan de slå forespørgsler vedrørende Apple Pay fra i anonymitetsindstillingerne til Safari på iPhone-, iPad- og Mac-enheder.

Når en butikssession er bekræftet, er alle foranstaltninger med hensyn til anonymitet og sikkerhed de samme, som når brugeren betaler fra en app.

Hvis brugeren sender oplysninger om betalingen fra en Mac til en iPhone eller et Apple Watch, bruger Apple Pay Handoff IDS-protokollen med end-to-end-kryptering til at sende oplysninger om betalingen mellem brugerens Mac og den enhed, der skal stå for godkendelsen. IDS-klienten på Mac anvender brugerens nøgler til enheden til at foretage kryptering, så ingen andre enheder kan dekryptere oplysningerne. Nøglerne er heller ikke tilgængelige for Apple. Søgning efter enheder i forbindelse med Handoff og Apple Pay indeholder brugerens kreditkorttype og entydige id sammen med nogle metadata. Brugerens korts enhedsspecifikke kontonummer deles ikke. Det opbevares fortsat sikkert på brugerens iPhone eller Apple Watch. Apple overfører brugerens senest anvendte kontakt-, leverings- og faktureringsadresser via iCloud-nøglering med en sikker metode.

Når brugeren har godkendt betaling med Face ID, Touch ID, kode eller to tryk på sideknappen på Apple Watch, overføres et betalingstoken, der er krypteret ud fra hvert websteds butikscertifikat, sikkert fra brugerens iPhone eller Apple Watch til brugerens Mac. Derefter overføres det til butikkens websted.

Kun enheder, der er i nærheden af hinanden, kan anmode om og gennemføre en betaling. Nærheden afgøres ved hjælp af Bluetooth Low Energy-annonceringer (BLE).

Kontaktløse kort i Apple Pay

Apple bruger sin Apple VAS-protokol (Value Added Services) til at overføre data fra understøttede kort til kompatible NFC-terminaler. VAS-protokollen kan implementeres på kontaktløse terminaler og i apps til iPhone og benytter NFC til at kommunikere med understøttede Apple-enheder. VAS-protokollen kan benyttes over kort afstand og kan bruges til at vise kontaktløse kort uafhængigt eller som en del af en Apple Pay-transaktion.

Når enheden holdes tæt på NFC-terminalen, starter terminalen modtagelsen af kortoplysningerne ved at sende en anmodning om et kort. Hvis brugeren har et kort med kortudstederens id, bliver brugeren bedt om at godkende, at det bruges, ved hjælp af Face ID, Touch ID eller en kode. Kortoplysningerne, et tidsstempel og en tilfældig ECDH P-256-nøgle til engangsbrug bruges sammen med kortudstederens offentlige nøgle til at udlede en krypteringsnøgle til kortdataene, som sendes til terminalen.

Fra iOS 12.0.1 til og med iOS 13 kan brugere manuelt vælge et kort, inden de viser det til butikkens NFC-terminal. I iOS 13.1 eller nyere versioner kan kortudstedere konfigurere manuelt udvalgte kort til enten at kræve brugergodkendelse eller til at blive brugt uden godkendelse.

Markering af kort som ubrugelige i Apple Pay

De kreditkort, debetkort og forudbetalte kort, der er føjet til Secure Element, kan kun bruges, hvis Secure Element modtager en godkendelse med samme pardannelsesnøgle og AR-værdi (Authorization Random), som blev brugt, da kortet blev tilføjet. Når Secure Element modtager en ny AR-værdi, markerer elementet tidligere tilføjede kort som slettet. På den måde kan operativsystemet give Secure Enclave besked på at gøre kort ubrugelige, ved at enklavens kopi af AR-værdien markeres som ugyldig i følgende situationer:

Metode	Enhed
Koden slås fra.	iPhone, iPad og Apple Watch
Adgangskoden slås fra.	Mac
Brugeren logger ud af iCloud.	iPhone, iPad, Mac og Apple Watch
Brugeren vælger Slet alt indhold og alle indstillinger.	iPhone, iPad, Mac og Apple Watch
Enheden gendannes med gendannelsesfunktionen.	iPhone, iPad, Mac og Apple Watch
Ophævelse af pardannelse	Apple Watch

Suspendering, fjernelse og sletning af kort

Brugerne kan spærre Apple Pay på iPhone, iPad og Apple Watch ved at bruge funktionen Mistet i Find på deres enhed. Brugerne kan også fjerne og slette deres kort fra Apple Pay ved hjælp af Find, iCloud.com eller direkte på deres enheder med Apple Wallet. På Apple Watch kan kort fjernes ved hjælp af iCloud-indstillinger eller appen Apple Watch på iPhone. De kan også fjernes direkte på uret. Muligheden for at foretage betalinger ved hjælp af kort på enheden bliver spærret eller fjernet fra Apple Pay af kortudstederen eller det relevante betalingsnetværk. Dette gælder også, hvis enheden er offline og ikke har forbindelse til et mobil- eller Wi-Fi-netværk. Brugere kan også kontakte kortudstederen for at få kort spærret eller fjernet fra Apple Pay.

Hvis en bruger sletter hele enheden ved at bruge Slet alt indhold og alle indstillinger eller bruger Find eller gendanner sin enhed med gendannelsesfunktionen, får Secure Element besked på at markere alle kort som slettet på iPhone, iPad, iPod touch, Mac og Apple Watch. Det bevirker, at alle kort straks markeres som ubrugelige, indtil Apple Pay-serverne kan kontaktes for at få slettet kortene fuldstændigt fra Secure Element. Samtidig markerer Secure Enclave AR-værdien som ugyldig, så der ikke kan foretages nye betalingsgodkendelser for tidligere tilmeldte kort. Når enheden er online, prøver den at kontakte Apple Pay-serverne for at være med til at sikre, at alle kort i Secure Element er slettet.

Apple Card-sikkerhed

På understøttede modeller af iPhone og Mac kan en bruger ansøge om et Apple Card på en sikker måde.

Ansøgning om Apple Card

I iOS 12.4 og nyere versioner, macOS 10.14.6 og nyere versioner og watchOS 5.3 og nyere versioner kan Apple Card bruges sammen med Apple Pay til at foretage køb i butikker, i apps og på internettet.

For at kunne anmode om et Apple Card skal brugeren være logget ind på sin iCloud-konto på en iOS- eller iPadOS-enhed med Apple Pay, og tofaktorgodkendelse skal være indstillet på iCloud-kontoen. Når ansøgningen er godkendt, er Apple Card tilgængeligt i Apple Wallet eller i Indstillinger > Wallet & Apple Pay på alle de enheder, hvor brugeren er logget ind med sit Apple-id.

Når en bruger ansøger om et Apple Card, bliver vedkommendes identitet kontrolleret på en sikker måde af Apples identitetsudbyderpartnere og derefter delt med Goldman Sachs Bank i USA med henblik på identitetsbekræftelse og kreditvurdering.

Oplysninger som cpr-nummer eller et billede af brugerens id-kort, som afleveres i ansøgningsprocessen, bliver overført på en sikker måde til Apples identitetsudbyderpartnere og/eller Goldman Sachs Bank i USA krypteret med disses respektive nøgler. Apple kan ikke dekryptere disse data.

De oplysninger, der gives i forbindelse med ansøgningen, og de bankkontooplysninger, der bruges til betaling, bliver overført på en sikker måde til Goldman Sachs Bank USA krypteret med deres nøgle. Bankkontooplysningerne bliver gemt i nøgleringen. Apple kan ikke dekryptere disse data.

Når Apple Card føjes til Apple Wallet, kan de samme oplysninger, som en bruger afgiver i forbindelse med tilføjelse af et kredit- eller debetkort, blive delt med Apples partnerbank Goldman Sachs Bank i USA og med Apple Payments Inc. Oplysningerne bruges udelukkende til fejlfinding, forebyggelse af bedrageri og lovgivningsmæssige formål.

I iOS 14.6 og nyere versioner, iPadOS 14.6 og nyere versioner og watchOS 7.5 og nyere versioner kan den ansvarlige for en iCloud-familie med et Apple Card dele kortet med medlemmer af sin iCloud-familie, der er over 13 år. Brugeren skal godkendes for at acceptere invitationen. Apple Wallet bruger en nøgle i Secure Enclave til at danne en signatur, der forbinder ejeren og den inviterede. Signaturen valideres på Apples servere.

Den ansvarlige for familien har mulighed for at indstille en transaktionsgrænse for medlemmerne. Medlemmers kort kan altid låses via Apple Wallet for at sætte deres forbrug på pause. Når et medlem over 18 år eller en anden ejer accepterer invitationen og ansøger, gennemgår vedkommende samme ansøgningsproces som den, der er defineret i afsnittet om ansøgning om Apple Card under Apple Wallet.

Brug af Apple Card

Der kan bestilles et fysisk kort fra Apple Card i Apple Wallet. Når brugeren har modtaget det fysiske kort, gøres kortet aktivt ved hjælp af det NFC-mærke, der følger med det fysiske kort i den dobbelte kuvert. Mærket er unikt for hvert kort og kan ikke bruges til at aktivere en anden brugers kort. Kortet kan også aktiveres manuelt i indstillingerne til Apple Wallet. Desuden kan brugeren når som helst vælge at låse det fysiske kort op eller lukke det i Apple Wallet.

Betalinger med Apple Card og detaljer om kundekort i Apple Wallet

Betalinger, der er forfaldne fra Apple Card-kontoen, kan betales i Apple Wallet i iOS med Apple Cash og en bankkonto. Betaling af regninger kan planlægges som tilbagevendende eller som en engangsbetaling på en specifik dato med Apple Cash og en bankkonto. Når en bruger foretager en betaling, foretages der et opkald til Apple Pay-serverne for at rekvirere en kryptografisk nonce-værdi, som ligner den, der bruges i Apple Cash. Sammen med betalingsoplysningerne overføres nonce-værdien til Secure Element for at få beregnet en signatur. Signaturen sendes derefter tilbage til Apple Pay-serverne. Betalingens ægthed, integritet og korrekthed bliver bekræftet gennem signaturen og nonce-værdien af Apple Pay-serverne, og ordren sendes videre til Goldman Sachs Bank USA til behandling.

Apple Wallet henter Apple Card-nummeret ved at fremvise et certifikat. Apple Pay-serveren kontrollerer certifikatet for at sikre, at nøglen er blevet genereret i Secure Enclave. Den bruger derefter nøglen til at kryptere Apple Card-nummeret, før det sendes tilbage til Apple Wallet, så kun den iPhone, der har anmodet om Apple Card-nummeret, kan dekryptere det. Efter dekrypteringen gemmes Apple Card-nummeret i iCloud-nøglering.

Det kræver brugergodkendelse med Face ID, Touch ID eller en kode at få vist Apple Card-oplysningerne på kortet ved brug af Apple Wallet. Det kan erstattes af brugeren i afsnittet om kortoplysninger, hvorved det tidligere kort bliver slået fra.

Avanceret beskyttelse mod svindel

I iOS 15 og nyere versioner og iPadOS 15 og nyere versioner kan Apple Card-brugeren slå Avanceret beskyttelse mod svindel til i Apple Wallet. Når det er slået til, opdateres sikkerhedskoden til kort med et par dages mellemrum.

Apple Cash-sikkerhed

I iOS 11.2 og nyere versioner, iPadOS 13.1 og nyere versioner og watchOS 4.2 og nyere versioner kan Apple Pay bruges på en iPhone eller iPad eller et Apple Watch til at sende, modtage og anmode om penge fra andre brugere. Når en bruger modtager penge, føjes de til en Apple Cash-konto, som brugeren har adgang til i Apple Wallet eller i Indstillinger > Wallet & Apple Pay på alle de enheder, hvor Apple Cash er slået til, og hvor brugeren er logget ind med sit Apple-id.

I iOS 14, iPadOS 14 og watchOS 7 kan den ansvarlige for en iCloud-familie, som har bekræftet sin identitet med Apple Cash, slå Apple Cash til for familiemedlemmer, der ikke er fyldt 18 år. Den ansvarlige for familien kan også begrænse funktionerne for disse brugere, så de ikke kan sende penge til andre end familiemedlemmer eller kontakter. Hvis et familiemedlem, som er under 18, udfører en gendannelse af sin Apple-id-konto, skal den ansvarlige for familien manuelt slå Apple Cash-kortet til igen for denne bruger. Hvis et familiemedlem, som er under 18, ikke længere indgår i iCloud-familien, overføres deres Apple Cash-saldo automatisk til kontoen tilhørende den ansvarlige for familien.

Når brugeren indstiller Apple Cash, kan de samme oplysninger, som når brugeren tilføjer et kredit- eller debetkort, blive delt med vores partnerbank Green Dot Bank og med Apple Payments Inc., som er et 100 % ejet datterselskab, der er oprettet for at beskytte brugerens anonymitet ved at opbevare og behandle oplysninger isoleret fra resten af Apple på en måde, som resten af Apple ikke kender til. Oplysningerne bruges udelukkende til fejlfinding, forebyggelse af bedrageri og lovgivningsmæssige formål.

Brug af Apple Cash i iMessage

Brugere, der vil benytte betalinger til og fra andre personer og Apple Cash, skal være logget ind på deres iCloud-konto på en enhed, der er kompatibel med Apple Cash, og tofaktorgodkendelse skal være indstillet på iCloud-kontoen. Anmodninger om og overførsler af penge mellem brugere startes fra appen Beskeder eller ved hjælp af Siri. Når en bruger vil sende penge, viser iMessage Apple Pay-arket. Apple Cash-saldoen bruges altid først. Er der brug for flere midler, opkræves de fra et andet kredit- eller debetkort, som brugeren har føjet til Apple Wallet.

Brug af Apple Cash i butikker, i apps og på internettet

Apple Cash-kortet i Apple Wallet kan bruges sammen med Apple Pay til at betale i butikker, i apps og på internettet. Penge på Apple Cash-kontoen kan også overføres til en bankkonto. Penge, der modtages fra en anden bruger, indsættes på Apple Cash-kontoen, og brugeren kan også selv indsætte penge fra et debetkort eller et forudbetalt kort i Apple Wallet.

Når en transaktion er gennemført, opbevarer Apple Payments Inc. brugerens transaktionsdata og kan bruge dem med henblik på fejlfinding, forebyggelse af bedrageri og opfyldelse af lovgivningsmæssige krav. Resten af Apple ved ikke, hvem brugeren har sendt penge til eller modtaget penge fra, eller hvor brugeren har foretaget et køb med sit Apple Cash-kort.

Når brugeren sender penge med Apple Pay, sætter penge ind på en Apple Cash-konto eller overfører penge til en bankkonto, foretages der et kald til Apple Pay-serverne for at rekvirere en kryptografisk nonce-værdi, som ligner den værdi, der returneres for Apple Pay i apps. Sammen med andre transaktionsdata overføres nonce-værdien til Secure Element for at få beregnet en betalingssignatur. Signaturen sendes tilbage til Apple Pay-serverne. Apple Pay-serverne kontrollerer transaktionens ægthed, integritet og korrekthed via betalingssignaturen og nonce-værdien. Pengeoverførslen startes derefter, og brugeren får besked om, at transaktionen er gennemført.

Hvis transaktionen omfatter:

- et debetkort for at føje penge til Apple Cash
- at der tilføjes flere penge, hvis Apple Cash-saldoen ikke rækker

dannes der også krypterede godkendelsesoplysninger, som sendes til Apple Pay-servere, svarende til den måde, Apple Pay fungerer på i apps og på websteder.

Hvis saldoen på Apple Cash-kontoen overstiger et bestemt beløb, eller hvis der registreres unormal aktivitet, bliver brugeren bedt om at bekræfte sin identitet. Oplysninger, der skal bekræfte brugerens identitet, f.eks. cpr-nummer eller svar på spørgsmål (eksempelvis navnet på den vej, brugeren tidligere har boet på), sendes på en sikker måde til Apple-partneren og krypteres med partnerens nøgle. Apple kan ikke dekryptere disse data. Brugeren bliver bedt om at bekræfte sin identitet igen, hvis vedkommende udfører en gendannelse af sin Apple-id-konto, inden der er givet adgang til Apple Cash-saldoen igen.

Sikkerhed ved Betal med et tryk på iPhone

Betal med et tryk på iPhone, der findes i iOS 15.4, giver butikker i USA mulighed for at acceptere Apple Pay-betalinger og andre kontaktløse betalinger, der foretages med en iPhone og en partnerunderstøttet iOS-app. Med denne tjeneste kan brugere med understøttede iPhone-enheder acceptere kontaktløse betalinger og NFC-kompatible *Apple Pay*-kort på en sikker måde. Med Betal med et tryk på iPhone behøver butikker ikke ekstra hardware for at acceptere kontaktløse betalinger.

Betal med et tryk på iPhone Apple Pay er designet, så det beskytter betalerens personlige oplysninger. Tjenesten indsamler ingen transaktionsoplysninger, der kan spores tilbage til betaleren. Oplysningerne på betalingskortet, f.eks. nummeret på kredit-/debetkortet, beskyttes af Secure Element og er ikke tilgængelige for butikken. Oplysningerne på betalingskortet udveksles kun mellem butikkens betalingstjenesteudbyder, betaleren og kortudstederen. Betal med et tryk indsamler heller ikke betalerens navn, adresse eller telefonnummer.

Betal med et tryk på iPhone er blevet vurderet eksternt af et anerkendt sikkerhedslaboratorium og godkendt af American Express, Discover, Mastercard og Visa.

Komponentsikkerhed ved kontaktløse betalinger

- *Secure Element:* Secure Element indeholder de betalingskerner, som læser og beskytter data på kort til kontaktløs betaling.
- *NFC-kontrolenhed:* NFC-kontrolenheden håndterer NFC-protokoller (Near Field Communication) og dirigerer kommunikationen mellem app-processoren og Secure Element og mellem Secure Element og kortet til kontaktløs betaling.
- *Betal med et tryk på iPhone-servere:* Betal med et tryk på iPhone-serverne håndterer indstilling og tilknytning af betalingskernerne på enheden. Serverne overvåger også sikkerheden for Betal med et tryk på iPhone-enheder på en måde, der er kompatibel med CPOC-standarden (Contactless Payments on COTS) fra PCI SSC (Payment Card Industry Security Standards Council) og overholder PCI DSS.

Sådan læses kreditkort, debetkort og forudbetalte kort af Betal med et tryk

Oversigt over sikkerhed ved tilknytning

Ved første brug af Betal med et tryk på iPhone fra en app med tilstrækkelige rettigheder fastlægger Betal med et tryk på iPhone-serveren, om enheden opfylder kvalifikationskriterierne, f.eks. enhedens model, iOS-version og indstillet kode. Når kontrollen er gennemført, hentes miniappen til betalingsaccept fra Betal med et tryk på iPhone-serveren og installeres i Secure Element sammen med den tilhørende konfiguration af betalingskernen. Handlingen foretages på en sikker måde mellem Betal med et tryk på iPhone-serverne og Secure Element. Secure Element kontrollerer disse datas integritet og ægthed forud for installeringen.

Oversigt over sikkerheden ved læsning kort

Når appen Betal med et tryk på iPhone anmoder om en kortlæsning fra ProximityReader-framework, vises et ark, som styres af iOS, og brugeren bliver bedt om at trykke på et betalingskort. iOS initialiserer betalingskortlæseren og anmoder derefter betalingskernerne i Secure Element om at starte en kortlæsning.

På dette tidspunkt overtager Secure Element kontrollen over NFC-kontrolenheden i læsertilstand. I denne tilstand kan der kun udveksles kortdata mellem betalingskortet og Secure Element via NFC-kontrolenheden. Betalingskort kan kun læses i denne tilstand.

Når miniappen til betalingsaccept i Secure Element har gennemført kortlæsningen, krypterer og signerer den kortets data. Kortets data forbliver krypterede og godkendte, indtil de når frem til betalingstjenesteudbyderen. Det er kun den betalingstjenesteudbyder, som appen bruger til at anmode om kortlæsningen, der kan dekryptere kortets data. Betalingstjenesteudbyderen skal anmode om krypteringsnøglen fra Betal med et tryk på iPhone-serveren. Betal med et tryk på iPhone-serveren udsteder dekrypteringsnøgler til betalingstjenesteudbyderen efter at have kontrolleret dataenes integritet og ægthed og efter at have bekræftet, at kortlæsningen blev foretaget inden for 60 sekunder fra kortlæsningen på enheden.

Denne model er med til at sikre, at kortets data ikke kan dekrypteres af andre end den betalingstjenesteudbyder, som behandler transaktionen for butikken.

Brug af Apple Wallet

Adgang via Apple Wallet

I Apple Wallet på understøttede iPhone- og Apple Watch-enheder kan brugerne opbevare nøgler til deres hjem, bil og hotelværelse. De kan tilmed opbevare personalekort og studiekort. Når en bruger står foran en dør, præsenteres det rigtige kort automatisk, så brugeren med et enkelt tryk ved hjælp af NFC (Near Field Communication) kan åbne døren.

Brugervenlighed

Når en nøgle, et adgangskort, et studiekort eller et personalekort føjes til Apple Wallet, bliver Ekspresfunktion som standard slået til. Kort med Ekspresfunktion slået til interagerer med understøttende terminaler uden brug af Face ID, Touch ID, kode eller to tryk på sideknappen på Apple Watch. Brugerne kan slå Ekspresfunktion fra ved at trykke på knappen Mere på forsiden af kortet i Apple Wallet. Hvis de vil slå Ekspresfunktion til igen, skal de bruge Face ID, Touch ID eller en kode.

Anonymitet og sikkerhed

Nøgler i Apple Wallet udnytter den anonymitet og sikkerhed, der er indbygget i iPhone og Apple Watch, fuldt ud. Hvornår eller hvor en person bruger sine nøgler i Apple Wallet deles aldrig med Apple og opbevares aldrig på Apples servere, og godkendelsesoplysninger opbevares sikkert i understøttede enheders Secure Element (SE). SE råder over specialdesignede miniapps, der administrerer og opbevarer adgangsnøgler sikkert, og sikrer dermed, at nøglerne ikke kan hentes frem.

Inden tilknytning af adgangsnøgler skal en bruger logge ind på sin iCloud-konto på en kompatibel iPhone og have slået tofaktorgodkendelse til for sin iCloud-konto. Med studiekort behøver tofaktorgodkendelse ikke at være slået til.

Når en bruger indleder tilknytningsprocessen, gennemføres stort set samme trin som ved tilknytning af kredit- og debetkort, f.eks. forbind og tilknyt. Under en transaktion kommunikerer læseren med Secure Element via NFC-kontrolenheden (Near Field Communication) gennem en etableret sikker kanal.

Antallet af enheder, herunder iPhone og Apple Watch, der kan forsynes med en adgangsnøgle, defineres og styres af hver partner og kan svinge fra partner til partner. Det betyder, at hver partner kan bestemme det maksimale antal tilknyttede adgangsnøgler pr. enhedstype efter sit behov. Apple forsyner partnere med enhedstypen og anonymiserede enheds-id'er til dette formål. Af hensyn til anonymiteten og sikkerheden er id'erne til hver partner forskellige.

Nøgler kan slås fra eller fjernes ved at:

- Slette enheden eksternt med Find
- Slå Mistet til i Find
- Modtage en kommando til ekstern sletning fra administration af mobile enheder (MDM)
- Fjerne alle kort fra kontosiden i deres Apple-id
- Fjerne alle kort fra iCloud.com
- Fjerne alle kort fra Apple Wallet
- Fjerne kortet i udstederens app

Hvis en bruger med iOS 15.4 eller en nyere version trykker to gange på sideknappen på en iPhone med Face ID eller to gange på knappen Hjem på en iPhone med Touch ID, vises først oplysninger om brugerens kort og adgangsnøgler, efter brugeren er blevet godkendt på enheden. Der kræves godkendelse med Face ID, Touch ID eller kode, før kortspecifikke oplysninger, f.eks. om en hotelreservation, vises i Apple Wallet.

Typer af adgangsgodkendelse

Der er forskellige typer adgang fra Apple Wallet, f.eks. overnatningssteder, personalekort, studiekort, nøgler til hjemmet og bilnøgler.

Overnatningssteder

Med nøgler til hotelværelser i Apple Wallet får gæster en bekvem og kontaktløs oplevelse lige fra indtjekning til udtjekning og opnår samtidig øget anonymitet og sikkerhed i forhold til traditionelle hotelnøglekort af plastic. Hotelgæster på understøttede lokaliteter kan trykke for at låse op med værelsesnøglen i Apple Wallet på deres kompatible iPhone eller Apple Watch Series 4 og nyere modeller.

Funktionerne i Apple Wallet er designet til at spare kunden for besvær:

- Tilknytning af et kort fra hotellets app før ankomsten, så kortet kan føjes til Apple Wallet inden et ophold
- Kortsegmenter til indtjekning med henblik på at starte indtjekning og værelsestildeling fra Apple Wallet
- Opdatering af nøgler efter tilknytning for at gøre det muligt at ændre eller forlænge opholdet
- Understøttelse af flere nøgler til et enkelt kort i Apple Wallet
- Automatisk arkivering af udløbne nøgler i Apple Wallet

Personalekort

Medarbejderkort fra understøttede partnere kan føjes til Apple Wallet på iPhone og Apple Watch, så medarbejdere i hele verden kan få kontaktløs adgang til deres arbejdssted. En medarbejder, der vil tilføje et kort, skal have slået multifaktorgodkendelse til på den konto, medarbejderen bruger til at logge ind i den app, som arbejdsgiveren har stillet til rådighed.

