iOS-sikkerhed

iOS 12.3

Maj 2019

Indhold

Introduktion

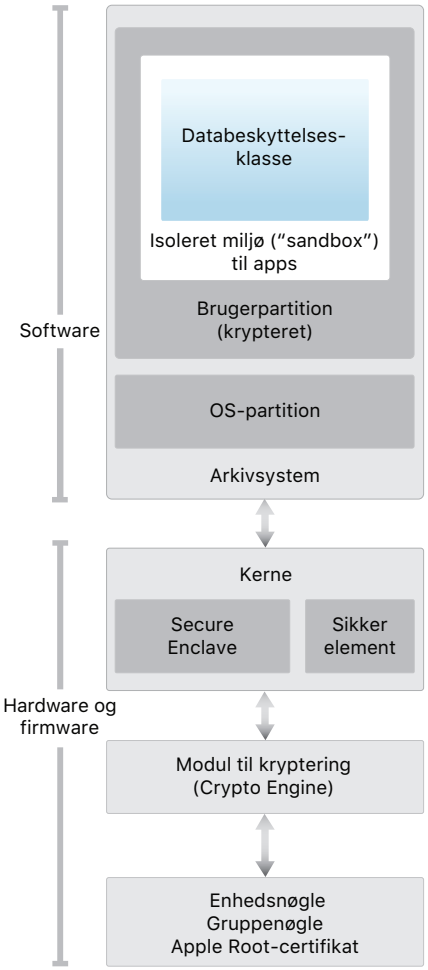


Diagram over sikkerhedsarkitekturen i iOS, som giver et visuelt overblik over de forskellige teknologier, der er beskrevet i dette dokument.

Apple designede iOS-platformen med sikkerhed som et centralt element. Da vi besluttede at skabe den bedst mulige mobile platform, byggede vi en helt ny arkitektur på grundlag af mange års erfaring. Vi havde sikkerhedsrisiciene ved skrivebordsmodeller for øje og etablerede en helt ny indgangsvinkel til sikkerhed i designet af iOS. Vi udviklede og indbyggede nyskabende funktioner, der som standard øger mobilsikkerheden og beskytter hele systemet. Det betyder, at iOS udgør et kvantespring inden for sikkerhed for mobile enheder.

Alle iOS-enheder kombinerer software, hardware og tjenester, der har til formål at arbejde sammen for at give den maksimale sikkerhed og en transparent brugeroplevelse. iOS beskytter ikke blot enheden og dens data, men hele økosystemet – både det, som brugerne foretager sig lokalt på netværket og med vigtige tjenester på internettet.

iOS og iOS-enheder indeholder avancerede sikkerhedsfunktioner, men de er samtidig lette at bruge. Mange af disse funktioner er aktiveret som standard, så it-afdelingerne ikke behøver at foretage omfattende konfigurationer. Det er ikke muligt at konfigurere vigtige sikkerheds-funktioner som enhedskryptering, så det er ikke muligt for brugerne at slå dem fra ved en fejl. Andre funktioner, f.eks. Face ID, forbedrer brugeroplevelsen ved at gøre det enklere og mere intuitivt at sikre enheden.

Dette dokument indeholder detaljer om, hvordan sikkerhedsteknologi og -funktioner er implementeret på iOS-platformen. Det hjælper også organisationer med at kombinere

iOS-platformens sikkerhedsteknologi og -funktioner med deres egne strategier og procedurer med henblik på at opfylde deres særlige sikkerhedsbehov.

Dokumentet er inddelt i følgende emneområder:

- **Systemsikkerhed:** Den integrerede og sikre software og hardware, der udgør platformen for iPhone, iPad og iPod touch.
- **Kryptering og databeskyttelse:** Den arkitektur og det design, der beskytter brugerdata, hvis enheden bliver væk eller stjålet, eller hvis en uautoriseret person forsøger at bruge eller modificere den.
- **Sikkerhed for apps og programmer:** De systemer, der gør det muligt at afvikle apps sikkert uden at bringe platformens integritet i fare.
- **Netværkssikkerhed:** Netværksprotokoller, der er standard i branchen, og som leverer sikker godkendelse og kryptering af data under overførsler.
- **Apple Pay:** Apples implementering af sikker betaling.
- **Internettjenester:** Apples netværksbaserede infrastruktur til beskeder, synkronisering og sikkerhedskopiering.
- **Administration af brugeradgangskode:** Adgangskodebegrænsninger og adgang til adgangskoder fra andre godkendte kilder.
- **Styring af enheder:** Metoder, der gør det muligt at administrere iOS-enheder, forhindre uautoriseret brug og slå ekstern sletning til, hvis en enhed mistes eller bliver stjålet.
- **Håndtering af Anonymitet:** Funktioner i iOS, der kan bruges til at styre adgangen til Lokalitetstjenester og brugerdata.
- **Sikkerhedscertifikater og -programmer:** Oplysninger om ISO-certificater, Kryptografisk validering, Common Criteria-certificering og CSFC (Commercial Solutions for Classified).

Systemsikkerhed

Systemsikkerheden er designet, så både software og hardware er sikret i alle kernekomponenter i alle iOS-enheder. Også startprocessen, software-opdateringer og Secure Enclave er omfattet. Denne arkitektur er et centralt element for sikkerheden i iOS og forringer aldrig enhedens brugervenlighed.

Den tætte integration mellem hardware, software og tjenester i iOS-enheder sikrer, at hver komponent i systemet er godkendt, og at systemet som helhed er valideret. Fra første start over softwareopdateringer til iOS til apps fra tredjeparter analyseres og kontrolleres hvert trin for at sikre, at hardware og software arbejder sammen optimalt og bruger ressourcerne korrekt.

Sikker start (secure boot chain)

Hvert trin i startprocessen indeholder komponenter, der er signeret kryptografisk af Apple for at sikre integriteten, og som først går videre, når godkendelseskæden er verificeret. Det omfatter bootloader-programmerne, kernen, kerneudvidelserne og mobilkommunikationssoftwaren. Denne sikre startkæde hjælper med at sikre, at software på laveste niveau ikke modificeres.

Når en iOS-enhed tændes, udfører dens programprocessor 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 Apple Root CA-nøgle, som bruges til at kontrollere, at bootloader-programmet **iBoot** er signeret af Apple, før indlæsningen af det tillades. Det er det første trin i den tillidskæde, hvor hvert trin sikrer, at det næste trin er signeret af Apple. Når iBoot er færdig med sine opgaver, kontrolleres og afvikles iOS-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 de følgende trin håndteres forskelligt afhængigt af hardwaren:

- **Boot ROM kan ikke indlæse LLB (ældre enheder):** DFU-funktion
- **LLB eller iBoot:** Gendannelsesfunktion

I begge tilfælde skal der oprettes forbindelse fra enheden til iTunes via USB, og standardindstillingerne skal gendannes på enheden.

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 A12 SoC
- **Gendannelsesfunktion:** Indstilles af iBoot på enheder med Apple A10, S2 og nyere **SoCs (System on Chip)**

Du kan få flere oplysninger i afsnittet Kryptering og databeskyttelse i dette dokument.

På enheder med mobiladgang benytter basisbånd-subsystemet også sin egen lignende proces med sikker systemstart, hvor softwaren og nøglerne er signeret og godkendt af basisbåndprocessoren.

Secure Enclave-hjælpeprocessoren benytter også en sikker startproces, der sikrer, at dens særskilte software er godkendt og signeret af Apple. Se afsnittet Secure Enclave i dette dokument.

Her kan du få flere oplysninger om, hvordan du skifter manuelt til gendannelsesfunktionen: https://support.apple.com/HT201263

Godkendelse af systemsoftware

Apple frigiver regelmæssigt softwareopdateringer for at imødegå potentielle sikkerhedsproblemer og samtidig levere nye funktioner. Opdateringerne stilles til rådighed for alle understøttede enheder på samme tid. Brugerne modtager meddelelser om iOS-opdateringer på enheden og via iTunes, og opdateringer leveres trådløst, så de nyeste sikkerhedsrettelser hurtigt kan installeres.

Den startproces, der er beskrevet tidligere, hjælper med at sikre, at kun kode signeret af Apple kan installeres på en enhed. iOS bruger en proces kaldet System Software Authorization (godkendelse af systemsoftware) til at forhindre, at enheder nedgraderes til en ældre version, hvor de nyeste sikkerhedsopdateringer mangler. Hvis det var muligt at nedgradere, kunne en person med ondsindede hensigter, som kommer i besiddelse af en enhed, installere en ældre version af iOS og udnytte en sårbarhed, der er blevet fjernet i den nyere version.

På en enhed med Secure Enclave benytter Secure Enclave-hjælpe-processoren også godkendelse af systemsoftware til at sikre processor-softwarens integritet og forhindre nedgraderinger. Se afsnittet Secure Enclave i dette dokument.

iOS-softwareopdateringer kan installeres ved hjælp af iTunes eller trådløst via OTA (Over The Air) på enheden. Med iTunes hentes og installeres en komplet kopi af iOS. Ved softwareopdateringer via OTA hentes kun de komponenter, der kræves for at fuldføre en opdatering, i stedet for hele operativsystemet. Det sker af hensyn til netværkseffektiviteten. Det er også muligt at opbevare softwareopdateringer i bufferen på en Mac med macOS High Sierra, hvor Indlæsning af indhold i buffer er slået til, så iOS-enheder ikke behøver at hente den nødvendige opdatering igen fra internettet. De skal stadig kontakte Apple-servere for at gennemføre opdateringen.

Under en iOS-opgradering opretter iTunes (eller enheden selv i tilfælde af OTA-softwareopdateringer) forbindelse til Apples godkendelsesserver til installering og sender en liste med kryptografiske målinger for hvert af de elementer i installeringspakken, der skal installeres (f.eks. iBoot, kerne og OS-billede), en tilfældig værdi, der forhindrer genafspilning (nonce), og enhedens entydige **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, sikrer serveren, at opdateringerne foretages præcist, som Apple har fastlagt.

Evalueringen i tillidskæden på starttidspunktet kontrollerer, at signaturen stammer fra Apple, og at målingen for det emne, der indlæses fra disken, sammen med enhedens ECID modsvarer det, som signaturen dækker. Disse trin sikrer, at godkendelsen sker for en bestemt enhed, og at en gammel iOS-version ikke kan kopieres fra en enhed til en anden enhed. Nonce-værdien forhindrer en person med ondsindede hensigter i at opsnappe serverens svar og bruge det til at modificere en enhed eller ændre systemsoftwaren.

Secure Enclave

Secure Enclave er en hjælpeprocessor, der er indbygget i SoC (System on Chip). Den bruger krypteret hukommelse og indeholder en tilfældighedsgenerator. Secure Enclave leverer alle kryptografiske funktioner til administration af nøgler til **databeskyttelse** og opretholder databeskyttelsen, også selvom kernen er blevet angrebet. Kommunikationen mellem Secure Enclave og programprocessoren er begrænset til en interruptstyret postkasse og fælles databuffere i hukommelsen.

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

Secure Enclave bruger et Secure Enclave-operativsystem baseret på en Apple-tilpasset version af L4-mikrokernen. Dette Secure Enclave-operativsystem er signeret af Apple, godkendt af Secure Enclave Boot ROM og opdateret via en personligt tilpasset softwareopdateringsproces.

Når enheden starter, opretter Secure Enclave Boot ROM en midlertidig nøgle til beskyttelse af hukommelsen, som kombineres med enhedens UID og bruges til at kryptere Secure Enclave-delen af enhedens hukommelsesområde. Secure Enclave-hukommelsen godkendes også med nøglen til beskyttelse af hukommelsen, dog ikke i Apple A7. I A11 og nyere og i S4 SoC'er bruges et integritetshierarki til at forhindre genafspilning af Secure Enclave-hukommelse, der er kritisk for sikkerheden, og som godkendes af nøglen til beskyttelse af hukommelsen og nonce-værdier, der opbevares i processorens SRAM.

Data, der arkiveres i arkivsystemet af Secure Enclave, krypteres med en nøgle kombineret med UID og en tæller, der modvirker genafspilning. Tælleren, der modvirker genafspilning, opbevares i et dedikeret **integreret kredsløb)** med ikke-flygtig hukommelse.

På enheder med A12 og S4 SoC'er er Secure Enclave parret med et integreret kredsløb til sikker opbevaring for at modvirke genafspilning ved opbevaring af tælleren. Det integrerede kredsløb til sikker opbevaring er designet med uforanderlig ROM-kode, en hardwarebaseret tilfældighedsgenerator, kryptografimoduler og registrering af fysisk manipulation. For at kunne læse og opdatere tællere benytter Secure Enclave en sikker protokol, der sikrer eksklusiv adgang til tællerne.

Secure Enclave-tjenester, der modvirker genafspilning, bruges til at tilbagekalde data til begivenheder, som markerer grænser i forbindelse med forhindring af genafspilning. Det gælder blandt andet følgende tjenester:

- Skift adgangskode
- Slå Touch ID eller Face ID til/fra
- Tilføj/slet Touch ID-fingeraftryk
- Nulstil Face ID

- Tilføj/fjern Apple Pay-kort
- Slet alt indhold og alle indstillinger

Secure Enclave har også ansvaret for at behandle fingeraftryks- og ansigtsdata fra sensorerne til Touch ID og Face ID, fastlægge, om der er et match, og derefter tillade adgang eller køb på brugerens vegne.

Beskyttelse af operativsystemets integritet

Beskyttelse af kernens integritet

Når iOS-kernen har gennemført initialiseringen, aktiveres beskyttelsen af kernens integritet (KIP – Kernel Integrity Protection) for 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 fuldført, afviser styreenheden til hukommelse skrivninger til det beskyttede område af den fysiske hukommelse. Derudover konfigureres programprocessorens MMU (Memory Management Unit) for at forhindre mapning af privilegeret kode fra fysisk hukommelse uden for det beskyttede hukommelsesområde og for at forhindre skrivbare mapninger af fysisk hukommelse inden for kernehukommelsesområdet.

Den hardware, der bruges til at aktivere KIP, låses efter fuldførelsen af startprocessen for at forhindre rekonfigurering. KIP understøttes på SoC'er fra A10 og S4 og frem.

Beskyttelse af systemhjælpeprocessorers integritet

Systemhjælpeprocessorer er CPU'er på samme SoC som program-processoren. Systemhjælpeprocessorer er dedikeret til et bestemt formål, og iOS-kernen delegerer mange opgaver til dem. Eksempler:

- Secure Enclave
- Billedsensorprocessor
- Bevægelseshjælpeprocessor

Da hjælpeprocessorfirmware håndterer mange kritiske systemopgaver, er sikringen af denne firmware en vigtig del af hele systemets sikkerhed.

Beskyttelse af systemhjælpeprocessorers integritet (SCIP – System Coprocessor Integrity Protection) bruger en mekanisme svarende til KIP for at forhindre modificering af hjælpeprocessorfirmware. I forbindelse med 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 enheder til hukommelses-administration for at forhindre:

- Eksekverbare mapninger uden for dens del af det beskyttede hukommelsesområde
- Skrivbare mapninger inden for dens del af det beskyttede hukommelsesområde

Secure Enclave-operativsystemet er ansvarligt for at konfigurere Secure Enclaves SCIP i forbindelse med opstarten.

Den hardware, der bruges til at aktivere SCIP, låses efter fuldførelsen af startprocessen for at forhindre rekonfigurering. SCIP understøtttes på A12- og S4-SoC'er og derover.

Koder til markørgodkendelse

Koder til markørgodkendelse (PAC – Pointer Authentication Codes) bruges til at beskytte mod udnyttelse af fejl, der ødelægger hukommelsen. Systemsoftware og indbyggede apps bruger PAC til at forhindre modificering af funktionsmarkører og returadresser (kodemarkører). Herved vanskeliggøres mange angreb. Eksempelvis forsøger et ROP-angreb (Return Oriented Programming) at narre enheden til at afvikle eksisterende kode på en ondsindet måde ved at manipulere funktionsreturadresser, der opbevares i stakken.

PAC understøtttes på A12- og S4-SoC'er.

Touch ID

Touch ID er det system til registrering af fingeraftryk, der gør sikker adgang til iPhone og iPad 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.

Face ID

Med et enkelt blik låser Face ID Apple-enheder, der har denne funktion, op på en sikker måde. Det er en intuitiv og sikker godkendelsesmetode, der styres af TrueDepth-kamerasystemet, som bruger avanceret teknologi til at kortlægge dit ansigts geometri. Face ID bruger neurale netværk til at vurdere opmærksomhed, sammenligne ansigtstræk og modvirke spoofing, så du kan låse din telefon op med et blik. Face ID tilpasser sig automatisk ændringer i dit udseende og beskytter omhyggeligt dine biometriske datas anonymitet og sikkerhed.

Touch ID, Face ID og adgangskoder

Hvis du vil bruge Touch ID eller Face ID, skal du indstille din enhed, så der kræves en adgangskode for at låse den op. Når Touch ID eller Face ID finder et match, låses enheden op, uden at enhedens adgangskode skal indtastes. Det betyder, at det er langt nemmere at benytte mere komplekse adgangskoder, fordi du ikke behøver at indtaste dem så tit. Touch ID og Face ID erstatter ikke din adgangskode, men giver nem adgang til din enhed, hvis nøje fastlagte begrænsninger i forhold til tid og andre faktorer tillader det. Det er vigtigt, eftersom en stærk adgangskode udgør grundlaget for, hvordan din iOS-enhed beskytter dine data kryptografisk.

Du kan altid vælge at bruge din adgangskode i stedet for Touch ID eller Face ID, men ved følgende handlinger kræves det, at du bruger en adgangskode i stedet for biometrik:

- Opdatering af din software.
- Sletning af din enhed.
- Visning eller sletning af indstillinger til adgangskode.
- Installation af iOS-konfigurationsbeskrivelser.

Der kræves også adgangskode i følgende tilfælde:

- Enheden er lige blevet tændt eller genstartet.
- Enheden har ikke været låst op i mere end 48 timer.