Medarbejderkort udnytter Apples adgangsfunktioner og giver brugerne følgende muligheder:

- Automatisk føje et medarbejderkort til deres parrede Apple Watch via videreført tilknytning, der ikke kræver installering af en partners app
- Problemfri adgang til kontorfaciliteter ved brug af Ekspresfunktion
- Adgang til arbejdsstedet, selvom deres iPhone løber tør for strøm

Studiekort

I iOS 12 og nyere versioner kan studerende, lærerstaben og personale på deltagende uddannelsesinstitutioner føje deres studiekort til Apple Wallet på understøttede iPhone-modeller og Apple Watch for at få adgang til lokaliteter og foretage betalinger, hvor kortet accepteres.

En bruger føjer sit studiekort til Apple Wallet via en app, som kortudstederen eller den deltagende uddannelsesinstitution har stillet til rådighed. Den tekniske proces for dette er den samme som beskrevet tidligere i Tilføjelse af kredit- eller debetkort fra en kortudsteders app. Derudover skal de udstedte apps understøtte tofaktorgodkendelse for de konti, der beskytter adgangen til deres studiekort. Et kort kan indstilles samtidig på op til to understøttede Apple-enheder, der er logget ind med det samme Apple-id.

Flerfamilieboliger

Lejere og personale på understøttede partnerfaciliteter kan bruge deres nøgle til hjemmet i Apple Wallet til at få adgang til bygningen, deres boligenhed og fællesarealer. Nøglen til hjemmet kan tilknyttes i den app, som partneren stiller til rådighed. Ejendomsadministratorer, som bruger partnere, der understøtter problemfri tilknytning, kan sende et link til deres lejere via deres foretrukne beskedkanal (f.eks. e-mail eller sms), så lejerne kun behøver at klikke på linket for at indløse nøglen. En anden sikker og nem metode er app-klip, der gør det muligt at tilknytte en nøgle uden at installere en partners app. Du kan få flere oplysninger i Apple-supportartiklen Brug app-klip på iPhone.

Nøgle til hjemmet

En nøgle til hjemmet i Apple Wallet kan bruges sammen med NFC-kompatible dørlåse med et enkelt tryk på en iPhone eller et Apple Watch. Du kan læse mere om, hvordan en bruger kan indstille og bruge en nøgle til hjemmet, i Apple-supportartiklen Lås døren op med en nøgle til hjemmet på iPhone.

Når en bruger indstiller en nøgle til hjemmet, modtager alle husstandens medlemmer automatisk nøglen til hjemmet. Ejeren af et hjem kan dele en nøgle til hjemmet med flere eller fjerne et medlem fra et delt hjem ved at bruge appen Hjem til at administrere invitationer og medlemmer. Når en bruger vælger at acceptere en invitation til at blive medlem af et hjem med en nøgle til hjemmet, startes tilknytningen af nøglen til hjemmet i Apple Wallet på brugerens enheder. Hvis en bruger vælger at forlade et hjem, eller hvis ejeren af hjemmet trækker adgangstilladelsen tilbage, bliver brugeren og nøglen til hjemmet fjernet fra Apple Wallet.

Bilnøgle

Opbevaring af bilnøgler digitalt i Apple Wallet understøttes direkte på iPhone-enheder, som har denne funktion, og på parrede Apple Watch-enheder. Bilnøgler vises som kort (oprettet af Apple på bilproducentens vegne) i Apple Wallet og understøtter hele kortforløbet for Apple Pay (funktionen Mistet i iCloud, ekstern sletning, sletning af lokale kort og Slet alt indhold og indstillinger). Ud over standardfunktionerne til kortadministration i Apple Pay kan delte bilnøgler slettes fra ejerens iPhone, ejerens Apple Watch og i bilens HMI-brugerflade (Human Machine Interface).

Bilnøgler kan bruges til at låse bilen og låse den op, starte motoren eller sætte den i køreklar tilstand. "Standardtransaktionen" indebærer gensidig godkendelse og er nødvendig, før motoren kan startes. Transaktionerne lås og lås op kan bruge en "hurtig transaktion" ved behov af hensyn til ydeevnen.

Nøglerne oprettes ved parring af en iPhone med en bil, der ejes af brugeren og understøtter funktionen. Alle nøgler oprettes i det integrerede Secure Element, baseret på elliptisk kurvegenerering (NIST P-256) af nøgle på enheden (ECC-OBKG), og de private nøgler forlader aldrig Secure Element. Kommunikationen mellem enheder og bil bruger enten NFC eller en kombination af Bluetooth LE og UWB, og nøgleadministrationen bruger et API mellem Apple og bilproducentens server med TLS med gensidig godkendelse. Når en nøgle er parret med en iPhone, kan ethvert Apple Watch, der er parret med den pågældende iPhone, også modtage en nøgle. En nøgle, der slettes i bilen eller på enheden, kan ikke gendannes. Nøgler på mistede eller stjålne enheder kan suspenderes og tages i brug igen, men brug af dem på en ny enhed kræver fornyet parring eller deling.

Sikkerhed i forbindelse med bilnøgler i iOS

Udviklere kan understøtte sikre nøglefri måder at åbne en bil på fra en understøttet iPhone og et parret Apple Watch.

Pardannelse med ejerens enhed

Ejeren skal fremlægge bevis for ejerskab af bilen (metoden afhænger af bilproducenten) og kan så starte pardannelsesprocessen ved at bruge bilproducentens app via et link i en e-mail, som ejeren modtager fra bilproducenten, eller via bilens menu. I alle tilfælde skal ejeren tilføre sin iPhone en fortrolig engangsadgangskode til pardannelse, som bruges til at oprette en sikker kanal til pardannelse via protokollen SPAKE2+ med NIST P-256-kurven. Når appen eller linket i e-mailen bruges, overføres adgangskoden automatisk til iPhone, hvor den skal indtastes manuelt, når pardannelsen startes fra bilen.

Deling af nøgler

Ejerens parrede iPhone kan dele nøgler med familiemedlemmers og venners iPhone-enheder, hvis de har denne funktion (og med deres parrede Apple Watch-enheder), ved at sende en enhedsspecifik invitation via iMessage og IDS (Apple Identity Service). Alle kommandoer om deling udveksles via IDS-funktionen, der er end-to-end-krypteret. Ejerens parrede iPhone sørger for, at IDS-kanalen ikke skifter under delingsprocessen. Det sker for at forhindre videresendelse af invitationen.

Når et familiemedlem eller en ven accepterer invitationen, opretter denne persons iPhone en digital nøgle og sender certifikatkæden for nøgleoprettelse tilbage til ejerens parrede iPhone for at bekræfte, at nøglen blev oprettet på en ægte Apple-enhed. Ejerens parrede iPhone signerer den offentlige ECC-nøgle modtaget fra den iPhone, der tilhører familiemedlemmet eller vennen, og sender signaturen tilbage til denne persons iPhone. Signeringsfunktionen på ejerens enhed kræver brugergodkendelse (Face ID, Touch ID eller indtastning af kode) og en sikker hensigt fra brugerens side som beskrevet i Anvendelsesmuligheder for Face ID og Touch ID. Der anmodes om godkendelse, når invitationen sendes, og godkendelsen opbevares i Secure Element til brug, når vennens enhed sender signeringsanmodningen tilbage. Nøgletilladelserne overføres online til bilen af bilens OEM-server, eller når den delte nøgle bruges første gang til bilen.

Sletning af nøgler

Nøgler kan slettes på nøgleindehaverens enhed fra ejerens enhed eller i bilen. Sletning på nøgleindehaverens iPhone træder straks i kraft, også selvom nøgleindehaveren bruger nøglen. Der vises derefter en kraftig advarsel før sletningen. Sletning af nøgler i bilen kan være muligt på alle tidspunkter, eller kun når bilen er online.

I begge tilfælde rapporteres sletningen på nøgleindehaverens enhed eller i bilen til en nøgleopbevaringsserver hos bilproducenten, som registrerer udstedte nøgler til en bil til forsikringsformål.

Ejeren kan anmode om sletning fra bagsiden af ejerpasset. Anmodningen sendes først til bilproducenten for at fjerne nøglen i bilen. Betingelserne for, at nøglen kan fjernes fra bilen, er defineret af bilproducenten. Først når nøglen er fjernet i bilen, sender bilproducenten en ekstern anmodning om ophør til nøgleindehaverens enhed.

Når en nøgle er bragt til ophør i en enhed, opretter den miniapp, som administrerer digitale bilnøgler, en kryptografisk signeret ophørsattest, som bruges som bevis for sletningen af bilproducenten og til at fjerne nøglen fra nøgleopbevaringsserveren.

NFC-standardtransaktioner

Ved biler, der bruger en NFC-nøgle, indledes etableringen en sikker kanal mellem læseren og en iPhone ved, at der genereres et midlertidigt nøglepar på læseren og iPhone. Ved hjælp af en nøgleaftalemetode kan der dannes en nøgle (“shared secret”) på begge sider, som kan bruges til at generere en delt symmetrisk nøgle ved brug af Diffie-Hellman, en funktion til nøgleafledning og signaturer fra den langtidsholdbare nøgle, der blev fastlagt under pardannelsen.

Den midlertidige offentlige nøgle, der blev genereret på bilens side, signeres med læserens langtidsholdbare private nøgle, og resultatet er, at læseren godkendes af iPhone-enheden. Fra iPhone-enhedens perspektiv har denne protokol til formål at forhindre, at data, der hører privatlivet til, kan ses af en hacker, der opsnapper kommunikationen.

Til sidst bruger iPhone den etablerede sikre kanal til at kryptere sit offentlige nøgle-id sammen med den signatur, der er beregnet ud fra en læsers dataafledte udfordring og nogle ekstra app-specifikke data. Denne validering af iPhone-enhedens signatur fra læserens side sætter læseren i stand til at godkende enheden.

Hurtige transaktioner

iPhone genererer et kryptogram ud fra en hemmelighed, der tidligere er blevet delt under en standardtransaktion. Dette kryptogram giver bilen mulighed for hurtigt at godkende enheden i situationer, hvor ydeevnen er vigtig. Der kan desuden etableres en sikker kanal mellem bilen og enheden, ved at der afledes sessionsnøgler ud fra en hemmelighed, der tidligere er blevet delt under en standardtransaktion, og et nyt midlertidigt nøglepar. Bilens evne til at etablere den sikre kanal godkender bilen over for iPhone.

BLE/UWB-standardtransaktioner

Til biler, der bruger en UWB-nøgle, etableres en Bluetooth LE-session mellem bilen og iPhone. I lighed med NFC-transaktionen udledes en nøgle (shared secret) på begge sider, som bruges til at etablere en sikker session. Sessionen bruges derefter til at udlede og blive enige om en URSK-nøgle (UWB Ranging Secret Key). URSK overføres til UWB-radioen i brugerens enhed og i bilen med henblik på at fastlægge den præcise placering af brugerens enhed i nærheden af eller i bilen. Bilen bruger derefter enhedens placering til at tillade, om bilen må låses op eller startes. URSK'er har en foruddefineret TTL. Med henblik på at undgå afbrydelse af placeringssporing, når en TTL udløber, kan URSK'er udledes på forhånd i enhedens SE og bilens HSM/SE, mens sikker placeringssporing ikke er aktiv, men BLE er tilsluttet. Det fjerner behovet for, at en standardtransaktion skal udlede en ny URSK i en situation, hvor tiden er kritisk. Den URSK, der er udledt på forhånd, kan meget hurtigt overføres til UWB-radioen i bilen og på enheden for at undgå afbrydelse af UWB-placeringssporingen.

Anonymitet

Bilproducentens nøgleopbevaringsserver (KIS) opbevarer ikke enhedens id, SEID eller Apple-id. Den opbevarer kun et id, der kan ændres – certifikatmyndighedens instans-id. Dette id er ikke knyttet til nogen private data i enheden eller på serveren, og det slettes, når brugeren sletter sin enhed helt (ved at bruge Slet alt indhold og alle indstillinger).

Tilføjelse af rejsekort og eMoney-kort i Apple Wallet

Mange steder i verden kan brugere føje understøttede rejsekort og eMoney-kort til Apple Wallet på understøttede modeller af iPhone og Apple Watch. Afhængigt af operatøren kan det gøres ved enten at overføre værdien eller kortet (eller begge dele) fra et fysisk kort til kortets digitale repræsentation i Apple Wallet eller ved at tilknytte et nyt rejsekort eller eMoney-kort fra Apple Wallet eller kortudstederens app. Når rejsekort er føjet til Apple Wallet, kan brugerne benytte offentlige transportmidler ved at holde deres iPhone eller Apple Watch op mod kortlæserne. Nogle rejsekort kan også bruges til at foretage betalinger.

Sådan fungerer rejsekort og eMoney-kort

Tilføjede rejsekort og eMoney-kort er knyttet til en brugers iCloud-konto. Hvis en bruger føjer mere end et kort til Apple Wallet, kan Apple eller kortudstederen måske koble brugerens personlige oplysninger og de tilhørende kontooplysninger til flere kort. Rejsekort og eMoney-kort og transaktioner beskyttes med et sæt hierarkiske kryptografiske nøgler.

Når saldoen på et fysisk kort skal overføres til Apple Wallet, skal brugerne indtaste kortspecifikke oplysninger. Brugerne skal muligvis angive personlige oplysninger som bevis på, at kortet er i deres besiddelse. Når der overføres kort fra iPhone til Apple Watch, skal begge enheder have forbindelse til internettet.

Brugerne kan forøge saldoen ved at tanke op fra kreditkort, debetkort eller forudbetalte kort via Apple Wallet eller rejsekort- eller eMoney-kortudstederens app. Sikkerheden i forbindelse med optankning ved hjælp af Apple Pay er beskrevet i Betaling med kort i apps. Du kan læse, hvordan kortet tilknyttes fra kortudstederens app, i Tilføjelse af kredit- eller debetkort fra en kortudsteders app.

Hvis tilknytning af et fysisk kort understøttes, har udstederen af rejsekortet eller eMoney-kortet de kryptografiske nøgler, der kræves for at godkende det fysiske kort og bekræfte brugerens indtastede data. Når data er bekræftet, kan systemet oprette et kontonummer til enheden til Secure Element og aktivere det netop tilføjede kort i Apple Wallet med den overførte saldo. I nogle tilfælde bliver det fysiske kort inaktivt, når tilknytningen af det fysiske kort er gennemført.

Efter tilknytningen – uanset typen – krypteres saldoen på kortet, hvis den opbevares på enheden, og gemmes af en specifik miniapp i Secure Element. Operatøren har de nøgler, der skal bruges til at udføre kryptografiske funktioner på kortets data i forbindelse med saldotransaktioner.

Brugere af rejsekort har som standard mulighed for ekspresbetaling uden brug af Face ID, Touch ID eller en kode, når de benytter offentlig transport. Oplysninger som senest besøgte stationer, transaktionshistorik og ekstra billetter kan hentes af alle kontaktløse kortlæsere i nærheden, når Ekspresfunktion er slået til. Brugerne kan slå krav om godkendelse med Face ID, Touch ID eller kode til ved at slå Ekspresrejse fra i Wallet & Apple Pay. Ekspresfunktion understøttes ikke til eMoney-kort.

I lighed med andre Apple Pay-kort kan brugerne spærre eller fjerne eMoney-kort ved at:

- Slette enheden eksternt med Find
- Slå Mistet til i Find
- Bruge en kommando til ekstern sletning fra administration af mobile enheder (MDM)
- Fjerne alle kort fra kontosiden i deres Apple-id
- Fjerne alle kort fra iCloud.com
- Fjerne alle kort fra Apple Wallet
- Fjerne kortet i udstederens app

Apple Pay-servere giver kortoperatøren besked på at spærre eller slå de pågældende kort fra. Hvis en bruger fjerner et rejsekort eller et eMoney-kort fra en onlineenhed, kan saldoen overføres, hvis kortet tilføjes på en enhed, der er logget ind med samme Apple-id. Hvis en enhed er offline, slukket eller ubrugelig, kan overførsel muligvis ikke finde sted.

Tilføjelse af rejsekort og eMoney-kort til et familiemedlems Apple Watch

I iOS 15 og watchOS 8 kan den ansvarlige for en iCloud-familie føje rejsekort og eMoney-kort til sine familiemedlemmers Apple Watch-enheder fra appen Apple Watch på sin iPhone. Når et af disse kort skal tilknyttes et familiemedlems Apple Watch, skal uret være i nærheden og have forbindelse til den ansvarliges iPhone via Wi-Fi eller Bluetooth. Desuden skal familiemedlemmerne have slået tofaktorgodkendelse til for deres Apple-id.

Familiemedlemmer kan sende en anmodning om at overføre penge til et rejsekort eller eMoney-kort fra deres Apple Watch via iMessage. Indholdet af beskeden beskyttes med kryptering hele vejen fra afsender til modtager som beskrevet i Oversigt over iMessage-sikkerhed. Der kan overføres penge til et kort på et familiemedlems Apple Watch via en forbindelse til et Wi-Fi-netværk eller mobilnetværket. Enheden behøver ikke at være i nærheden.

Bemærk: Denne funktion er muligvis ikke tilgængelig i alle lande eller områder.

Kredit- og debetkort

I nogle byer accepterer kortlæsere EMV-kort (Smart Cards) som betalingsmiddel for rejser. Når brugerne holder et EMV-kreditkort eller -debetkort mod kortlæserne, kræves der brugergodkendelse lige som ved "Betal med kredit- og debetkort i butikker".

I iOS 12.3 og nyere versioner kan Ekspresrejse slås til for nogle eksisterende EMV-kredit-/debetkort i Apple Wallet. Med Ekspresrejse kan brugerne betale for en tur med understøttede transportoperatører uden brug af Face ID, Touch ID eller en kode. Når en bruger tilknytter et EMV-kredit- eller debetkort, bliver Ekspresrejse slået til for det første kort, der tilknyttes Apple Wallet. Brugeren kan trykke på knappen Mere på forsiden af kortet i Apple Wallet og slå Ekspresrejse fra for det pågældende kort ved at indstille Indstillinger til ekspresrejser til Ingen. Brugeren kan også vælge et andet kredit- eller debetkort som ekspresrejsekort i Apple Wallet. Der kræves Face ID, Touch ID eller en kode for at slå ekspresrejser til igen eller vælge et nyt kort.

Apple Card og Apple Cash kan bruges til ekspresrejser.

Id'er i Apple Wallet

På iPhone 8 og nyere modeller med iOS 15.4 eller en nyere version og Apple Watch Series 4 og nyere modeller med watchOS 8.4 eller en nyere version kan brugerne føje et officielt udstedt identitetskort eller deres kørekort til Apple Wallet og hurtigt og nemt præsentere kortet på understøttede steder ved at trykke på deres iPhone eller Apple Watch.

Bemærk: Funktionen kan kun bruges i stater i USA, hvor funktionen understøttes.

Identitetskort i Apple Wallet bruger sikkerhedsfunktioner, der er indbygget i hardware og software på brugerens enhed, som hjælp til at beskytte deres identitet og personlige oplysninger.

Tilføjelse af et kørekort eller et officielt udstedt identitetskort til Apple Wallet

På iPhone kan brugerne bare trykke på knappen Tilføj (+) nederst på skærmen i Apple Wallet for at begynde at tilføje deres kørekort eller identitetskort. Hvis brugerne har et Apple Watch, der er parret på indstillingstidspunktet, bliver de spurgt, om de også vil føje kørekortet eller identitetskortet til deres Apple Wallet på Apple Watch.

Brugerne bliver først bedt om at bruge deres iPhone til at scanne for- og bagsiden af deres fysiske kørekort eller officielt udstedte identitetskort. iPhone vurderer billedernes kvalitet og type for at sikre, at de kan accepteres af statens udstedelsesmyndighed. Billederne af identitetskortet krypteres mod den statslige udstedelsesmyndigheds nøgle på enheden og sendes derefter til statens udstedelsesmyndighed.

Brugeren bliver derefter bedt om at udføre en række bevægelser med ansigtet og hovedet. Bevægelserne vurderes af brugerens enhed og af Apple som hjælp til at forhindre, at nogen bruger et foto, en video eller en maske til at forsøge at føje en anden persons identitetskort til Apple Wallet. Resultaterne af analysen af bevægelserne, men ikke selve videoen af bevægelserne, sendes derefter til statens udstedelsesmyndighed.

Som led i at sikre, at identitetskortet tilhører den person, der vil føje identitetskort til Apple Wallet, bliver brugerne bedt om at tage en selfie. Inden brugerens foto sendes til statens udstedelsesmyndighed, sammenligner Apples servere og brugerens enhed fotoet med udseendet på den person, der udførte de forskellige bevægelser med ansigtet og hovedet. Det er med til at sikre, at det foto, der sendes, er af en levende person med samme udseende som på identitetskortet. Efter sammenligningen krypteres fotoet på enheden og sendes derefter til statens udstedelsesmyndighed for at blive sammenlignet med det registrerede billede til vedkommendes identitetskort.

Til sidst bliver brugerne bedt om at foretage en godkendelse med Face ID eller Touch ID. Brugerens enhed kobler den biometriske Face ID- eller Touch ID-oplysning til det officielt udstedte identitetskort for at sikre, at kun den person, der føjede identitetskortet til den pågældende iPhone, kan fremvise det. Andre tilmeldte biometriske oplysninger kan ikke bruges til at godkende fremvisning af identitetskortet. Dette sker kun på enheden, og oplysningen sendes ikke til statens udstedelsesmyndighed.

Statens udstedelsesmyndighed modtager de oplysninger, der er nødvendige for at indstille den digitale identifikation. Det omfatter billederne af for- og bagsiden af brugerens identitetskort, data læst fra PDF417-stregkoden samt den selfie, som brugeren tog som led i godkendelsesprocessen for identitetskortet. Den udstedende stat modtager også en værdi på et enkelt ciffer, der bruges til at forhindre svindel, og som er baseret på brugerens mønstre for brug af enheden, indstillingsdata og oplysninger om brugerens personlige Apple-id. I sidste ende er det den udstedende stats beslutning, om det identitetskort, der føjes til Apple Wallet, skal godkendes eller afvises.

Når statens udstedelsesmyndighed godkender, at det officielt udstedte identitetskort eller kørekortet føjes til Apple Wallet, genereres et nøglepar i Secure Element af iPhone, som kobler brugerens identitetskort til netop den enhed. Hvis det føjes til Apple Watch, genereres et nøglepar i Secure Element af Apple Watch.

Når identitetskortet er på iPhone, gemmes oplysningerne under brugerens identitetskort i Apple Wallet i krypteret format og beskyttet af Secure Enclave.

Brug af et kørekort eller et officielt udstedt identitetskort i Apple Wallet

Når brugerne vil benytte deres identitetskort i Apple Wallet, skal de godkendes på den enhed med Face ID eller Touch ID, der er knyttet til identitetskortet i Apple Wallet, før iPhone fremviser oplysningerne for id-læseren.

Når brugerne vil benytte deres identitetskort i Apple Wallet på Apple Watch, skal de låse deres iPhone op ved hjælp af det tilknyttede Face ID-udseende eller Touch ID-fingeraftryk, hver gang de tager deres Apple Watch på. Derefter kan de bruge deres identitetskort i Apple Wallet uden godkendelse, indtil de tager Apple Watch af igen. Denne mulighed udnytter de fundamentale funktioner til Automatisk oplåsning, der er beskrevet i Systemsikkerhed til watchOS.

Når brugerne holder deres iPhone eller Apple Watch op foran id-læseren, vises på enheden en meddelelse om, hvilke oplysninger der anmodes om, af hvem, og om de har til hensigt at gemme dem. Efter godkendelse med det tilknyttede Face ID eller Touch ID frigives de ønskede identitetsoplysninger fra enheden.

Vigtigt: Brugerne behøver ikke at låse deres enhed op, vise den frem eller overdrage den for at fremvise deres id.

Hvis brugerne har slået en tilgængelighedsfunktion som Stemmekontrol, Knapbetjening eller Assistive Touch til i stedet for Face ID eller Touch ID, kan de bruge deres kode til at få adgang til og fremvise deres oplysninger.

Overførslen af identitetsdata til id-læseren følger ISO/IEC 18013-5-standarden, som foreskriver, at der skal være flere sikkerhedsmekanismer til stede, som kan registrere, afværge og mindske sikkerhedsrisici. Det gælder integritet af identitetsdata, forhindring af forfalskning, sammenkædning af enheder, informeret samtykke og sikring af anonymitet i forbindelse med brugerdata via radioforbindelser.

Integritet af identitetsdata og forhindring af forfalskning

Identitetskort i Apple Wallet bruger en signatur fra udstederen til at give enhver ISO/IEC 18013-5-kompatibel læser tilladelse til at kontrollere en brugers id i Apple Wallet. Alle dataelementer i Wallet er desuden individuelt beskyttet mod forfalskning. Det sætter id-læseren i stand til at anmode om et bestemt udsnit af dataelementerne på identitetskortet i Apple Wallet og giver identitetskortet i Apple Wallet mulighed for at svare med det samme udsnit, så kun de ønskede data deles, og brugerens anonymitet beskyttes i størst muligt omfang.

Sammenkædning af enheder

Ved godkendelse af identitetskort i Apple Wallet bruges en enhedssignatur til at beskytte mod kloning af en identitet og genafspilning af en identitetstransaktion. Da den private nøgle til identitetsgodkendelse opbevares i iPhone-enhedens Secure Element, er identitetskortet kædet sammen med samme enhed, som statens udstedelsesmyndighed oprettede identitetskortet til.

Informeret samtykke

Ved godkendelse af identitetskort i Apple Wallet godkendes id-læseren ved brug af den protokol, der er defineret i ISO/IEC 18013-5-standarden. Under fremvisning vises et symbol hentet fra læserens certifikat for brugeren for at give brugeren tillid til, at interaktionen sker med den tilsigtede part.