- Adgangskoden har ikke været brugt til at låse enheden op de sidste 156 timer (seks en halv dag), og biometriske data har ikke låst enheden op de sidste fire timer.
- Enheden har modtaget en ekstern kommando til låsning.
- Efter fem forgæves forsøg på biometrisk match.
- Efter Sluk/Nødopkald SOS.

Når Touch ID eller Face ID er slået til, låses enheden straks, når der trykkes på sideknappen, og når den går på vågeblus. Touch ID og Face ID kræver et match eller eventuelt adgangskoden, hver gang vågeblus afbrydes.

Sandsynligheden for, at en tilfældig person i befolkningen kan låse din iPhone op er 1 ud af 50.000 med Touch ID og 1 ud af 1.000.000 med Face ID. 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 Touch ID og Face ID tillader kun fem forgæves matchforsøg, før du skal indtaste adgangskoden for at få adgang til din enhed. Det giver ekstra beskyttelse. Med Face ID er sandsynligheden for et forkert match anderledes for tvillinger og for søskende, der ligner dig, og for børn under 13 år (fordi deres ansigtstræk måske endnu ikke er fuldt udviklet). Hvis du er bekymret for det, anbefaler Apple, at du bruger en adgangskode til at legitimere dig.

Touch ID-sikkerhed

Fingeraftrykssensoren bliver først aktiv, når den kapacitive stålring omkring knappen Hjem registrerer en finger. Det får det avancerede billedbehandlingsarray til at scanne fingeren og sende scanningen til Secure Enclave. Kommunikationen mellem processoren og sensoren til Touch ID 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 fælles nøgle, som blev tilknyttet hver sensor til Touch ID og dens tilhørende Secure Enclave på fabrikken. Den fælles nøgle er stærk, tilfældig og unik for hver sensor til Touch ID. Udvekslingen af sessionsnøglen bruger AES-**nøgleindpakning**, hvor begge parter leverer en tilfældig nøgle, der fastlægger sessionsnøglen og bruger AES-CCM-transportkryptering.

Rasterscanningen opbevares midlertidigt i et krypteret hukommelsesområde i Secure Enclave, mens den vektoriseres forud for analysen, hvorefter den kasseres. Under analysen sammenlignes **kortlægning af rillers vinkel og forløb** i underhuden. Under denne proces kasseres data om meget små detaljer, der ellers kunne bruges til at rekonstruere brugerens ægte fingeraftryk. Resultatet af processen er et kort med detaljer. Det opbevares uden identitetsoplysninger i krypteret format, der kun kan læses af Secure Enclave. Disse data forlader aldrig enheden. De sendes ikke til Apple, og de indgår ikke i sikkerhedskopieringer af enheden.

Face ID-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 dit ansigt, når du afbryder vågeblus på Apple-enheder med Face ID ved at løfte enheden eller trykke på skærmen, og når disse enheder forsøger at godkende dig for at vise en indgående meddelelse, 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 dette fra, når VoiceOver er slået til. Det kan slås helt fra, hvis det ønskes.

Når TrueDepth-kameraet har bekræftet, at et ansigt har opmærksomheden rettet mod det, projicerer og læser kameraet mere end 30.000 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 det neurale modul i A11 og nyere SoC'er – 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 dit ansigt med forskellige udtryk og fra forskellige synsvinkler.

Sammenligning af ansigter udføres i Secure Enclave ved hjælp af neurale netværk, der er trænet med netop det formål for øje. Vi 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 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 solbriller. 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 iPhone X op med fotos eller masker.

Face ID-data, inklusive matematiske repræsentationer af dit 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 arkiveres og krypteres følgende Face ID-data kun til brug for Secure Enclave:

- De matematiske repræsentationer af dit ansigt, der beregnes under registreringen.
- De matematiske repræsentationer af dit 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, arkiveres ikke, men slettes, så snart den matematiske repræsentation er beregnet, enten til registrering eller sammenligning med de registrerede Face ID-data.

Sådan låser Touch ID eller Face ID en iOS-enhed op

Hvis Touch ID eller Face ID er slået fra, når en enhed 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 du låser enheden op ved at indtaste din adgangskode.

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

Når enheden starter igen, går de nøgler, som Touch ID eller Face ID skal bruge til at låse enheden op med, tabt. De kasseres af Secure Enclave, hvis en betingelse, der betyder, at adgangskoden skal indtastes, er opfyldt (f.eks. at enheden ikke har været låst op i 48 timer, eller der har været fem forgæves forsøg på at finde et match).

Face ID udvider sin arkiverede matematiske repræsentation over tid for at forbedre oplåsningsfunktionen og holde trit med de naturlige ændringer af dit ansigt og udseende. Når der er gennemført en oplåsning, kan Face ID bruge den netop beregnede matematiske repræsentation – hvis kvaliteten af den er god nok – til et begrænset antal yderligere oplåsninger, før disse data kasseres. Hvis Face ID derimod ikke genkender dig, men kvaliteten af sammenligningen er højere end en bestemt grænseværdi, og du straks efter den manglende genkendelse indtaster din adgangskode, 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 du ikke længere sammenlignes med dem og efter et bestemt antal oplåsninger. Med disse udvidelser kan Face ID holde trit med større ændringer af hår på hovedet og i ansigtet og brug af makeup, og samtidig mindskes antallet af forkerte godkendelser.

Touch ID, Face ID og Apple Pay

Du kan også bruge Touch ID og Face ID med Apple Pay til at foretage køb på en nem og sikker måde i butikker og apps og på internettet. Du kan få flere oplysninger om Touch ID og Apple Pay i afsnittet om Apple Pay i dette dokument.

Før du kan godkende en betaling i en butik med Face ID, skal du bekræfte, at du har til hensigt at betale, ved at trykke to gange på sideknappen. Derefter bruger du Face ID til at legitimere dig, før du anbringer din iPhone X i nærheden af den kontaktfri læser til betaling. Hvis du vil vælge en anden Apple Pay-betalingsmetode, efter du er blevet godkendt med Face ID, skal du godkendes igen, men du behøver ikke at trykke to gange på sideknappen igen.

Før du kan foretage en betaling fra apps og på internettet, skal du bekræfte, at du har til hensigt at betale, ved at trykke to gange på sideknappen og derefter godkende betalingen ved at blive godkendt med Face ID. Hvis din Apple Pay-transaktion ikke er gennemført højst 30 sekunder efter, du har trykket to gangen på sideknappen, skal du bekræfte, at du har til hensigt at betale, ved at trykke to gange igen.

Face ID-diagnostik

Data til Face ID forlader aldrig din enhed, og de sikkerhedskopieres aldrig til iCloud eller andre steder. Oplysningerne overføres kun fra din enhed, hvis du ønsker at levere diagnosticeringsdata til Face ID til AppleCare for at få support. Når du vil slå Face ID-diagnostik til, kræves en digitalt signeret godkendelse fra Apple, der ligner den, som bruges, når

softwareopdateringer skal gøres personlige. Efter godkendelsen kan du slå Face ID-diagnostik til og starte indstillingen fra appen Indstillinger på enheder, der understøtter Face ID.

Under indstillingen af Face ID-diagnostik slettes din eksisterende registrering til Face ID, og du bliver bedt om at registrere Face ID igen. Enheder, der understøtter Face ID, vil registrere Face ID-billeder fra godkendelsesforsøg de næste 10 dage. Derefter stopper de automatisk arkiveringen af billeder. Face ID-diagnostik sender ikke automatisk data til Apple. Du kan gennemse og godkende billeder fra registrering og oplåsning (både gennemførte og mislykkede forsøg), der er en del af de Face ID-diagnosticeringsdata, der indsamles af diagnosticeringsfunktionen, før de sendes til Apple. Face ID-diagnostik overfører kun de billeder fra Face ID-diagnostik, som du har godkendt. Dataene krypteres, inden de overføres, og når de er overført, slettes de straks fra enheden. Billeder, du afviser, slettes med det samme.

Hvis du ikke afslutter Face ID-diagnosticeringssessionen ved at gennemse billeder og overføre godkendte billeder, stopper Face ID-diagnostik automatisk efter 40 dage, og alle diagnosticeringsbilleder slettes fra enheden. Du kan altid selv slå Face ID-diagnostik fra. Hvis du gør det, slettes alle lokale billeder straks, og ingen Face ID-data deles med Apple.

Andre anvendelsesmuligheder for Touch ID og Face ID

Apps fra tredjeparter kan bruge system-API'er til at bede brugeren om at legitimere sig vha. Touch ID eller Face ID eller en adgangskode. Apps, der understøtter Touch ID, understøtter automatisk Face ID uden nogen ændringer. Når Touch ID eller Face ID bruges, informeres appen kun om, hvorvidt godkendelsen lykkedes. Den kan ikke få adgang til Touch ID, Face ID eller de data, der er knyttet til den registrerede bruger. Emner i nøgleringen kan også beskyttes med Touch ID eller Face ID, så de kun frigives af Secure Enclave, hvis der bliver fundet et match, eller hvis adgangskoden til enheden indtastes. Appudviklere har API'er til kontrol af, om en bruger har indstillet en adgangskode, før de kræver, at Touch ID, Face ID eller en adgangskode bruges til at låse emner i nøgleringen op. Appudviklere kan gøre følgende:

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

Du kan også konfigurere Touch ID eller Face ID til at godkende køb i iTunes Store, App Store og Apple Books, så du ikke behøver at indtaste adgangskoden til dit Apple-id. I iOS 11 og nyere versioner bruges ECC-nøgler i Secure Enclave, som er beskyttet med Touch ID og Face ID, til at godkende et køb via signering af anmodningen til butikken.

Kryptering og databeskyttelse

Slet alt indhold og alle indstillinger
Muligheden Slet alt indhold og alle indstillinger i Indstillinger sletter alle nøglerne i Effaceable Storage, så der ikke længere er kryptografisk adgang til nogen brugerdata på enheden. Det er derfor en ideel metode til at sikre, at alle personlige oplysninger er fjernet fra en enhed, før den overdrages til en anden person eller indleveres til reparation.

Vigtigt: Brug ikke Slet alt indhold og alle indstillinger, før enheden er sikkerhedskopieret, da de slettede data ikke kan gendannes på nogen måde.

Både den sikre startkæde, signeringen af kode og sikkerheden under programafviklingen bidrager til at sikre, at kun godkendt kode og godkendte apps kan afvikles på en enhed. iOS omfatter yderligere krypterings- og databeskyttelsesfunktioner, der har til formål at beskytte brugerdata, også i situationer, hvor andre dele af sikkerhedsinfrastrukturen er blevet svækket (f.eks. på en enhed med ikke-godkendte modifikationer). Dette indebærer store fordele for både brugere og it-administratorer. Personlige oplysninger og virksomhedsdata er under konstant beskyttelse, og hvis en enhed stjæles eller bliver væk, kan den øjeblikkeligt slettes fuldstændigt eksternt.

Sikkerhedsfunktioner i hardware

De kritiske aspekter ved mobile enheder er hastighed og energieffektivitet. Kryptografiske funktioner er komplekse og kan give problemer med ydeevnen eller batteritiden, hvis funktionerne ikke designes og implementeres med disse prioriteter for øje.

Alle iOS-enheder har et dedikeret modul til AES-256-kryptering, der er indbygget i DMA-stien mellem flashlageret og den primære systemhukommelse, hvilket gør krypteringen af arkiver yderst effektiv. I A9-processorer og nyere processorer i A-serien er flashlagerets undersystem placeret i en isoleret bus, der kun får adgang til hukommelse med brugerdata gennem modulet til DMA-kryptering.

Enhedens **entydige id'er (UID'er)** og **gruppe-id'er (GID'er)** er AES 256 bit-nøgler, der blev brændt (UID) eller kompileret (GID) ind i program-processoren og Secure Enclave under fremstillingsprocessen. Ingen software eller firmware kan læse dem direkte. Software og firmware kan kun se resultatet af den kryptering eller afkryptering, som udføres af de dedikerede AES-moduler, der er implementeret i silicium med UID eller GID som nøgle. Programprocessoren og Secure Enclave har hver deres UID og GID. Secure Enclave-UID og -GID kan kun bruges af det AES-modul, som er dedikeret til Secure Enclave. Der er heller ikke adgang til UID og GID gennem **JTAG (Joint Test Action Group)** eller andre fejlfindingsgrænseflader.

Med undtagelse af Apple A8 og tidligere SoC'er genererer hver enkelt Secure Enclave sit eget entydige id (UID – unique ID) i fremstillings-processen. Eftersom dette UID er entydigt for hver enhed, og det er genereret fuldt ud i Secure Enclave i stedet for et fremstillingssystem uden for enheden, kan hverken Apple eller nogen af Apples leverandører få adgang til det eller opbevare det.

Software, der afvikles i Secure Enclave, benytter dette UID til at beskytte hemmeligheder, der hører til 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 hukommelseskredsene flyttes fysisk fra en enhed til en anden. UID er ikke forbundet med andre id'er på enheden.

GID er fælles for alle processorer i en klasse med enheder (f.eks. alle enheder, der bruger Apples A8-processor).

Alle andre kryptografiske nøgler end UID og GID dannes af systemets tilfældighedsgenerator ved hjælp af en algoritme baseret på CTR_DRBG-kildekode. Systemets entropi skabes af tidsmæssige variationer under start samt af interrupttider, efter enheden er startet. Nøgler, der genereres i Secure Enclave, bruger dens hardwarebaserede tilfældighedsgenerator på grundlag af flere ringoscillatorer, der efterbehandles med CTR_DRBG.

Sikker sletning af arkiverede nøgler er lige så vigtigt som dannelsen af nøglerne. Det kan især være en udfordring i forbindelse med f.eks. et flashlager, hvor slidudjævning kan betyde, at flere kopier af data skal slettes. Denne udfordring håndteres på iOS-enheder med en funktion, der er specifikt beregnet til sikker sletning af data, og som kaldes **Effaceable Storage** (sletbart lager). Funktionen benytter den underliggende lagringsteknologi (f.eks. NAND) til at adressere et lille antal blokke på meget lavt niveau og slette dem.

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 rejsekort, der er valgt som Ekspresrejsekort
- Studiekort med Ekspresfunktion slået til

Ved tryk på sideknappen vises symbolet for lav batterispænding samt en tekst om, at ekspreskort kan bruges. NFC-kontrolenheden udfører transaktioner med ekspreskort under samme forhold, som når iOS kører, bortset fra at transaktionerne kun vises med en haptisk meddelelse. Der kommer ikke nogen synlig meddelelse.

Denne funktion er ikke tilgængelig, når brugeren har udført en standard-nedlukning.

Beskyttelse af arkivdata

Ud over de funktioner til hardwarekryptering, der er indbygget i iOS-enheder, bruger Apple en teknologi kaldet Databeskyttelse til yderligere beskyttelse af data, der opbevares i flashhukommelsen på enheden. Databeskyttelsen sætter enheden i stand til at reagere på almindelige begivenheder som indgående telefonopkald, men den gør det også muligt at kryptere brugerdata på højt niveau. Vigtige systemapps, f.eks. Beskeder, Mail, Kalender, Kontakter, Fotos og data fra Sundhed, bruger som standard databeskyttelsen, og apps fra tredjeparter, som installeres på iOS 7 og nyere versioner, får automatisk denne beskyttelse.

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

Oversigt over arkitekturen

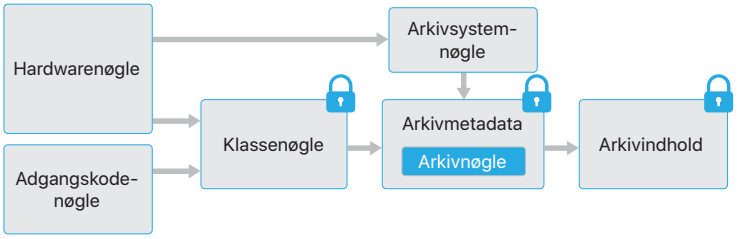
Hver gang der oprettes et arkiv i datapartitionen, opretter Databeskyttelse en ny 256 bit nøgle (arkivnøglen). Nøglen overdrages til AES-modulet i hardwaren, som bruger nøglen til at kryptere arkivet, når det skrives til flashhukommelsen med AES-XTS-funktionen. På enheder med en A7, S2 eller S3-SoC bruges AES-CBS. Initialiseringsvektoren beregnes med blokforskydningen ind i arkivet, som er krypteret med **arkivnøglens** værdi fra SHA-1-hashing.

Arkivnøglen (eller områdenøglen) pakkes med en af flere mulige klassenøgler, afhængigt af i hvilke situationer der skal være adgang til arkivet. Som ved alle andre indpakninger sker det ved hjælp af NIST AES-nøgleindpakning i overensstemmelse med RFC 3394. Den indpakkede arkivnøgle opbevares 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, afkrypteres 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 afkrypterer arkivet, mens det læses fra flashhukommelsen. Al håndtering af den indpakkede arkivnøgle finder sted i Secure Enclave. Arkivnøglen vises aldrig direkte til programprocessoren. Ved start forhandler 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 programprocessoren.

Metadata til alle arkiver i arkivsystemet krypteres med en tilfældig nøgle, som oprettes, når iOS installeres første gang, eller når enheden slettes af en bruger. På enheder, der understøtter APFS-arkivsystemet, indpakkes nøglen til arkivsystemets metadata med Secure Enclave UID-nøglen med henblik på langtidsopbevaring. Ligesom arkivnøgler eller områdenøgler vises metadatanøglen aldrig direkte for programprocessoren. 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. 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 MDM-løsning, 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 adgangskode. Dette hierarki er både fleksibelt og effektivt. Således skal arkivnøglen blot pakkes om, hvis et arkivs klasse ændres, mens en ændring af adgangskoden kun kræver, at klassenøglen pakkes om.

Adgangskoder

Når brugeren indstiller en adgangskode til enheden, aktiveres data-beskyttelsen automatisk. iOS understøtter adgangskoder på seks eller fire cifre og alfanumeriske adgangskoder med en vilkårlig længde. Ud over at låse enheden op sørger 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 adgangskoden.