Sikring af anonymitet i forbindelse med brugerdata via radioforbindelse

Sessionskryptering er med til at sikre, at alle oplysninger, der kan identificere en person, og som udveksles mellem identitetskortet i Apple Wallet og id-læseren, krypteres. Kryptering foretages af app-laget. Sikkerheden ved sessionskryptering afhænger dermed ikke af den sikkerhed, der implementeres af transmissionslaget (f.eks. NFC, Bluetooth og Wi-Fi).

Identitetskort i Apple Wallet er med til at forhindre, at brugernes oplysningerne kan læses af uvedkommende

Identitetskort i Apple Wallet følger den proces til hentning af enheder, der er beskrevet i ISO/IEC 18013-5. Hentning af enheder fjerner behovet for at foretage kald til en server under fremvisning og beskytter derved brugerne mod at blive sporet af Apple og udstederen.

iMessage

Oversigt over iMessage-sikkerhed

Apple iMessage er en beskedtjeneste til iOS- og iPadOS-enheder, Apple Watch og Mac-computere. iMessage understøtter tekst og bilag, f.eks. fotos, kontakter og lokaliteter, links og indbyggede bilag til beskeden, f.eks. et tommelfinger opad-symbol. Beskederne vises på alle brugerens registrerede enheder, så en samtale kan fortsættes på en anden af brugerens enheder. iMessage gør udstrakt brug af tjenesten Apple Push Notification (APNs). Apple gemmer ikke indholdet af beskeder eller bilag i en log, og indholdet er beskyttet af end-to-end-kryptering, så kun afsenderen og modtageren har adgang til det. Apple kan ikke dekryptere dataene.

Når en bruger slår iMessage til på en enhed, genererer enheden en kryptering og signerer nøglepar, der bruges sammen med tjenesten. Krypteringen foregår med en krypteret RSA 1280-bit-nøgle samt en krypteret EC 256-bit-nøgle på NIST P-256-kurven. Til signaturer bruges 256-bit signeringsnøgler af typen ECDSA (Elliptic Curve Digital Signature Algorithm). De private nøgler gemmes i enhedens nøglering og er først tilgængelige, når enheden er blevet låst op. De offentlige nøgler sendes sammen med enhedens APNs-adresse til Apple Identity Service (IDS), hvor de knyttes til brugerens telefonnummer eller e-mailadresse.

Efterhånden som brugerne slår iMessage til på flere enheder, føjes deres offentlige nøgler til kryptering og signering, APNs-adresser og tilknyttede telefonnumre til bibliotekstjenesten. Brugerne kan også tilføje flere e-mailadresser, som skal bekræftes via et bekræftelseslink. Telefonnumre bekræftes af operatørens netværk og af SIM-kortet. På nogle netværk er det nødvendigt at bruge sms (brugeren får vist en bekræftelsesdialog, hvis sms'en ikke er gratis). Flere andre systemtjenester ud over iMessage, f.eks. FaceTime og iCloud, kan kræve, at telefonnumre bekræftes. Der vises en advarsel på alle brugerens registrerede enheder, når der tilføjes en ny enhed, et nyt telefonnummer eller en ny e-mailadresse.

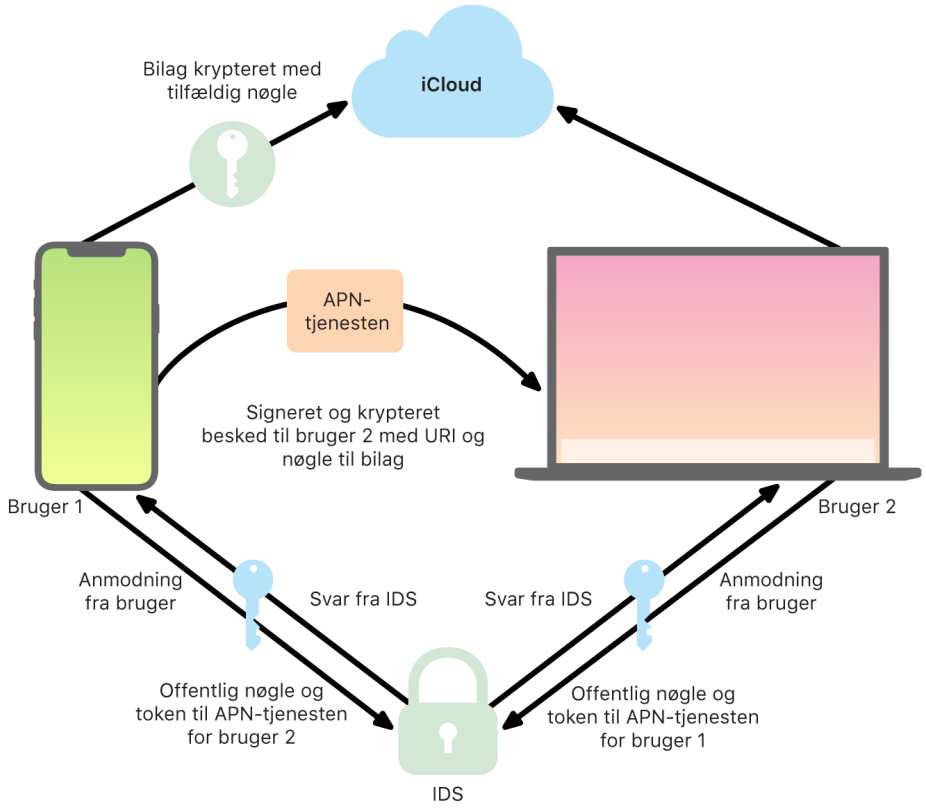
Sikker afsendelse og modtagelse af beskeder via iMessage

Brugerne starter en ny iMessage-samtale ved at skrive en adresse eller et navn. Hvis de skriver et telefonnummer eller en e-mailadresse, kontakter enheden IDS (Apple Identity Service) for at hente de offentlige nøgler og APNs-adresser til alle de enheder, der er knyttet til adressaten. Hvis brugeren skriver et navn, bruger enheden først appen Kontakter på brugerens enhed til at indsamle de telefonnumre og e-mailadresser, der er knyttet til navnet, og henter derefter de offentlige nøgler og APNs-adresserne fra IDS.

Brugerens udgående besked krypteres særskilt til hver af modtagerens enheder. Modtagerenhedernes offentlige krypterings- og signeringsnøgler hentes fra IDS. For hver modtagerenhed genererer afsenderenheden en tilfældig 88 bit værdi og bruger den som en HMAC-SHA256-nøgle til at danne en værdi på 40 bit ud fra afsenderens og modtagerens offentlige nøgle og den almindelige tekst. Sammenkædningen af værdierne på 88 bit og 40 bit giver en nøgle på 128 bit, som beskeden krypteres med ved hjælp af AES med tællerfunktion (CTR). Værdien på 40 bit bruges på modtagersiden til at bekræfte, at den dekrypterede almindelige tekst ikke er blevet ændret. AES-nøglen til hver besked krypteres, ved at RSA-OAEP bruges til modtagerenhedens offentlige nøgle. Kombinationen af den krypterede beskedtekst og den krypterede beskednøgle hash-behandles derefter med SHA-1, hvorefter hash-værdien signeres med ECDSA (Elliptic Curve Digital Signature Algorithm) med brug af afsenderenhedens private signeringsnøgle. I iOS 13 og nyere versioner og iPadOS 13.1 og nyere versioner kan enheder bruge ECIES-kryptering (Elliptic Curve Integrated Encryption Scheme) i stedet for RSA-kryptering.

Resultatet er en besked til hver modtagerenhed, som består af den krypterede beskedtekst, den krypterede beskednøgle og afsenderens digitale signatur. De overdrages derefter til APNs til levering. Metadata, f.eks. tidsstemplet og APNs-ruteoplysningerne, krypteres ikke. Kommunikationen med APNs krypteres med en TLS-kanal med Forward Secrecy.

APNs kan kun videresende beskeder med en størrelse på op til 4 eller 16 KB, afhængigt af iOS- eller iPadOS-versionen. Hvis beskedens tekst er for lang, eller hvis der er vedhæftet et bilag, f.eks. et foto, krypteres bilaget med AES CTR med en tilfældig 256-bit nøgle og overføres til iCloud. Derefter sendes bilagets AES-nøgle, dets Uniform Resource Identifier (URI) og en SHA-1 hash-værdi for bilagets krypterede format til modtageren i en iMessage, og værdiernes fortrolighed og integritet beskyttes med den almindelige iMessage-kryptering som vist i nedenstående diagram.



Ved gruppesamtaler gentages processen for hver modtager og hver modtagers enheder.

Hver modtagerenhed modtager sin kopi af beskeden fra APNs og henter om nødvendigt bilaget fra iCloud. Afsenderens indgående telefonnummer eller e-mailadresse sammenlignes med modtagerens kontakter, så der kan vises et navn, hvis det findes.

Som ved alle andre push-notifikationer slettes beskeden fra APNs, når den er leveret. I modsætning til andre APNs-notifikationer sættes iMessage-beskeder imidlertid i kø til levering til enheder, der er offline. Beskeder opbevares på Apples servere i op til 30 dage.

Sikker deling af navn og foto i iMessage

Deling af navn og foto i iMessage gør det muligt for en bruger at dele et navn og et foto ved brug af iMessage. Brugeren kan vælge oplysningerne fra Mit kort eller redigere navnet og inkludere et billede efter eget valg. Deling af navn og foto i iMessage benytter et totrinssystem til at distribuere navnet og fotoet.

Oplysningerne underopdeles i felter, der bliver krypteret og godkendt hver for sig samt godkendt samlet i nedenstående proces. Der er tre felter:

- Navn
- Foto
- Fotoarkivnavn

Et af de første trin i datagenereringen er at generere en tilfældig 128-bit postnøgle på enheden. Denne postnøgle bliver derefter afledt med HKDF-HMAC-SHA256 for at oprette tre undernøgler: Nøgle 1:Nøgle 2:Nøgle 3 = HKDF (postnøgle, "kaldenavne"). For hvert felt genereres der en 96 bit IV-værdi (Initialization Vector), og oplysningerne bliver krypteret med AES-CTR og Nøgle 1. Der bliver beregnet en MAC-værdi (kode til godkendelse af besked) med HMAC-SHA256 ved brug af Nøgle 2, som dækker feltnavnet, felt-IV og feltets ciffertekst. Til sidst bliver de individuelle MAC-feltværdier sammenkædet, og deres MAC beregnet med HMAC-SHA256 ved brug af Nøgle 3. 256-bit MAC-værdien bliver gemt sammen med de krypterede data. De første 128 bits i denne MAC-værdi bliver brugt som RecordID.

Den krypterede post bliver derefter gemt i den offentlige database i CloudKit under sit RecordID. Denne post bliver aldrig ændret, og når brugeren vælger at ændre sit navn og foto, bliver der hver gang genereret en ny krypteret post. Når bruger 1 vælger at dele sit navn og foto med bruger 2, sendes postnøglen sammen med recordID'et inde i iMessage-datastrømmen, som er krypteret.

Når bruger 2's enhed modtager disse iMessage-data, noterer den, at dataene indholder et kaldenavn og et foto-recordID samt en nøgle. Bruger 2's enhed foretager et opkald i den offentlige CloudKit-database for at hente det krypterede navn og foto i recordID-posten og sender oplysningerne videre ved hjælp af iMessage.

Når beskeden er modtaget, dekrypterer bruger 2's enhed dataene og kontrollerer signaturen ved at bruge selve recordID'et. Hvis dette godkendes, får bruger 2 navn og foto, og vedkommende kan vælge at føje dette til sine kontakter eller bruge det til iMessage.

Sikker Apple Messages for Business

Apple Messages for Business er en beskedtjeneste, der gør det muligt for brugere at kommunikere med virksomheder ved hjælp af appen Beskeder. Med Apple Messages for Business har brugeren altid kontrol over samtalen. Brugeren kan også slette samtalen og blokere for, at virksomheder fremover sender beskeder til brugeren. Af hensyn til anonymitet modtager virksomheden ikke brugerens telefonnummer, e-mailadresse eller iCloud-kontooplysninger. I stedet opretter Apple Identity Service (IDS) et specielt unikt id, der kaldes *Opaque ID*, som deles med virksomheden. Opaque ID er unikt for relationen mellem brugerens Apple-id og virksomhedens Business ID. En bruger har et Opaque ID til hver virksomhed, som brugeren kontakter via Apple Messages for Business. Brugeren beslutter, hvis og hvornår eventuelle oplysninger, der identificerer brugeren som person, skal deles med virksomheden, og Apple Messages for Business gemmer aldrig samtalehistorik.

Apple Messages for Business understøtter administrerede Apple-id'er fra Apple Business Manager og undersøger i Apple School Manager, om de er slået til for iMessage og FaceTime.

Beskeder sendt til virksomheden krypteres mellem brugerens enhed og Apples beskedservere og bruger samme sikkerhed og Apple-beskedservere som beskeder i iMessage. Apples beskedservere dekrypterer disse beskeder i RAM og videresender dem til virksomheden via et krypteret link med TLS 1.2. Beskeder opbevares aldrig i ukrypteret format under overførslen via Apple Messages for Business. Virksomheders svar sendes ligeledes med TLS 1.2 til Apple-beskedserverne, hvor de krypteres med hver modtagerenheds unikke offentlige nøgle.

Hvis brugerenhederne er online, leveres beskeden med det samme og opbevares ikke i bufferen på Apple-beskedserverne. Hvis en brugers enhed ikke er online, opbevares den krypterede besked i bufferen i op til 30 dage, så brugeren kan modtage den, når enheden er online igen. Så snart enheden er online igen, bliver beskeden leveret og slettet fra bufferen. Efter 30 dage uden levering udløber beskeden i bufferen, og den slettes permanent.

FaceTime-sikkerhed

FaceTime er Apples tjeneste til video- og samtaleopkald. FaceTime bruger ligesom iMessage Apples tjeneste til push-notifikationer (APNs) til at etablere den første forbindelse til brugerens registrerede enheder. Samtale- eller videoindholdet af FaceTime-opkald beskyttes med kryptering hele vejen fra afsender til modtager, så ingen andre kan få adgang til det. Apple kan ikke dekryptere dataene.

Den første FaceTime-forbindelse foretages via en Apple-serverinfrastruktur, som sender datapakker mellem brugerens registrerede enheder. Enhederne bekræfter deres identitetscertifikater ved hjælp af APNs- og STUN-beskeder (Session Traversal Utilities for NAT) og etablerer en nøgle (“shared secret”) til hver session. Nøglen (”shared secret”) bruges til at udlede sessionsnøgler til mediekanaler, der streames ved brug af SRTP (Secure Real-time Transport Protocol). SRTP-pakker krypteres ved hjælp af AES256 med CM-funktion (Counter Mode) og godkendes med HMAC-SHA1. Efter den første forbindelse og indstilling af sikkerhed bruger FaceTime STUN og ICE (Internet Connectivity Establishment) til at etablere en forbindelse mellem enheder, hvis det er muligt.

Med FaceTime-gruppe udvides FaceTime til at understøtte op til 33 deltagere på samme tid. Ligesom i klassisk en-til-en-FaceTime end-to-end-krypteres opkaldene mellem de inviterede deltageres enheder. Selvom FaceTime-gruppe genbruger en stor del af infrastrukturen og designet fra en-til-en-FaceTime, har disse gruppeopkald en mekanisme til etablering af nøgler, der er bygget oven på den pålidelighed, som IDS (Apple Identity Service) leverer. Denne protokol leverer Forward Secrecy, hvilket betyder, at en kompromitteret brugerenhed ikke lækker indholdet af tidligere opkald. Sessionsnøgler indpakkes ved brug af AES-SIV og distribueres mellem deltagerne vha. en ECIES-konstruktion med midlertidige P-256 ECDH-nøgler.

Når et nyt telefonnummer eller en ny e-mailadresse føjes til et igangværende FaceTime-gruppeopkald, opretter de aktive enheder nye medienøgler, og de deler aldrig tidligere anvendte nøgler med de nye inviterede enheder.

Find

Sikkerhed i Find

Appen Find til Apple-enheder er bygget på basis af avanceret kryptografi med offentlige nøgler.

Oversigt

Find er en kombination af Find min iPhone og Find mine venner i en app til iOS, iPadOS og macOS. Find kan hjælpe brugere med at finde en mistet enhed, selv en Mac uden internetforbindelse. En enhed med internetforbindelse kan simpelthen rapportere sin lokalitet til brugeren via iCloud. Find fungerer uden internetforbindelse ved at udsende kortrækkende Bluetooth-signaler fra den mistede enhed, der kan registreres af andre Apple-enheder, der bruges i nærheden. Disse enheder i nærheden videresender så den mistede enheds registrerede lokalitet til iCloud, så brugere kan finde den i appen Find – samtidig med at alle involverede brugeres anonymitet og sikkerhed beskyttes. Find fungerer endda med en Mac, der er offline og på vågeblus.

Ved hjælp af Bluetooth og de mange hundrede millioner aktive iOS-, iPadOS- og macOS-enheder, der er i brug verden over, kan en bruger lokalisere sin mistede enhed, også selvom den ikke har forbindelse til et Wi-Fi- eller mobilnetværk. Alle iOS-, iPadOS- eller macOS-enheder med "find offline" slået til i indstillingerne til Find kan fungere som "finde-enhed". Det betyder, at enheden kan registrere tilstedeværelsen af en anden mistet enhed, der er offline, ved hjælp af Bluetooth og derefter bruge sin netværksforbindelse til at give besked om en omtrentlig lokalitet til ejeren. Når find offline er slået til på en enhed, betyder det også, at den kan lokaliseres af andre deltagere på samme måde. Hele denne interaktion er end-to-end-krypteret, anonym og designet til at være både batteri- og dataeffektiv. Batteritid og dataabonnement påvirkes så lidt som muligt, og brugerens anonymitet beskyttes.

Bemærk: Find er muligvis ikke tilgængelig i alle lande eller områder.

End-to-end-kryptering

Find er bygget på basis af avanceret offentlig nøglekryptografi. Når Find offline er slået til i indstillingerne til Find, bliver et privat EC (Elliptic Curve) P-224-krypteringsnøglepar noteret som {d,P} genereret direkte på enheden, hvor *d* er den private nøgle, og *P* er den offentlige nøgle. Desuden bliver en hemmelig 256-bit SK_0 og en tæller $_i$ sat til 0 fra starten. Dette private nøglepar og hemmeligheden bliver aldrig sendt til Apple og synkroniseres kun mellem brugerens øvrige enheder med end-to-end-kryptering ved brug af iCloud-nøglering. Hemmeligheden og tælleren bruges til at udlede den nuværende symmetriske SK_i-nøgle med den følgende rekursive konstruktion: $SK_i = KDF(SK_{i-1}, \text{“update”})$.

Baseret på SK_i-nøglen bliver to store tal u_i og v_i beregnet med $(u_i,v_i) = KDF(SK_i, \text{“diversify”})$. Både den private P-224-nøgle med markøren *d* og den tilsvarende offentlige nøgle, der kaldes *P*, bliver derefter beregnet med en tilhørende relation, der involverer de to tal med henblik på at beregne et kortlivet nøglepar: Den beregnede private nøgle er d_i, hvor $d_i = u_i * d + v_i$ (modulo potensen af P-224-kurven) og den tilsvarende offentlige del er P_i og verificerer, at $P_i = u_i*P + v_i*G$.

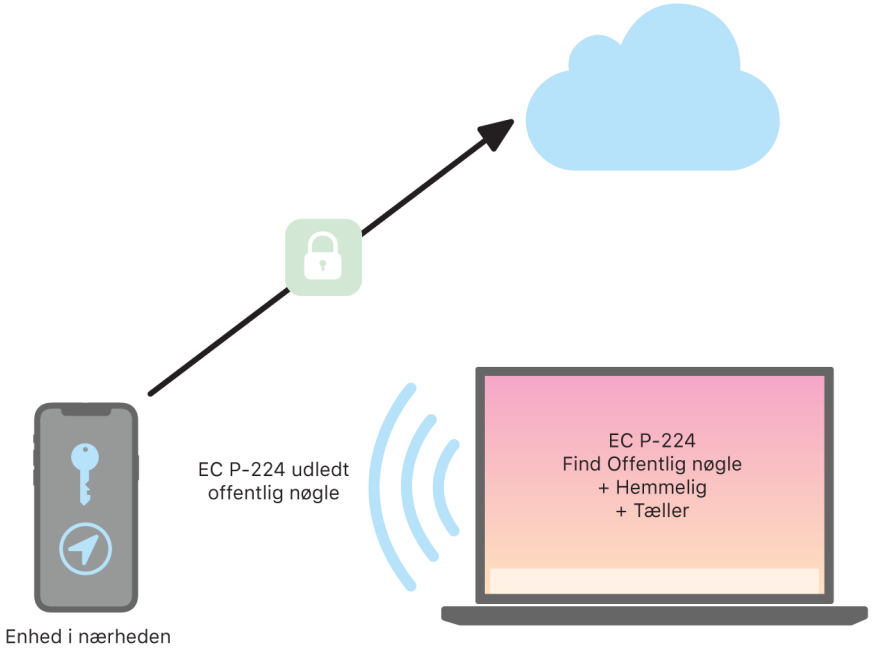
Når en enhed mistes og ikke kan oprette forbindelse til Wi-Fi- eller mobilnetværket – eksempelvis hvis en MacBook Pro bliver efterladt på en bænk i en park – begynder den at udsende den beregnede offentlige nøgle P_i i et begrænset tidsrum som Bluetooth-data. Ved brug af P-224 kan repræsentationen af den offentlige nøgle være i en enkelt Bluetooth-datapakke. De omkringstående enheder kan derefter hjælpe med at finde den enhed, der er offline, ved at kryptere deres lokalitet til den offentlige nøgle. Cirka hvert kvarter bliver den offentlige nøgle erstattet af en ny ved brug af en højere værdi af tælleren og ovenstående proces, så brugeren ikke kan spores af en vedholdende identifikator. Beregningsmekanismen har til formål at forhindre de forskellige offentlige nøgler P_i i at blive forbundet med samme enhed.

Sikring af brugere og enheders anonymitet

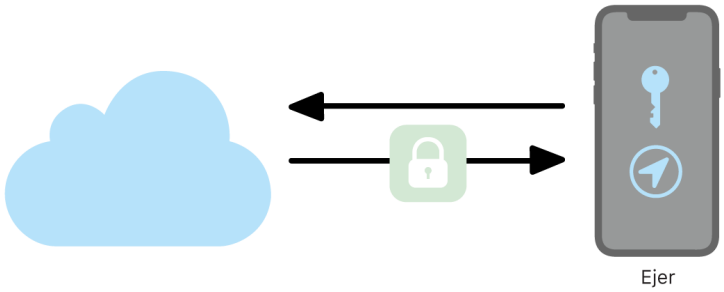
Det bliver sikret, at lokalitetsoplysninger og andre oplysninger er fuldt krypterede, og deltagernes identitet holdes hemmelig – både dem imellem og over for Apple. Trafikken, der sendes til Apple af finde-enheder, indeholder ingen godkendelsesoplysninger i indhold eller overskrifter. Derfor ved Apple ikke, hvem finderen er, og hvis enhed det er, der er blevet fundet. Ydermere registrerer Apple ikke oplysninger, der kan afsløre finderens identitet, og gemmer heller ikke oplysninger, der ville gøre det muligt at finde en forbindelse mellem finder og ejer. Enhedens ejer modtager kun de krypterede lokalitetsoplysninger, der er dekrypteret og vises i Find uden nogen oplysninger om, hvem der har fundet enheden.

Brug af Find til at lokalisere mistede Apple-enheder

Alle Apple-enheder inden for Bluetooth-rækkevidde, hvor Find offline er slået til, kan opfange et signal fra en anden Apple-enhed, der er indstillet til at tillade Find, og læse den P_i-nøgle, der sendes ud på det pågældende tidspunkt. Ved brug af en ECIES-konstruktion og den offentlige nøgle P_i, der udsendes, krypterer finde-enhederne deres aktuelle lokalitetsoplysninger og sender dem til Apple. Den krypterede lokalitet bliver forbundet med et serverindeks, der beregnes som SHA256-hash-værdien af den offentlige P-224 P_i-nøgle, der hentes i Bluetooth-datapakken. Apple har aldrig dekrypteringsnøglen, så Apple kan ikke læse den krypterede lokalitet i finde-enheden. Ejeren af den mistede enhed kan rekonstruere indekset og dekryptere den krypterede lokalitet.



En forventet række tællerværdier anslås i den periode, der søges efter lokaliteten, når den mistede enhed forsøges fundet. Med kendskab til den originale private P-224-nøgle *d* og de hemmelige SK_i-værdier inden for tællerværdiområdet i søgeperioden kan ejeren rekonstruere værdisættet $\{d_i, SHA256(P_i)\}$ for hele søgeperioden. Ejerenheden, der bruges til at lokalisere den mistede enhed, kan derefter sende forespørgsler til serveren ved brug af indeksværdierne $SHA256(P_i)$ og hente den krypterede lokalitet fra serveren. Find dekrypterer derpå lokalt de krypterede lokaliteter med de matchende private nøgler d_i og viser den mistede enheds omtrentlige lokalitet. Lokalitetsrapporter fra flere finde-enheder bliver kombineret i ejerens app, så en mere præcis lokalitet kan findes.



Lokalisering af enheder, der er offline

Hvis en bruger har slået Find min iPhone til på sin enhed, er Find offline slået til som standard, når enheden opgraderes til iOS 13 eller en nyere version, iPadOS 13.1 eller en nyere version eller macOS 10.15 eller en nyere version. Formålet er at sikre, at alle brugere har den bedste mulighed for at finde deres enhed, hvis den skulle blive væk. Men hvis brugeren på et tidspunkt ikke ønsker at være med, kan find offline slås fra i indstillingerne til Find på brugerens enhed. Når find offline er slået fra, virker enheden ikke længere som finde-enhed og kan heller ikke findes af andre finde-enheder. Men brugeren kan stadig finde enheden, så længe den kan oprette forbindelse til et Wi-Fi-netværk eller et mobilnetværk.