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

Adgangskoden er kombineret med enhedens UID, så det er nødvendigt at udføre såkaldte brute-force-forsøg direkte på den fysiske enhed. Et stort antal gentagelser bruges til at gøre hvert forsøg langsommere. Antallet af gentagelser er kalibreret, så hvert forsøg tager ca. 80 millisekunder. Det betyder, at det vil tage mere end fem et halvt år at prøve med alle kombinationer af en alfanumerisk adgangskode på seks tegn bestående af små bogstaver og tal.

Jo stærkere brugerens adgangskode er, des stærkere bliver krypteringsnøglen. Touch ID og Face ID kan bruges til at forbedre sikkerheden ved at lade brugeren oprette en langt stærkere adgangskode, end det normalt ville være praktisk muligt. Det øger det effektive omfang af entropi, som beskytter de krypteringsnøgler, der bruges til databeskyttelse, uden at det bliver besværligt for brugeren at låse en iOS-enhed op flere gange om dagen.

Forsinkelser mellem adgangskodeforsøg

Forsøg	Gennemtvunget forsinkelse
1-4	ingen
5	1 minut
6	5 minutter
7-8	15 minutter
9	1 time

Brute-force-angreb på adgangskoder gøres endnu mere besværlige vha. en trinvis forøgelse af tidsforsinkelsen, når der er indtastet en ugyldig adgangskode på den låste skærm. Hvis Indstillinger > Touch ID & adgangskode > Slet data er slået til, slettes enheden automatisk efter 10 på hinanden følgende forgæves forsøg på indtastning af adgangskoden. Flere på hinanden følgende forsøg med den samme forkerte adgangskode tæller kun som et forgæves forsøg. Denne indstilling er også tilgængelig som en administrativ politik via en MDM-løsning, der understøtter denne funktion, og Exchange ActiveSync og kan indstilles til en lavere grænse.

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

Der kræves Touch ID, Face ID eller indtastning af adgangskode for at aktivere dataforbindelse gennem Lightning-, USB- eller Smart Connector-grænsefladen, hvis der ikke er blevet oprettet nogen dataforbindelse for nylig. Det sker for at øge sikkerheden, samtidig med at brugervenligheden bevares. Det begrænser angrebsfladen mod fysisk tilsluttede enheder som ondsindede opladere og giver samtidig mulighed for at bruge andet tilbehør inden for rimelige tidsrammer. Hvis der er gået mere end en time,

Skift til DFU-funktionen (Device Firmware Upgrade)
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.

Slut først enheden til en computer med et USB-kabel.

Gør et af følgende afhængigt af enheden:

iPhone X eller nyere modeller, iPhone 8 eller iPhone 8 Plus. Tryk kort på knappen Lydstyrke op. Tryk kort på knappen Lydstyrke ned. Hold fingeren på sideknappen, og tryk derefter på knappen Lydstyrke ned igen. Giv slip på sideknappen efter fem sekunder, og fortsæt med at holde fingeren på knappen Lydstyrke ned, indtil du ser en sort skærm.

iPhone 7 eller iPhone 7 Plus. Tryk samtidig på sideknappen og knappen Lydstyrke ned, og hold dem nede. Giv slip på sideknappen efter otte sekunder, og fortsæt med at holde fingeren på knappen Lydstyrke ned, indtil du ser en sort skærm.

iPhone 6s og tidligere modeller, iPad eller iPod touch. Tryk samtidig på knappen Hjem og den øverste knap (eller sideknappen), og hold dem nede. Giv slip på den øverste knap (eller sideknappen) efter fem sekunder, og fortsæt med at holde fingeren på knappen Hjem, indtil du ser en sort skærm.

Apple TV. Slut enheden til din computer ved hjælp af et Micro-USB-kabel, og tving derefter enheden til at genstarte ved at holde knapperne Menu og Ned nede samtidig i seks til syv sekunder. Tryk øjeblikkeligt efter genstart på Menu og Afspil samtidig, indtil der vises en besked i iTunes om, at der er fundet en Apple TV-enhed i Gendannelsesfunktion.

Bemærk: Der vises ikke noget på skærmen, mens DFU-funktionen er aktiv på enheden. Hvis Apple-logoet vises, blev sideknappen eller knappen Vågeblus til/fra holdt nede for længe. Hvis enheden er gået i DFU-funktion, bliver skærmen sort, og iTunes viser beskeden "iTunes har fundet en (iPad, iPhone eller iPod touch) i Gendannelsesfunktion. Du skal gendanne denne (iPad, iPhone eller iPod touch), før du kan bruge den med iTunes."

siden iOS-enheden blev låst, eller siden et tilbehørs dataforbindelse er ophørt, tillader enheden ikke 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. 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:

- Sikrer, 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 en 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 den er blevet låst, hvis der er gået mere end tre dage, siden en dataforbindelse blev etableret med et tilbehør. Det øger sikkerheden for brugere, der sjældent benytter sådant tilbehør. Dataforbindelser gennem Lightning, USB og Smart Connector slås også fra, når enheden er i en tilstand, hvor den kræver en adgangskode for at slå biometrisk genkendelse til igen.

DFU- og gendannelsesfunktion

På enheder med Apple A10, A11 og S3 SoC'er er der ikke adgang til klassenøgler, der er beskyttet af brugerens adgangskode, fra gendannelsesfunktionen. A12 og S4 SoC'er udvider denne beskyttelse til også at gælde DFU-funktionen (Device Firmware Update).

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.

Seed bits startede på Apple A10 og S3 SoC'er og er dedikeret til at skelne nøgler, der er beskyttet af brugerens adgangskode. Seed bit'en indstilles til nøgler, der kræver brugerens adgangskode (herunder nøgler til databeskyttelsesklasse A, B og C), og slettes til nøgler, der ikke kræver brugerens adgangskode (herunder nøglen til arkivsystemmetadata og nøgler til klasse D).

På A12 SoC'er låser Secure Enclave Boot ROM adgangskodens seed bit, hvis programprocessoren er i DFU-funktion eller Gendannelsesfunktion. Når adgangskode-seed bit'en er låst, tillades ændringer af den ikke, hvilket forhindrer adgang til data, der er beskyttet af brugerens adgangskode.

På Apple A10, A11, S3 og S4 SoC'er er adgangskodens seed bit låst af Secure Enclave OS, hvis enheden er i Gendannelsesfunktion. Secure Enclave Boot ROM og OS tjekker begge BPR (Boot Progress Register) for på sikker vis at afgøre enhedens aktuelle funktion.

Databeskyttelsesklasser

Når der oprettes et nyt arkiv på en iOS-enhed, 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.

Fuldstændig beskyttelse

`(NSFileProtectionComplete)`: Klassenøglen beskyttes med en nøgle, der er afledt af brugerens 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 adgangskoden igen eller låser enheden op ved hjælp af Touch ID eller Face ID.

Beskyttet, hvis ikke åben

`(NSFileProtectionCompleteUnlessOpen)`: Det kan være nødvendigt at skrive visse arkiver, mens enheden er låst. 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. SHA-256 bruges som hashing-funktion. Så snart arkivet lukkes, slettes arkivnøglen fra hukommelsen. Når arkivet skal åbnes igen, oprettes den fælles hemmelighed ("shared secret") igen ved hjælp af den private nøgle til klassen NSFileProtectionCompleteUnlessOpen (Beskyttet, hvis ikke åbent) og arkivets midlertidige offentlige nøgle, som bruges til at pakke arkivnøglen ud. Derefter afkrypteres arkivet med arkivnøglen.

Beskyttet indtil første brugergodkendelse

`(NSFileProtectionCompleteUntilFirstUserAuthentication)`: Denne klasse fungerer på samme måde som NSFileProtectionComplete (Fuldstændig beskyttelse), bortset fra at den afkrypterede klassenøgle ikke fjernes fra hukommelsen, når enheden låses. 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.

Ingen beskyttelse

`(NSFileProtectionNone)`: Denne klassenøgle er kun beskyttet med UID og opbevares i Effaceable Storage. Eftersom alle de nøgler, der skal bruges til at afkryptere 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 en iOS-enhed).

Klassenøgle til databeskyttelse

Klasse A	Fuldstændig beskyttelse	(NSFileProtectionComplete)
Klasse B	Beskyttet, hvis ikke åben	(NSFileProtectionCompleteUnlessOpen)
Klasse C	Beskyttet indtil første brugergodkendelse	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Klasse D	Ingen beskyttelse	(NSFileProtectionNone)

Komponenter i et emne i nøgleringen
Ud over adgangsgruppen indeholder hvert emne i nøgleringen administrative metadata (f.eks. tidsstemplerne "oprettet" og "sidst opdateret").

Det indeholder også SHA-1 hash-værdier til de attributter, der bruges i forespørgsler om emnet (f.eks. kontonavn og servernavn), så det er muligt at foretage opslag uden at afkryptere de enkelte emner. Endelig indeholder det også krypteringsdata, som omfatter følgende:

- Versionsnummer
- Adgangskontrollistedata (ACL'er)
- En værdi, der angiver emnets beskyttelsesklasse
- Emnenøgle, der er pakket med beskyttelsesklassenøglen
- Ordbog med attributter, der beskriver emnet (som overføres til SecItemAdd), kodet som en binær plist (egenskabsliste) og krypteret med emnenøglen

Krypteringen er AES-256 GCM (Galois/Counter Mode). Adgangsgruppen indgår i egenskaberne og beskyttes med det GMAC-mærke, der blev beregnet under krypteringen.

Databeskyttelse af nøglering

Mange apps skal kunne håndtere adgangskoder og andre korte, men følsomme datasekvenser, f.eks. nøgler og log ind-tokens. Med nøgleringen i iOS kan disse emner opbevares på en sikker måde.

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 søgehastigheden, mens den hemmelige værdi (kSecValueData) krypteres med den hemmelige nøgle. Metadatanøglen beskyttes af Secure Enclave-processoren, men indlæses i programprocessoren for at tillade hurtige nøgleringsforespørgsler. Den hemmelige nøgle kræver altid en rundtur gennem Secure Enclave-processoren.

Nøgleringen er implementeret som en SQLite-database i arkivsystemet. Der er kun en database, og *securityd*-dæmonen bestemmer, hvilke emner i nøgleringen hver proces eller app har adgang til. API'er til nøglerings-adgang 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. Det styres med et krav om, at apps fra tredjeparter bruger adgangsgrupper med et præfiks, de har fået tildelt via Apple Developer Program (via programgrupper). Præfikskravet og programgruppernes forskellighed opretholdes ved hjælp af kodesignering, **programbeskrivelser** og Apple Developer Program.

Data i nøgleringe beskyttes med en klassestruktur, som ligner den, der bruges til beskyttelse af arkivdata. Disse klassers funktionsmåde ligner den for klasserne til beskyttelse af arkivdata, men deres nøgler er forskellige, og klasserne indgår i API'er med andre navne.

Tilgængelighed	Beskyttelse af arkivdata	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
Adgangskode slået til	Ikke aktuelt	kSecAttrAccessible WhenPasscodeSetThisDeviceOnly

Apps, som benytter 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 adgangskode. Denne klasse eksisterer kun i system**nøglesamlingen**. De:

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

Hvis adgangskoden 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 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.

Til emner i nøgleringen, som oprettes af iOS, benyttes følgende klassebeskyttelse:

Emne	Tilgængeligt
Wi-Fi-adgangskoder	Efter enheden er låst op første gang
E-mailkonti	Efter enheden er låst op første gang
Exchange-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
Adgangskode til deling i hjemmet	Når låst op
Safari-adgangskoder	Når låst op
Safari-bogmærker	Når låst op
iTunes-sikkerhedskopiering	Når låst op, ikke-flytbart
VPN-certifikater	Altid, ikke-flytbart
Bluetooth®-nøgler	Altid, ikke-flytbart
Token for APNs (Apple Push Notification service)	Altid, ikke-flytbart
Certifikater og privat nøgle til iCloud	Altid, ikke-flytbart
iMessage-nøgler	Altid, ikke-flytbart
Certifikater og private nøgler installeret af en konfigurationsbeskrivelse	Altid, ikke-flytbart
PIN-kode til SIM	Altid, ikke-flytbart
Token til Find min iPhone	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. Touch ID eller Face ID eller ved at indtaste enhedens adgangskode. Adgang til emner kan også begrænses via en angivelse af, at Touch ID- eller Face 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.

Nøglesamlinger

Nøglerne til klasserne til beskyttelse af data i såvel arkiver som nøgleringe indsamles og administreres i nøglesamlinger ("keybags"). iOS bruger disse nøglesamlinger: Bruger, Enhed, Sikkerhedskopi, Depot og iCloud-sikkerhedskopi.

Nøglesamlingen Bruger er det sted, hvor de indpakkede klassenøgler, som bruges under den normale drift af enheden, opbevares. Når der f.eks. indtastes en adgangskode, indlæses nøglen til `NSFileProtectionComplete` fra nøglesamlingen Bruger og pakkes ud. Det er en binær egenskabsliste (.plist), der opbevares i klassen Ingen beskyttelse, hvis indhold er krypteret med en nøgle, der opbevares i Effaceable Storage. Fremadrettet sikkerhed til nøglesamlinger sikres ved, at denne nøgle slettes og dannes igen, hver gang en bruger skifter adgangskode. Kerneudvidelsen `AppleKeyStore` 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 bruges til at opbevare de indpakkede klassenøgler, der bruges til funktioner i forbindelse med enhedsspecifikke data. iOS-enheder, der er konfigureret til delt brug, har sommetider brug for adgang til godkendelsesoplysninger, før en bruger har logget ind. Der er derfor behov for en nøglesamling, der ikke er beskyttet med brugerens adgangskode. iOS understøtter ikke kryptografisk adskillelse af arkivsystemindhold pr. bruger, hvilket betyder, at systemet vil bruge klassenøgler fra nøglesamlingen Enhed til at indpakke arkivnøgler. Nøgleringen bruger derimod klassenøgler fra nøglesamlingen Bruger til at beskytte emner i brugerens nøglering. På iOS-enheder, der er konfigureret til en enkelt bruger (standardkonfigurationen), er nøglesamlingen Enhed og nøglesamlingen Bruger ens og er beskyttet af brugerens adgangskode.

Nøglesamlingen Sikkerhedskopi oprettes, når iTunes opretter en krypteret sikkerhedskopi og arkiverer 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 fås adgang til dem på en anden enhed.

Nøglesamlingen beskyttes med den adgangskode, der er indstillet i iTunes og behandlet med 10 millioner gennemløb af PBKDF2. 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 en iTunes-sikkerhedskopi, krypteres de sikkerhedskopierede arkiver ikke 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 bruges til iTunes-synkronisering og MDM. Denne nøglesamling giver iTunes mulighed for at sikkerhedskopiere og synkronisere, uden at brugeren skal indtaste en adgangskode, og det sætter en MDM-løsning i stand til at slette en brugers adgangskode eksternt. Den opbevares på den computer, der bruges til at synkronisere med 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 adgangskodebeskyttet enhed opretter forbindelse til iTunes, bliver brugeren bedt om at indtaste en adgangskode. 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 adgangskoden til enheden skal indtastes, før brugeren kan sikkerhedskopiere med iTunes første gang efter en genstart.

Hvis softwareopdateringen sker via en trådløs forbindelse, bliver brugeren bedt om at indtaste sin adgangskode, 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 adgangskode indtastes, og alle tidligere genererede tokens gøres ugyldige, hvis brugerens adgangskode 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.

Når tælleren til engangstokenet til oplåsning øges med 1 i Secure Enclave, gøres alle eksisterende tokens ugyldige. Tælleren øges med 1, når et token bruges, efter første oplåsning af en genstartet enhed, når en softwareopdatering annulleres (af brugeren eller af systemet), og når politiktimeren for et token er udløbet.

Engangstokenet til oplåsning til overvågede softwareopdateringer udløber efter 20 minutter. Dette token eksporteres fra Secure Enclave og skrives til Effaceable Storage. En politiktimer forøger tælleren med 1, hvis enheden ikke genstartes inden for 20 minutter.

Uovervågede softwareopdateringer foretages, når systemet opdager en tilgængelig opdatering, og:

- Automatiske opdateringer konfigureres i iOS 12 (eller en nyere version).

  eller

- Brugeren vælger "Installer senere", når der kommer en meddelelse om opdateringen.

Når brugeren har indtastet adgangskoden, 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 ligner nøglesamlingen Sikkerhedskopi. Alle klassenøglerne i denne nøglesamling er asymmetriske (vha. Curve25519 ligesom databeskyttelsesklassen Beskyttet, hvis ikke åben), så iCloud-sikkerhedskopieringen kan udføres i baggrunden. For alle databeskyttelsesklasser undtagen Ingen beskyttelse gælder, at de krypterede data læses fra enheden og sendes til iCloud. De tilhørende klassenøgler beskyttes af iCloud-nøgler. Ligesom ved en ikke-krypteret iTunes-sikkerhedskopi er klassenøglerne til nøgleringen pakket med en nøgle, der er afledt af UID. Der bruges også en asymmetrisk nøglesamling til sikkerhedskopien i forbindelse med gendannelse af iCloud-nøgleringen.

Appsikkerhed

Apps er et af de mest kritiske elementer i en moderne sikkerhedsarkitektur til mobile enheder. 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.

iOS indeholder derfor flere beskyttelseslag for at sikre, at apps er signeret og godkendt, og at de afvikles i et isoleret miljø ("sandbox") for at beskytte brugerdataene. Disse elementer skaber en stabil og sikker platform til apps, så tusindvis af udviklere kan levere hundredtusindvis af apps til iOS uden at skade systemintegriteten. Brugerne kan benytte disse apps på deres iOS-enheder uden unødig frygt for virus, malware og angreb fra uautoriserede personer.

Signering af appkode

Efter iOS-kernen er startet, styrer den, hvilke brugerprocesser og apps der kan afvikles. For at sikre, at alle apps kommer fra en kendt og godkendt kilde og ikke er blevet modificeret, kræver iOS, at al programkode skal signeres 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 tillidskæde fra operativsystemet til apps og forhindrer apps fra tredjeparter i at indlæse ikke-signerede koderessourcer eller benytte selvmodificerende kode.

Før udviklere kan udvikle og installere apps på iOS-enheder, skal de 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 der udstedes et certifikat. Med certifikatet kan udviklere signere programmer og indsende dem til App Store, så de kan distribueres derfra. Det betyder, at alle programmer i App Store er indsendt af en person eller organisation, der kan identificeres. Det modvirker udvikling af ondsindede programmer. Appene er også blevet gennemgået af Apple for at sikre, at de fungerer som beskrevet og ikke indeholder åbenlyse fejl eller andre problemer. Ud over den teknologi der allerede er beskrevet, giver denne kuratering kunderne tillid til kvaliteten af de apps, de køber.

iOS 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. Et program kan henvise til et hvilket som helst platformbibliotek, der følger med systemet, eller til et bibliotek med samme team-id i dets kodesignatur som hovedprogramarkivet. Eftersom de programarkiver, der følger med systemet, ikke har et team-id, kan de kun henvise til biblioteker, som følger med systemet.

Virksomheder har også mulighed for at udvikle interne apps 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) med deres D-U-N-S-nummer. Apple godkender ansøgere efter at have bekræftet deres identitet og berettigelse. Når en organisation er blevet medlem af ADEP, kan den registrere sig for at få en programbeskrivelse, der tillader, at interne apps afvikles på enheder, som den godkender. Programbeskrivelsen skal være installeret hos brugerne, før de kan afvikle de interne apps. Derved sikres, at kun organisationens godkendte brugere er i stand til at indlæse appene på deres iOS-enheder. Apps, der installeres via MDM, er implicit godkendt, fordi relationen mellem organisationen og enheden allerede er etableret. Ellers skal brugerne godkende appens programbeskrivelse under Indstillinger. Organisationer kan forhindre brugere i at godkende apps fra ukendte udviklere. Første gang en firmaapp startes, skal enheden modtage en positiv bekræftelse fra Apple af, at appen har tilladelse til at blive afviklet.

I modsætning til nogle andre mobile platforme tillader iOS ikke, at brugerne installerer potentielt ondsindede ikke-signerede apps fra websteder eller afvikler kode, der ikke er godkendt. Under programafviklingen foretages kontrol af kodesignaturer for alle programsider i hukommelsen for at sikre, at en app ikke er blevet modificeret, efter at den blev installeret eller sidst blev opdateret.

Sikkerhed under programafvikling

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

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. Derved forhindres, at apps indsamler eller ændrer oplysninger, som andre apps har arkiveret. 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.

Systemarkiver og -ressourcer skærmes også mod brugerens apps. Størstedelen af iOS afvikles som brugeren “mobile”, der ikke har nogen særlige tilladelser. Det samme gør alle apps fra tredjeparter. Hele partitionen med operativsystemet er aktiveret som skrivebeskyttet. Unødvendige værktøjer, f.eks. tjenesterne til ekstern log ind, indgår ikke i systemsoftwaren, og API'er tillader ikke, at apps eskalerer deres tilladelser for at ændre andre apps eller iOS selv.

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 programafviklingsfaktorer, 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 et systemprogram 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) beskytter mod udnyttelse af fejl, der ødelægger hukommelsen. Indbyggede apps bruger ASLR til at sikre en tilfældig placering af alle hukommelsesområder, når de startes. Tilfældig placering af hukommelsesadresserne til programkode, systembiblioteker og relaterede programmeringskonstruktioner mindsker sandsynligheden for mange avancerede 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 langt sværere at foretage et angreb, især på flere enheder samtidig. Xcode, der er udviklingsmiljøet i iOS, kompilerer automatisk programmer fra tredjeparter med ASLR-understøttelse slået til.

Yderligere beskyttelse opnås ved, at iOS bruger ARM-funktionen Execute Never (XN), som markerer hukommelsessider som ikke-programsider. Hukommelsessider, der både er markeret med skriveadgang og som programsider, 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 programside, der er skriveadgang til, og som er tildelt en tilfældig adresse. Safari bruger denne funktionalitet til sin JavaScript JIT-compiler.

Udvidelser

iOS giver ved hjælp af udvidelser apps mulighed for at stille funktionalitet til rådighed for andre apps. Udvidelser er signerede binære programarkiver til bestemte formål, som er indpakket i en app. Systemet registrerer automatisk udvidelser på installeringstidspunktet og gør dem tilgængelige for andre apps ved hjælp af et sammenligningssystem.

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 systemprogrammer. Den widget, der viser oversigten "I dag", findes f.eks. kun i Meddelelsescenter, og en udvidelse vedrørende deling er kun tilgængelig fra vinduet Deling. Der er følgende udvidelsespunkter: "I dag"-widgets, Del, Specielle handlinger, Fotoredigering, Dokument-udbyder og Specielt tastatur.

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.

Specielle tastaturer er en særlig type udvidelse, fordi de aktiveres af brugeren til hele systemet. Når en tastaturudvidelse er aktiveret, bruges den til alle tekstfelter, undtagen indtastning af adgangskoder 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 lade udvidelsen blive afviklet i det isolerede standardmiljø, hvis brugeren giver sit samtykke.

For enheder, der er tilmeldt en MDM-løsning, gælder, at dokument- og tastaturudvidelser overholder administrerede "Åbn i"-regler. MDM-løsningen kan f.eks. forhindre en bruger 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 appudviklere forhindre brugen af tastaturudvidelser fra tredjeparter i deres app.

Appgrupper

Apps og udvidelser, der ejes af en given udvikler, kan dele indhold, når de konfigureres som en del af en appgruppe. 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 appgruppe, har de adgang til følgende:

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

Apple Developer Portal garanterer, at alle appgruppe-id'er er forskellige i hele økosystemet til apps.

Databeskyttelse i apps

iOS Software Development Kit (SDK) 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 adgangskode 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.

Tilbehør

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-enhed via et Lightning-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-kablet eller lokalitetsoplysninger leveret via Bluetooth. Et integreret kredsløb til godkendelse sikrer, 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 benytter MFi-SAP (Secure Association Protocol), som krypterer kommunikationen mellem tilbehøret og enheden ved hjælp af AES-128 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).

HomeKit

HomeKit er en infrastruktur til automatisering i hjemmet, som benytter iCloud- og iOS-sikkerhed til at beskytte og synkronisere private data, uden at Apple kan se dem.

HomeKit-identitet

Identitet og sikkerhed i HomeKit bygger på Ed25519-par med offentlige-private nøgler. Der genereres et Ed25519-nøglepar på iOS-enheden til hver bruger af HomeKit, og dette nøglepar bliver brugerens HomeKit-identitet. Det bruges til at godkende kommunikation mellem iOS-enheder og mellem iOS-enheder og tilbehør.

Nøglerne opbevares i nøgleringen og medtages kun i krypterede sikkerheds-kopier af nøgleringen. Nøglerne synkroniseres mellem enheder ved hjælp af 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 med HomeKit-tilbehør

HomeKit-tilbehør genererer deres eget Ed25519-nøglepar, der skal bruges til at kommunikere med iOS-enheder. Hvis standardindstillingerne gendannes på tilbehøret, genereres et nyt nøglepar.

Med henblik på at skabe en relation mellem en iOS-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-enheden af brugeren, hvorefter den krypteres vha. CHACHA20-POLY1305 AEAD med nøgler afledt af HKDF-SHA-512. Tilbehørets MFi-certificering kontrolleres under indstillingen. Tilbehør uden en MFi-chip kan indbygge understøttelse af softwaregodkendelse på iOS 11.3 og nyere versioner.

Når iOS-enheden og HomeKit-tilbehøret kommunikerer under brugen, godkender de hinanden ved at bruge de nøgler, der blev udvekslet i processen ovenfor. Hver session etableres vha. STS-protokollen og krypteres med nøgler afledt af HKDF-SHA-512 på basis af Curve25519-nøgler pr. session. Det gælder både for IP-baseret tilbehør og Bluetooth LE-tilbehør (Low Energy).

Når det gælder Bluetooth Low Energy-enheder, der understøtter udsendelsesmeddelelser, forsyner en parret iOS-enhed tilbehøret med en udsendelseskrypteringsnøgle i en sikker session. Denne nøgle bruges til at kryptere de data om statusændringer på tilbehøret, som meddeles via Bluetooth Low Energy-annonceringerne. Krypteringsnøglen til annonceringer er afledt af HKDF-SHA-512, og dataene krypteres ved hjælp af algoritmen CHACHA20-POLY1305 AEAD (Authenticated Encryption with Associated Data). Udsendelseskrypteringsnøglen ændres med jævne mellemrum af iOS-enheden og synkroniseres til andre enheder via iCloud som beskrevet i afsnittet "Datasynkronisering mellem enheder og brugere" nedenfor.

Lokal datalagring

HomeKit arkiverer data om hjemmene, tilbehøret, scenerne og brugerne på en brugers iOS-enhed. De arkiverede data krypteres med nøgler afledt af brugerens HomeKit-id-nøgler plus en tilfældig nonce-værdi. Desuden arkiveres HomeKit-data ved hjælp af databeskyttelsesklassen Beskyttet indtil første brugergodkendelse. HomeKit-data sikkerhedskopieres kun i krypterede sikkerhedskopier, så ikke-krypterede iTunes-sikkerhedskopier indeholder f.eks. ikke HomeKit-data.

Datasynkronisering mellem enheder og brugere

HomeKit-data kan synkroniseres mellem en brugers iOS-enheder vha. iCloud og iCloud-nøglering. HomeKit-data krypteres under synkroniseringen med nøgler afledt af brugerens HomeKit-id og en tilfældig nonce-værdi. Disse data behandles som et uigennemsigtigt dataobjekt ("opaque blob") under synkroniseringen. Det nyeste "blob" arkiveres i iCloud for at gøre synkronisering mulig, men det bruges ikke til noget andet formål. Da krypteringen foretages med nøgler, der kun er tilgængelige på brugerens iOS-enheder, er der ikke adgang til dataene under overførslen og på iCloud-lagringspladsen.

HomeKit-data synkroniseres også mellem flere brugere i samme hjem. Denne proces bruger samme godkendelse og kryptering som mellem en iOS-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 et samlingspunkt i hjemmet, hvor handlingen færdiggøres.

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-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-enheder, der indgår i HomeKit-hjemmet.

Hvis en bruger ikke har flere enheder og nægter at give flere brugere adgang til sit hjem, synkroniseres der ikke nogen HomeKit-data til iCloud.

Hjemmedata og apps

Adgang til hjemmedata fra apps styres af brugerens anonymitets-indstillinger. Brugerne bliver bedt om at give adgang, når apps anmoder om hjemmedata, i lighed med Kontakter, Fotos og andre iOS-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 her: https://developer.apple.com/homekit/.

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. Du kan få flere oplysninger under "Siri" i afsnittet Internettjenester i dette dokument.

IP-kameraer i HomeKit

IP-kameraer i HomeKit sender video- og lydstreaming direkte til den iOS-enhed på det lokale netværk, der opretter adgang til streamingen. Streamingen krypteres med tilfældige nøgler på iOS-enheden og IP-kameraet, som udveksles via den sikre HomeKit-session med kameraet. Når iOS-enheden ikke er på det lokale netværk, viderestilles streamingen via en hub i hjemmet til iOS-enheden. Hub'en i hjemmet afkrypterer ikke streamingen og fungerer kun som et viderestillingspunkt mellem iOS-enheden og IP-kameraet. Når en app viser videobilledet fra IP-kameraet i HomeKit for brugeren, gengiver HomeKit videobillederne sikkert fra en separat systemproces, så appen ikke kan få adgang til eller arkivere videostreamingen. Apps har heller ikke tilladelse til at arkivere skærmbilleder fra streamingen.

Ekstern adgang til iCloud til HomeKit-tilbehør

HomeKit-tilbehør kan oprette direkte forbindelse til iCloud for at gøre det muligt for iOS-enheder at styre tilbehøret, når der ikke er adgang til Bluetooth- eller Wi-Fi-kommunikation.

Ekstern adgang til iCloud er omhyggeligt designet, så tilbehør kan styres og sende meddelelser, uden at Apple kan se, hvad tilbehøret er, eller hvilke kommandoer og meddelelser der sendes. HomeKit sender ikke oplysninger om hjemmet via ekstern adgang til iCloud.

Når en bruger sender en kommando via ekstern adgang til iCloud, godkendes tilbehøret og iOS-enheden gensidigt, og data krypteres vha. den samme procedure som beskrevet for lokale forbindelser. Indholdet af kommunikationen krypteres og er ikke synligt for Apple. Adresseringen gennem iCloud er baseret på de iCloud-id'er, som er registreret under indstillingen.

Tilbehør, der understøtter ekstern adgang til iCloud, tilknyttes under indstillingen af tilbehøret. Tilknytningsprocessen starter med, at brugeren logger ind på iCloud. Derefter beder iOS-enheden tilbehøret om at signere en udfordring vha. den Apple Authentication-hjælpeprocessor, som er indbygget i alt Built for HomeKit-tilbehør. Tilbehøret genererer også elliptiske prime256v1-kurvenøgler, og den offentlige nøgle sendes til iOS-enheden sammen med den signerede udfordring og X.509-certifikatet til hjælpeprocessoren til godkendelse. Disse bruges til anmodning om et certifikat til tilbehøret fra iCloud-tilknytningsserveren. Certifikatet opbevares af tilbehøret, men det indeholder ingen oplysninger, der afslører tilbehørets identitet, ud over at det har fået adgang til ekstern adgang til iCloud i HomeKit. iOS-enheden, der udfører tilknytningen, sender også en samling til tilbehøret, der indeholder de URL-adresser og andre oplysninger, som skal bruges ved oprettelse af forbindelse til serveren til ekstern adgang til iCloud. Disse oplysninger er ikke specifikke for nogen bruger eller noget tilbehør.

Hvert enkelt tilbehør registrerer en liste over tilladte brugere på serveren til ekstern adgang til iCloud. Disse brugere har fået tilladelse til at styre tilbehøret af brugeren, der har føjet tilbehøret til hjemmet. Brugere tildeles et id af iCloud-serveren og kan overføres til en iCloud-konto med det formål at levere beskeder og svar fra tilbehør. Tilbehør har på samme måde id'er, som er udstedt af iCloud, men disse id'er er uigennemsigtige og viser ingen oplysninger om selve tilbehøret.

Når et tilbehør opretter forbindelse til serveren til ekstern adgang til iCloud i HomeKit, oplyser det sit certifikat og et kort. Kortet kommer fra en anden iCloud-server og er ikke forskelligt for hvert tilbehør. Når et tilbehør anmoder om et kort, inkluderer det sin producent, model og firmwareversion i anmodningen. Der sendes ingen oplysninger, der identificerer brugeren eller hjemmet, i anmodningen. Forbindelsen til kortserveren er ikke godkendt. Dette skyldes hensynet til anonymiteten.

Tilbehør opretter forbindelse til serveren til ekstern adgang til iCloud vha. HTTP/2, der er sikret vha. TLS v1.2 med AES-128-GCM og SHA-256. Tilbehøret undlader at afbryde sin forbindelse til serveren til ekstern adgang til iCloud, så det kan modtage indgående beskeder og sende svar og udgående meddelelser til iOS-enheder.

HomeKit TV-fjernbetjeningstilbehør

HomeKit-tv-fjernbetjeningstilbehør fra tredjepart leverer HID-begivenheder og Siri-lyd til en tilknyttet Apple TV-enhed, der er tilføjet via appen Hjem. HID-begivenhederne sendes i en sikker session mellem Apple TV og fjernbetjeningen. 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. Lydrammer sendes direkte til Apple TV via en dedikeret lokal netværksforbindelse mellem Apple TV og fjernbetjeningen. Den lokale netværksforbindelse krypteres med et nøglepar pr. session, som er afledt af HKDF-SHA-512 og forhandles i HomeKit-sessionen mellem Apple TV og tv-fjernbetjeningen. HomeKit afkrypterer 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.

SiriKit

Siri bruger iOS-udvidelsesteknikken til at kommunikere med apps fra tredjeparter. Selvom Siri har adgang til kontakter i iOS og enhedens aktuelle lokalitet, kontrollerer Siri tilladelsen for den app, der indeholder udvidelsen, til at få adgang til brugerdata, som beskyttes af iOS, for at sikre, at appen har adgang, før oplysningerne stilles til rådighed for den. Siri overfører kun den relevante del af den oprindelige forespørgselstekst fra brugeren til udvidelsen. Hvis appen f.eks. ikke har adgang til kontakter i iOS, fortolker Siri ikke en relation i en brugerforespørgsel som "Send 10 dollar til min mor med app til mobilbetaling". I det tilfælde ser udvidelsens app kun "mor" gennem det ubehandlede talefragment, der overføres til den. Hvis appen derimod har adgang til kontakterne i iOS, modtager den oplysninger om brugerens mor fra Kontakter i iOS. Hvis en kontakt bliver omtalt i brødteksten i en besked, f.eks. "Skriv til min mor, at min bror er genial, i appen Besked", fortolker Siri ikke "min bror" uanset appens TCC'er. Indhold, der præsenteres af appen, kan blive sendt til serveren for at give Siri mulighed for at forstå de gloser, som en bruger anvender i appen.

I tilfælde som "Skaf kørsel hjem til min mor med <appnavn>" – hvor brugerens anmodning indebærer, at der skal hentes lokalitetsoplysninger fra brugerens kontakter – stiller Siri disse lokalitetsoplysninger til rådighed for appens udvidelse alene for denne anmodning, uanset appens adgang til lokaliteter eller kontakter.

Under afviklingen af appen giver Siri den app, som SiriKit understøtter, mulighed for at levere et sæt specielle ord, som er specifikke for appforekomsten. De specielle ord er knyttet til det tilfældige id, som er beskrevet i afsnittet om Siri i dette dokument, og har samme levetid.

HealthKit

HealthKit arkiverer og samler data fra sundheds- og træningsapps med brugerens tilladelse. 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.