Når en mistet enhed bliver lokaliseret, modtager brugeren en notifikation og en e-mail om, at enheden er blevet fundet. Brugere kan se den mistede enheds lokalitet ved at åbne Find og vælge fanen Enheder. Frem for at vise enheden på et tomt kort, hvilket ellers ville være tilfældet, inden enheden blev lokaliseret, viser Find en lokalitet på kortet med en omtrentlig adresse og oplysninger om, hvor længe siden det er, at enheden blev opdaget. Hvis der kommer flere lokalitetsrapporter ind, bliver både den nuværende lokalitet og tidspunktet automatisk opdateret. Brugere kan ikke afspille lyd eksternt på en enhed, der er offline, eller slette den, men de kan bruge lokalitetsoplysningerne eller benytte andre metoder til at få fat i enheden igen.

Kontinuitet

Oversigt over sikkerhed i Kontinuitet

Kontinuitet udnytter teknologier som iCloud, Bluetooth og Wi-Fi til at sætte brugerne i stand til at fortsætte en aktivitet på en anden enhed, foretage og modtage telefonopkald, sende og modtage sms'er og dele en internetforbindelse via mobilnetværket.

Handoff-sikkerhed

Apple håndterer overdragelser med Handoff på en sikker måde, uanset om det sker mellem to enheder eller mellem en indbygget app og et websted – selv overdragelser af store mængder data.

Sådan fungerer Handoff sikkert

Med Handoff kan en bruger automatisk overføre igangværende aktiviteter mellem sine iOS-, iPadOS- og macOS-enheder, når enhederne er i nærheden af hinanden. Handoff giver brugeren mulighed for at skifte enhed og straks fortsætte sit arbejde.

Når en bruger logger ind på iCloud på en anden enhed med Handoff, danner de to enheder et Bluetooth Low Energy (BLE) 4.2 OOB-par (Out-Of-Band) ved hjælp af APNs. De enkelte beskeder krypteres på stort set samme måde som beskeder i iMessage. Når enhederne har dannet par, genererer hver enhed en symmetrisk 256-bit AES-nøgle, der bliver gemt i enhedens nøglering. Nøglen kan kryptere og godkende BLE-annonceringerne om enhedens aktuelle aktivitet over for andre parrede iCloud-enheder ved hjælp af AES256 GCM med beskyttelsesforanstaltninger mod genafspilning.

Første gang en enhed modtager en annoncering fra en ny nøgle, etablerer den en BLE-forbindelse til ophavsenheden og udveksler krypteringsnøgler til annonceringer. Forbindelsen sikres med BLE 4.2-standardkryptering samt kryptering af de enkelte beskeder, som ligner den måde, iMessage-beskeder krypteres på. I nogle situationer sendes disse beskeder ved hjælp af APNs i stedet for BLE. Aktivitetsdataene beskyttes og overføres på samme måde som en iMessage-besked.

Handoff mellem lokale apps og websteder

Handoff giver lokale apps i iOS, iPadOS og macOS mulighed for at genoptage brugeraktiviteten på en webside i domæner, der styres af app-udvikleren på lovlig vis. Det er også muligt at fortsætte den brugeraktivitet, der var i gang i den lokale app, i en webbrowser.

Den lokale app skal bevise, at den har tilladelse til at styre det webdomæne, den vil genoptage. Det sker for at bidrage til at forhindre, at lokale apps prøver at genoptage websteder, som ikke styres af udviklerne. Styring af et webdomæne etableres via mekanismen til delte webgodkendelsesoplysninger. Yderligere oplysninger: App-adgang til gemte adgangskoder. Systemet skal bekræfte appens styring af domænenavnet, før appen får tilladelse til at acceptere overdragelsen af brugeraktivitet via Handoff.

Kilden til overdragelse af en webside via Handoff kan være en hvilken som helst browser, der har implementeret API'erne til Handoff. Når brugeren får vist en webside, annoncerer systemet domænenavnet i de krypterede Handoff-annonceringsbyte. Kun brugerens andre enheder kan dekryptere annonceringsbytene.

På en modtagerenhed registrerer systemet, at en installeret lokal app accepterer Handoff-overdragelser fra det annoncerede domænenavn og viser den lokale apps symbol som Handoff-mulighed. Når den lokale app er startet, modtager den hele URL'en og websidens titel. Der overføres ikke andre oplysninger fra browseren til den lokale app.

I modsat retning kan en lokal app angive en alternativ URL, der bruges, når en enhed, som modtager en Handoff-overdragelse, ikke har samme lokale app installeret. I det tilfælde viser systemet brugerens standardbrowser som mulig Handoff-app (hvis denne browser har implementeret API'erne til Handoff). Når der anmodes om Handoff, startes browseren og får oplyst den alternative URL, som afsenderappen har angivet. Der er ikke noget krav om, at den alternative URL begrænses til domænenavne, der styres af udvikleren af den lokale app.

Handoff til store datamængder

Ud over den grundlæggende Handoff-funktion kan nogle apps vælge at bruge API'er, der gør det muligt at sende store mængder data ved hjælp af Peer-to-Peer Wi-Fi-teknologi udviklet af Apple (stort set som med AirDrop). Appen Mail bruger f.eks. disse API'er til at overdrage et e-mailudkast, måske med store bilag.

Når apps bruger disse API'er, starter udvekslingen mellem de to enheder ligesom ved Handoff. Efter at have modtaget de første data via Bluetooth Low Energy (BLE) starter modtagerenheden imidlertid en ny forbindelse via Wi-Fi. Forbindelsen krypteres (med TLS), og den opnår godkendelse via en identitet, der deles via iCloud-nøglering. Identiteten i certifikaterne sammenlignes med brugerens identitet. Derefter sendes flere data via den krypterede forbindelse, indtil overførslen er færdig.

Universel udklipsholder

Universel udklipsholder benytter Handoff til at overføre indholdet af udklipsholderen sikkert mellem enheder, så brugeren kan kopiere indhold på en enhed og indsætte det på en anden. Indhold beskyttes på samme måde som andre Handoff-data og deles som standard med Universel udklipsholder, medmindre app-udvikleren har valgt at slå deling fra.

Apps har adgang til data i udklipsholderen, uanset om brugeren har indsat udklipsholderen i appen. Med Universel udklipsholder udvides denne dataadgang til apps på brugerens andre enheder (som fremgår af deres login på iCloud).

Sikkerhed ved opkald via en iPhone-mobilforbindelse

Når en brugers Mac, iPad, iPod touch eller HomePod er på samme Wi-Fi-netværk som brugerens iPhone, kan enheden foretage og modtage telefonopkald via iPhone-mobilforbindelsen. Konfigurationen forudsætter, at enhederne er logget ind på både iCloud og FaceTime med samme Apple-id-konto.

Når der kommer et indgående opkald, informeres alle konfigurerede enheder via notifikationer fra APNs (Apple Push Notification service). Notifikationerne bruger samme kryptering hele vejen fra afsender til modtager som iMessage. Notifikationen om det indgående opkald vises på skærmen på enheder på samme netværk. Når brugeren besvarer opkaldet, sendes lyden fra brugerens iPhone via en sikker forbindelse direkte mellem de to enheder.

Når et opkald besvares på en enhed, stoppes ringningen på parrede iCloud-enheder i nærheden ved hjælp af en kort annoncering via Bluetooth Low Energy (BLE). Annonceringsbyte krypteres med samme metode som Handoff-annonceringer.

Udgående opkald viderestilles ligeledes til iPhone via APNs, og lyden sendes på samme måde via den sikre forbindelse mellem enhederne. Brugerne kan slå viderestilling af telefonopkald fra på en enhed ved at slå iPhone-mobilopkald fra under FaceTime.

Sikkerhed ved videresendelse af sms fra iPhone

Videresendelse af sms sender automatisk sms'er modtaget på en iPhone til en brugers tilmeldte iPad, iPod touch eller Mac. Hver enhed skal være logget ind på iMessage-tjenesten med samme Apple-id-konto. Når Videresendelse af sms er slået til, tilmeldes enheder i en brugers godkendelseskæde automatisk, hvis tofaktorgodkendelse er slået til. Ellers skal tilmeldingen bekræftes på hver enhed, ved at der indtastes en tilfældig numerisk kode på seks cifre, der er genereret af iPhone.

Når enhederne er blevet forbundet, krypterer iPhone indgående sms'er og videresender dem til hver enhed ved hjælp af de metoder, der er beskrevet i Oversigt over iMessage-sikkerhed. Svar sendes tilbage til iPhone med samme metode, hvorefter iPhone sender svaret som en sms via operatørens mekanisme til sms-transmission. Videresendelse af sms kan slås til og fra i Beskeder.

Instant Hotspot-sikkerhed

Instant Hotspot forbinder andre Apple-enheder med et personligt iOS- eller iPadOS-hotspot. iOS- og iPadOS-enheder, der understøtter Instant Hotspot, bruger Bluetooth Low Energy (BLE) til at finde og kommunikere med alle enheder, der er logget ind på samme individuelle iCloud-konto eller -konti, der bruges sammen med Familiedeling (i iOS 13 og iPadOS). Kompatible Mac-computere med OS X 10.10 eller nyere versioner bruger samme teknologi til at finde og kommunikere med iOS- og iPadOS-enheder med Instant Hotspot.

Når en bruger første gang åbner Wi-Fi-indstillingerne på en enhed, udsender den en BLE-annoncering, der indeholder et id, som alle de enheder, der er logget ind på samme iCloud-konto, er blevet enige om. Id'et genereres ud fra en DSID-værdi (Destination Signaling Identifier), der er knyttet til iCloud-kontoen, og som udskiftes regelmæssigt. Når andre enheder, der er logget ind på samme iCloud-konto, er i nærheden og understøtter Internetdeling, registrerer de signalet og svarer med angivelse af muligheden for at bruge Instant Hotspot.

Når en bruger, der ikke er del af Familiedeling, vælger en iPhone eller iPad til Internetdeling, sendes der en anmodning om aktivering af Internetdeling til enheden. Anmodningen sendes via en forbindelse, der er krypteret med BLE-kryptering, og anmodningen krypteres på stort set samme måde som iMessage-beskeder. Enheden sender et svar via samme BLE-forbindelse med samme beskedkryptering med oplysninger om delingen af internetforbindelsen.

For brugere, der er en del af Familiedeling, deles oplysninger om forbindelse via Internetdeling på en sikker måde ved hjælp af en mekanisme, der ligner den, som HomeKit-enheder bruger til at synkronisere oplysninger. Mere præcist beskyttes forbindelser, der deler oplysninger om internetdeling, med en midlertidig nøgle af typen ECDH (Curve25519), der godkendes med hver brugers enhedsspecifikke offentlige Ed25519-nøgle. De offentlige nøgler, der bruges, er dem, der tidligere blev synkroniseret mellem medlemmerne af Familiedeling ved hjælp af IDS, da Familiedeling blev slået til.

Netværkssikkerhed

Oversigt over netværkssikkerhed

Ud over de indbyggede sikkerhedsforanstaltninger, som Apple bruger til at beskytte de gemte data på Apple-enheder, findes der mange forholdsregler, som organisationer kan tage for at sikre oplysninger under overførslen til og fra en enhed. Alle disse sikkerhedsforanstaltninger og forholdsregler hører ind under netværkssikkerhed.

Da brugerne skal kunne få adgang til virksomheders netværk overalt i verden, er det vigtigt at bidrage til, at de bliver godkendt, og at deres data beskyttes under overførslen. Disse sikkerhedsmål nås i kraft af integrationen af afprøvede teknologier og de nyeste standarder for både Wi-Fi-forbindelser og forbindelser via mobildatanetværk i iOS, iPadOS og macOS. Det er grunden til, at vores operativsystemer bruger – og giver udviklere adgang til – netværksstandardprotokoller for bekræftet, godkendt og krypteret kommunikation.

TLS-sikkerhed

iOS, iPadOS og macOS understøtter Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) og Datagram Transport Layer Security (DTLS). TLS-protokollen understøtter både AES128 og AES256 og foretrækker kodepakker med Forward Secrecy. Internetapps som Safari, Kalender og Mail bruger automatisk denne protokol til at åbne en krypteret kommunikationskanal mellem enheden og netværkstjenester. API'er på højt niveau (f.eks. CFNetwork) gør det nemt for udviklere at benytte TLS i deres apps, og API'er på lavt niveau (f.eks. Network.framework) indeholder fintmaskede kontrolmuligheder. CFNetwork tillader ikke brug af SSL 3, og apps, der bruger WebKit (f.eks. Safari), forhindres i at oprette en SSL 3-forbindelse.

I iOS 11 og nyere versioner og macOS 10.13 og nyere versioner er SHA-1-certifikater ikke længere tilladt for TLS-forbindelser, medmindre brugeren godkender dem. Certifikater med RSA-nøgler på under 2048 bit er heller ikke tilladt. Den symmetriske RC4-kodepakke er udfaset i iOS 10 og macOS 10.12. RC4-kodepakker er som standard ikke slået til for TLS-klienter og -servere, der er implementeret med SecureTransport-API'er, og disse klienter og servere kan derfor ikke oprette forbindelse, når RC4 er den eneste tilgængelige kodepakke. Tjenester og apps, der kræver RC4, bør opgraderes, så de bruger sikre kodepakker. I iOS 12.1 skal certifikater, der er udstedt efter 15. oktober 2018 fra et systemgodkendt rodcertifikat, logges i en godkendt CT-log (Certificate Transparency) for at blive tilladt til TLS-forbindelser. I iOS 12.2 er TLS 1.3 som standard slået til for Network. framework- og NSURLSession-API'er. TLS-klienter, der bruger SecureTransport API'er, kan ikke bruge TLS 1.3.

App Transport Security

App Transport Security sørger for standardkrav til forbindelser, så apps følger den bedste praksis for sikre forbindelser ved brug af NSURLConnection-, CFURL- eller NSURLSession-API'er. App Transport Security begrænser som standard kodningsvalget, så kun pakker med Forward Secrecy er inkluderet, nærmere bestemt:

- ECDHE_ECDSA_AES og ECDHE_RSA_AES med Galois-/tællerfunktion (GCM)
- CBC-funktion (Cipher Block Chaining)

Apps kan slå kravet om Forward Secrecy fra pr. domæne. Hvis de gør det, føjes RSA_AES til sættet med tilgængelige kodninger.

Servere skal understøtte TLS 1.2 med Forward Secrecy, og certifikater skal være gyldige og skal signeres vha. SHA256 eller en bedre metode og som minimum have en 2048-bit RSA-nøgle eller en 256-bit elliptisk kurvenøgle.

Netværksforbindelser, der ikke overholder disse krav, vil mislykkes, medmindre appen tilsidesætter App Transport Security. Ugyldige certifikater vil altid mislykkes, så der ikke oprettes forbindelse. App Transport Security anvendes automatisk på apps, der er kompileret til iOS 9 og nyere versioner og macOS 10.11 og nyere versioner.

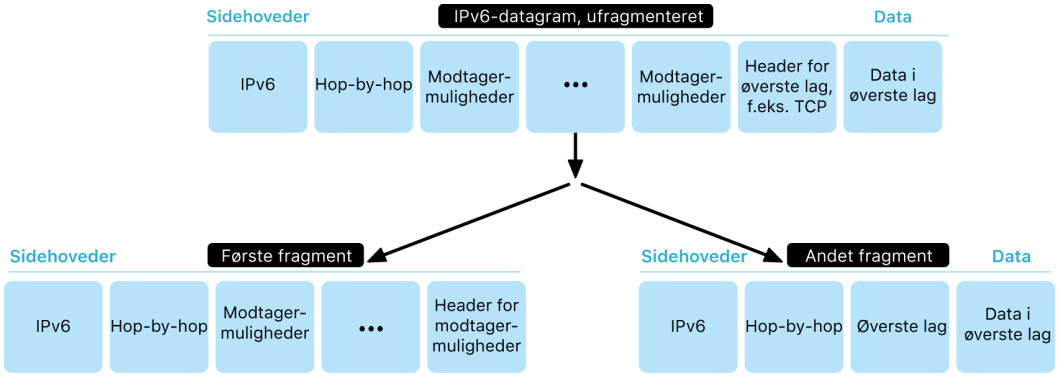
Kontrol af certifikaters gyldighed

Status for godkendelse af et TLS-certifikat foretages i henhold til etablerede branchestandarder som fastlagt i RFC 5280 og inkorporerer nye standarder, f.eks. RFC 6962 (om certifikaters gennemsigtighed). Apple-enheder med iOS 11 eller en nyere version eller macOS 10.13 eller en nyere version opdateres jævnligt med en aktuel liste med tilbagekaldte certifikater og certifikater med begrænsninger. Listen dannes ud fra lister med tilbagekaldte certifikater, som udgives af hver af de indbyggede rodcertifikatmyndigheder, som er godkendt af Apple, samt af deres underordnede CA-udstedere. Efter Apples valg kan listen også omfatte andre begrænsninger. Der slås op i disse oplysninger, hver gang en funktion i et netværks-API bruges til at oprette en sikker forbindelse. Hvis der er for mange tilbagekaldte certifikater fra en certifikatmyndighed til, at de alle kan anføres på listen, kan en evaluering af tillid i stedet bestemme, at der er behov for et svar på et onlinecertifikats status (OCSP). Hvis der ikke kommer et svar, kan evalueringen ikke gennemføres.

IPv6-sikkerhed

Alle Apples operativsystemer understøtter IPv6 og implementerer flere mekanismer for at beskytte brugernes anonymitet og netværksstakkens stabilitet. Når der bruges Stateless Address Autoconfiguration (SLAAC), genereres IPv6-adresserne for alle brugerflader på en måde, der er med til at blokere sporingsenheder på tværs af netværk og samtidig giver en god brugeroplevelse ved at sikre adressernes stabilitet, når der ikke sker nogen netværksændringer. Algoritmen til generering af adresser er baseret på kryptografisk genererede adresser i henhold til RFC 3972. Den er forbedret gennem en brugerfladespecifik modifikator for at garantere, at selv forskellige brugerflader på samme netværk har forskellige adresser til sidst. Desuden oprettes midlertidige adresser med en foretrukket levetid på 24 timer, og de bruges som standard til alle nye forbindelser. På linje med funktionen Privat Wi-Fi-adresse, som blev indført i iOS 14 og iPadOS 14 og watchOS 7, genereres der en unik "link-local" adresse for hvert Wi-Fi-netværk, en enhed opretter forbindelse til. Netværkets SSID inkorporeres som et yderligere element til generering af adressen i lighed med parameteren Network_ID i henhold til RFC 7217. Fremgangsmåden bruges i iOS 14, iPadOS 14 og watchOS 7.

Som beskyttelse mod angreb baseret på IPv6-udvidelsesoverskrifter og -fragmentering implementerer Apple-enheder beskyttelsesforanstaltninger, der er beskrevet i RFC 6980, RFC 7112 og RFC 8021. De modvirker blandt andet angreb, hvor overskriften i det øverste lag kun kan findes i det andet fragment, hvilket kunne skabe tvetydighed for sikkerhedsforanstaltninger som tilstandsløse pakkefiltre.



Derudover håndhæver Apple-enheder forskellige grænser for IPv6-relaterede datastrukturer, f.eks. antallet af præfikser pr. brugerflade. Det gøres for at bidrage til at sikre IPv6-stakkens robusthed.

Sikkerhed i virtuelle private netværk (VPN)

Der kræves normalt minimal indstilling og konfiguration, før sikre netværkstjenester som VPN (Virtual Private Networks) fungerer på iOS-, iPadOS- og macOS-enheder.

Understøttede protokoller

Disse enheder kan arbejde sammen med VPN-servere, der understøtter følgende protokoller og godkendelsesmetoder:

- IKEv2/IPsec med godkendelse via nøgle ("shared secret"), RSA-certifikater, ECDSA (Elliptic Curve Digital Signature Algorithm)-certifikater, EAP-MSCHAPv2 eller EAP-TLS
- SSL-VPN sammen med den relevante klientapp fra App Store
- L2TP/IPsec med brugergodkendelse via MS-CHAPV2-adgangskode og maskingodkendelse via nøgle ("shared secret") (iOS, iPadOS og macOS) og RSA SecurID eller CRYPTOCard (kun macOS)
- Cisco IPsec med brugergodkendelse via adgangskode, RSA SecurID eller CRYPTOCard og maskingodkendelse via nøgle ("shared secret") og certifikater (kun macOS)

Understøttede VPN-implementeringer

iOS, iPadOS og macOS understøtter følgende:

- *VPN On Demand:* Til netværk, der bruger godkendelse baseret på certifikater. It-politikker fastlægger, hvilke domæner der kræver en VPN-forbindelse, ved at bruge en VPN-konfigurationsprofil.
- *VPN til hver app:* Giver langt mere detaljerede administrationsmuligheder for VPN-forbindelser. I løsninger til administration af mobile enheder (MDM) kan der angives en forbindelse for hver administreret app og særskilte domæner i Safari. Det bidrager til at sikre, at data altid sendes til og fra virksomhedens netværk, og at brugerens personlige data ikke gør.

iOS og iPadOS understøtter følgende:

- *Altid til-VPN:* Til enheder, der administreres via en MDM-løsning og er under tilsyn ved hjælp af Apple Configurator til Mac, Apple School Manager eller Apple Business Manager. Med Altid til-VPN behøver brugerne ikke længere at slå VPN til for at aktivere beskyttelse, når de opretter forbindelse til mobil- og Wi-Fi-netværk. Det giver også en organisation fuld kontrol over trafik til og fra enheder, idet al IP-trafik kanaliseres tilbage til organisationen. Standardudvekslingen af parametre og nøgler til den efterfølgende kryptering, IKEv2, sørger for sikker transmission med datakryptering. Organisationen kan overvåge og filtrere trafik til og fra dens enheder, sikre data i dens netværk og begrænse enheders adgang til internettet.

Wi-Fi-sikkerhed

Sikker adgang til trådløse netværk

Alle Apple-platforme understøtter Wi-Fi-protokoller, der er standard i branchen, til godkendelse og kryptering med henblik på godkendt adgang og datafortrolighed ved oprettelse af forbindelse til følgende sikre trådløse netværk:

- WPA2 Personal
- WPA2 Enterprise
- WPA2/WPA3 Transitional
- WPA3 Personal
- WPA3 Enterprise
- WPA3 Enterprise med 192-bit sikkerhed

WPA2 og WPA3 godkender hver forbindelse og benytter 128-bit AES-kryptering til at bidrage til at bevare fortroligheden af data, der sendes trådløst. Det giver brugerne størst mulig sikkerhed for, at deres data fortsat er beskyttet, når de sender og modtager data via en Wi-Fi-netværksforbindelse.

WPA3-understøttelse

WPA3 understøttes på følgende Apple-enheder:

- iPhone 7 og nyere modeller
- iPad (5. generation og nyere modeller)
- Apple TV 4K og nyere modeller
- Apple Watch Series 3 og nyere modeller
- Mac-computere (ultimo 2013 og nyere med 802.11ac eller en nyere version)

Nyere enheder understøtter godkendelse med WPA3 Enterprise 192-bit sikkerhed, herunder understøttelse af 256-bit AES-kryptering, når der oprettelse forbindelse til trådløse adgangspunkter. Det giver endnu større beskyttelse af fortroligheden af trådløs trafik. WPA3 Enterprise 192-bit sikkerhed understøttes på iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max og nyere iOS- og iPadOS-enheder.

PMF-understøttelse

Ud over beskyttelse af data, der sendes trådløst, udvider Apple-platforme beskyttelsen på WPA2- og WPA3-niveau til unicast- og multicast-administrationsdataenheder via tjenesten Protected Management Frame, der er defineret i 802.11w. PMF understøttes på følgende Apple-enheder:

- iPhone 6 og nyere modeller
- iPad Air 2 og nyere modeller
- Apple TV HD og nyere modeller
- Apple Watch Series 3 og nyere modeller
- Mac-computere (ultimo 2013 og nyere med 802.11ac eller en nyere version)

Med understøttelsen af 802.1X kan Apple-enheder integreres i en lang række RADIUS-godkendelsesmiljøer. De trådløse 802.1X-godkendelsesmetoder, der understøttes, omfatter EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 og PEAPv1.

Beskyttelsesforanstaltninger for platforme

Apples operativsystemer beskytter enheder mod sårbarheder i netværksprocessorens firmware. Det betyder, at netværkscontrollere med Wi-Fi har begrænset adgang til app-processorens hukommelse.

- Når USB eller SDIO (Secure Digital Input Output) bruges til interaktion med netværksprocessoren, kan netværksprocessoren ikke starte DMA-transaktioner (Direct Memory Access) mod app-processoren.
- Når PCIe bruges, er hver netværksprocessor på sin egen isolerede PCIe-bus. En IOMMU (Input/Output Memory Management Unit) på hver PCIe-bus begrænser netværksprocessorens DMA-adgang yderligere, så den kun har adgang til hukommelse og ressourcer, der indeholder dens netværkspakker og kontrolstrukturer.

Udfasede protokoller

Apple-produkter understøtter følgende udfasede Wi-Fi-protokoller til godkendelse og kryptering:

- WEP Open med både 40-bit og 104-bit nøgler
- WEP Shared med både 40-bit og 104-bit nøgler
- Dynamisk WEP
- TKIP (Temporal Key Integrity Protocol)
- WPA
- WPA/WPA2 Transitional

Disse protokoller betragtes ikke længere som sikre, og af hensyn til kompatibilitet, driftsikkerhed, ydelse og sikkerhed frarådes det kraftigt at bruge dem. De understøttes kun af hensyn til bagudkompatibiliteten og bliver måske fjernet i kommende softwareversioner.