Sundhedsdata

HealthKit giver brugerne mulighed for at opbevare og samle deres sundhedsdata fra kilder som apps, enheder og sundhedsinstitutioner. De opbevares i databeskyttelsesklassen Beskyttet, hvis ikke åben. Adgang til dataene ophører, 10 minutter efter at enheden låses, og der bliver adgang til dataene igen, næste gang brugeren indtaster adgangskoden eller bruger Touch ID eller Face ID til at låse enheden op.

HealthKit samler også administrationsdata, f.eks. adgangstilladelser til apps, navne på enheder med forbindelse til HealthKit og planlægnings-oplysninger, der bruges til at starte apps, når nye data er tilgængelige. Disse data opbevares i databeskyttelsesklassen Beskyttet indtil første brugergodkendelse.

I midlertidige journalarkiver arkiveres helbredsjournaler, der genereres, når enheden er låst, f.eks. når brugeren træner. De opbevares i data-beskyttelsesklassen Beskyttet, hvis ikke åben. Når enheden låses op, importeres de midlertidige journalarkiver i de primære sundhedsdatabaser og slettes, når fletningen er færdig.

Sundhedsdata kan arkiveres i iCloud. Kryptering fra start til slut for Sundhedsdata kræver iOS 12 eller en nyere version og tofaktorgodkendelse. Ellers vil dine data stadigvæk blive krypteret under overførsel og lagring, men de vil ikke blive krypteret fra start til slut. Når du har slået tofaktorgodkendelse til, og du har opdateret til iOS 12 eller en nyere version, vil dine data fra Sundhed blive migreret til kryptering fra start til slut.

Hvis du sikkerhedskopierer din enhed med iTunes, lagres data fra Sundhed kun, hvis sikkerhedskopien er krypteret.

Sygejournaler

Brugere kan logge ind på understøttede sundhedssystemer med 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. Efter der er oprettet forbindelse, hentes sygejournaldata direkte fra sundhedsinstitutionen via en TLS v1.2-beskyttet forbindelse. Når de er hentet, opbevares sygejournalerne sikkert sammen med andre sundhedsdata.

Dataintegritet

De data, der arkiveres i databasen, omfatter metadata, der holder styr på, hvor hver datapost stammer fra. Metadataene inkluderer et app-id, der viser, hvilken app der arkiverede 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 IETF RFC 5652.

Adgang fra apps fra tredjeparter

Adgangen til HealthKit API'et styres med berettigelser, og appene 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 appene forsyner brugerne med en anonymitetspolitik, som i detaljer beskriver appenes brug af sundhedsdata.

Adgang til sundhedsdata fra apps styres af brugerens anonymitets-indstillinger. 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 på fanen Kilder i appen Sundhed.

Hvis apps får tilladelse til at skrive data, kan appene også læse de data, de skriver. Hvis de 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 forhindrer apps i at udlede brugerens sundhedstilstand ved at lære, hvilke typer data brugeren registrerer.

Nødinfo

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 arkiveres på enheden ved hjælp af databeskyttelsesklassen *Ingen beskyttelse*, så der er adgang til dem uden indtastning af adgangskoden 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 og synkroniseres ikke mellem enheder, der benytter CloudKit.

ReplayKit

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 fra 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 fra appens proces i dæmonen *replayd* i ReplayKit. Det sikrer, at appens proces aldrig har adgang til det optagede indhold.
- **Oprettelse og opbevaring af film:** Filmarkivet skrives til et bibliotek, som kun ReplayKits subsystemer har adgang til. Apps kan aldrig få adgang. Det forhindrer, at optagelser kan bruges af tredjeparter 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.

Udsendelse

- **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 sikrer, at værtsapps ikke har nogen rettigheder til det udsendte video- og lydindhold. Kun ReplayKit og tredjeparters udvidelser til udsendelse har adgang.
- **Vælger til udsendelser:** ReplayKit indeholder en funktion til styring af oversigter (der ligner UIActivityViewController), som udvikleren kan vise i sin app for at give brugeren mulighed for at vælge, hvilken tjeneste til udsendelse der skal bruges. Funktionen til styring af oversigter er implementeret ved hjælp af UIRemoteViewController SPI og er en udvidelse i ReplayKit-framework. Den er ikke til rådighed for værtsappens proces.
- **Vælger til systemudsendelser:** Det giver brugere mulighed for at starte systemudsendelser direkte fra appen ved brug af samme systemdefinerede brugergrænseflade som den, der er tilgængelig via Kontrolcenter. Brugergrænsefladen er implementeret ved hjælp af UIRemoteViewController SPI og er en udvidelse i ReplayKit-framework. Den er ikke til rådighed for værtsappens proces.
- **Udvidelse til overførsel:** Den udvidelse til overførsel, som tredjeparters tjenester til udsendelse implementerer for at håndtere video- og lydindhold under udsendelse, kan vælge at modtage indhold på to måder:
  - Små kodede MP4-klip
  - Ubehandlede eksempelbuffere, der ikke er kodet
    - **Håndtering af MP4-klip:** Med denne håndteringsfunktion oprettes de små kodede MP4-klip af *replayd* og opbevares på en privat placering, som kun ReplayKits subsystemer har adgang til. Efter et filmklip er blevet oprettet, videregiver *replayd* filmklippets placering til tredjepartens udvidelse til overførsel via anmodnings-SPI'et NSExtension (XPC-baseret). *replayd* opretter desuden et engangstoken til sandbox, som også videregives til udvidelsen til overførsel. Det giver udvidelsen adgang til det pågældende filmklip under udvidelsesanmodningen.
    - **Håndtering af eksempelbuffer:** 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 IOSurface-objektet uddrages fra bufferen med videoeksempler, kodes sikkert som et XPC-objekt, sendes via XPC til tredjepartens udvidelse og afkodes sikkert til et IOSurface-objekt igen.

Sikre noter

Appen Noter indeholder en funktion til sikre noter, der giver en bruger mulighed for at beskytte indholdet af bestemte noter. Sikre noter krypteres med en adgangskode, som brugeren angiver, og som skal indtastes for at se noterne i iOS og macOS og på iCloud-webstedet.

Når en bruger sikrer en note, dannes en nøgle på 16 byte ud fra brugerens adgangskode ved hjælp af PBKDF2 og SHA256. Notens indhold krypteres ved hjælp af AES-GCM. Der oprettes nye poster i Core Data og CloudKit til opbevaring af den krypterede note, mærket og initialiseringsvektoren. De oprindelige noteposter slettes, og de krypterede data skrives ikke i stedet. Bilag krypteres på samme måde. De understøttede bilag er 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.

Når en bruger har indtastet adgangskoden for at se eller oprette en sikker note, åbner Noter en sikker session. Mens den er åben, behøver brugeren ikke indtaste adgangskoden eller bruge Touch ID eller Face ID for at se eller sikre andre noter. Den sikre session kan dog kun anvendes til noter, der er beskyttet af den aktuelle adgangskode, ikke til noter 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.
- Enheden låses.

Brugere, som glemmer deres adgangskode, kan se sikre noter eller sikre nye noter, hvis de har slået Touch ID eller Face ID til på deres enheder. Efter tre forgæves forsøg på at indtaste adgangskoden viser Noter et stikord, som brugeren har angivet. Brugeren skal kende den nuværende adgangskode for at skifte den.

Brugerne kan nulstille adgangskoden, hvis de har glemt den nuværende adgangskode. Det sætter brugerne i stand til at oprette nye sikre noter med en ny adgangskode, men det 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 kan deles med andre. Delte noter er ikke krypteret fra start til slut. Apple bruger 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 afkryptere hinandens data.

Apple Watch

Apple Watch bruger sikkerhedsfunktionerne og -teknologien bygget til iOS til at beskytte data på enheden samt kommunikationen med dens iPhone-partner og internettet. Det inkluderer teknologier som databeskyttelse og kontrol af adgang til nøgleringen. Brugerens adgangskode er også tæt forbundet med enhedens UID til oprettelse af krypteringsnøgler.

Pardannelse mellem Apple Watch og iPhone sikres vha. en OOB-proces (Out-Of-Band) til udveksling af offentlige nøgler efterfulgt af BLE-linket "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-adgangskodeoptegnelse som reservemetode til pardannelse, hvis det viser sig nødvendigt.

Når BLE-sessionen er etableret og krypteret vha. den højeste sikkerheds-protokol, der er tilgængelig i Bluetooth Core Specification, udveksler Apple Watch og iPhone nøgler vha. en metode, der er tilpasset fra IDS (Apple identity service) som beskrevet under "iMessage" i afsnittet Internettjenester i dette dokument. Når nøglerne er blevet udvekslet, kasseres Bluetooth-sessionsnøglen, og al kommunikation mellem Apple Watch og iPhone krypteres vha. IDS, hvor de krypterede Bluetooth-, Wi-Fi- og mobilnetværkslinks leverer et sekundært krypteringslag. BLE-adressen skifter hvert 15. minut for at reducere risikoen for, at trafikken bliver kompromitteret.

For at understøtte apps, der kræver streaming-data, leveres kryptering vha. metoder beskrevet under "FaceTime" i afsnittet Internettjenester i dette dokument ved brug af den IDS-tjeneste, som enten leveres af den iPhone, der dannes par med, eller af en direkte internetforbindelse.

Apple Watch implementerer hardwarekrypteret og klassebaseret beskyttelse af arkiver og nøgleringsemner som beskrevet i afsnittet Kryptering og databeskyttelse i dette dokument. Adgangskontrollerede nøglesamlinger til nøgleringsemner bruges også. Nøgler brugt til kommunikation mellem uret og iPhone sikres også vha. klassebaseret beskyttelse.

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 i Wi-Fi-delen af appen Indstillinger på Apple Watch. Hvis ingen af enhederne tidligere har oprettet forbindelse til et Wi-Fi-netværk, kan der manuelt oprettes forbindelse til dette netværk i Wi-Fi-delen af appen 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 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.

Du kan låse Apple Watch manuelt ved at holde sideknappen nede. Desuden låses enheden automatisk, kort efter den er blevet fjernet fra brugerens håndled, medmindre Registrering af håndled er slået fra. Når Apple Watch er låst, kan Apple Pay kun bruges, hvis adgangskoden til uret indtastes. Registrering af håndled slås fra med appen Apple Watch på iPhone. Denne indstilling kan også håndhæves vha. en MDM-løsning.

Den iPhone, der dannes par med, kan også låse uret op, hvis uret bæres på armen. Det udføres, ved at der etableres en forbindelse godkendt af de nøgler, der blev oprettet under parring. iPhone sender nøglen, som uret bruger til at låse sine databeskyttelsesnøgler op med. Urets adgangskode kendes ikke af iPhone og sendes heller ikke. Du kan slå denne funktion fra vha. appen Apple Watch på iPhone.

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

Apple Watch kan konfigureres til en opdatering af systemsoftware samme nat. Der er flere oplysninger om, hvordan Apple Watch-adgangskoden opbevares, så den kan bruges under opdateringen, i afsnittet Nøglesamlinger i dette dokument.

Hvis Find min iPhone slås til på den iPhone, som Apple Watch danner par med, kan Aktiveringslås bruges på Apple Watch. 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.

Netværkssikkerhed

Ud over de indbyggede sikkerhedsforanstaltninger, som Apple bruger til at beskytte de arkiverede data på iOS-enheder, findes der mange forholdsregler med hensyn til netværkssikkerhed, som organisationer kan tage for at sikre oplysninger under overførslen til og fra en iOS-enhed.

Da mobile brugere skal kunne få adgang til virksomhedens netværk overalt i verden, er det vigtigt at sørge for, at de er godkendt, og at deres data beskyttes under overførslen. iOS bruger – og giver udviklere adgang til – standardnetværksprotokoller til godkendt, autoriseret og krypteret kommunikation. 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.

På andre platforme er det nødvendigt at bruge firewallsoftware til at beskytte åbne kommunikationsporte mod indtrængen. Eftersom iOS er mindre udsat for angreb, fordi antallet af lyttende porte er begrænset, og unødvendige netværkshjælpeprogrammer, f.eks. telnet og shells, og en webserver er fjernet, er der ikke behov for firewallsoftware på iOS-enheder.

TLS

iOS understøtter TLS v1.0, TLS v1.1, TLS v1.2, TLSv1.3 (Transport Layer Security) og DTLS. Det understøtter både AES-128 og AES-256 med præference for kodepakker med PFS (Perfect Forward Secrecy). Safari, Kalender, Mail og andre internetapps 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 (Network.framework) indeholder fintmaskede kontrolmuligheder. CFNetwork tillader ikke brug af SSLv3, og apps, der bruger WebKit (f.eks. Safari) forhindres i at oprette en SSLv3-forbindelse.

I iOS 11 og nyere versioner og macOS High Sierra 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 Sierra. 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, apps og programmer, der kræver RC4, bør opgraderes, så de bruger moderne og 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 overholder 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 GCM- eller CBC-funktion. 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 v1.2 med Forward Secrecy, og certifikater skal være gyldige og signerede vha. SHA-256 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.

VPN

Der kræves normalt minimal indstilling og konfiguration, før sikre netværkstjenester som VPN (Virtual Private Networking) fungerer på iOS-enheder. iOS-enheder kan arbejde sammen med VPN-servere, der understøtter følgende protokoller og godkendelsesmetoder:

- IKEv2/IPSec med godkendelse via fælles hemmelighed (“shared secret”), RSA-certifikater, **ECDSA**-certifikater, EAP-MSCHAPv2 eller EAP-TLS
- SSL-VPN sammen med den relevante klientapp fra App Store
- Cisco IPSec med brugergodkendelse via adgangskode og maskingodkendelse via fælles hemmelighed (“shared secret”) og certifikater
- L2TP/IPSec med brugergodkendelse via MS-CHAPV2-adgangskode og maskingodkendelse via fælles hemmelighed (“shared secret”)

iOS understøtter følgende:

- **VPN On Demand** i netværk, der bruger godkendelse baseret på certifikater. It-politikker fastlægger, hvilke domæner der kræver en VPN-forbindelse, ved at bruge en VPN-konfigurationsbeskrivelse.
- **Per-App-VPN,** hvilket giver langt mere detaljerede administrationsmuligheder for VPN-forbindelser. I MDM kan der angives en forbindelse for hver administreret app og/eller bestemte domæner i Safari. Det bidrager til at sikre, at data altid sendes til og fra virksomhedens netværk, og at brugerens personlige data ikke gør.
- **Altid til-VPN (Always-On VPN),** som kan konfigureres for enheder, der administreres via en MDM-løsning (Mobile Device Management) og er under tilsyn ved hjælp af Apple Configurator 2, Apple School Manager eller Apple Business Manager. Brugerne behøver nu ikke længere slå VPN til for at aktivere beskyttelse, når de opretter forbindelse til mobil- og Wi-Fi-netværk. Altid til-VPN giver en organisation fuld kontrol over trafik til og fra enheder, idet al IP-trafik kanaliseres tilbage til organisationen. Standardprotokollen til kanalisering, IKEv2, sørger for sikker trafik 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

iOS understøtter Wi-Fi-protokoller, der er standard i branchen, herunder WPA2 Enterprise, med henblik på godkendt adgang til trådløse netværk i virksomheder. WPA2 Enterprise bruger 128 bit AES-kryptering, hvilket giver brugerne størst mulig sikkerhed for, at deres data fortsat er beskyttet, når de sender og modtager data via en Wi-Fi-netværksforbindelse. Med understøttelse af 802.1X kan iOS-enheder integreres i et bredt udsnit af RADIUS-godkendelsesmiljøer. De trådløse 802.1X-godkendelsesmetoder, der understøttes på iPhone og iPad, omfatter EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1 og LEAP.

Ud over beskyttelse af data udvider iOS beskyttelsen på WPA2-niveau til unicast- og multicast-administrationsdataenheder via tjenesten Protected Management Frame, der beskrives i 802.11w. iPhone 6 og iPad Air 2 og nyere modeller understøtter Protected Management Frame.

iOS bruger en tilfældig MAC-adresse (Media Access Control) under udførelse af Wi-FI-scanninger, når en enhed ikke har forbindelse til et Wi-Fi-netværk. Disse scanninger kan udføres for at finde og oprette forbindelse til et foretrukket 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.

iOS 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, og 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 nu skifter, 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 bruger tilfældige MAC-adresser, og at hverken Apple eller producenterne kan forudsige disse tilfældige MAC-adresser. Tilfældige MAC-adresser til Wi-Fi understøttes ikke på iPhone 4s og tidligere modeller.

På iPhone 6s og nyere modeller er et kendt Wi-Fi-netværks skjulte egenskab kendt og opdateres automatisk. Hvis et Wi-Fi-netværks SSID (Service Set Identifier) udsendes, sender iOS-enheden ikke en test med SSID'et indeholdt i anmodningen. Det forhindrer enheden i at udsende navnet på ikke-skjulte netværk.

For at beskytte enheden mod sårbarheder i netværksprocessorens firmware har netværksgrænseflader, herunder Wi-Fi og basisbånd, begrænset adgang til programprocessorens hukommelse. Når USB eller SDIO bruges til interaktion med netværksprocessoren, kan netværksprocessoren ikke starte DMA-transaktioner (Direct Memory Access) til programprocessoren. Når PCIe bruges, er hver netværksprocessor på sin egen isolerede PCIe-bus. En IOMMU på hver PCIe-bus begrænser netværksprocessorens DMA-adgang til sider i hukommelsen, der indeholder dens netværkspakker eller kontrolstrukturer.

Bluetooth

Bluetooth-understøttelsen i iOS er designet, så den bidrager med nyttige funktioner uden at forøge adgangen til private data unødigt. iOS-enheder understøtter forbindelser med krypteringsfunktion 3, sikkerhedsfunktion 4 og Service Level 1. iOS understøtter følgende Bluetooth-beskrivelser:

- HFP (Hands-Free Profile)
- PBAP (Phone Book Access Profile)
- MAP (Message Access Profile)
- A2DP (Advanced Audio Distribution Profile)
- AVRCP (Audio/Video Remote Control Profile)
- PAN-beskrivelsen (Personal Area Network)
- HID-beskrivelsen (Human Interface Device)

Understøttelsen af disse beskrivelser afhænger af enheden.