Det anbefales, at alle Wi-Fi-implementeringer flyttes over på WPA3 Personal eller WPA3 Enterprise for at få så driftssikre, beskyttede og kompatible Wi-Fi-forbindelser som muligt.

Wi-Fi-anonymitet

Brug af tilfældige MAC-adresser

Apple bruger en tilfældig MAC-adresse (Media Access Control) under udførelse af Wi-Fi-scanninger, når enheden ikke har forbindelse til et Wi-Fi-netværk. Disse scanninger kan udføres for at finde og oprette forbindelse til et kendt Wi-Fi-netværk eller hjælpe Lokalitetstjenester i forbindelse med apps, der bruger "geofences" (elektroniske hegn), f.eks. lokalitetsbaserede påmindelser eller fast placering af en lokalitet i Apples Kort. Bemærk, at Wi-Fi-scanninger, som foretages under forsøg på at oprette forbindelse til et foretrukket Wi-Fi-netværk, ikke bruger tilfældige adresser. Tilfældige MAC-adresser til Wi-Fi understøttes ikke på iPhone 5 og nyere modeller.

Apple-platforme bruger også en tilfældig MAC-adresse under udførelse af ePNO-scanninger (Enhanced Preferred Network Offload), når en enhed ikke har forbindelse til et Wi-Fi-netværk, eller dens processor er på vågeblus. ePNO-scanninger foretages, når en enhed bruger Lokalitetstjenester til apps, som benytter elektroniske hegn, f.eks. lokalitetsbaserede påmindelser, der afgør, om enheden er i nærheden af en angivet lokalitet.

Da en enheds MAC-adresse ændres, når dens forbindelse til et Wi-Fi-netværk afbrydes, kan passive observatører af Wi-Fi-trafik ikke bruge den til at spore en enhed konstant, heller ikke når enheden har forbindelse til et mobilnetværk. Apple har informeret Wi-Fi-producenter om, at Wi-Fi-scanninger i iOS og iPadOS bruger tilfældige MAC-adresser, og at hverken Apple eller producenterne kan forudsige disse tilfældige MAC-adresser.

I iOS 14 og nyere versioner, iPadOS 14 og nyere versioner og watchOS 7 og nyere versioner gælder, at når en iPhone, iPad eller iPod touch eller et Apple Watch opretter forbindelse til et Wi-Fi-netværk, identificerer enheden sig selv med en unik (tilfældig) MAC-adresse. Funktionen kan slås fra af brugeren eller ved hjælp af en ny mulighed i Wi-Fi-dataene. Under visse omstændigheder vil enheden gå tilbage til sin faktiske MAC-adresse.

Du kan få flere oplysninger i Apple-supportartiklen Brug private Wi-Fi-adresser på iPhone, iPad, iPod touch og Apple Watch.

Brug af tilfældige sekvensnumre til Wi-Fi-frames

Wi-Fi-frames indeholder et sekvensnummer, som bruges af 802.11-protokollen på lavt niveau til at gøre Wi-Fi-kommunikation effektiv og robust. Da disse sekvensnumre tælles op for hver sendt frame, kan de bruges til at sammenholde oplysninger, der sendes under Wi-Fi-scanninger, med andre rammer, som sendes af samme enhed.

Apple-enheder forhindrer dette ved at gøre sekvensnumrene tilfældige, hver gang en MAC-adresse ændres til en ny tilfældig adresse. Også sekvensnumrene til hver ny scanningsanmodning, der startes, mens enheden ikke har nogen tilknytning, gøres tilfældige. Brug af tilfældige numre understøttes på følgende enheder:

- iPhone 7 og nyere modeller
- iPad (5. generation og nyere modeller)
- Apple TV 4K og nyere modeller
- Apple Watch Series 3 og nyere modeller
- iMac Pro (Retina 5K, 27", 2017) og nyere modeller

- MacBook Pro (13", 2018) og nyere modeller
- MacBook Pro (15", 2018) og nyere modeller
- MacBook Air (Retina, 13", 2018) og nyere modeller
- Mac mini (2018) og nyere modeller
- iMac (Retina 4K, 21,5", 2019) og nyere modeller
- iMac (Retina 5K, 27", 2019) og nyere modeller
- Mac Pro (2019) og nyere modeller

Wi-Fi-forbindelser

Apple genererer tilfældige MAC-adresser til Peer-to-Peer Wi-Fi-forbindelser, der bruges til AirDrop og AirPlay. Der bruges også tilfældige adresser til Internetdeling i iOS og iPadOS (med et SIM-kort) og Internetdeling i macOS.

Der genereres nye tilfældige adresser, hver gang disse netværksgrænseflader startes, og der genereres unikke adresser særskilt til hver grænseflade efter behov.

Skjulte netværk

Wi-Fi-netværk kan kendes på deres netværksnavn, som også kaldes et *SSID (Service Set Identifier)*. Nogle Wi-Fi-netværk er indstillet til at skjule deres SSID, så det trådløse adgangspunkt ikke udsender netværkets navn. De kaldes *skjulte netværk*. iPhone 6s og nyere modeller registrerer automatisk, når et netværk er skjult. Hvis et netværk er skjult, sender iOS- eller iPadOS-enheden SSID'et i anmodningen – ellers ikke. Det er med til at forhindre enheden i at udsende navne på tidligere skjulte netværk, som en bruger har haft forbindelse til, hvilket beskytter anonymiteten yderligere.

Bluetooth-sikkerhed

Der er to typer Bluetooth i Apple-enheder, Bluetooth Classic og Bluetooth Low Energy (BLE). Bluetooth-sikkerhedsmodellen til begge udgaver har følgende særskilte sikkerhedsfunktioner:

- *Pardannelse:* Den proces, hvor der oprettes en eller flere nøgler ("shared secret")
- *Tilknytning:* Det, der sker, når der oprettes nøgler under pardannelse, som opbevares og bruges til at danne et godkendt enhedspar i efterfølgende forbindelser
- *Godkendelse:* Bekræftelse af, at to enheder har de samme nøgler
- *Kryptering:* Funktion, der beskytter fortrolige beskeder
- *Beskedintegritet:* Beskyttelse mod forfalskning af beskeder
- *SSP (Secure Simple Pairing):* Beskyttelse mod passiv aflytning og mod MITM-angreb (man-in-the-middle)

Funktionen Secure Connections blev føjet til den fysiske Bluetooth Classic-transport (BR/EDR) i Bluetooth version 4.1.

Sikkerhedsfunktionerne for hver Bluetooth-type er anført nedenfor.

Understøttelse	**Bluetooth Classic**	**Bluetooth Low Energy**
Pardannelse	P-256 elliptisk kurve	Algoritmer godkendt af FIPS (AES-CMAC og P-256 elliptisk kurve)
Tilknytning	Oplysninger om pardannelse, der opbevares et sikkert sted på iOS-, iPadOS-, macOS-, tvOS- og watchOS-enheder	Oplysninger om pardannelse, der opbevares et sikkert sted på iOS-, iPadOS-, macOS-, tvOS- og watchOS-enheder
Godkendelse	Algoritmer godkendt af FIPS (HMAC-SHA256 og AES-CTR)	Algoritmer godkendt af FIPS
Kryptering	Kryptografiske AES-CCM-funktioner, der foretages i styreenheden	Kryptografiske AES-CCM-funktioner, der foretages i styreenheden
Beskedintegritet	AES-CCM, der bruges til beskedintegritet	AES-CCM, der bruges til beskedintegritet
SSP (Secure Simple Pairing): Beskyttelse mod passiv aflytning	ECDHE (Elliptic Curve Diffie-Hellman Exchange Ephemeral)	ECDHE (Elliptic Curve Diffie-Hellman Exchange)
SSP (Secure Simple Pairing): Beskyttelse mod MITM-angreb (man-in-the-middle attack)	To numeriske metoder med brugermedvirken: numerisk sammenligning eller indtastning af adgangsnøgle	To numeriske metoder med brugermedvirken: numerisk sammenligning eller indtastning af adgangsnøgle Pardannelser kræver brugersvar, også alle pardannelsesfunktioner uden MITM
Bluetooth 4.1 og nyere versioner	iMac fra sidst i 2015 og frem MacBook Pro fra starten af 2015 og frem	iOS 9 og nyere versioner iPadOS 13.1 og nyere versioner macOS 10.12 og nyere versioner tvOS 9 og nyere versioner watchOS 2.0 og nyere versioner

Understøttelse	Bluetooth Classic	Bluetooth Low Energy
Bluetooth 4.2 og nyere versioner	iPhone 6 og nyere modeller	iOS 9 og nyere versioner iPadOS 13.1 og nyere versioner macOS 10.12 og nyere versioner tvOS 9 og nyere versioner watchOS 2.0 og nyere versioner

Anonymitet ved Bluetooth Low Energy

BLE har to funktioner, tilfældige adresser og nøgleafledning under transport, der bidrager til at beskytte brugerens anonymitet.

Tilfældige adresser er en funktion, der regelmæssigt ændrer en Bluetooth-enheds adresse og dermed gør det sværere at følge BLE-enheden et stykke tid. Hvis en enhed, der bruger anonymitetsfunktionen, skal kunne oprette forbindelse til kendte enheder igen, skal enhedens adresse, der kaldes den *private adresse*, kunne fortolkes af den anden enhed. Den private adresse genereres ud fra enhedens identitetsnøgle til brug for fortolkning, som udveksles under pardannelsen.

iOS 13 og nyere versioner og iPadOS 13.1 og nyere versioner er i stand til at aflede linknøgler under transport. Funktionen kaldes *nøgleafledning under transport*. Eksempelvis kan en linknøgle, der er genereret med BLE, bruges til at aflede en linknøgle til Bluetooth Classic. Apple har desuden føjet Bluetooth Classic til BLE-understøttelsen på enheder, der understøtter funktionen Secured Connections, som blev lanceret i Bluetooth Core Specification 4.1 (se Bluetooth Core Specification 5.1).

Sikkerhed med ultrabredbånd i iOS

Den nye U1-chip udviklet af Apple bruger ultrabredbåndsteknologien til rumlig bevidsthed. Det sætter iPhone 11, iPhone 11 Pro og iPhone 11 Pro Max og nyere iPhone-modeller i stand til at finde den præcise lokalitet af andre Apple-enheder udstyret med U1. Ultrabredbåndsteknologi bruger den samme teknologi til at generere tilfældige data, som findes på andre understøttede Apple-enheder:

- Brug af tilfældige MAC-adresser
- Brug af tilfældige sekvensnumre til Wi-Fi-rammer

Single sign-on

Sikkerhed i Single sign-on

Single sign-on

iOS og iPadOS understøtter godkendelse i virksomhedsnetværk via SSO (Single sign-on). SSO godkender i samarbejde med Kerberos-baserede netværk brugeres adgang til tjenester, de har tilladelse til at få adgang til. SSO kan bruges til en lang række netværksaktiviteter lige fra sikre Safari-sessioner til apps fra tredjeparter. Godkendelse baseret på certifikater såsom PKINIT understøttes også.

macOS understøtter godkendelse i virksomhedsnetværk via Kerberos. Apps kan bruge Kerberos til at godkende brugeres adgang til tjenester, de er godkendt til. Kerberos kan også bruges til en lang række netværksaktiviteter lige fra sikre Safari-sessioner og godkendelse af netværksarkivsystemer til apps fra tredjeparter. Godkendelse baseret på certifikater understøttes, men det kræver brug af et udvikler-API til apps.

SSO i iOS, iPadOS og macOS benytter SPNEGO-tokens og HTTP Negotiate-protokollen til at arbejde sammen med Kerberos-baserede godkendelsesgateways og systemer med Windows-integreret godkendelse, som understøtter Kerberos-billetter. SSO-understøttelsen er baseret på Open Source-projektet Heimdal.

Følgende krypteringstyper understøttes i iOS, iPadOS og macOS:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari understøtter SSO, og apps fra tredjeparter kan også konfigureres til at bruge SSO, hvis de bruger standardnetværks-API'er i iOS og iPadOS. Til konfigurationen af SSO understøtter iOS og iPadOS konfigurationsprofildata, der giver løsninger til administration af mobile enheder (MDM) mulighed for at overføre de nødvendige indstillinger. Det gælder indstilling af brugerens principal-navn (dvs. Active Directory-brugerkontoen) og Kerberos-områdeindstillinger samt konfiguration af, hvilke apps og URL-adresser i Safari der har tilladelse til at bruge SSO.

I macOS konfigurerer brugeren Kerberos ved at hente billetter fra Ticket Viewer, logge ind på et Windows Active Directory-domæne eller bruge værktøjet `kinit` fra kommandolinjen.

Udvidet SSO

App-udviklere kan skabe deres egne implementeringer af SSO ved at bruge SSO-udvidelser. SSO-udvidelserne kaldes, når en indbygget app eller en webapp skal bruge en eller anden identitetsudbyder til brugergodkendelse. Udviklere kan levere to typer udvidelser: Omdirigering (HTTPS) og udfordring/svar (Kerberos). Det betyder, at godkendelsesmekanismerne OpenID, OAuth, SAML2 og Kerberos kan bruges af udvidet SSO.

En app, der vil bruge en SSO-udvidelse, kan enten bruge API'et AuthenticationServices eller benytte den mekanisme til opsnapning af URL-adresser, som er indeholdt i operativsystemet. WebKit og CFNetwork har et opsnapningslag, der giver alle indbyggede apps og WebKit-apps mulighed for at bruge SSO uden videre. Før en SSO-udvidelse kan kaldes, skal en konfiguration udarbejdet af en administrator installeres via en profil til administration af mobile enheder (MDM). Udvidelser af omdirigeringstypen skal derudover bruge data om tilknyttede domæner til at bevise, at den identitetsserver, de understøtter, er klar over deres eksistens.

Den eneste udvidelse, der følger med operativsystemet, er Kerberos SSO-udvidelsen.

AirDrop-sikkerhed

Apple-enheder, der understøtter AirDrop, bruger Bluetooth Low Energy (BLE) og Peer-to-Peer Wi-Fi-teknologi udviklet af Apple til at sende arkiver og oplysninger til enheder i nærheden, inklusive iOS-enheder og iPad-enheder med AirDrop og iOS 7 eller en nyere version og Mac-computere med OS X 10.11 eller en nyere version. Wi-Fi-radioen bruges til at kommunikere direkte mellem enheder uden brug af en internetforbindelse eller et trådløst adgangspunkt. Denne forbindelse krypteres med TLS.

Deling via AirDrop er som standard indstillet til Kun kontakter. Brugerne kan vælge at bruge AirDrop til at dele med alle, eller de kan slå funktionen helt fra. Organisationer kan begrænse brugen af AirDrop sammen med enheder eller apps, der administreres af en løsning til administration af mobile enheder (MDM).

AirDrop-virkemåde

AirDrop bruger iCloud-tjenester til at hjælpe brugerne med at blive godkendt. Når en bruger logger ind på iCloud, gemmes en 2048-bit RSA-identitet på enheden, og når brugeren slår AirDrop til, oprettes en kort hash-værdi til AirDrop-identiteten på basis af de e-mailadresser og telefonnumre, der er knyttet til brugerens Apple-id.

Når en bruger vælger AirDrop som metode til at dele et emne, udsender afsenderenheden et AirDrop-signal via BLE, der indeholder brugerens korte hash-værdi til AirDrop-identiteten. Andre Apple-enheder, der er i umiddelbar nærhed, som ikke er på vågeblus, og hvor AirDrop er slået til, registrerer signalet og svarer ved hjælp af Peer-to-Peer Wi-Fi, så afsenderenheden kan se identiteten på de enheder, der svarer.

Når Kun kontakter bruges, sammenlignes den modtagne korte hash-værdi til AirDrop-identiteten med hash-værdien til personer i appen Kontakter på modtagerenheden. Hvis der bliver fundet et match, svarer modtagerenheden gennem Peer-to-Peer Wi-Fi med sine identitetsoplysninger. Enheden svarer ikke, hvis der ikke bliver fundet et match.

Samme generelle proces bruges, hvis funktionen Alle er valgt. Dog svarer modtagerenheden også, selvom der ikke bliver fundet et match i Kontakter.

Afsenderenheden starter derefter en AirDrop-forbindelse ved hjælp af Peer-to-Peer Wi-Fi og bruger denne forbindelse til at sende en lang hash-værdi til identiteten til modtagerenheden. Hvis den lange hash-værdi til identiteten stemmer overens med hash-værdien til en kendt person i modtagerens Kontakter, svarer modtageren med sine lange hash-værdier til identiteten.

Hvis hash-værdierne bekræftes, vises modtagerens fornavn og foto (hvis emnerne findes i Kontakter) i afsenderens AirDrop-deleark. I iOS og iPadOS vises de under "Personer" eller "Enheder". Enheder, der ikke er bekræftet eller godkendt, vises i afsenderens AirDrop-deleark med en silhuet og enhedens navn, der er defineret i Indstillinger > Generelt > Om > Navn. I iOS og iPadOS findes de under "Andre personer" i AirDrop-delearket.

Afsenderen kan derefter vælge, hvem vedkommende vil dele med. Når der er valgt en bruger, åbner afsenderenheden en krypteret forbindelse (TLS) til modtagerenheden, og enhederne udveksler deres iCloud-identitetscertifikater. Identiteten i certifikaterne kontrolleres i Kontakter hos hver bruger.

Hvis certifikaterne bekræftes, bliver modtagerbrugeren bedt om at acceptere den indgående overførsel fra den identificerede bruger eller enhed. Hvis der er valgt flere modtagere, gentages processen for hver modtager.

Sikkerhed ved deling af Wi-Fi-adgangskode på iPhone og iPad

iOS- og iPadOS-enheder, der understøtter deling af Wi-Fi-adgangskode, bruger en mekanisme, der ligner AirDrop, til at sende en Wi-Fi-adgangskode fra en enhed til en anden.

Når en bruger vælger et Wi-Fi-netværk (anmoderen) og bliver bedt om at skrive Wi-Fi-adgangskoden, starter Apple-enheden en Bluetooth Low Energy-annoncering (BLE), der anmoder om adgangskoden til Wi-Fi. Andre Apple-enheder, der er i umiddelbar nærhed, som ikke er på vågeblus og har adgangskoden til det valgte Wi-Fi-netværk, opretter forbindelse via BLE til den enhed, der har sendt anmodningen.

Den enhed, der har Wi-Fi-adgangskoden (tildeleren), kræver anmoderens kontaktoplysninger, og anmoderen skal bevise sin identitet vha. en mekanisme, der ligner AirDrop. Når identiteten er bevist, sender tildeleren den kode, som også kan bruges til at oprette forbindelse til netværket, til anmoderen.

Organisationer kan begrænse deling af Wi-Fi-adgangskoder til enheder eller apps, der administreres af en løsning til administration af mobile enheder (MDM).

Firewall-sikkerhed i macOS

macOS har en indbygget firewall, der beskytter Mac mod netværksadgang og DoS-angreb (Denial-of-Service). Den kan konfigureres i vinduet Sikkerhed & anonymitet i Systemindstillinger og understøtter følgende konfigurationer:

- Bloker alle indkommende forbindelser, uanset appen.
- Tillad automatisk indbygget software at modtage indkommende forbindelser.
- Tillad automatisk hentet og signeret software at modtage indkommende forbindelser.
- Giv eller afvis adgang ud fra de apps, brugeren har valgt.
- Tillad ikke, at Mac svarer på ICMP-forespørgsler (Internet Control Message Protocol) og anmodninger om portscanning.

Sikkerhed i Developer Kits

Oversigt over sikkerhed i Developer Kits

Apple stiller en række "kit frameworks" til rådighed, som udviklere uden for Apple kan bruge til at udvide Apples tjenester. Brugernes anonymitet og sikkerhed er et centralt element i disse frameworks:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

HomeKit-sikkerhed

HomeKit-kommunikationssikkerhed

HomeKit er en infrastruktur til automatisering i hjemmet, som benytter iCloud og sikkerheden i iOS, iPadOS og macOS til at beskytte og synkronisere private data, uden at Apple kan se dem.

Identitet og sikkerhed i HomeKit bygger på Ed25519-par med offentlige-private nøgler. Der genereres et Ed25519-nøglepar på iOS-, iPadOS- og macOS-enheden til hver bruger af HomeKit, og dette nøglepar bliver brugerens HomeKit-identitet. Det bruges til at godkende kommunikation mellem iOS-, iPadOS- og macOS-enheder og mellem iOS-, iPadOS- og macOS-enheder og tilbehør.

Nøglerne – som opbevares i Nøglering og kun inkluderes i krypterede sikkerhedskopier af Nøglering – synkroniseres mellem enheder vha. iCloud-nøglering, hvis den er tilgængelig. HomePod og Apple TV modtager nøgler via tryk-for-at-indstille eller den indstillingsfunktion, der beskrives nedenfor. Nøgler deles fra en iPhone til et parret Apple Watch via IDS (Apple Identity Service).

Kommunikation mellem HomeKit-tilbehør

HomeKit-tilbehør genererer deres eget Ed25519-nøglepar, der skal bruges til at kommunikere med iOS-, iPadOS- og macOS-enheder. Hvis standardindstillingerne gendannes på tilbehøret, genereres et nyt nøglepar.

Med henblik på at skabe en relation mellem en iOS-, iPadOS- eller macOS-enhed og HomeKit-tilbehør udveksles nøgler via protokollen Secure Remote Password (3072 bit) ved brug af en ottecifret kode, der leveres af producenten af tilbehøret og indtastes på iOS-, iPadOS- eller macOS-enheden af brugeren, hvorefter den krypteres vha. ChaCha20-Poly1305 AEAD med nøgler afledt af HKDF-SHA512. Tilbehørets MFi-certificering kontrolleres under indstillingen. Tilbehør uden en MFi-chip kan indbygge understøttelse af softwaregodkendelse i iOS 11.3 og nyere versioner.

Når iOS-, iPadOS- eller macOS-enheden og HomeKit-tilbehøret kommunikerer under brugen, godkender de hinanden vha. de nøgler, der blev udvekslet i processen ovenfor. Hver session etableres vha. STS-protokollen og krypteres med nøgler afledt af HKDF-SHA512 på basis af Curve25519-nøgler pr. session. Det gælder både for IP-baseret tilbehør og BLE-tilbehør (Bluetooth Low Energy).

Når det gælder BLE-enheder, der understøtter udsendelsesnotifikationer, forsyner en parret iOS-, iPadOS- eller macOS-enhed tilbehøret med en udsendelseskrypteringsnøgle i en sikker session. Denne nøgle bruges til at kryptere de data om statusændringer på tilbehøret, som meddeles via BLE-annonceringerne. Krypteringsnøglen til annonceringer er afledt af HKDF-SHA512, og dataene krypteres ved hjælp af algoritmen ChaCha20-Poly1305 AEAD. Udsendelseskrypteringsnøglen ændres med jævne mellemrum af iOS-, iPadOS- eller macOS-enheden og opdateres til andre enheder via iCloud som beskrevet i HomeKit-datasikkerhed.

HomeKit og Siri

Siri kan bruges til at sende forespørgsler til og styre tilbehør og til at aktivere scener. Der videregives minimale oplysninger om konfigurationen af hjemmet til Siri, dvs. navnene på værelser, tilbehør og scener, der er nødvendige for at genkende kommandoer. Lyd, der sendes til Siri, kan angive særligt tilbehør eller særlige kommandoer, men disse Siri-data er ikke forbundet med andre Apple-funktioner som f.eks. HomeKit.

Siri-kompatibelt HomeKit-tilbehør

Brugerne kan i appen Hjem slå nye funktioner som Siri og andre HomePod-funktioner som tidtagninger, alarmer, samtaleanlæg og dørklokker på Siri-kompatibelt tilbehør til. Når disse funktioner er slået til, koordinerer tilbehøret med en parret HomePod på det lokale netværk, hvor der er adgang til disse Apple-funktioner. Lyden overføres mellem enhederne i krypterede kanaler, der både bruger HomeKit- og AirPlay-protokollen.

Når Lyt efter Hej Siri er slået til, lytter tilbehøret efter udtrykket “Hej Siri” ved at bruge en funktion, der afvikles lokalt, til at registrere udløsende udtryk. Hvis funktionen registrerer udtrykket, sendes lydrammerne direkte til en parret HomePod via HomeKit. HomePod foretager en ny kontrol af lyden og kan afvise lydsessionen, hvis udtrykket ikke ser ud til at indeholde det udløsende udtryk.

Når Rør og hold for Siri er slået til, kan brugeren trykke på en særlig knap på tilbehøret for at starte en samtale med Siri. Lydrammerne sendes direkte til den parrede HomePod.

Når et ønske om start af Siri registreres, sender HomePod lyden til Siri-servere og efterkommer brugerens ønske ved brug af samme sikkerheds-, anonymitets- og krypteringsforanstaltninger, som HomePod benytter til anmodninger fra brugere til HomePod selv. Hvis Siri svarer med lyd, sendes Siris svar via en AirPlay-lydkanal til tilbehøret. Nogle Siri-anmodninger kræver flere oplysninger fra brugeren (f.eks. hvis Siri spørger, om brugeren vil høre flere muligheder). I det tilfælde får tilbehøret besked om, at brugeren skal anmodes om oplysninger, og den ekstra lyd overføres til HomePod.

Det er et krav, at tilbehøret har en visuel indikation, der kan signalere over for en bruger, at tilbehøret lytter aktivt. Det kan f.eks. være LED-lys. Tilbehøret har intet kendskab til hensigten med Siri-anmodningen, bortset fra adgang til lydoverførsel, og ingen data gemmes på tilbehøret.

HomeKit-datasikkerhed

HomeKit-data kan opdateres sikkert mellem en brugers iOS-, iPadOS- og macOS-enheder vha. iCloud og iCloud-nøglering. Som led i denne proces krypteres HomeKit-data med nøgler afledt af brugerens HomeKit-id og en tilfældig nonce-værdi, og disse data behandles som et *blob* – et uigennemsigtigt binært stort objekt. Det nyeste "blob" opbevares i iCloud, men bruges ikke til noget andet formål. Da krypteringen foretages med nøgler, der kun er tilgængelige på brugerens iOS-, iPadOS- og macOS-enheder, er der ikke adgang til dataene under overførslen eller på iCloud-lagringspladsen.

HomeKit-data synkroniseres også mellem flere brugere i samme hjem. Denne proces bruger samme godkendelse og kryptering som mellem en iOS-, iPadOS- eller macOS-enhed og et HomeKit-tilbehør. Godkendelsen er baseret på offentlige Ed25519-nøgler, der udveksles mellem enhederne, når en bruger føjes til et hjem. Når en ny bruger er føjet til et hjem, godkendes og krypteres al yderligere kommunikation via STS-protokollen og nøgler pr. session.

Den bruger, som oprindeligt oprettede hjemmet i HomeKit, og andre brugere med redigeringstilladelse kan tilføje nye brugere. Ejerens enhed konfigurerer tilbehøret med den nye brugers offentlige nøgle, så tilbehøret kan godkende og modtage kommandoer fra den nye bruger. Når en bruger med redigeringstilladelse tilføjer en ny bruger, overdrages processen til en hub for hjemmet, hvor handlingen færdiggøres.

HomeKit og Apple TV

Apple TV stilles automatisk til rådighed for HomeKit, når brugeren logger ind på iCloud. Tofaktorgodkendelse skal være slået til for iCloud-kontoen. Apple TV og ejerens enhed udveksler midlertidige, offentlige Ed25519-nøgler via iCloud. Når ejerens enhed og Apple TV er på samme lokalnetværk, bruges de midlertidige nøgler til at gøre forbindelser via lokalnetværket sikre ved hjælp af STS-protokollen (Station-to-Station) og nøgler pr. session. Denne proces bruger samme godkendelse og kryptering som mellem en iOS-, iPadOS- eller macOS-enhed og et HomeKit-tilbehør. Ejerens enhed overfører brugerens Ed25519-par med offentlige-private nøgler til Apple TV via denne sikre lokale forbindelse. Nøglerne bruges derefter til at gøre kommunikationen sikker mellem Apple TV og HomeKit-tilbehør og mellem Apple TV og andre iOS-, iPadOS- og macOS-enheder, der indgår i HomeKit-hjemmet.

Hvis en bruger ikke har flere enheder og ikke giver flere brugere adgang til sit hjem, overføres der ikke nogen HomeKit-data til iCloud.

Hjemmedata og apps

Adgang til hjemmedata fra apps styres af brugerens anonymitetsindstillinger. Brugerne bliver bedt om at give adgang, når apps anmoder om hjemmedata, i lighed med Kontakter, Fotos og andre iOS-, iPadOS- og macOS-datakilder. Hvis brugeren godkender det, har apps adgang til navne på værelser, navne på tilbehør, og hvilket værelse hvert enkelt tilbehør er placeret i, samt andre oplysninger, som er beskrevet i HomeKit-dokumentationen til udviklere på https://developer.apple.com/homekit/.

Lokal datalagring

HomeKit gemmer data om hjem, tilbehør, scener og brugere på en brugers iOS-, iPadOS- og macOS-enheder. De gemte data krypteres med nøgler afledt af brugerens HomeKit-id-nøgler plus en tilfældig nonce-værdi. Desuden bruges klassen Beskyttet indtil første brugergodkendelse i Databeskyttelse til opbevaring af HomeKit-data. HomeKit-data sikkerhedskopieres kun i krypterede sikkerhedskopier, så ikke-krypterede Finder-sikkerhedskopier (macOS 10.15 og nyere versioner) eller iTunes (i macOS 10.14 og tidligere versioner) via USB indeholder ikke HomeKit-data.

Beskyttelse af routere med HomeKit

Routere, der understøtter HomeKit, giver brugerne mulighed for at forbedre sikkerheden på brugernes hjemmenetværk ved at administrere den Wi-Fi-adgang, HomeKit-tilbehør har til det lokale netværk og til internettet. Routerne understøtter også PPSK-godkendelse (Private PSK), så tilbehør kan føjes til Wi-Fi-netværket med en nøgle, der er specifik for tilbehøret, og som kan tilbagekaldes efter behov. PPSK-godkendelse øger sikkerheden ved ikke at afsløre den primære Wi-Fi-adgangskode for tilbehør samt ved at give routeren mulighed for sikkert at identificere tilbehør, selvom det skulle ændre dens MAC-adresse.

Med appen Hjem kan en bruger konfigurere adgangsbegrænsninger for grupper af tilbehør som følger:

- *Ingen begrænsning:* Tillad ubegrænset adgang til internettet og det lokale netværk.
- *Automatisk:* Dette er standardindstillingen. Tillad adgang til internettet og det lokale netværk baseret på en liste over websteder og lokale porte, som Apple har modtaget fra tilbehørsproducenten. Denne liste omfatter alle de websteder og porte, som tilbehøret skal bruge for at fungere korrekt. (indtil en sådan liste er tilgængelig, gælder Ingen begrænsning).
- *Begræns til Hjem:* Ingen adgang til internettet eller det lokale netværk med undtagelse af de forbindelser, der kræves, for at HomeKit kan registrere og betjene tilbehøret fra det lokale netværk (herunder fra hubben for hjemmet for at understøtte fjernbetjening).

En PPSK er en stærk, personlig, tilbehørsspecifik WPA2-adgangskode, som genereres automatisk af HomeKit og tilbagekaldes, hvis tilbehøret senere fjernes fra hjemmet. En PPSK bruges, når tilbehør føjes til Wi-Fi-netværket af HomeKit i et hjem, der er konfigureret med en HomeKit-router. Tilføjelsen vises som Godkendelsesoplysninger til Wi-Fi: HomeKit-administreret på skærmen med indstillinger til tilbehøret i appen Hjem. Tilbehør, der blev føjet til Wi-Fi-netværket, før routeren blev tilføjet, omkonfigureres til at bruge en PPSK, hvis tilbehøret understøtter denne godkendelse, og ellers beholder tilbehøret de eksisterende godkendelsesoplysninger.

Som et yderligere sikkerhedstiltag skal brugerne konfigurere HomeKit-routeren vha. routerproducentens app, så appen kan validere, at brugerne har adgang til routeren og kan føje den til appen Hjem.

HomeKit-kamerasikkerhed

Kameraer, der har en internetprotokoladresse (IP) i HomeKit, sender video- og lydstreaming direkte til den iOS-, iPadOS-, tvOS- eller macOS-enhed på det lokale netværk, der opretter adgang til streamingen. Streamingen krypteres med tilfældige nøgler på enheden og IP-kameraet, og de udveksles via den sikre HomeKit-session med kameraet. Når en enhed ikke er på det lokale netværk, viderestilles den krypterede streaming via en hub for hjemmet til enheden. Hubben for hjemmet dekrypterer ikke streamingen. Den fungerer kun som et viderestillingspunkt mellem enheden og IP-kameraet. Når en app viser videobilledet fra IP-kameraet i HomeKit for brugeren, gengiver HomeKit videobillederne sikkert fra en separat systemproces. Det bevirker, at appen ikke kan få adgang til eller gemme videostreamingen. Apps har heller ikke tilladelse til at gemme skærmbilleder fra streamingen.

Sikker HomeKit-video

HomeKit har en mekanisme, der giver sikkerhed og anonymitet fra start til slut, til at optage, analysere og se klip fra HomeKit IP-kameraer, uden at dette videoindhold kan ses af Apple eller tredjepart. Når IP-kameraet registrerer bevægelse, sendes videoklip direkte til en Apple-enhed, der fungerer som hub for hjemmet, via en dedikeret lokal netværksforbindelse mellem denne hub og IP-kameraet. Den lokale netværksforbindelse krypteres med et nøglepar pr. session, som er afledt af HKDF-SHA512 og forhandles i HomeKit-sessionen mellem hubben for hjemmet og IP-kameraet. HomeKit dekrypterer lyd- og videostreams på hubben for hjemmet og analyserer videobillederne lokalt for at finde evt. vigtige begivenheder. Hvis HomeKit registrerer en vigtig begivenhed, krypteres videoklippet vha. AES-256-GCM med en tilfældig AES256-nøgle. HomeKit genererer også plakatbilleder for hvert klip, og disse plakatbilleder krypteres med samme AES256-nøgle. De krypterede plakatbilleder samt lyd- og videodata overføres til iCloud-servere. De relaterede metadata til hvert klip, herunder krypteringsnøglen, overføres til CloudKit vha. end-to-end-kryptering af iCloud.

Til klassificering af ansigter gemmer HomeKit alle de data, der bruges til at klassificere en bestemt persons ansigt, i CloudKit vha. end-to-end-kryptering af iCloud. De gemte data omfatter oplysninger om den enkelte person, f.eks. navn samt billeder, der repræsenterer personens ansigt. Disse ansigtsbilleder kan hentes fra en brugers Fotos, hvis brugeren vælger det, eller de kan indsamles fra videooptagelser fra IP-kameraet, der blev analyseret tidligere. Ved en analyseproces i Sikker HomeKit-video bruges disse klassificeringsdata til at identificere ansigter i den sikre videostreaming, den modtager direkte fra IP-kameraet, og disse id-oplysninger bliver så inkluderet i de metadata til klip, der blev nævnt ovenfor.

Når appen Hjem bruges til at se kameraklip, hentes dataene fra iCloud, og nøglerne til dekryptering af streams pakkes ud lokalt vha. end-to-end-kryptering af iCloud. Det krypterede videoindhold streames fra serverne, og dekrypteres lokalt på iOS-enheden, før det vises i fremviseren. Hver videoklipsession kan inddeles i undersektioner, hvor hver undersektion krypterer indholdsstreamen med sin egen unikke nøgle.

HomeKit-sikkerhed med Apple TV

HomeKit opretter sikre forbindelser mellem visse fjernbetjeningstilbehør fra tredjeparter og Apple TV og understøtter tilføjelse af brugerprofiler til ejeren af hjemmets Apple TV.

Brug af fjernbetjeningstilbehør fra tredjeparter med Apple TV

Visse typer tv-fjernbetjeningstilbehør fra tredjeparter leverer HID-begivenheder (Human Interface Design, dvs. brugergrænseflade) og Siri-lyd til en tilknyttet Apple TV-enhed, der er tilføjet via appen Hjem. Fjernbetjeningen sender HID-begivenhederne i den sikre session til Apple TV. En tv-fjernbetjening med Siri-funktion sender lyddata til Apple TV, når brugeren udtrykkeligt aktiverer mikrofonen på fjernbetjeningen ved at trykke på en dedikeret Siri-knap. Fjernbetjeningen sender lydrammerne direkte til Apple TV via en dedikeret lokal netværksforbindelse. Et nøglepar pr. session, som er afledt af HKDF-SHA512 og forhandles i HomeKit-sessionen mellem Apple TV og tv-fjernbetjeningen, bruges til at kryptere den lokale netværksforbindelse. HomeKit dekrypterer lydrammerne på Apple TV og sender dem til appen Siri, hvor de behandles med samme beskyttelse af anonymitet som al anden indgående lyd på Siri.

Apple TV-profiler til HomeKit-hjem

Når en bruger af et HomeKit-hjem føjer sin profil til ejeren af hjemmets Apple TV-enhed, får brugeren adgang til ejerens tv-udsendelser, musik og podcasts. Hver brugers indstillinger i forbindelse med brugerens profilbrug på Apple TV-enheden deles med ejerens iCloud-konto vha. end-to-end-kryptering af iCloud. Dataene ejes af brugeren og deles som skrivebeskyttede data med ejeren. Hver bruger af hjemmet kan ændre disse værdier i appen Hjem, og ejerens Apple TV-enhed bruger indstillingerne.

Når en indstilling slås til, bliver brugerens iTunes-konto tilgængelig på Apple TV-enheden. Når en indstilling slås fra, slettes den konto og alle de data, der tilhører brugeren, på Apple TV-enheden. Den første CloudKit-deling startes af brugerens enhed, og det token, der skal etablere den sikre CloudKit-deling, sendes via samme sikre kanal, som bruges til at synkronisere data mellem brugerne af hjemmet.

SiriKit-sikkerhed til iOS, iPadOS og watchOS

Siri bruger app-udvidelsessystemet til at kommunikere med apps fra tredjeparter. På en enhed kan Siri få adgang til brugerens kontaktoplysninger og enhedens aktuelle lokalitet. Før Siri giver en app adgang til beskyttede data, kontrollerer Siri appens brugerdefinerede adgangstilladelser. I henhold til disse tilladelser overfører Siri kun den relevante del af brugerens oprindelige talte besked til app-udvidelsen. Hvis en app f.eks. ikke har adgang til kontaktoplysninger, fortolker Siri ikke en relation i en brugerforespørgsel som "Send 100 kroner til min mor med Betalingsapp". Appen ville i dette tilfælde kun se "min mor" som almindelig tekst.

Hvis brugeren derimod har givet appen adgang til kontaktoplysninger, vil appen modtage fortolkede oplysninger om brugerens mor. Hvis en relation bliver omtalt i brødteksten i en besked, f.eks. "Skriv til min mor i BeskedApp, at min bror er genial", fortolker Siri ikke "min bror" uanset appens tilladelser.

Apps, som SiriKit er slået til for, kan sende app-specifikke eller brugerspecifikke gloser til Siri, f.eks. navnet på brugerens kontakter. Oplysningerne sætter Siris talegenkendelse og forståelse af naturligt sprog i stand til at genkende gloser til appen, og de er knyttet til et tilfældigt id. De specielle oplysninger er tilgængelige, så længe dette id er i brug, eller indtil brugeren slår appens integration med Siri fra i Indstillinger, eller appen, som SiriKit er slået til for, fjernes.

En anmodning som "Skaf kørsel hjem til min mor med SamkørselsApp" kræver lokalitetsdata fra brugerens kontakter. Siri leverer de ønskede oplysninger til appens udvidelse for den anmodning alene, uanset hvilke tilladelser brugeren har indstillet til lokalitets- eller kontaktoplysninger til appen.

DriverKit-sikkerhed til macOS

DriverKit er det framework, der sætter udviklere i stand til at oprette enhedsdrivere, som brugeren installerer på sin Mac. Drivere udviklet med DriverKit afvikles i området til brugere i stedet for som kerneudvidelser for at skabe større systemsikkerhed og -stabilitet. Det gør installeringen lettere og gør macOS mere stabilt og sikkert.

Brugeren henter blot appen (når der bruges systemudvidelser eller DriverKit, er installeringsapps ikke nødvendige), og udvidelsen slås kun til, når der er behov for den. På mange anvendelsesområder erstatter de kext'er, som kræver administratorrettigheder for at blive installeret i /System/Bibliotek eller /Bibliotek.

It-administratorer, som bruger enhedsdrivere, løsninger til lagring i skyen, netværksforbindelser og sikkerhedsapps, der kræver kerneudvidelser, opfordres til at skifte til nyere versioner, som bygger på systemudvidelser. De nyere versioner gør risikoen for kernepanik på Mac meget mindre og gør også angrebsfladen mindre. De nye udvidelser afvikles i området til brugere, kræver ikke særlige rettigheder til installering og fjernes automatisk, når den app, de er indeholdt i, flyttes til papirkurven.

DriverKit-framework indeholder C++ klasser til I/O-tjenester, matchning af enheder, hukommelsesbeskrivelser og afviklingskøer. Det definerer også I/O-relevante typer til tal, samlinger, strenge og andre almindelige datatyper. Brugeren anvender dem med familiespecifikke driver-frameworks som USBDriverKit og HIDDriverKit. Brug frameworket System Extensions til at installere og opgradere en driver.

ReplayKit-sikkerhed i iOS og iPadOS

ReplayKit er et framework, som udviklere kan bruge til at tilføje optagelses- og liveudsendelsesfunktioner i deres apps. Det giver også brugerne mulighed for at føje noter til deres optagelser og udsendelser ved hjælp af kameraet og mikrofonen på enhedens forside.

Optagelse af film

Der er flere indbyggede sikkerhedslag, når der optages film:

- *Dialogen Tilladelser:* Inden optagelsen starter, viser ReplayKit en samtykkeadvarsel for brugerne, der giver dem mulighed for at bekræfte, at de har til hensigt at optage skærmen, mikrofonen og kameraet på forsiden. Advarslen vises en gang pr. proces i appen. Hvis appen er i baggrunden længere end 8 minutter, vises advarslen igen.
- *Optagelse af skærm og lyd:* Optagelse af skærm og lyd sker uden for appens proces i dæmonen replayd i ReplayKit. Formålet er at sikre, at appens proces aldrig har adgang til det optagede indhold.
- *Optagelse af skærm og lyd fra app:* Dette sætter en app i stand til at hente video- og eksempelbuffere, som beskyttes af tilladelsesdialogen.
- *Oprettelse og opbevaring af film:* Filmarkivet skrives til et bibliotek, som kun ReplayKit-subsystemerne har adgang til. Apps kan aldrig få adgang. Det er med til at forhindre, at optagelser kan bruges af tredjepart uden brugerens samtykke.
- *Brugerens filmfremvisning og deling:* Brugeren kan se et eksempel på og dele filmen fra en brugergrænseflade, der stilles til rådighed af ReplayKit. Brugergrænsefladen præsenteres uden om processen via udvidelsesinfrastrukturen i iOS og har adgang til det oprettede filmarkiv.

ReplayKit-udsendelse

Der er flere indbyggede sikkerhedslag, når der udsendes film:

- *Optagelse af skærm og lyd:* Teknikken til optagelse af skærm og lyd under udsendelse er den samme som til filmoptagelse og foregår i `replayd`.
- *Udvidelser til udsendelse:* Hvis tjenester fra tredjeparter vil deltage i udsendelse via ReplayKit, skal de oprette to nye udvidelser, der konfigureres med slutpunktet com.apple.broadcast-services:
  - En udvidelse af brugergrænsefladen, der gør det muligt for brugeren at indstille sin udsendelse
  - En udvidelse til overførsel, der håndterer overførsel af video- og lyddata til tjenestens backend-servere

Arkitekturen er med til at sikre, at værtsapps ikke har nogen rettigheder til det udsendte video- og lydindhold. Kun ReplayKit og tredjeparters udvidelser til udsendelse har adgang.

- *Vælger til udsendelser:* Med vælgeren til udsendelser kan brugere starte systemudsendelser direkte fra appen vha. den samme systemdefinerede brugergrænseflade som den, der er tilgængelig via Kontrolcenter. Brugergrænsefladen er implementeret ved hjælp af et privat API og er en udvidelse i ReplayKit-framework. Den er ikke til rådighed for værtsappens proces.
- *Udvidelse til overførsel:* Den udvidelse, som tredjeparters tjenester til udsendelse implementerer for at håndtere video- og lydindhold under udsendelse, bruger ubehandlede eksempelbuffere, der ikke er kodet. Med denne håndteringsfunktion serialiseres video- og lyddata og videregives til tredjepartens udvidelse til overførsel i realtid via en direkte XPC-forbindelse. Videodata kodes ved at uddrage IOSurface-objektet fra bufferen med videoeksempler, kode denne sikkert som et XPC-objekt, sende den via XPC til tredjepartens udvidelse og afkode den sikkert til et IOSurface-objekt igen.

ARKit-sikkerhed i iOS og iPadOS

ARKit er et framework, som udviklere kan bruge til at skabe AR-oplevelser (augmented reality) i deres apps og spil. Udviklerne kan tilføje 2D- eller 3D-elementer via kameraerne på forsiden og bagsiden af en iOS- eller iPadOS-enhed.

Apple har udviklet kameraer med anonymitet for øje, og apps fra tredjeparter skal have brugerens samtykke, før de får adgang til kameraet. I iOS og iPadOS kan en app, som brugeren giver adgang til kameraet, få adgang til billeder i realtid fra kameraerne på forsiden og bagsiden. Apps har ikke tilladelse til at bruge kameraet uden at oplyse om, at det er i brug.

Fotos og videoer, der er taget med kameraet, kan indeholde oplysninger, f.eks. hvor og hvornår de blev taget eller optaget, dybdeeffekten og overcapture. Hvis brugerne ikke ønsker, at de fotos og videoer, der tages eller optages med appen Kamera, skal indeholde lokalitet, kan de altid ændre det ved at gå til Indstillinger > Anonymitet > Lokalitetstjenester > Kamera. Hvis brugerne ikke ønsker, at fotos og videoer indeholder lokalitet, når de deles, kan de slå lokalitet fra på menuen Indstillinger på siden til deling.

For bedre at positionere brugerens AR-oplevelse kan apps, der bruger ARKit, bruge verdens- eller ansigtsregistreringsoplysninger fra det andet kamera. Verdensregistrering bruger algoritmer på brugerens enhed til at behandle oplysninger fra disse sensorer med henblik på at bestemme deres position i forhold til et fysisk sted. Verdensregistrering slår funktioner som Optisk retning til i Kort.

Sikker administration af enheder

Oversigt over sikker administration af enheder

iOS, iPadOS, macOS og tvOS understøtter fleksible sikkerhedspolitikker og -konfigurationer, der er nemme at håndhæve og administrere. Via dem kan organisationerne beskytte virksomhedens oplysninger og bidrage til at sikre, at medarbejderne opfylder kravene i virksomheden, også selvom de bruger enheder, de selv har medbragt, f.eks. som et led i et BYOD-program ("bring your own device").

Organisationerne kan bruge ressourcer som adgangskodebeskyttelse, konfigurationsprofiler, ekstern sletning og løsninger til administration af mobile enheder (MDM) fra tredjeparter til at administrere samlinger af enheder og hjælpe med at beskytte virksomhedens data, også selvom medarbejderne opretter adgang til data fra deres personlige enheder.

Apple-enheder med iOS 13 og nyere versioner, iPadOS 13.1 og nyere versioner eller macOS 10.15 og nyere versioner understøtter en ny mulighed for brugertilmelding, der er udviklet specielt til BYOD-programmer. Brugertilmelding giver brugerne større råderet på deres egne enheder og øger samtidig sikkerheden for virksomhedens data, der opbevares på en separat APFS-enhed (Apple File System), der er beskyttet kryptografisk. Det giver en bedre balance mellem sikkerhed, anonymitet og brugeroplevelse i BYOD-programmer.

Sikkerhed i pardannelsesmodel på iPhone og iPad

iOS og iPadOS bruger en pardannelsesmodel til at styre adgangen til en enhed fra en værtscomputer. Under pardannelse etableres en godkendt relation mellem enheden og dens tilsluttede vært i kraft af udveksling af en offentlig nøgle. iOS og iPadOS bruger også denne godkendelse til at slå yderligere funktionalitet til for den tilsluttede vært, f.eks. datasynkronisering. I iOS 9 og nyere versioner gælder, at tjenester:

- der kræver pardannelse, ikke kan startes, før brugeren har låst enheden op
- ikke starter, medmindre enheden er blevet låst op for nylig
- (f.eks. ved synkronisering af fotos) måske kræver, at enheden er låst op, før de kan startes

Under pardannelsesprocessen skal brugeren låse enheden op og acceptere anmodningen om pardannelse fra værten. I iOS 9 og nyere versioner skal brugeren også indtaste sin kode, hvorefter værten og enheden udveksler og gemmer de offentlige 2048-bit RSA-nøgler. Værten får derefter en 256-bit nøgle, der kan låse en nøglesamling af typen Depot, som er gemt på enheden, op. De udvekslede nøgler bruges til at starte en krypteret SSL-session, som skal være åbnet, før enheden sender beskyttede data til værten eller starter en tjeneste (synkronisering i iTunes eller Finder, arkivoverførsler, Xcode-udvikling osv.). Enheden kræver forbindelser fra en vært via Wi-Fi, før denne krypterede session kan bruges til al kommunikation, så der skal tidligere have været etableret pardannelse via USB. Ved pardannelsen slås desuden flere muligheder for diagnosticering til. I iOS 9 udløber en pardannelsespost, hvis den ikke har været brugt i mere end 6 måneder. I iOS 11 og nyere versioner er denne periode forkortet til 30 dage.

Visse diagnosticeringstjenester, herunder com.apple.mobile.pcapd, er begrænset, så de kun fungerer via USB. Tjenesten com.apple.file_relay kræver desuden, at der installeres en konfigurationsprofil, der er signeret af Apple. I iOS 11 og nyere versioner kan Apple TV bruge SRP-protokollen (Secure Remote Password) til at danne par trådløst.

En bruger kan rydde listen over godkendte værter med valgmuligheden Nulstil netværksindstillinger eller Nulstil lokalitet & anonymitet.

Administration af mobile enheder

Oversigt over sikkerhed i administration af mobile enheder

Apples operativsystemer understøtter administration af mobile enheder (MDM), som sætter organisationer i stand til at konfigurere og administrere skalerede udrulninger af Apple-enheder på en sikker måde.

Sådan fungerer MDM sikkert

MDM-funktionerne bygger på eksisterende operativsystemteknologier som konfigurationsprofiler, trådløs tilmelding og tjenesten Apple Push Notification (APNs). APNs bruges f.eks. til at afbryde vågeblus på en enhed, så den kan kommunikere direkte med sin MDM-løsning via en sikker forbindelse. Med APNs overføres ingen fortrolige oplysninger eller oplysninger tilhørende virksomheden.

Med MDM kan it-afdelinger indrullere Apple-enheder i et virksomhedsmiljø, konfigurere og opdatere indstillinger trådløst, overvåge overholdelse af virksomhedens politikker, administrere politikker for softwareopdateringer og endda slette eller låse administrerede enheder eksternt.