Du kan få flere oplysninger her:
https://support.apple.com/HT204387

Single sign-on

iOS 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 (PKINIT) understøttes også.

SSO i iOS 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:

- 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. Til konfigurationen af SSO understøtter iOS konfigurationsbeskrivelsesdata, der giver MDM-løsninger 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.

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

Med Handoff kan en bruger automatisk overføre sin igangværende aktivitet mellem sine iOS-enheder og sin Mac-computer, 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 4.2 OOB-par (Out-Of-Band) ved hjælp af APNs. De enkelte beskeder krypteres på stort set samme måde som iMessage-beskeder. Efter enhederne har dannet par, genererer hver af dem en symmetrisk 256 bit AES-nøgle, der bliver arkiveret i enhedens nøglering. Nøglen kan kryptere og godkende Bluetooth Low Energy-annonceringerne om enhedens aktuelle aktivitet over for andre parrede iCloud-enheder ved hjælp af AES-256 GCM med beskyttelsesforanstaltninger mod genafspilning.

Første gang en enhed modtager en annoncering fra en ny nøgle, etablerer den en Bluetooth Low Energy-forbindelse til ophavsenheden og udveksler krypteringsnøgler til annonceringer. Forbindelsen sikres med Bluetooth Low Energy 4.2-standardkryptering samt kryptering af de enkelte beskeder, som ligner den måde, iMessage-beskeder krypteres på. I nogle situationer går disse beskeder via APNs i stedet for Bluetooth Low Energy. Aktivitetsdataene beskyttes og overføres på samme måde som en iMessage-besked.

Handoff mellem lokale apps og websteder

Handoff giver en lokal app i iOS mulighed for at genoptage websider i domæner, der styres af appudvikleren 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 forhindre, at lokale apps prøver at genoptage websteder, som ikke styres af udviklerne. Styring af et webdomæne etableres via mekanismen til fælles webgodkendelsesoplysninger. Der er flere oplysninger under "App-adgang til arkiverede adgangskoder" i afsnittet Administration af brugeradgangskode i dette dokument. 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 afkryptere annonceringsbytene (som beskrevet tidligere i dette afsnit).

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 (i lighed med AirDrop). Appen Mail bruger f.eks. disse API'er til at overdrage et e-mailudkast, måske med store bilag, via Handoff.

Når en app bruger denne facilitet, starter udvekslingen mellem de to enheder ligesom ved Handoff (se de foregående afsnit). Efter at have modtaget de første data via Bluetooth Low Energy starter modtagerenheden imidlertid en ny forbindelse via Wi-Fi. Forbindelsen krypteres (TLS), hvorved deres iCloud-identitetscertifikater udveksles. 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 appudvikleren 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, der afvikles på brugerens andre enheder (som bruger samme iCloud-konto).

Lås automatisk op

Mac-systemer, der understøtter Lås automatisk op, bruger Bluetooth Low Energy og Peer-to-Peer Wi-Fi til at give brugerens Apple Watch tilladelse til at låse brugerens Mac op på en sikker måde. Alle Mac-computere og Apple Watch-enheder med funktionen og en iCloud-konto skal bruge tofaktorgodkendelse.

Når oplåsning af en Mac slås til på et Apple Watch, oprettes et sikkert link ved hjælp af identiteterne til automatisk oplåsning. Mac opretter en tilfældig hemmelig engangsnøgle til oplåsning og sender den til Apple Watch via linket. Nøglen opbevares på Apple Watch og er kun tilgængelig, når Apple Watch er låst op (se "Databeskyttelsesklasser" i afsnittet Databeskyttelse). Den nye hemmelige nøgle kan ikke være brugerens adgangskode.

Under oplåsning bruger Mac Bluetooth Low Energy til at oprette forbindelse til Apple Watch. Der oprettes derefter et sikkert link mellem de to enheder ved hjælp af de fælles nøgler, der blev brugt, første gang det blev slået til. Mac og Apple bruger så Peer-to-Peer Wi-Fi og en sikker nøgle, der er afledt af det sikre link, til at bestemme afstanden mellem de to enheder. Hvis enhederne er inden for hinandens rækkevidde, bruges det sikre link til at overføre den allerede fastlagte fælles nøgle, der låser Mac op. Når Mac er låst op, erstatter Mac den nuværende nøgle til oplåsning med en ny nøgle til oplåsning, der kan bruges en gang, og sender den nye nøgle til Apple Watch via linket.

Opkald via iPhones mobilforbindelse

Når en brugers Mac, iPad eller iPod touch er på samme Wi-Fi-netværk som brugerens iPhone, kan enheden foretage og modtage telefonopkald via iPhones mobilforbindelse. 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 **meddelelser fra APNs (Apple Push Notification service)**. Meddelelserne bruger samme kryptering hele vejen fra afsender til modtager som iMessage. På skærmen på enheder på samme netværk vises en meddelelse om det indgående opkald. Når opkaldet besvares, 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. Annonceringsbyte krypteres med samme metode som Handoff-annonceringer.

Udgående opkald viderestilles ligeledes til iPhone via tjenesten Apple Push Notification, 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.

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.

Efter at enhederne er blevet forbundet, krypterer iPhone indgående sms'er og videresender dem til hver enhed ved hjælp af de metoder, der er beskrevet under iMessage i dette afsnit af dette dokument. 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

iOS-enheder, der understøtter Instant Hotspot, bruger Bluetooth Low Energy til at finde og kommunikere med enheder, der er logget ind på samme iCloud-konto. Kompatible Mac-computere med OS X Yosemite eller nyere versioner bruger samme teknologi til at finde og kommunikere med iOS-enheder med Instant Hotspot.

Når en bruger skifter til Wi-Fi-indstillinger på iOS-enheden, udsender enheden en Bluetooth Low Energy-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 det udskiftes regelmæssigt. Når andre enheder, der er logget ind på samme iCloud-konto, er i nærheden og understøtter Personlig internetdeling, registrerer de signalet og svarer med angivelse af deres tilgængelighed.

Når en bruger vælger en enhed, der kan bruges til Personlig internetdeling, sendes en anmodning om aktivering af Personlig internetdeling til enheden. Anmodningen sendes via en forbindelse, der er krypteret med Bluetooth Low Energy-standardkryptering, og anmodningen krypteres på stort set samme måde som iMessage-beskeder. Enheden sender et svar med oplysninger om delingen af internetforbindelsen via samme Bluetooth Low Energy-forbindelse og samme beskedkryptering.

AirDrop-sikkerhed

iOS-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 Mac-computere med AirDrop og 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 Wi-Fi-adgangspunkt.

Når en bruger logger ind på iCloud-tjenesten, arkiveres en 2048 bit RSA-identitet på enheden. Når brugeren slår AirDrop til, oprettes der desuden 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 Bluetooth Low Energy, der indeholder brugerens korte hash-værdi til AirDrop-identiteten. Andre enheder, der er i umiddelbar nærhed, 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 opdage identiteten på eventuelle besvarende enheder.

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. 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. Afsenderenheden starter derefter en AirDrop-forbindelse ved hjælp af Peer-to-Peer Wi-Fi, og afsenderenheden sender gennem denne forbindelse en lang hash-værdi for identiteten til modtagerenheden. Hvis den lange hash-værdi for identiteten stemmer overens med en hash-værdi for en kendt person i modtagerens Kontakter, svarer modtageren med sine lange hash-værdier for identiteten. Derefter vises modtagerens fornavn og fotografi (hvis emnerne findes i Kontakter) i afsenderens AirDrop-deleark.

Når der bruges AirDrop, vælger afsenderne, hvem de vil dele med. Afsenderenheden åbner en krypteret forbindelse (TLS) til modtager-enheden, og enhederne udveksler certifikater for deres iCloud-id'er. Identiteten i certifikaterne kontrolleres i appen Kontakter hos hver bruger. Derefter bliver modtagerbrugeren bedt om at acceptere den indgående overførsel fra den identificerede person eller enhed. Hvis der er valgt flere modtagere, gentages processen for hver modtager.

I indstillingen Alle bruges samme proces, men hvis der ikke findes et match i Kontakter, vises modtagerenhederne i AirDrops deleark med en silhuet med enhedens navn, der er defineret i Indstillinger > Generelt > Om > Navn.

Organisationer kan begrænse brug af AirDrop sammen med enheder eller apps, der administreres af en MDM-løsning.

Deling af Wi-Fi-adgangskode

iOS-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, der anmoder om Wi-Fi-adgangskoden. Andre enheder, der er i umiddelbar nærhed, ikke er på vågeblus og har adgangskoden til det valgte Wi-Fi-netværk, opretter forbindelse via Bluetooth Low Energy 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 PSK-værdien på 64 tegn, som også kan bruges til at oprette forbindelse til netværket, til anmoderen.

Organisationer kan begrænse deling af adgangskoder for enheder eller apps, der administreres af en MDM-løsning.

Apple Pay

Med Apple Pay kan brugere benytte understøttede iOS-enheder, Apple Watch og Mac 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 til 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 ikke nogen transaktionsoplysninger, der kan spores tilbage til brugeren. Betalingstransaktionerne foregår mellem brugeren, butikken og kortudstederen.

Komponenter i Apple Pay

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.

NFC-kontrolenhed: NFC-kontrolenheden håndterer NFC-protokoller (Near Field Communication) og dirigerer kommunikationen mellem programprocessoren og det sikre element og mellem det sikre element og betalingsterminalen.

Wallet: 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 Wallet. Brugerne kan også føje kort til Apple Pay i:

- Indstillingsassistent og Indstillinger i iOS
- Appen Watch til Apple Watch
- Wallet & Apple Pay i Systemindstillinger til Mac.

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

Secure Enclave: Secure Enclave på iPhone, iPad og Apple Watch 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 det sikre element eller den sikre enklave, hvis den er tilgængelig, uden at passere gennem programprocessoren.

Apple Pay-servere: Apple Pay-servere administrerer indstilling og tilknytning af kredit-, debet-, rejse- og studiekort i Wallet og de kontonumre for enheden, der opbevares i det sikre element. De kommunikerer både med enheden og betalingsnetværkets eller kortudstederens servere. Apple Pay-serverne har også ansvaret for at omkryptere godkendelsesoplysninger til betalinger fra apps.

Brug af Secure Element i Apple Pay

Secure Element (det sikre element) indeholder et miniprogram, der er specifikt designet til at administrere Apple Pay. Det inkluderer også miniprogrammer, der er certificeret af betalingsnetværk eller kortudstedere. Data til kreditkort, debetkort og forudbetalte kort, der sendes fra betalingsnetværket eller kortudstederen til disse miniprogrammer, er krypteret ved hjælp af nøgler, der kun kendes af betalingsnetværket eller kortudstederen og miniprogrammernes sikkerhedsdomæne. Dataene arkiveres i disse miniprogrammer og beskyttes af sikkerhedsfunktionerne i det sikre element. Under en transaktion kommunikerer terminalen direkte med det sikre element via NFC-kontrolenheden (Near Field Communication) gennem en dedikeret hardwarebus.

Brug af NFC-kontrolenheden i Apple Pay

Som indgangsport til det sikre element sikrer NFC-kontrolenheden, at alle kontaktfri 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 kontaktfri transaktioner.

Når en betaling med kredit-, debet- eller forudbetalt kort (inklusive butikskort) er godkendt af kortindehaveren vha. Touch ID, Face ID eller adgangskode eller via to tryk på sideknappen på et oplåst Apple Watch, sendes de kontaktfri svar, som betalingsminiprogrammerne i det sikre element har udarbejdet, udelukkende til NFC-feltet af kontrolenheden. Detaljer om godkendte betalinger i kontaktfri betalingstransaktioner holdes således inden for det lokale NFC-felt og kan aldrig ses af programprocessoren. Derimod sendes detaljer om godkendte betalinger, der er foretaget fra en app eller internettet, til programprocessoren, men først efter de er blevet krypteret af det sikre element og overført til Apple Pay-serveren.

Anvendelse af kreditkort, debetkort og forudbetalte kort

Når en bruger føjer et kreditkort, et debetkort eller et forudbetalt kort (herunder butikskort) til 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 den kan godkende, at kortet føjes til Wallet.

Apple Pay bruger tre kald på serversiden til at sende og modtage kommunikation til/fra kortudstederen eller netværket under tilknytningen af kort: *Påkrævede felter*, *Kontroller kort* og *Forbind og tilknyt*. Kortudstederen eller netværket bruger kaldene til at bekræfte og godkende kort og føje kort til Wallet. Disse klient-serversessioner krypteres ved hjælp af TLS v1.2.

De fuldstændige kortnumre opbevares ikke på enhederne eller Apple-serverne. I stedet oprettes et entydigt kontonummer for enheden, der krypteres og derefter arkiveres i det sikre element. Det entydige kontonummer for enheden er krypteret på en måde, så Apple ikke kan få adgang til det. Dette kontonummer for enheden er entydigt og forskelligt fra almindelige kredit- eller debetkortnumre. Kortudstederen eller betalingsnetværket kan forhindre brugen af det på kort med magnetstribe, telefonisk eller på websteder. Enhedens kontonummer i det sikre element er isoleret fra iOS og watchOS, det opbevares aldrig på Apple-servere, og det sikkerhedskopieres aldrig til iCloud.

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 det sikre element på Apple Watch.

Når der tilføjes kredit-, debet- eller forudbetalte kort (inklusive butikskort), vises de på en liste med kort under 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 syv dage. Denne funktion kræver tofaktorgodkendelse for at blive slået til i den pågældende iCloud-konto.

Manuel tilføjelse af et kredit- eller debetkort til Apple Pay

Når et kort tilføjes manuelt, bruges navnet, kortnummeret, udløbsdatoen og sikkerhedskoden til tilknytningsprocessen. Via Indstillinger, Wallet-appen eller Apple Watch-appen kan brugere 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. Fotografiet arkiveres aldrig på enheden og opbevares ikke i fotobiblioteket. Når alle felterne er udfyldt, kontrollerer processen Kontroller kort alle felterne bortset fra sikkerhedskoden. Oplysningerne krypteres 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. I processen Forbind og tilknyt indgår også, at Apple deler oplysninger fra enheden med kortudstederen eller netværket, f.eks. oplysninger om dine aktiviteter i iTunes og App Store (eksempelvis om du har foretaget køb i iTunes igennem længere tid), oplysninger om din enhed (f.eks. enhedens telefonnummer, navn og model samt en evt. tilhørende iOS-enhed, der kræves til indstilling af Apple Pay) samt din omtrentlige lokalitet på det tidspunkt, du tilføjer kortet (hvis Lokalitetstjenester er slået til). Ud fra oplysningerne afgør kortudstederen, om kortet kan føjes til Apple Pay.

Der sker to ting som følge af processen Forbind og tilknyt:

- Enheden begynder at hente det arkiv med kortet til Wallet, der repræsenterer kredit- eller debetkortet.
- Enheden begynder at binde kortet til det sikre element.

Kortarkivet indeholder URL-adresser til hentning 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 det sikre 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 til Apple Pay

For et kredit- eller debetkort, der er registreret i iTunes, kræves det måske, at brugeren indtaster 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 appen registreres til brug sammen med Apple Pay, oprettes nøgler til appen og kortudstederens server. Disse nøgler bruges til at kryptere de kortoplysninger, der sendes til kortudstederen. Dette forhindrer, at oplysningerne bliver læst af iOS-enheden. Tilknytningsflowet svarer til det, som er beskrevet tidligere for kort, der tilføjes manuelt, bortset fra at der bruges engangsadgangskoder i stedet for sikkerhedskoden.

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 Wallet, Indstillinger eller Apple Watch-appen. I tilfælde af brug af kundeservice eller godkendelse via en app benytter udstederen sin egen kommunikationsproces.

Betalingsgodkendelse

På enheder med en sikker enklave tillader det sikre element først, at der foretages betaling, når det har modtaget en godkendelse fra den sikre enklave. På iPhone og iPad indebærer det en bekræftelse af, at brugeren har legitimeret sig med Touch ID, Face ID eller adgangskoden til enheden. Hvis Touch ID eller Face ID er tilgængelig, er det standardmetoden, men adgangskoden 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 adgangskoden. Efter fem forgæves forsøg kræves, at adgangskoden indtastes. Der skal også bruges en adgangskode, hvis Touch ID eller Face ID ikke er konfigureret eller ikke er indstillet til Apple Pay. På Apple Watch skal enheden låses op med adgangskoden, eller der skal trykkes to gange på sideknappen, før en betaling gennemføres.

Kommunikationen mellem den sikre enklave og det sikre element foregår via en seriel grænseflade, hvor det sikre element er forbundet med NFC-kontrolenheden, som på sin side er forbundet med programprocessoren. Selvom den sikre enklave og det sikre element ikke er forbundet direkte, kan de kommunikere sikkert ved at bruge en fælles 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 den sikre enklave ud fra UID-nøglen og det sikre elements entydige id. På fabrikken overføres pardannelsesnøglen sikkert fra Secure Enclave til et **hardwaresikkerhedsmodul (HSM)**, som har det nødvendige nøglemateriale for derefter at skyde pardannelsesnøglen ind i det sikre element.

Når brugeren godkender en transaktion, sender den sikre enklave signerede data om transaktionens type (kontaktfri eller fra en app) til det sikre element sammen med en tilfældig godkendelsesværdi (AR - Authorization Random). AR-værdien genereres i den sikre enklave, første gang en bruger tilknytter et kreditkort. Den bevares, så længe Apple Pay er aktiveret og beskyttes af den sikre enklaves kryptering og forsvarsmekanisme mod rollback-angreb. Den overføres på en sikker måde til det sikre element gennem pardannelsesnøglen. Når det sikre element modtager en ny AR-værdi, markerer elementet tidligere tilføjede kort som slettet.

De kreditkort, debetkort og forudbetalte kort, der er føjet til det sikre element, kan kun bruges, hvis det sikre element modtager en godkendelse med samme pardannelsesnøgle og AR-værdi, som blev brugt, da kortet blev tilføjet. iOS kan derfor give den sikre enklave besked på at gøre kort ubrugelige, ved at enklavens kopi af AR-værdien markeres som ugyldig i følgende situationer:

- Adgangskoden slås fra.
- Brugeren logger ud af iCloud.
- Brugeren vælger Slet alt indhold og alle indstillinger.
- Enheden gendannes med gendannelsesfunktionen.