Udover de traditionelle enhedstilmeldinger, der understøttes af iOS, iPadOS, macOS og tvOS, er der tilføjet en tilmeldingstype i iOS 13 og nyere versioner, iPadOS 13.1 og nyere versioner og macOS 10.15 og nyere versioner – Brugertilmelding. Brugertilmeldinger er MDM-tilmeldinger, der retter sig specifikt mod BYOD-implementeringer (Bring Your Own Device), hvor enheden er ejet personligt, men bruges i et administreret miljø. Brugertilmelding giver MDM-løsningen mere begrænsede rettigheder i forhold til tilmelding af enheder, der ikke er under tilsyn, og adskiller brugerdata og virksomhedsdata ved hjælp af kryptografi.

Tilmeldingstyper

- *Automatisk tilmelding af enhed:* Automatisk tilmelding af enhed giver organisationer mulighed for at konfigurere og administrere enheder fra det øjeblik, enhederne tages ud af æsken (som led i en proces kaldet *Auto Advance-implementering*). Disse enheder betegnes som *under tilsyn*, og it-afdelingen kan vælge at forhindre, at brugeren kan fjerne MDM-profilen. Automatisk tilmelding af enhed er beregnet til enheder ejet af en organisation.
- *Tilmelding af enhed:* Med tilmelding af enheder kan organisationer vælge, at de vil lade brugerne tilmelde enheder manuelt, og derefter stadig administrere mange forskellige aspekter af enhedsbrug, herunder muligheden for at slette enheden. Tilmelding af enhed omfatter også et større udvalg af data og begrænsninger, der kan anvendes på enheden. Når en bruger fjerner en tilmeldingsprofil, bliver alle konfigurationsprofiler, deres indstillinger og administrerede apps, som er baseret på denne tilmeldingsprofil, også fjernet.
- *Brugertilmelding:* Brugertilmelding er designet til enheder, der ejes af brugeren, og er integreret med Administrerede Apple-id'er for at etablere en brugeridentitet på enheden. Administrerede Apple-id'er er en del af brugertilmeldingsprofilen og skal godkendes, før tilmeldingen kan gennemføres. Administrerede Apple-id'er kan bruges sideløbende med et personligt Apple-id, som brugeren allerede er logget ind med. Administrerede apps og konti bruger et administreret Apple-id, og personlige apps og konti bruger et personligt Apple-id.

Begrænsninger for enheder

Administratorer kan slå begrænsninger til og i nogle tilfælde slå dem fra for at bidrage til at forhindre brugerne i at få adgang til bestemte apps, tjenester eller funktioner på en iPhone, iPad, Mac eller Apple TV-enhed, der er tilmeldt en MDM-løsning. Begrænsninger sendes til enheder i begrænsningsdata, som indgår i en konfigurationsprofil. Visse begrænsninger på en iPhone kan blive dubleret på et parret Apple Watch.

Administration af indstillinger til koder og adgangskoder

Brugerens kode kan som standard defineres som en numerisk PIN-kode. På iOS- og iPadOS-enheder med Face ID eller Touch ID skal koden have mindst fire cifre. Det anbefales at bruge længere og mere komplekse koder, fordi de er sværere at gætte eller angribe.

Administratorer kan gennemtvinge krav om komplekse koder og andre politikker via MDM eller Microsoft Exchange ActiveSync eller ved at kræve, at brugerne manuelt installerer konfigurationsprofiler. Der skal bruges en administratoradgangskode til installering af data til kodepolitik i macOS. Nogle kodepolitikker kan fastlægge, at koder skal have en bestemt længde eller sammensætning eller andre egenskaber.

Håndhævelse af konfigurationsprofiler

Konfigurationsprofiler er den metode, som en MDM-løsning primært bruger til at levere og administrere politikker og begrænsninger på administrerede enheder. Hvis organisationer har brug for at konfigurere et stort antal enheder – eller overføre mange specielle e-mailindstillinger, netværksindstillinger eller certifikater til et stort antal enheder – kan det gøres på en sikker måde ved hjælp af konfigurationsprofiler.

Konfigurationsprofiler

En *konfigurationsprofil* er et XML-arkiv (hvis navn ender på .mobileconfig), som består af data, der indlæser indstillinger og oplysninger om godkendelse på Apple-enheder. Konfigurationsprofiler sørger for, at konfigurationen af indstillinger, konti, begrænsninger og godkendelsesoplysninger sker automatisk. Disse arkiver kan oprettes af en MDM-løsning eller Apple Configurator til Mac, eller de kan oprettes manuelt. Inden organisationer sender en konfigurationsprofil til en enhed, skal de tilmelde enheden i MDM-løsningen ved hjælp af en tilmeldingsprofil.

Tilmeldingsprofiler

En *tilmeldingsprofil* er en konfigurationsprofil med MDM-data, der tilmelder enheden i den MDM-løsning, der er anført for den pågældende enhed. Dermed kan MDM-løsningen sende kommandoer og konfigurationsprofiler til enheden og forespørgsler om visse aspekter af enheden. Når en bruger fjerner en tilmeldingsprofil, bliver alle konfigurationsprofiler, deres indstillinger og administrerede apps, som er baseret på denne tilmeldingsprofil, også fjernet. Der kan kun være en tilmeldingsprofil ad gangen på en enhed.

Indstillinger til konfigurationsprofil

En konfigurationsprofil indeholder et antal indstillinger i bestemte data, der kan angives, herunder (men ikke begrænset til):

- Politikker for koder og adgangskoder
- Begrænsning af funktioner på enheden (f.eks. slå kameraet fra)
- Netværks- og VPN-indstillinger
- Microsoft Exchange-indstillinger
- E-mailindstillinger
- Kontoindstillinger
- Indstillinger til LDAP-bibliotekstjenesten
- Indstillinger til CalDAV-kalendertjenesten
- Godkendelsesoplysninger og nøgler
- Softwareopdateringer

Profilsignering og -kryptering

Konfigurationsprofiler kan signeres med henblik på at bekræfte deres oprindelse og krypteres for at bidrage til at sikre deres integritet og beskytte deres indhold. Konfigurationsprofiler til iOS og iPadOS krypteres ved hjælp af CMS (Cryptographic Message Syntax), der er defineret i RFC 5652 og understøtter 3DES og AES128.

Installering af profiler

Brugerne kan installere konfigurationsprofiler direkte på deres enheder ved at bruge Apple Configurator til Mac, eller de kan hentes via Safari, sendes som et bilag til en e-mail, overføres via AirDrop eller appen Arkiver i iOS og iPadOS eller overføres trådløst via en løsning til administration af mobile enheder (MDM). Når en bruger indstiller en enhed i Apple School Manager eller Apple Business Manager, henter og installerer enheden en profil til tilmelding til MDM. Du kan læse, hvordan du fjerner profiler, i Introduktion til administration af mobile enheder i Implementering af Apples platforme.

Bemærk: På enheder under tilsyn kan konfigurationsprofiler fastlåses på en enhed. Formålet er at forhindre, at de fjernes, eller bestemme, at de kun kan fjernes med en adgangskode. Da mange organisationer selv ejer deres iOS- eller iPadOS-enheder, er det muligt at fjerne konfigurationsprofiler, der binder en enhed til en MDM-løsning, men hvis de fjernes, bliver alle administrerede konfigurationsoplysninger, data og apps også fjernet.

Automatisk tilmelding af enhed

Organisationer kan automatisk tilmelde iOS-, iPadOS-, macOS- og tvOS-enheder til administration af mobile enheder (MDM) uden at røre eller klargøre enhederne fysisk, før brugerne får dem. Når administratorerne har tilmeldt sig en af tjenesterne, logger de ind på tjenestens websted og knytter appen til deres MDM-løsning. De enheder, de har købt, kan derefter tildeles til brugerne via MDM. Under konfiguration af enheden kan sikkerheden for følsomme data øges ved at sikre, at de rette sikkerhedsforanstaltninger er på plads. F.eks.:

- Sørge for, at brugerne skal godkendes som en del af den første indstillingsprocedure i Apple-enhedens Indstillingsassistent under aktivering.
- Sørge for at have en foreløbig konfiguration med begrænset adgang og kræve yderligere enhedskonfiguration, før der gives adgang til følsomme data.

Når en bruger er blevet tilmeldt, installeres alle konfigurationer, begrænsninger eller betjeningsmuligheder, der er angivet i MDM, automatisk. Al kommunikation mellem enheder og Apple-servere krypteres under overførsel ved hjælp af HTTPS (TLS).

Indstillingsprocessen for brugerne kan forenkles yderligere, ved at bestemte trin i Indstillingsassistent fjernes for enheder, så brugerne hurtigt kommer op at køre. Administratorerne kan også styre, om brugerne må fjerne MDM-profilen fra enheden, og de kan være med til at sikre, at enhedsbegrænsningerne håndhæves i hele enhedens levetid. Når enheden er pakket ud og aktiveret, kan den tilmeldes organisationens MDM-løsning, og alle administrationsindstillinger, apps og bøger installeres som defineret af MDM-administratoren.

Apple School Manager, Apple Business Manager og Apple Business Essentials

Apple School Manager, Apple Business Manager, and Apple Business Essentials er tjenester til it-administratorer, der gør dem i stand til at implementere Apple-enheder, som en organisation har købt direkte fra Apple eller via autoriserede Apple-forhandlere eller -udbydere, der deltager i programmet.

Når der bruges en MDM-løsning, kan administratorerne forenkle processen for brugerne, konfigurere enhedsindstillinger og distribuere apps og bøger, der er købt hos disse tre tjenester. Apple School Manager kan integreres med Student Information Systems (SIS'er) direkte eller via SFTP, og alle tre tjenester kan bruge SCIM (System for Cross-domain Identity Management) eller godkendelse via organisationsnetværket med Microsoft Azure Active Directory (Azure AD), så administratorer hurtigt kan oprette konti.

Apple opretholder certificeringer i overensstemmelse med standarderne ISO/IEC 27001 og 27018 for at give Apples kunder mulighed for at opfylde deres lovgivnings- og kontraktmæssige forpligtelser. Disse certificeringer forsyner vores kunder med et uafhængigt vidnesbyrd om Apples praksis med hensyn til informationsanonymitet og -sikkerhed i behandlede systemer. Du kan få flere oplysninger under Sikkerhedscertificeringer af Apples internettjenester i Certificeringer af Apples platforme.

Bemærk: Du kan se, om et Apple-program er tilgængeligt i dit land eller område, i Apple-supportartiklen Tilgængelighed af Apple-programmer og betalingsmetoder for uddannelsesinstitutioner og virksomheder.

Tilsyn med enheder

Under tilsyn betyder almindeligvis, at enheden ejes af organisationen, der får ekstra kontrol over enhedens konfiguration og begrænsninger. Du kan få flere oplysninger i Om tilsyn med Apple-enheder i Implementering af Apples platforme.

Sikkerhed i Aktiveringslås

Apples måde at håndhæve Aktiveringslås på afhænger af, om enheden er en iPhone eller en iPad, en Mac med Apple Silicon eller en Intel-baseret Mac med Apple T2-sikkerhedschippen.

Virkemåde på iPhone og iPad

På iPhone- og iPad-enheder håndhæves Aktiveringslås under aktiveringen efter skærmen til valg af Wi-Fi i Indstillingsassistent i iOS og iPadOS. Når en enhed anfører, at den er ved at blive aktiveret, sender den en anmodning om et aktiveringscertifikat til en Apple-server. Enheder, der er låst med Aktiveringslås, beder brugeren om iCloud-godkendelsesoplysningerne til den bruger, der slog Aktiveringslås til denne gang. Indstillingsassistent i iOS og iPadOS fortsætter ikke, medmindre der kan fremskaffes et gyldigt certifikat.

Virkemåde på en Mac med Apple Silicon

På en Mac med Apple Silicon kontrollerer LLB, at der findes en gyldig LocalPolicy til enheden, og at nonce-værdierne til LocalPolicy-politikken svarer til de værdier, der opbevares i komponenten til sikker opbevaring. LLB starter i macOS-gendannelse, hvis:

- Der ikke er nogen LocalPolicy til det aktuelle macOS
- LocalPolicy er ugyldig for dette macOS
- Hash-værdierne til LocalPolicys nonce-værdi ikke svarer til hash-værdierne til de værdier, der opbevares i komponenten til sikker opbevaring

macOS-gendannelse registrerer, at Mac-computeren ikke er aktiveret og kontakter aktiveringsserveren for at rekvirere et aktiveringscertifikat. Hvis Aktiveringslås er slået til på enheden, beder macOS-gendannelse brugeren om de iCloud-godkendelsesoplysninger, der blev brugt til at slå Aktiveringslås til denne gang. Når der er rekvireret et gyldigt aktiveringscertifikat, bruges aktiveringscertifikatet til at fremskaffe et RemotePolicy-certifikat. Mac-computeren bruger LocalPolicy-nøglen og RemotePolicy-certifikatet til at danne en gyldig LocalPolicy. LLB tillader ikke, at computeren startes i macOS, medmindre der forefindes en gyldig LocalPolicy.

Virkemåde på Intel-baserede Mac-computere

På en Intel-baseret Mac med en T2-chip kontrollerer firmwaren på T2-chippen, at der forefindes et gyldigt aktiveringscertifikat, før den tillader, at computeren startes i macOS. UEFI-firmware, der er indlæst af T2-chippen, er ansvarlig for at anmode om enhedens aktiveringsstatus fra T2-chippen og starte i macOS-gendannelse i stedet for macOS, hvis der ikke forefindes et gyldigt aktiveringscertifikat. macOS-gendannelse registrerer, at Mac ikke er aktiveret, og kontakter aktiveringsserveren for at rekvirere et aktiveringscertifikat. Hvis Aktiveringslås er slået til på enheden, beder macOS-gendannelse brugeren om de iCloud-godkendelsesoplysninger, der blev brugt til at slå Aktiveringslås til denne gang. UEFI-firmwaren tillader ikke, at computeren startes i macOS, medmindre der forefindes et gyldigt aktiveringscertifikat.

Administreret mistet funktion og ekstern sletning

Administreret mistet funktion bruges til at finde enheder under tilsyn, der er blevet stjålet. Når de bliver fundet, kan de låses eller slettes eksternt.

Administreret mistet funktion

Hvis en iOS- eller iPadOS-enhed under tilsyn med iOS 9 eller en nyere version bliver væk eller bliver stjålet, kan en administrator af en løsning til administration af mobile enheder (MDM) eksternt slå funktionen Mistet (kaldes Administreret mistet funktion) til på enheden. Når Administreret mistet funktion slås til, logges den aktuelle bruger ud, og enheden kan ikke låses op. På skærmen vises en besked, som administratoren kan tilpasse. Det kan f.eks. være et telefonnummer, der kan ringes til, hvis nogen finder enheden. Administratoren kan også få enheden til at sende sin nuværende lokalitet (selvom Lokalitetstjenester er slået fra) og eventuelt afspille en lyd. Kun en administrator kan slå Administreret mistet funktion fra. Når funktionen slås fra, får brugeren besked om det på den låste skærm eller på hjemmeskærmen.

Ekstern sletning

iOS-, iPadOS- og macOS-enheder kan slettes eksternt af en administrator eller bruger (øjeblikkelig ekstern sletning er kun tilgængelig, hvis FileVault er slået til på Mac). Øjeblikkelig ekstern sletning foretages ved, at medienøglen slettes i Effaceable Storage (sletbart lager) på en sikker måde, hvorved alle data bliver ulæselige. I tilfælde af ekstern sletning via Microsoft Exchange ActiveSync udfører enheden en kontrol på Microsoft Exchange-serveren, inden den udfører sletningen.

Når en kommando til ekstern sletning udløses af MDM eller iCloud, sender iPhone-, iPad-, iPod touch- eller Mac-enheden en bekræftelse tilbage til MDM-løsningen og udfører sletningen.

Ekstern sletning er ikke mulig i følgende situationer:

- Sammen med Brugertilmelding
- Via Microsoft Exchange ActiveSync, hvis kontoen blev installeret med Brugertilmelding
- Via Microsoft Exchange ActiveSync, hvis enheden er under tilsyn

Brugerne kan også slette de iOS- og iPadOS-enheder, de råder over, ved at bruge appen Indstillinger. Som beskrevet tidligere kan iOS- og iPadOS-enheder indstilles, så de automatisk slettes efter en række mislykkede kodeforsøg.

Sikkerhed med Delt iPad i iPadOS

Delt iPad er en flerbrugerfunktion til brug i iPad-implementeringer. Den giver brugerne mulighed for at dele en iPad, uden at hver brugers dokumenter og data deles. Hver bruger får sin egen private og reserverede lagringsplads, som oprettes som en APFS-enhed (Apple File System), der beskyttes af brugerens godkendelsesoplysninger. Delt iPad forudsætter brug af administrerede Apple-id'er, der udstedes og ejes af organisationen.

Med delt iPad kan en studerende logge ind på en hvilken som helst enhed, der ejes af organisationen og er indstillet til at blive brugt af flere brugere. Brugernes data opbevares i særskilte mapper, der har hver sit databeskyttelsesdomæne og både beskyttes med UNIX-tilladelser og brug af et isoleret miljø (“sandbox”). I iPadOS 13.4 og nyere versioner kan brugerne også logge ind på en midlertidig session. Når en bruger logger ud af en midlertidig session, slettes brugerens APFS-enhed, og den reserverede plads på enheden leveres tilbage til systemet.

Log ind på Delt iPad

Administrerede Apple-id'er, der både er indbyggede og på organisationsnetværk, understøttes til login på Delt iPad. Første gang en bruger vil have adgang til en konto på organisationsnetværket, omdirigeres brugeren til identitetsudbyderens login-portal. Når brugeren er godkendt, udstedes et adgangstoken med kort levetid til de understøttende administrerede Apple-id'er, og login-processen fortsætter på samme måde som den indbyggede login-proces til administrerede Apple-id'er. Når brugeren er logget ind, bliver brugeren af Indstillingsassistent på Delt iPad bedt om at oprette en kode (godkendelsesoplysning), der skal bruges til at beskytte de lokale data på enheden og til at blive godkendt på login-skærmen fremover. På samme måde som en enhed med en enkelt bruger, hvor brugeren logger ind på sin konto på organisationsnetværket med sit administrerede Apple-id og derefter låser sin enhed op med koden, logger en bruger på Delt iPad ind på sin konto på organisationsnetværket første gang og bruger derefter sin oprettede kode.

Når en bruger logger ind uden godkendelse via organisationsnetværket, godkendes det administrerede Apple-id af Apples IDS (Identity Service) ved hjælp af SRP-protokollen. Hvis godkendelse lykkes, udstedes der et midlertidigt adgangstoken specielt til enheden. Hvis brugeren har brugt enheden før, har vedkommende allerede en lokal brugerkonto, der låses op med samme godkendelsesoplysninger.

Hvis brugeren ikke har brugt enheden før eller bruger funktionen med midlertidige sessioner, sørger Delt iPad for, at der oprettes et nyt UNIX-bruger-id, en APFS-enhed med brugerens personlige data og en lokal nøglering. Da lagringspladsen tildeles (reserveres) til brugeren på det tidspunkt, hvor APFS-enheden oprettes, er der måske ikke plads nok til at oprette en ny enhed. I så fald vil systemet finde en eksisterende bruger, hvis data er blevet synkroniseret til skyen, og fjerne den bruger fra enheden for at give den nye bruger mulighed for at logge ind. Hvis den usandsynlige situation skulle opstå, hvor ingen af de eksisterende brugeres data er færdige med at blive overført til skyen, kan den nye bruger ikke logge ind. Den nye bruger må vente med at logge ind, til synkroniseringen af en af de eksisterende brugeres data er færdig, eller få en administrator til at slette en eksisterende brugers konto med risiko for tab af data.

Hvis enheden ikke har forbindelse til internettet (f.eks. fordi brugeren ikke har et Wi-Fi-adgangspunkt), kan der foretages godkendelse i forhold til den lokale konto i et begrænset antal dage. I den situation kan kun brugere, der allerede har en lokal konto eller en midlertidig session, logge ind. Når den begrænsede tid er gået, skal brugerne godkendes på nettet, også selvom de allerede har en lokal konto.

Når en brugers lokale konto er låst op eller oprettet, konverteres det midlertidige token, som blev udstedt af Apples servere (hvis godkendelsen foretages eksternt), til et iCloud-token, der gør det muligt at logge ind på iCloud. Derefter gendannes brugerens indstillinger, og vedkommendes dokumenter og data synkroniseres fra iCloud.

Så længe en brugersession er aktiv, og enheden har forbindelse til internettet, gemmes oprettede og ændrede dokumenter og data i iCloud. En synkroniseringsfunktion i baggrunden er desuden med til at sørge for, at ændringer overføres til iCloud eller en anden webtjeneste ved hjælp af NSURLSession-baggrundssessioner, efter at brugeren har logget ud. Når synkronisering i baggrunden er færdig for brugeren, gøres brugerens APFS-enhed passiv, og den kan ikke aktiveres igen, uden at brugeren logger ind igen.

Midlertidige sessioner synkroniserer ikke data med iCloud, og selvom der kan logges ind på en synkroniseringstjeneste fra en tredjepart, f.eks. Box eller Google, fra en midlertidig session, er der ingen funktion, der kan fortsætte synkroniseringen af data, når den midlertidige session slutter.

Log ud af Delt iPad

Når en bruger logger ud af Delt iPad, låses den pågældende brugers nøglesamling med det samme, og alle apps lukkes ned. iPadOS udskyder nogle almindelige log ud-handlinger midlertidigt for at gøre processen hurtigere, når en ny bruger logger ind, og viser et vindue, hvor den nye bruger kan logge ind. Hvis en bruger logger ind i dette tidsrum (ca. 30 sekunder), udfører Delt iPad den udsatte oprydning som en del af processen, når den nye bruger logger ind. Hvis Delt iPad forbliver passiv, startes den udsatte oprydning. Login-vinduet genstartes under oprydningsprocessen, som hvis der var blevet logget ud igen.

Når en midlertidig session slutter, udfører Delt iPad hele log ud-processen og sletter straks den midlertidige sessions APFS-enhed.

Sikkerhed i Apple Configurator

Apple Configurator til Mac har et fleksibelt, sikkert design, der har fokus på enheder og sætter en administrator i stand til hurtigt og nemt at konfigurere en eller mange iOS-, iPadOS- og tvOS-enheder, der er sluttet til en Mac via USB (eller tvOS-enheder parret via Bonjour), inden enhederne udleveres til brugere. Med Apple Configurator til Mac kan en administrator opdatere software, installere apps og konfigurationsprofiler, omdøbe og skifte baggrund på enheder, eksportere enhedsoplysninger og dokumenter m.m.

Apple Configurator til Mac kan også genoplive eller gendanne Mac-computere med Apple Silicon og dem med Apple T2-sikkerhedschip. Når en Mac genoplives eller gendannes på denne måde, hentes det arkiv, der indeholder de seneste mindre opdateringer til operativsystemet (macOS, macOS-gendannelse til Apple Silicon eller sepOS til T2), på en sikker måde fra Apples servere og installeres direkte på Mac. Når genoplivningen eller gendannelsen er gennemført, slettes arkivet fra den Mac, hvor Apple Configurator afvikles. Brugeren kan på intet tidspunkt undersøge eller bruge dette arkiv uden for Apple Configurator.

Administratorer kan også vælge at føje enheder til Apple School Manager, Apple Business Manager eller Apple Business Essentials ved at bruge Apple Configurator til Mac eller Apple Configurator til iPhone, også selvom enhederne ikke er købt direkte fra Apple, en autoriseret Apple-forhandler eller en autoriseret mobiloperatør. Når administratoren indstiller en enhed, der er tilmeldt manuelt, fungerer den som alle andre enheder i en af disse tjenester med obligatorisk tilsyn og tilmelding til administration af mobile enheder (MDM). Brugerne af enheder, der ikke er købt direkte, har en frist på 30 dage til at fjerne enheden fra en af disse tjenester og fra tilsyn og MDM.

Organisationer kan også bruge Apple Configurator til Mac til at aktivere iOS-, iPadOS- og tvOS-enheder, som ikke har nogen form for internetforbindelse, ved at slutte dem til en Mac-værtscomputer med internetforbindelse, mens enhederne indstilles. Administratorer kan gendanne, aktivere og klargøre enheder med den nødvendige konfiguration, herunder apps, profiler og dokumenter, helt uden at oprette forbindelse til hverken Wi-Fi-netværk eller mobilnetværk. Denne funktion gør det ikke muligt for en administrator at tilsidesætte eventuelle krav til Aktiveringslås, som normalt kræves ved aktivering uden tilslutning til en værtscomputer.

Sikkerhed i Skærmtid

Skærmtid er en indbygget funktion, der kan registrere og administrere, hvor meget tid voksne og deres børn bruger på apps, websteder m.m. Der er to typer brugere: voksne og (administrerede) børn.

Skærmtid er ikke en ny systemsikkerhedsfunktion, men det er vigtigt at være klar over, hvordan funktionen sørger for anonymiteten og sikkerheden for de data, der indsamles og deles mellem enheder. Skærmtid er tilgængelig i iOS 12 og nyere versioner, iPadOS 13.1 og nyere versioner, macOS 10.15 og nyere versioner og nogle funktioner i watchOS 6 og nyere versioner.

I tabellen herunder beskrives de vigtigste funktioner i Skærmtid.

Funktion	Understøttet operativsystem
Se brugsdata	iOS iPadOS macOS
Gennemtvinge yderligere begrænsninger	iOS iPadOS macOS watchOS
Indstille grænser for brug af internettet	iOS iPadOS macOS
Indstille grænser for brug af apps	iOS iPadOS macOS watchOS
Konfigurere Skærmfri tid	iOS iPadOS macOS watchOS

Hvis brugerne administrerer deres egen enhed, kan betjeningsmuligheder for Skærmtid og brugsdata synkroniseres på tværs af enheder, der er knyttet til den samme iCloud-konto, vha. end-to-end-kryptering af CloudKit. Det kræver, at tofaktorgodkendelse er slået til i brugernes konto (synkronisering er som standard slået til). Skærmtid erstatter funktionen Begrænsninger i tidligere versioner af iOS og iPadOS samt funktionen Børnesikring i tidligere versioner af macOS.