Med Apple Watch markeres kort som ugyldige i følgende situationer:

- Urets adgangskode slås fra.
- Pardannelsen mellem uret og iPhone ophæves.

Før det sikre element slår betalingsminiprogrammet til for en kontaktfri betaling, kontrollerer det ved hjælp af pardannelsesnøglen og sin kopi af den aktuelle AR-værdi den godkendelse, der er modtaget fra den sikre enklave. Samme proces bruges, når der hentes krypterede betalingsdata fra et betalingsminiprogram i forbindelse med transaktioner fra apps.

Transaktionsspecifik dynamisk sikkerhedskode

Betalingstransaktioner fra betalingsminiprogrammerne indeholder et betalingskryptogram sammen med kontonummeret for en enhed. Dette kryptogram – en engangskode – beregnes ved hjælp af en transaktionstæller, der øges med 1 for hver ny transaktion, og en nøgle, der dannes i betalingsminiprogrammet under individualiseringen og kendes af betalingsnetværket og/eller kortudstederen. Afhængigt af betalingsmåden kan der også indgå andre data i beregningen, f.eks.:

- Et Terminal Unpredicable Number i forbindelse med en NFC-transaktion
- En Apple Pay-server nonce-værdi i tilfælde af transaktioner fra apps

Disse sikkerhedskoder videregives til betalingsnetværket og kortudstederen, så de kan godkende de enkelte transaktioner. Sikkerhedskodernes længde kan variere afhængigt af den type transaktion, der udføres.

Betaling med kredit- og debetkort i butikker

Hvis iPhone 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 appen Wallet og vælge et kort eller gøre et af følgende, hvis enheden er låst:

- Dobbeltklik på knappen Hjem på enheder med Touch ID.
- Dobbeltklik på sideknappen på enheder med Face ID.

Næste skridt er, at brugeren godkendes ved hjælp af Touch ID, Face ID eller adgangskode, før der sendes betalingsoplysninger. 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 tid og lokalitet, som kan hjælpe med at forbedre Apple Pay og andre produkter og tjenester fra Apple.

Betaling med kredit- og debetkort i apps

Apple Pay kan også bruges til at foretage betalinger fra iOS-apps og Apple Watch-apps. Når brugerne betaler fra apps med Apple Pay, modtager Apple krypterede transaktionsoplysninger og omkrypterer dem med en særlig udviklernøgle, før oplysningerne sendes til udvikleren eller butikken. Apple Pay arkiverer 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 omkrypterer Apple Pay-serverne den med en særlig nøgle til butikken, før transaktionen 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. faktureringsadresse, leveringsadresse og kontaktoplysninger. Appen anmoder derefter iOS om at vise Apple Pay-arket, der anmoder om oplysninger til appen og andre nødvendige oplysninger såsom hvilket kort, der skal bruges.

På dette tidspunkt modtager appen oplysninger om by, postnummer og eventuelt delstat, så den kan beregne de endelige leveringsomkostninger. Alle de oplysninger, appen har anmodet om, videregives først til appen, når brugeren har godkendt betalingen med Touch ID, Face ID eller adgangskoden til enheden. Når betalingen er godkendt, overføres de oplysninger, der vises i Apple Pay-arket, til butikken.

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 det sikre element for at få genereret godkendelsesoplysninger til betalingen, som vil blive krypteret med en Apple-nøgle. De krypterede godkendelsesoplysninger til betalingen overføres fra det sikre element til Apple Pay-serverne, som afkrypterer godkendelsesoplysningerne, kontrollerer nonce-værdien i godkendelsesoplysningerne i forhold til den nonce-værdi, som Apple Pay-serverne oprindeligt sendte, og omkrypterer godkendelsesoplysningerne med den nøgle, som er knyttet til butikkens id. De returneres derefter til enheden, som sender dem tilbage til appen via API'et. Appen sender dem derefter til behandling i butikkens system. Butikken kan nu afkryptere 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 til signering i det sikre element, f.eks. et ordrenummer eller et kunde-id, der sikrer, at transaktionen ikke kan omdirigeres til en anden kunde. Det gøres af appudvikleren, som kan angive programdata (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 for programdata (applicationData) matcher værdien i betalingsdataene.

Betaling med kredit- og debetkort på nettet

Apple Pay kan også bruges til at foretage betalinger på websteder med iOS-enheder, Apple Watch og Mac. 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. Apple-serverne udfører bekræftelse af domænenavne og udsteder 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 brugeren ikke ønsker at dele disse oplysninger, kan de slå forespørgsler vedrørende Apple Pay fra i Safaris anonymitetsindstillinger i iOS og macOS.

Når en butikssession er bekræftet, er alle foranstaltninger med hensyn til sikkerhed og anonymitet de samme, som når brugeren betaler fra en app.

Hvis der bruges Handoff fra Mac til iPhone eller Apple Watch, bruger Apple Pay IDS, der er krypteret fra start til slut, til at sende oplysninger om betalingen mellem brugerens Mac og den enhed, der skal stå for godkendelsen. IDS anvender brugerens nøgler til enheden til at foretage kryptering, så ingen andre enheder kan afkryptere oplysningerne. Nøglerne

er heller ikke tilgængelige for Apple. Søgning efter enheder i forbindelse med Handoff og Apple Pay indeholder brugerens kreditkorts type 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 seneste anvendte kontakt-, leverings- og faktureringsadresser via iCloud-nøglering med en sikker metode.

Når brugeren har godkendt betaling med Touch ID, Face ID, adgangskode 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.

Kontaktfrie kort

Wallet understøtter VAS-protokollen (Value-Added Service), der kan sende data fra understøttede kort til kompatible NFC-terminaler. VAS-protokollen kan implementeres på kontaktløse terminaler og benytter NFC til at kommunikere med understøttede Apple-enheder. VAS-protokollen kan benyttes over kort afstand og kan bruges til at vise kontaktfrie 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 butikkens id, bliver brugeren bedt om at godkende, at det bruges, ved hjælp af Touch ID, Face ID eller en adgangskode. Kortoplysningerne, et tidsstempel og en tilfældig ECDH P-256-nøgle til engangsbrug bruges sammen med butikkens offentlige nøgle til at udlede en krypteringsnøgle til kortdataene, som sendes til terminalen.

Brugerne kan også vælge et kort manuelt og godkende det ved hjælp af Touch ID, Face ID eller en adgangskode, før det vises til butikkens NFC-terminal.

Apple Pay Cash

I iOS 11.2 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 Pay Cash-konto, som brugeren har adgang til i Wallet eller i Indstillinger > Wallet & Apple Pay på alle de enheder, hvor Apple Pay Cash er slået til, og hvor brugeren er logget ind med sit Apple-id.

Brugere, der vil benytte betalinger til og fra andre personer og Apple Pay Cash, skal være logget ind på deres iCloud-konto på en enhed, der er kompatibel med Apple Pay Cash, og tofaktorgodkendelse skal være indstillet på iCloud-kontoen.

Når du indstiller Apple Pay Cash, kan de samme oplysninger, som når du 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 din 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.

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 Pay Cash-saldoen bruges altid først. Er der brug for flere midler, opkræves de fra et andet kredit- eller debetkort, som brugeren har føjet til Wallet.

Apple Pay Cash-kortet i Wallet kan bruges med Apple Pay til at betale i butikker, i apps og på internettet. Penge på Apple Pay Cash-kontoen kan også overføres til en bankkonto. Penge, der modtages fra en anden bruger, indsættes på Apple Pay Cash-kontoen, og brugeren kan også selv indsætte penge fra et debetkort eller et forudbetalt kort i Wallet.

Når en transaktion er gennemført, opbevarer Apple Payments Inc. dine transaktionsdata og kan bruge dem med henblik på fejlfinding, forebyggelse af bedrageri og opfyldelse af lovgivningsmæssige krav. Resten af Apple ved ikke, hvem du har sendt penge til eller modtaget penge fra, eller hvor du har foretaget et køb med dit Apple Pay Cash-kort.

Når du sender penge med Apple Pay, sætter penge ind på en Apple Pay 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 det sikre element for at få genereret en betalingssignatur. Betalingssignaturen afleveres af det sikre element og sendes videre til Apple Pay-serverne. Apple Pay-serverne kontrollerer transaktionens ægthed, integritet og korrekthed via betalingssignaturen og nonce-værdien. Pengeoverførslen startes derefter, og du får besked om, at transaktionen er gennemført.

Hvis transaktionen involverer et kredit- eller debetkort for at føje penge til Apple Pay Cash, sende penge til en anden bruger eller tilføje flere penge, hvis Apple Pay Cash-saldoen ikke rækker, dannes der også krypterede godkendelsesoplysninger, som sendes til Apple Pay-servere, hvilket ligner den proces, der bruges til Apple Pay i apps og på websteder.

Hvis saldoen på Apple Pay 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 Apples partner og krypteres med partnerens nøgle. Apple kan ikke afkryptere disse data.

Rejsekort

I Kina og Japan kan brugere føje understøttede rejsekort til Wallet på understøttede modeller af iPhone og Apple Watch. De kan enten gøre det ved at overføre værdien og rejsekortet fra et fysisk kort til kortets digitale repræsentation i Wallet eller ved at tilknytte et nyt rejsekort i Wallet fra rejsekortudstederens app. Når rejsekort er blevet føjet til Wallet, kan brugerne bruge offentlige transportmidler ved at holde iPhone eller Apple Watch mod kortlæserne. I Japan kan Suica-kortet også bruges til at foretage betalinger.

Tilføjede rejsekort knyttes til en brugers iCloud-konto. Hvis en bruger føjer mere end et kort til Wallet, kan Apple eller udstederen af rejsekortet måske koble brugerens personlige oplysninger og de tilhørende kontooplysninger til flere kort. MySuica-kort kan f.eks. kobles til anonyme Suica-kort. Rejsekort og transaktioner beskyttes med et sæt hierarkiske kryptografiske nøgler.

Når saldoen på et fysisk kort skal overføres til Wallet, skal brugerne indtaste identificerende cifre fra kortets serienummer. Brugerne skal muligvis angive personlige oplysninger som bevis på, at kortet er i deres besiddelse. Hvis kortet er et MySuica-kort eller et Suica-kort, der indeholder et rejsekort, skal brugerne også indtaste deres fødselsdato. Når der overføres kort fra iPhone til Apple Watch, skal begge enheder have forbindelse til internettet under overførslen.

Brugerne kan forøge saldoen ved at tanke op fra kreditkort eller forudbetalte kort via Wallet eller rejsekortudstederens app. Sikkerheden i forbindelse med optankning ved hjælp af Apple Pay er beskrevet i afsnittet "Betaling med kredit- og debetkort i apps" i dette dokument.

Tilknytning af rejsekortet fra rejsekortudstederens app er beskrevet i afsnittet "Tilføjelse af kredit- eller debetkort fra en kortudsteders app" i dette dokument.

Udstederen af rejsekortet har de kryptografiske nøgler, der kræves for at blive godkendt over for det fysiske kort og bekræfte brugerens indtastede data. Efter bekræftelsen kan systemet oprette et kontonummer for enheden til det sikre element og gøre det netop tilføjede kort aktivt i Wallet med den overførte saldo. I Japan bliver det fysiske Suica-kort inaktivt, når tilknytningen fra det fysiske kort er gennemført.

Efter tilknytningen, uanset typen, krypteres saldoen på rejsekortet og opbevares af et specifikt miniprogram i det sikre element. Den offentlige transportoperatør har de nøgler, der skal bruges til at udføre kryptografiske funktioner på kortets data i forbindelse med saldotransaktioner.

Brugerne har som standard mulighed for ekspresbetaling uden brug af Touch ID, Face ID eller en adgangskode, når de benytter offentlig transport. Oplysninger som senest besøgte stationer, transaktionshistorik og ekstra billetter kan hentes af alle kontaktfri kortlæsere i nærheden, når Ekspresfunktion er slået til. Brugerne kan slå krav om godkendelse med Touch ID, Face ID eller adgangskode til ved at slå Ekspresrejse fra i Wallet & Apple Pay.

I lighed med andre Apple Pay-kort kan brugerne suspendere eller fjerne rejsekort på følgende måder:

- Slet enheden eksternt med Find min iPhone
- Slå Mistet til i Find min iPhone
- Udløs kommando til ekstern sletning fra MDM (Mobile Device Management)
- Fjern alle kort fra kontosiden til deres Apple-id
- Fjern alle kort fra iCloud.com
- Fjern kortet fra Wallet
- Fjern kortet i udstederens app

Apple Pay-servere giver den offentlige transportoperatør besked på at suspendere eller slå de pågældende kort fra. Hvis brugernes enheder er offline, når de prøver at slette deres Suica-kort, kan kortene muligvis stadig bruges på visse terminaler indtil kl. 12:01 JST den følgende dag. Hvis brugernes enhed er offline, kan rejsekort i Kina stadig bruges.

Hvis brugere fjerner deres rejsekort, kan saldoen overføres ved at tilføje kortene igen på en enhed, der er logget ind med samme Apple-id.

Studiekort

I iOS 12 kan studerende, lærerstaben og personale hos deltagende uddannelsesinstitutioner føje deres id-kort til Wallet for at få adgang til lokaliteter og foretage betalinger, hvor kortet accepteres.

En bruger føjer sit id-kort til Wallet via en app, som kortudstederen eller den deltagende skole angiver. Den tekniske proces for dette er den samme som beskrevet tidligere i afsnittet "Tilføjelse af kredit- eller debetkort fra en kortudsteders app". Derudover skal apps fra udstedere understøtte tofaktorgodkendelse for de konti, der beskytter adgang til deres id'er. Et kort kan indstilles samtidig på op til to understøttede Apple-enheder, der er logget ind med det samme Apple-id.

Når der føjes et studiekort til Wallet, slås Ekspresfunktion til som standard. Studiekort med Ekspresfunktion slået til interagerer med terminaler, der accepterer dette, uden behov for godkendelse med Touch ID, Face ID eller en adgangskode. Brugeren kan trykke på knappen Mere på forsiden af studiekortet i Wallet og slå Ekspresfunktion fra. Touch ID, Face ID eller en adgangskode kræves for at slå Ekspresfunktion til igen.

Studiekort kan slås fra eller fjernes ved at gøre et af følgende:

- Slet enheden eksternt med Find min iPhone
- Slå Mistet til i Find min iPhone
- Udløs kommando til ekstern sletning fra MDM (Mobile Device Management)
- Fjern alle kort fra kontosiden til deres Apple-id
- Fjern alle kort fra iCloud.com
- Fjern kortet fra Wallet
- Fjern kortet i udstederens app

Suspendering, fjernelse og sletning af kort

Brugerne kan suspendere Apple Pay på iPhone, iPad og Apple Watch ved at bruge funktionen Mistet i Find min iPhone til deres enhed. Brugerne kan også fjerne og slette deres kort fra Apple Pay ved hjælp af Find min iPhone, iCloud.com eller direkte på deres enheder med 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 suspenderet 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 suspenderet eller fjernet fra Apple Pay.

Hvis en bruger sletter hele enheden ved at bruge Slet alt indhold og alle indstillinger eller Find min iPhone eller ved at gendanne deres enhed med gendannelsesfunktionen, får det sikre element af iOS besked på at markere alle kort som slettet. Det bevirker, at alle kort straks markeres som ubrugelige, indtil Apple Pay-serverne kan kontaktes for at få slettet kortene fuldstændigt fra det sikre 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 sikre, at alle kort i det sikre element er slettet.

Internettjenester

Oprettelse af stærke adgangskoder til Apple-id
Apple-id'er bruges til at oprette forbindelse til en række tjenester, herunder iCloud, FaceTime og iMessage. For at hjælpe brugerne med at oprette stærke adgangskoder er det et krav, at adgangskoder til alle nye konti skal have følgende egenskaber:

- Mindst otte tegn
- Mindst et bogstav
- Mindst et stort bogstav
- Mindst et tal
- Højst tre ens tegn efter hinanden
- Ikke magen til kontonavnet

Apple har udviklet et sæt effektive tjenester, der giver brugerne mulighed for at få endnu mere anvendelighed og produktivitet ud af deres enheder, herunder iMessage, FaceTime, Siri-forslag, iCloud, iCloud-sikkerhedskopi og iCloud-nøglering.

Disse internettjenester er udviklet med de samme sikkerhedsmål for øje som på hele iOS-platformen. Målene omfatter bl.a. sikker håndtering af data, uanset om de findes på enheden eller overføres via trådløse netværk, beskyttelse af brugernes personlige oplysninger og trusselsbeskyttelse mod ondsindet eller uautoriseret adgang til oplysninger og tjenester. Hver tjeneste bruger sin egen effektive sikkerhedsarkitektur uden at forringe den samlede brugervenlighed i iOS.

Apple-id

Et Apple-id er den konto, som bruges til at logge ind på Apple-tjenester som iCloud, iMessage, FaceTime, iTunes Store, Apple Books, App Store m.m. Det er vigtigt, at brugerne beskytter deres Apple-id for at forhindre uautoriseret adgang til deres konti. Et led i beskyttelsen er Apples krav om stærke adgangskoder, der ikke må være for almindelige, skal indeholde mindst otte tegn, både bogstaver og tal, og ikke må indeholde tre ens tegn efter hinanden. Det er en god ide, hvis brugerne gør deres adgangskode endnu stærkere ved at bruge symboler og flere tegn. Apple kræver også, at brugerne indstiller tre sikkerhedsspørgsmål, der kan være med til at bekræfte ejerens identitet, når ejeren foretager ændringer af sine kontooplysninger eller nulstiller en glemt adgangskode.

Apple sender e-mails og push-beskeder til brugerne, hvis der er sket noget vigtigt i forbindelse med deres konto, f.eks. hvis adgangskoden eller faktureringsoplysningerne er ændret, eller hvis Apple-id'et 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 kundens sikkerhed.