I iOS 13 og nyere versioner, iPadOS 13.1 og nyere versioner og macOS 10.15 og nyere versioner deler brugere og administrerede børn i Skærmtid automatisk deres brug mellem enheder, hvis tofaktorgodkendelse er slået til for deres iCloud-konto. Når en bruger rydder Safaris historik eller fjerner en app, fjernes de tilsvarende brugsdata fra enheden og alle synkroniserede enheder.

Forældre og Skærmtid

Forældre kan bruge Skærmtid på iOS-, iPadOS- og macOS-enheder til at forstå og styre deres børns brug. Hvis en forælder er den ansvarlige for familien (i iCloud-familiedeling), kan vedkommende se brugsdata og administrere indstillinger for Skærmtid for sine børn. Børnene får en meddelelse, når forældrene slår Skærmtid til, og de kan også overvåge deres egen brug. Når forældrene slår Skærmtid til for deres børn, kan de indstille en kode, så børnene ikke kan foretage nogen ændringer. Når børnene bliver myndige (myndighedsalderen afhænger af land og område), kan de slå denne overvågning fra.

Brugsdata og konfigurationsindstillinger overføres mellem forælderens og barnets enhed vha. protokollen IDS (Apple Identity Service), der er end-to-end-krypteret. Krypterede data kan blive lagret midlertidigt på IDS-servere, indtil de læses af modtagerenheden (f.eks. så snart iPhone, iPad eller iPod touch tændes, hvis den var slukket). Disse data kan ikke læses af Apple.

Skærmtid-analyse

Hvis brugeren slår Del iPhone- & Apple Watch-analyse til, indsamles kun følgende anonymiserede data, så Apple bedre kan forstå, hvordan Skærmtid bruges:

- Blev Skærmtid slået til under Indstillingsassistent eller senere i Indstillinger
- Ændring i kategoribrug, efter der var indstillet en grænse for brugen (op til 90 dage derefter)
- Er Skærmtid slået til
- Er Skærmfri tid slået til
- Antal gange der blev anmodet om mere tid
- Antal af app-tidsgrænser
- Det antal gange, brugere har kigget på brug i indstillingerne til Skærmtid, pr. brugertype og pr. visningstype (lokal, ekstern, widget)
- Antal gange, brugere ignorerer en begrænsning, pr. brugertype
- Antal gange, brugere sletter en begrænsning, pr. brugertype

Ingen specifikke data om brug af apps eller websteder indsamles af Apple. Når en bruger ser en liste med apps med oplysninger om brug i Skærmtid, er app-symbolerne hentet direkte fra App Store, og de indeholder ikke nogen data fra disse anmodninger.

Ordliste

administration af mobile enheder (MDM) En tjeneste, der giver en administrator mulighed for at administrere tilmeldte enheder eksternt. Når en enhed er tilmeldt, kan administratoren benytte MDM-tjenesten til at konfigurere indstillinger og udføre andre opgaver på enheden via netværket, uden at brugeren skal gøre noget.

AES (Advanced Encryption Standard) En populær global krypteringsstandard, der bruges til at kryptere data, så uvedkommende ikke kan læse dem.

AES-XTS En funktion i AES, der er defineret i IEEE 1619-2007 med det formål at kryptere lagringsmedier.

APFS (Apple File System) Standardarkivsystemet til iOS, iPadOS, tvOS, watchOS og Mac-computere med macOS 10.13 og nyere versioner. APFS sørger for stærk kryptering, deling af plads, snapshots, hurtig størrelsesændring af biblioteker og forbedringer i det grundlæggende arkivsystem.

APNs (Apple Push Notification service) En tjeneste, som Apple tilbyder i hele verden, der sørger for push-notifikationer til Apple-enheder.

Apple Business Manager En overskuelig webbaseret portal til it-administratorer, der sætter organisationer i stand til på en hurtig og ensartet måde at implementere Apple-enheder, som organisationerne har købt direkte fra Apple eller via autoriserede Apple-forhandlere eller -udbydere, der deltager i programmet. De kan automatisk tilmelde enheder til deres løsning til administration af mobile enheder (MDM) uden at røre eller klargøre enhederne fysisk, før brugerne får dem.

Apple School Manager En overskuelig webbaseret portal til it-administratorer, der sætter organisationer i stand til på en hurtig og ensartet måde at implementere Apple-enheder, som organisationerne har købt direkte fra Apple eller via autoriserede Apple-forhandlere eller -udbydere, der deltager i programmet. De kan automatisk tilmelde enheder til deres løsning til administration af mobile enheder (MDM) uden at røre eller klargøre enhederne fysisk, før brugerne får dem.

Apples sikkerhedsdusører En belønning, der gives af Apple til brugere, som rapporterer sårbarheder, der berører de senest leverede operativsystemer og (hvis det er relevant) den nyeste hardware.

arkivnøgle Den nøgle, der bruges af Databeskyttelse til at kryptere et arkiv i arkivsystemet. Arkivnøglen pakkes med en klassenøgle og opbevares i arkivets metadata.

arkivsystemnøgle En nøgle, der krypterer hvert arkivs metadata, også arkivets klassenøgle. De opbevares i Effaceable Storage med henblik på hurtig sletning fremfor fortrolighed.

ASLR (Address Space Layout Randomization) En teknik, der benyttes af operativsystemer til at gøre det langt sværere at udnytte en fejl i softwaren. Den sørger for, at hukommelsesadresser og -forskydninger ikke kan forudsiges, og disse værdier kan derfor ikke kodes fast ind i ondsindet kode.

Boot Camp En hjælpeapp til Mac, der gør det muligt at installere Microsoft Windows på understøttede Mac-computere.

Boot ROM Den kode, der udføres af en enheds processor, når enheden startes. Det er en integreret del af processoren og kan ikke ændres, hverken af Apple eller af en person med ondsindede hensigter.

BPR (Boot Progress Register) Et sæt SoC-hardwareflag (System on Chip), som software kan bruge til at spore de startfunktioner, som enheden har anvendt, f.eks. DFU-funktion (Device Firmware Update) og gendannelsesfunktion. Når et BPR-flag er blevet sat, kan det ikke slettes. Det betyder, at efterfølgende software kan få en pålidelig indikation af systemets tilstand.

CKRecord En ordbog med parvise nøgler og værdier, som indeholder data, der er gemt i eller hentet fra CloudKit.

Data Vault En mekanisme, der håndhæves af kernen, og som beskytter mod uautoriseret adgang til data, uanset om den app, der sender anmodninger, selv afvikles i et isoleret miljø.

Databeskyttelse En mekanisme til beskyttelse af arkiver og nøglering på understøttede Apple-enheder. Mekanismen kan også referere til de API'er, som apps bruger til at beskytte arkiver og emner i nøgleringen.

DFU-funktion (Device Firmware Upgrade) En proces, hvor en enheds Boot ROM-kode venter på at blive gendannet via USB. Skærmen er sort under DFU-processen, men når der er oprettet forbindelse til en computer, hvor iTunes eller Finder er startet, vises en meddelelse i stil med denne: "iTunes (eller Finder) har fundet en (iPad, iPhone eller iPod touch), som er indstillet til gendannelse. Du skal gendanne denne (iPad, iPhone eller iPod touch), før du kan bruge den med iTunes (eller Finder)."

direkte hukommelsesadgang (DMA) En funktion, der sætter hardwaresubsystemer i stand til at få direkte adgang til hovedhukommelsen uden om CPU'en.

ECDHE (Elliptic Curve Diffie-Hellman Exchange Ephemeral) En mekanisme baseret på elliptiske kurver til udveksling af nøgler. ECDHE giver to parter mulighed for at blive enige om en hemmelig nøgle på en måde, der forhindrer, at nøglen bliver opdaget af en person, der holder øje med beskederne mellem de to parter.

ECDSA (Elliptic Curve Digital Signature Algorithm) En algoritme til digitale signaturer baseret på elliptisk kurvekryptografi.

ECID (Exclusive Chip Identification) Et processor-id på 64 bit, der er forskelligt på alle iOS- og iPadOS-enheder. Når et opkald besvares på en enhed, stoppes ringningen på parrede iCloud-enheder i nærheden ved hjælp af en kort annoncering via Bluetooth Low Energy (BLE) 4.0. Annonceringsbyte krypteres med samme metode som Handoff-annonceringer. Det bruges under den personlige indstilling og betragtes ikke som hemmeligt.

Effaceable Storage (sletbart lager) Et særligt område af NAND-lagringspladsen, der bruges til opbevaring af kryptografiske nøgler, og som kan adresseres direkte og slettes på en sikker måde. Det yder ikke beskyttelse, hvis en person med ondsindede hensigter er i fysisk besiddelse af en enhed, men nøglerne i Effaceable Storage kan indgå i et nøglehierarki, der giver mulighed for hurtig sletning og fremadrettet sikkerhed.

eSPI (Enhanced Serial Peripheral Interface) En komplet bus, der er designet til synkron seriel kommunikation.

Gatekeeper En teknologi i macOS, der har til formål at sikre, at kun godkendt software afvikles på en brugers Mac.

Gendannelsesfunktion En funktion, der bruges til at gendanne mange Apple-enheder, hvis den ikke genkender brugerens enhed, så brugeren kan installere operativsystemet igen.

godkendelse af systemsoftware En proces, der kombinerer kryptografiske nøgler, der er indbygget i hardware, med en onlinetjeneste for at kontrollere, at kun gyldig software fra Apple, der passer til understøttede enheder, leveres og installeres på opgraderingstidspunktet.

gruppe-id (GID) Ligner UID, men er fælles for alle processorer i en klasse.

hardwaresikkerhedsmodul (HSM) En specialiseret computer, der kan modstå forsøg på modificering, og som beskytter og administrerer digitale nøgler.

HMAC En kode til godkendelse af beskeder, som genereres ud fra en hash-værdi og er baseret på en kryptografisk hash-funktion.

iBoot Indlæsningsfunktion til startfase 2 til alle Apple-enheder. Kode, der indlæser XNU som led i den sikre startkæde. Afhængigt af SoC-genereringen (System on Chip) bliver iBoot indlæst af LLB (Low Level Bootloader) eller direkte af Boot ROM.

IDS (Apple Identity Service) Apples bibliotek med offentlige iMessage-nøgler, APN-adresser samt telefonnumre og e-mailadresser, der bruges til at slå nøgler og enhedsadresser op.

integreret kredsløb Kaldes også en *mikrochip*.

IOMMU (Input/Output Memory Management Unit) En enhed, der administrerer input til og output fra hukommelsen. Et subsystem i en integreret chip, der styrer adgangen til adresseområdet fra interne og ydre I/O-enheder.

JTAG (Joint Test Action Group) Et standardværktøj til hardwarefejlfinding, som bruges af programmører og mikrochipudviklere.

kombination af nøgler Den proces, hvor en brugers kode omdannes til en kryptografisk nøgle og forstærkes med enhedens UID. Processen er med til at sikre, at et brute-force-angreb skal udføres mod en given enhed. Det sænker hastigheden og forhindrer parallelle angreb. Algoritmen til kombination af nøgler er PBKDF2, som bruger AES med en nøgle dannet ud fra enhedens UID som tilfældighedsgenerator til hver gentagelse.

Komponent til sikker opbevaring En chip designet med uforanderlig ROM-kode, en hardwarebaseret tilfældighedsgenerator, kryptografimoduler og registrering af fysisk manipulation. På understøttede enheder dannes par mellem Secure Enclave og en komponent til sikker opbevaring af værdien, der forhindrer genafspilning. Secure Enclave og chippen til opbevaring benytter en sikker protokol, der er med til at sikre eksklusiv adgang til nonce-værdierne, når disse værdier skal læses og opdateres. Der er flere generationer af denne teknologi med forskellige sikkerhedsgarantier.

kortlægning af rillers vinkel og forløb En matematisk gengivelse af retning og bredde på riller, der udgør en del af et fingeraftryk.

Kryptografisk modul til AES En dedikeret hardwarekomponent, der implementerer AES.

LLB (Low Level Bootloader) På Mac-computere med startarkitektur i to trin indeholder LLB den kode, der startes af Boot ROM, og som derefter indlæser iBoot som led i den sikre startkæde.

medienøgle En del af det krypteringsnøglehierarki, der er med til at sørge for sikker og øjeblikkelig sletning. I iOS, iPadOS, tvOS og watchOS indpakker medienøglen metadataene på dataenheden (og dermed er det umuligt at få adgang til arkivnøgler uden medienøglen, så arkiver, der er beskyttet med Databeskyttelse, er utilgængelige). I macOS indpakker medienøglen nøglematerialet, alle metadata samt data på den enhed, der er beskyttet af FileVault. I begge tilfælde betyder sletning af medienøglen, at krypterede data bliver utilgængelige.

NAND Ikke-flygtig flash-hukommelse.

nonce-værdi Et entydigt engangsnummer, der bruges i forskellige sikkerhedsprotokoller.

Nøgle afledt af kode (PDK) Den krypteringsnøgle, der er afledt af kombinationen af brugeradgangskoden, den langtidsholdbare SKP-nøgle og Secure Enclaves UID.

nøgleindpakning Kryptering af en nøgle sammen med en anden nøgle. iOS og iPadOS bruger NIST AES-nøgleindpakning i overensstemmelse med RFC 3394.

nøglering Den infrastruktur og det sæt API'er, som bruges af Apples operativsystemer og apps fra tredjeparter til at gemme og hente adgangskoder, nøgler og andre følsomme godkendelsesoplysninger.

nøglesamling En datastruktur, hvori der opbevares en samling klassenøgler. Hver type (bruger, enhed, system, sikkerhedskopi, depot og iCloud-sikkerhedskopi) har samme format.

En header, der indeholder: Version (indstillet til fire i iOS 12 og nyere versioner), type (system, sikkerhedskopi, depot eller iCloud-sikkerhedskopi), UUID til nøglesamling, a HMAC-kode, hvis nøglesamlingen er signeret, og den metode, der er brugt til indpakning af klassenøglerne: kombination med UID eller PBKDF2, sammen med saltnøglen og antallet af gentagelser.

En liste med klassenøgler: Nøglens UUID, klasse (hvilken klasse i Databeskyttelse til arkiver eller nøglering), indpakningstype (kun nøgle afledt af UID eller nøgle afledt af UID og kode), indpakket klassenøgle og en offentlig nøgle til asymmetriske klasser.

programprofil En egenskabsliste (.plist-arkiv) signeret af Apple, som indeholder et sæt egenskaber og berettigelser, der tillader, at apps installeres og testes på en iOS- eller iPadOS-enhed. En programprofil til udvikling indeholder en liste med de enheder, som en udvikler har valgt til ad hoc-distribution, og en programprofil til distribution indeholder id'et til en app udviklet af en virksomhed.

SCIP (System Coprocessor Integrity Protection) En mekanisme, som Apple bruger med det formål at forhindre modificering af hjælpeprocessorfirmwaren.

Sealed Key Protection (SKP) En teknologi i Databeskyttelse, der beskytter (eller *forsegler*) krypteringsnøgler med målinger fra systemsoftware og nøgler, der kun findes i hardware (f.eks. Secure Enclaves UID).

sepOS Secure Enclave-firmwaren, der er baseret på en Apple-tilpasset version af L4-mikrokernen.

SoC (System on Chip) Et integreret kredsløb (IC), der samler flere komponenter på en enkelt chip. App-processoren, Secure Enclave og andre hjælpeprocessorer er komponenter i en SoC.

software seed bits Dedikerede bits i Secure Enclave AES-modulet, som bliver føjet til UID, når der genereres nøgler fra UID. Hver software seed bit har en tilsvarende lock bit. Secure Enclave Boot ROM og operativsystemet kan uafhængigt af hinanden ændre værdien af hver software seed bit, så længe den tilsvarende lock bit ikke er blevet indstillet. Når lock bit er indstillet, kan hverken software seed bit eller lock bit ændres. Software seed bits og deres locks nulstilles, når Secure Enclave genstarter.

SSD-styreenhed Et subsystem til hardware, der håndterer lagringsmediet (Solid-State Drive).

styreenhed til hukommelse Subsystemet i en SoC (System on Chip), der styrer grænsefladen mellem SoC'en og dens hovedhukommelse.

UEFi-firmware (Unified Extensible Firmware Interface) En erstatningsteknologi til BIOS, der kan forbinde firmware med en computers operativsystem.

UID (Unique ID) En 256-bit AES-nøgle, der er brændt ind i hver processor under fremstillingen. Den kan ikke læses af firmware eller software, og den bruges kun af processorens AES-modul til hardware. En person med ondsindede hensigter, der vil have fat i nøglen, vil være nødt til at foranstalte et yderst sofistikeret og dyrt fysisk angreb på processorens silicium. UID har ikke forbindelse til nogen andre id'er på enheden, heller ikke UDID.

URI (Uniform Resource Identifier) En række tegn, der identificerer en ressource på internettet.

xART En forkortelse for eXtended Anti-Replay Technology. Et sæt tjenester, der sørger for krypteret og godkendt vedvarende lagringsplads til Secure Enclave med funktioner, der forhindrer genafspilning, baseret på lagringspladsens fysiske arkitektur. Se Komponent til sikker opbevaring.

XNU Kernen i hjertet af Apples operativsystemer. Den betragtes som godkendt, og den sørger for, at sikkerhedsforanstaltninger såsom kodesignering, afvikling i et isoleret miljø (“sandbox”), kontrol af berettigelse og ASLR (Address Space Layout Randomization) overholdes.

XProtect En antivirusteknologi i macOS til signaturbaseret registrering og fjernelse af malware.

Dokumentrevisionshistorik

Dokumentrevisionshistorik

Dato	Resume
December 2022	Tilføjede emner: • Avanceret databeskyttelse til iCloud Opdaterede emner: • Oversigt over iCloud-sikkerhed • iCloud-kryptering • Sikkerheden i iCloud-sikkerhedskopiering • Sikkerhed i forbindelse med kontakter til kontogendannelse • Sikkerhed i forbindelse med arvekontakter
Maj 2022	Opdateret til: • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 Tilføjede emner: • Begrænsninger for parret macOS-gendannelse • Local Operating System Version (love) • Deling af sundhedsdata • Sikkerhed i forbindelse med kontakter til kontogendannelse • Sikkerhed i forbindelse med arvekontakter • Sikkerhed ved Betal med et tryk på iPhone • Adgang via Apple Wallet • Typer af adgangsgodkendelse • Id'er i Apple Wallet • Siri-kompatibelt HomeKit-tilbehør

Dato	Resume
Maj 2022	Opdaterede emner: • Magic Keyboard med Touch ID • Face ID, Touch ID, koder og adgangskoder • Sikkerhed ved sammenligning af ansigter • Ekspreskort og reservespænding • Startfunktioner på en Mac med Apple Silicon • Indholdet i et LocalPolicy-arkiv på en Mac med Apple Silicon • Sikkerhed på den signerede systemenhed i iOS, iPadOS og macOS • Systemsikkerhed til watchOS • Apples enhed til sikkerhedsforskning • Apples arkivsystems rolle • Beskyttelse af app-adgang til brugerdata • Introduktion til app-sikkerhed i macOS • Beskyttelse mod malware i macOS • Oversigt over iCloud-sikkerhed • Sikker synkronisering af nøglering • Sikker gendannelse af iCloud-nøglering • Betaling med kort og Apple Pay • Kontaktløse kort i Apple Pay • Markering af kort som ubrugelige i Apple Pay • Ansøgning om Apple Card • Apple Cash-sikkerhed • Tilføjelse af rejsekort og eMoney-kort i Apple Wallet • Sikker Apple Messages for Business • FaceTime-sikkerhed • Sikkerhed i forbindelse med bilnøgler i iOS • Sikkerhed i Apple Configurator Fjernede emner: • HomeKit-tilbehør og iCloud

Dato	Resume
Maj 2021	Opdateret til: • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 Tilføjede emner: • Magic Keyboard med Touch ID. • Sikker hensigt og sikre forbindelser til Secure Enclave. • Lås automatisk op og Apple Watch. • CustomOS Image4 Manifest Hash (coih). Redigerede emner: • Tilføjede to nye transaktioner til Ekspresfunktion i Ekspreskort og reservespænding. • Redigerede Opsummering af Secure Enclave-funktioner • Softwareopdateringsindhold føjet til Secure Multi-Boot (smb3). • Mere indhold om Sealed Key Protection (SKP).

Dato	Resume
Februar 2021	Opdateret til: • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 Tilføjede emner: • Hukommelsessikker iBoot-implementering • Startprocessen på en Mac-computer med Apple Silicon • Startfunktioner på en Mac med Apple Silicon • Styring af sikkerhedspolitik for Startdisk på en Mac med Apple Silicon • Oprettelse og administration af signeringsnøgler til LocalPolicy • Indholdet i et LocalPolicy-arkiv på en Mac med Apple Silicon • Sikkerhed på den signerede systemenhed i iOS, iPadOS og macOS • Apples enhed til sikkerhedsforskning • Overvågning af adgangskoder • IPv6-sikkerhed • Sikkerhed i forbindelse med bilnøgler i iOS Opdaterede emner: • Secure Enclave • Slå mikrofon fra via hardware • macOS-gendannelse og diagnosticeringsmiljøer til en Intel-baseret Mac • Direct Memory Access-beskyttelse på Mac-computere • Kerneudvidelser i macOS • Beskyttelse af systemets integritet • Systemsikkerhed til watchOS • Administration af FileVault i macOS • App-adgang til gemte adgangskoder • Sikkerhedsanbefalinger for adgangskoder • Apple Cash-sikkerhed • Sikker Apple Messages for Business • Wi-Fi-anonymitet • Sikkerhed i Aktiveringslås • Sikkerhed i Apple Configurator

Dato	Resume
April 2020	Opdateret til: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Opdateringer: • Slå mikrofon fra på iPad er føjet til Slå mikrofon fra via hardware. • Data Vault føjet til Beskyttelse af app-adgang til brugerdata. • Opdateringer af Administration af FileVault i macOS og Kommandolinjeværktøjer. • Tilføjelser til Værktøj til fjernelse af malware i Beskyttelse mod malware i macOS. • Opdateringer af Sikkerhed med Delt iPad i iPadOS.
December 2019	iOS-sikkerhedsvejledning, Sikkerhed i macOS – oversigt og Oversigt over Apple T2-sikkerhedschip blev kombineret. Opdateret til: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Håndtering af Anonymitet, Siri og Siri-forslag samt Intelligent beskyttelse mod sporing i Safari er blevet fjernet. Læs sidste nyt om disse funktioner på https://www.apple.com/dk/privacy/.
Maj 2019	Opdateret til iOS 12.3 • Understøttelse af TLS 1.3 • Revideret beskrivelse af AirDrop-sikkerhed • DFU-funktion og Gendannelsesfunktion • Kodekrav til tilbehørsforbindelser
November 2018	Opdateret til iOS 12.1 • FaceTime-gruppe
September 2018	Opdateret til iOS 12 Secure Enclave • Beskyttelse af operativsystemets integritet • Ekspreskort og reservespænding • DFU-funktion og Gendannelsesfunktion • Tv-fjernbetjeningstilbehør til HomeKit • Kontaktløse kort • Studiekort • Siri-forslag • Genveje i Siri • Appen Genveje • Administration af brugeradgangskode • Skærmtid • Sikkerhedscertifikater og -apps

Dato	Resume
Juli 2018	Opdateret til iOS 11.4 • Biometriske politikker • HomeKit • Apple Pay • Virksomhedschat • Beskeder i iCloud • Apple Business Manager
December 2017	Opdateret til iOS 11.2 • Apple Pay Cash
Oktober 2017	Opdateret til iOS 11.1 • Sikkerhedscertifikater og -apps • Touch ID/Face ID • Delte noter • End-to-end-kryptering af CloudKit • TLS-opdatering • Apple Pay, betaling med Apple Pay på internettet • Siri-forslag • Delt iPad
Juli 2017	Opdateret til iOS 10.3 • Secure Enclave • Beskyttelse af arkivdata • Nøglesamlinger • Sikkerhedscertifikater og -apps • SiriKit • HealthKit • Netværkssikkerhed • Bluetooth • Delt iPad • Funktionen Mistet • Aktiveringslås • Håndtering af Anonymitet
Marts 2017	Opdateret til iOS 10 Systemsikkerhed • Databeskyttelsesklasser • Sikkerhedscertifikater og -apps • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Single sign-on • Apple Pay, betaling med Apple Pay på internettet • Anvendelse af kreditkort, debetkort og forudbetalte kort • Safari-forslag

Dato	Resume
Maj 2016	Opdateret til iOS 9.3 • Administreret Apple-id • Tofaktorgodkendelse til Apple-id • Nøglesamlinger • Sikkerhedscertificeringer • Funktionen Mistet, Aktiveringslås • Sikre noter • Apple School Manager • Delt iPad
September 2015	Opdateret til iOS 9 Aktiveringslås på Apple Watch • Politikker til koder • API-understøttelse af Touch ID • Databeskyttelse på A8 bruger AES-XTS • Nøglesamlinger til uovervåget softwareopdatering • Certificeringsopdateringer • Model for app-godkendelse i virksomheder • Databeskyttelse til Safari-bogmærker • App Transport Security • VPN-specifikationer • Ekstern adgang til iCloud til HomeKit • Fordelskort til Apple Pay, kortudsteders app til Apple Pay • Spotlight-indeksering på enheden • Pardannelsesmodel for iOS • Apple Configurator 2 • Begrænsninger

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

DK028-00625