Tofaktorgodkendelse

Apple tilbyder *tofaktorgodkendelse*. Det 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 fås adgang til en brugers konto fra godkendte enheder som brugerens iPhone, iPad eller Mac. Når der logges ind første gang 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, macOS, tvOS, watchOS og de godkendelsessystemer, som bruges af Apples websteder.

Der er flere oplysninger om tofaktorgodkendelse her:
https://support.apple.com/HT204915

Bekræftelse i to trin

Apple har siden 2013 også haft en lignende sikkerhedsmetode, der kaldes *bekræftelse i to trin*. Når bekræftelse i to trin er slået til, skal brugerens identitet bekræftes via en midlertidig kode, der sendes til en af brugerens godkendte enheder, før der kan foretages ændringer af brugerens oplysninger under Apple-id-kontoen, før der kan logges ind på iCloud, iMessage, FaceTime eller Game Center, og før der kan foretages køb i iTunes Store, Apple Books eller App Store fra en ny enhed. Brugerne får også tildelt en gendannelsesnøgle på 14 tegn, der skal opbevares et sikkert sted og bruges, hvis de glemmer deres adgangskode eller mister adgangen til deres godkendte enheder. De fleste nye brugere opfordres til at bruge tofaktorgodkendelse, men der er stadig visse situationer, hvor bekræftelse i to trin anbefales i stedet.

Du kan få flere oplysninger om bekræftelse i to trin til Apple-id her:
https://support.apple.com/HT204152

Administrerede Apple-id'er

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

Nogle Apple-tjenester er slået fra for administrerede Apple-id'er, f.eks. Apple Pay, iCloud-nøglering, HomeKit og Find min iPhone.

Du kan få flere oplysninger om administrerede Apple-id'er her:
https://help.apple.com/schoolmanager/#/tes78b477c81

Revision af administrerede Apple-id'er

Administrerede Apple-id'er understøtter desuden revision, så institutioner kan overholde juridiske bestemmelser og bestemmelser vedrørende anonymitet. Administrator-, bestyrer- og lærerkonti kan tildeles revisionsrettigheder til bestemte administrerede Apple-id'er. Brugere med revisionstilladelser kan kun overvåge konti, der rangerer lavere end deres egen i skolens hierarki. Det vil sige, at lærere kan overvåge studerende, bestyrere kan foretage revision for lærere og studerende, mens administratorer kan foretage revision for bestyrere, lærere og studerende.

Når der anmodes om tilladelse til revision i Apple School Manager, oprettes en særlig konto, som kun har adgang til det administrerede Apple-id, der blev anmodet om revision af. Revisionstilladelsen udløber efter syv dage. I denne periode kan brugeren med revisionstilladelser læse og ændre brugerens indhold, som er arkiveret i apps, der kan arbejde med iCloud eller CloudKit. Alle anmodninger om revisionsadgang logges i Apple School Manager. Logarkiverne viser navnet på brugeren med revisionstilladelser,

det administrerede Apple-id, som brugeren med revisionstilladelser har anmodet om adgang til, tidspunktet for anmodningen og en oplysning om, hvorvidt revisionen blev foretaget.

Du kan få flere oplysninger om revision af administrerede Apple-id'er her: https://help.apple.com/schoolmanager/#/tesd8fcbdd99

Administrerede Apple-id'er og personlige enheder

Administrerede Apple-id'er kan også bruges til personligt ejede iOS-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 et administreret Apple-id bruges 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.

iMessage

Apple iMessage er en beskedtjeneste til iOS-enheder, Apple Watch og Mac-computere. iMessage understøtter tekst og bilag, f.eks. fotografier, kontakter og lokaliteter. 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 arkiverer ikke indholdet af beskeder eller bilag i en log, og indholdet beskyttes af kryptering fra start til slut, så kun afsenderen og modtageren har adgang til dem. Apple kan ikke afkryptere dataene.

Når en bruger slår iMessage til på en enhed, danner enheden to sæt nøgler til brug sammen med tjenesten: en RSA 1280 bit nøgle til kryptering og en ECDSA 256 bit nøgle på NIST P-256-kurven til signering. De private nøgler til begge nøglesæt arkiveres i enhedens nøglering, og de offentlige nøgler sendes sammen med enhedens APNs-adresse til IDS, hvor de knyttes til brugerens telefonnummer.

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.

I iOS 12 og nyere versioner bliver beskeder, der er sendt fra forskellige adresser, som er forbundet til det samme Apple-id, vist i en enkelt samtale på de enheder, der modtager dem. Det sker vha. et konto-id, der hentes fra IDS, sammen med de offentlige nøgler og APNs-adresser for en e-mailadresse eller et telefonnummer.

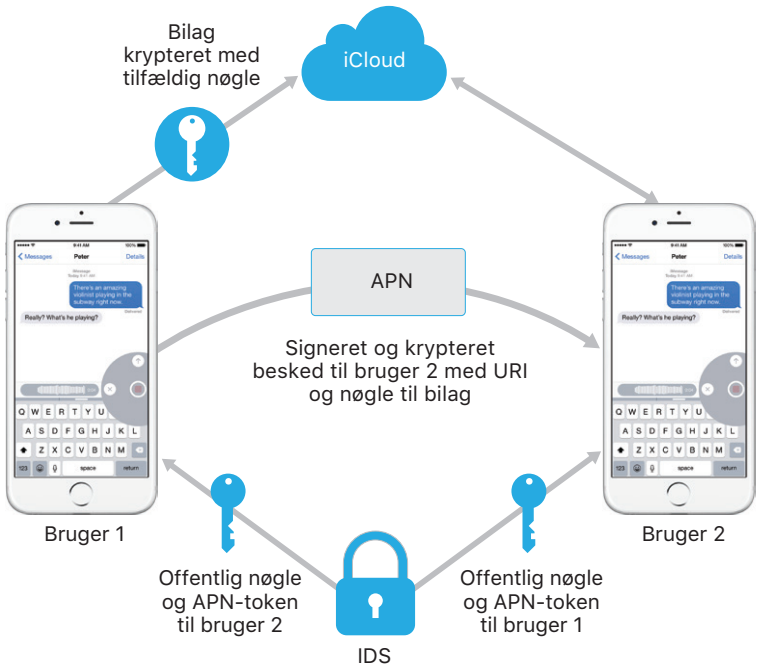
Afsendelse og modtagelse af beskeder via iMessage

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 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-adresser fra IDS.

Brugerens udgående besked krypteres særskilt til hver af modtagerens enheder. Modtagerenhedernes offentlige RSA-krypteringsnøgler 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, når funktionen CTR bruges. Værdien på 40 bit bruges på modtagersiden til at bekræfte, at den afkrypterede 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 ud fra afsenderenhedens private signeringsnøgle. 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 4KB eller 16KB, afhængigt af iOS-versionen. Hvis beskedens tekst er for lang, eller hvis der er vedhæftet et bilag, f.eks. et fotografi, krypteres bilaget med AES CTR med en tilfældig 256 bit nøgle og overføres til iCloud. Derefter sendes bilagets AES-nøgle, dets **URI (Uniform Resource Identifier)** 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-meddelelser slettes beskeden fra APNs, når den er leveret. I modsætning til andre APNs-meddelelser sættes iMessage-beskeder imidlertid i kø til levering til enheder, der er offline. Beskeder opbevares p.t. i op til 30 dage.

Virksomhedschat

Virksomhedschat er en meddelelsesservice, der gør det muligt for brugere at kommunikere med virksomheder ved hjælp af appen Beskeder. Det er kun brugerne, der kan indlede samtalen, og virksomheden modtager en uigennemsigtig identifikator for brugeren. Virksomheden modtager ikke brugerens telefonnummer, e-mailadresse eller iCloud-kontooplysninger. Når du skriver med Apple, modtager Apple et Virksomhedschat-id, der er tilknyttet dit Apple-id. Brugerne har kontrol over, om de vil kommunikere. Hvis en samtale slettes i Virksomhedschat, slettes den i brugerens app Beskeder, og virksomheden blokeres, så den ikke kan sende flere beskeder til brugeren.

Beskeder sendt til virksomheden krypteres individuelt mellem brugerens enhed og Apples beskedservere, og Apples beskedservere afkrypterer disse beskeder og videresender dem til virksomheden over TLS. Virksomheders svar sendes ligeledes over TLS til Apples beskedservere, som derefter genkrypterer beskeden til brugerens enhed. Som med iMessage bliver beskeder stillet i kø til levering til offline-enheder i op til 30 dage.

FaceTime

FaceTime er Apples tjeneste til video- og samtaleopkald. FaceTime bruger i lighed med iMessage også Apples tjeneste til push-beskeder 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 afkryptere dataene.

Den første FaceTime-forbindelse foretages via Apples 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 fælles hemmelighed til hver session. Den fælles hemmelighed bruges til at udlede sessionsnøgler til mediekanaler, der streames via SRTP (Secure Real-time Transport Protocol). SRTP-pakker krypteres ved hjælp af AES-256 med CM-funktion (Counter Mode) og 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. Mens en stor del af infrastrukturen og designet fra en-til-en-FaceTime genbruges, har FaceTime-gruppeopkald en ny mekanisme til etablering

af nøgler, der er bygget oven på den pålidelighed, som IDS leverer. Denne protokol leverer Forward Secrecy, hvilket betyder, at en kompromitteret brugerenhed ikke vil lække indholdet af tidligere opkald. Sessionsnøgler indpakkes via 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.

iCloud

iCloud opbevarer en brugers kontakter, kalendere, fotografier, 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 appdata, som udvikleren har defineret. Brugerne indstiller iCloud ved at logge ind med et Apple-id og vælge, hvilke tjenester de vil bruge. It-administratorer kan slå iCloud-funktioner, f.eks. Min fotostream, iCloud Drive og iCloud-sikkerhedskopi, fra via MDM-konfigurationsbeskrivelser. Tjenesten skelner ikke mellem forskellige typer emner, der opbevares, men behandler alt arkivindhold på samme måde – som en samling byte.

Hvert arkiv opdeles i mindre bidder og krypteres af iCloud med AES-128 og en nøgle, der er afledt af hver bids indhold og benytter SHA-256. Nøglerne og arkivets metadata arkiveres af Apple i brugerens iCloud-konto. Arkivets krypterede bidder arkiveres uden nogen oplysninger, der kan identificere brugeren, ved hjælp af lagringstjenester fra Apple og tredjeparter – såsom Amazon Web Services eller Google Cloud Platform – men disse partnere har ikke nøglerne til at afkryptere dine data, der opbevares på deres servere.

iCloud Drive

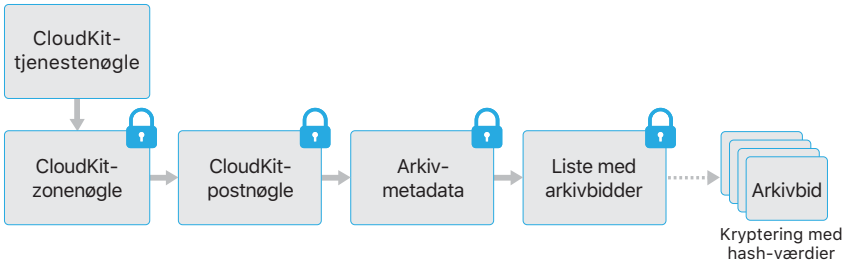
iCloud Drive tilføjer kontobaserede nøgler for at beskytte dokumenter, der er arkiveret i iCloud. Som ved andre iCloud-tjenester opdeles arkivindhold i mindre bidder og krypteres, hvorefter de krypterede bidder arkiveres ved hjælp af tjenester fra tredjeparter. Nøglerne til arkivindholdet indpakkes imidlertid af postnøgler, der opbevares sammen med metadataene til iCloud Drive. Disse postnøgler beskyttes med brugerens iCloud Drive-tjenestenøgle, som derefter opbevares sammen med brugerens iCloud-konto. Når brugerne skal have adgang til metadataene til deres iCloud-dokumenter, skal de godkendes af iCloud, men de skal også være i besiddelse af iCloud Drive-tjenestenøglen for at få vist beskyttede dele af det arkiverede indhold i iCloud Drive.

CloudKit

CloudKit gør det muligt for appudviklere at arkivere nøgleværdidata, strukturerede data og aktiver i iCloud. Adgangen til CloudKit styres ved hjælp af appberettigelser. CloudKit understøtter både offentlige og private databaser. Offentlige databaser bruges af alle kopier af appen, typisk til almindelige aktiver, og de er ikke krypteret. Brugerens data arkiveres i private databaser.

På samme måde som iCloud Drive bruger CloudKit kontobaserede nøgler til at beskytte de oplysninger, der er arkiveret i brugerens private database, og som ved andre iCloud-tjenester opdeles arkiver i bidder, krypteres og arkiveres ved hjælp af tjenester fra tredjeparter. CloudKit

benytter et hierarki med nøgler, der ligner systemet i databeskyttelsen. Arkivnøglerne indpakkes med CloudKit-postnøgler. Postnøglerne beskyttes med en zonenøgle, som beskyttes med brugerens CloudKit-tjenestenøgle. CloudKit-tjenestenøglen opbevares i brugeres iCloud-konto, og der er først adgang til den, når brugeren er godkendt af iCloud.



Gendannelsesmuligheder

Situation	Brugers gendannelses-muligheder i forbindelse med CloudKit-kryptering fra start til slut
Adgang til godkendt enhed	Datagendannelse er mulig via en godkendt enhed eller iCloud-nøgleringsgendannelse.
Ingen godkendte enheder	Datagendannelse er kun mulig via iCloud-nøgleringsgendannelse.

Situation	Brugers gendannelses-muligheder i forbindelse med Beskeder i iCloud
iCloud-sikkerheds-kopiering er slået til, og der er adgang til en godkendt enhed	Datagendannelse er mulig via iCloud-sikkerhedskopiering, adgang til en godkendt enhed eller iCloud-nøgleringsgendannelse.
iCloud-sikkerheds-kopiering er slået til, og der er ikke adgang til en godkendt enhed	Datagendannelse er mulig via iCloud-sikkerhedskopiering eller iCloud-nøgleringsgendannelse.
iCloud-sikkerheds-kopiering er slået fra, og der er adgang til en godkendt enhed	Datagendannelse er mulig via en godkendt enhed eller iCloud-nøgleringsgendannelse.
iCloud-sikkerheds-kopiering er slået fra, og der er ikke adgang til en godkendt enhed	Datagendannelse er kun mulig via iCloud-nøgleringsgendannelse.

CloudKit-kryptering fra start til slut

Mange Apple-tjenester, som er angivet i Apple Support-artiklen "Oversigt over sikkerheden i iCloud" (https://support.apple.com/HT202303), bruger kryptering fra start til slut med en CloudKit-tjenestenøgle, der beskyttes af synkroniseringen af iCloud-nøglering. Nøglehierarkiet til disse CloudKit-containere er baseret på iCloud-nøglering og deler derfor iCloud-nøgleringens sikkerhedsegenskaber – nøglerne er kun tilgængelige på brugerens godkendte enheder. Hverken Apple eller nogen tredjepart har adgang til dem. Hvis adgangen til data i iCloud-nøglering mistes (se afsnittet "Deponeringssikkerhed" senere i dette dokument), nulstilles dataene i CloudKit. Hvis dataene findes på den godkendte lokale enhed, overføres de igen til CloudKit.

Beskeder i iCloud bruger også CloudKit-kryptering fra start til slut med en CloudKit-tjenestenøgle, der beskyttes af synkroniseringen af iCloud-nøglering. Hvis brugeren har slået iCloud-sikkerhedskopi til, bliver CloudKit-tjenestenøglen, der bruges til Beskeder i iCloud-beholderen, sikkerhedskopieret til iCloud, så brugeren kan gendanne beskeder, selvom brugeren har mistet adgangen til iCloud-nøglering og sine godkendte enheder. Denne iCloud-tjenestenøgle udskiftes, hver gang brugeren slår iCloud-sikkerhedskopi fra.

iCloud-sikkerhedskopi

iCloud sikkerhedskopierer også oplysninger dagligt via Wi-Fi, herunder enhedsindstillinger, appdata, fotografier og videoer i Kamerarulle og samtaler i appen Beskeder. iCloud beskytter indholdet ved at kryptere det, når det sendes over internettet, arkivere det i krypteret format og bruge sikre tokens til godkendelse. 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, er systemet designet, så det beskytter data og samtidig tillader trinvis, uovervåget sikkerhedskopiering og gendannelse.

iCloud sikkerhedskopierer følgende emner:

- 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 iOS-enhed, men ikke selve det købte indhold. Når brugeren gendanner data fra en iCloud-sikkerhedskopi, hentes brugerens købte indhold automatisk fra iTunes Store, Apple Books eller

App Store. 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 butikken. En komplet købshistorik er knyttet til en brugers Apple-id.

- Fotos og videoer på en brugers iOS-enheder. Bemærk, at hvis en bruger slår iCloud-fotobibliotek til på sin iOS-enhed (iOS 8.1 eller en nyere version) eller Mac (OS X 10.10.3 eller en nyere version), medtages brugerens fotografier og videoer ikke i iCloud-sikkerhedskopier, fordi emnerne allerede opbevares i iCloud.
- Kontakter, kalenderbegivenheder, påmindelser og noter
- Enhedsindstillinger
- Appdata
- Opkaldshistorik og ringetoner
- Organisering af hjemmeskærm og apps
- HomeKit-konfiguration
- HealthKit-data
- Adgangskode til Visuel telefonsvarer (kræver det SIM-kort, der var i brug under sikkerhedskopieringen)
- iMessage, Virksomhedschat, sms'er og mms'er (kræver det SIM-kort, der var i brug under sikkerhedskopieringen)

  Bemærk: Når Beskeder i iCloud er slået til, fjernes iMessage, Virksomhedschat, sms'er og mms'er fra brugerens eksisterende iCloud-sikkerhedskopi og lagres i stedet i en CloudKit-beholder til Beskeder, der er krypteret fra start til slut. Brugerens iCloud-sikkerhedskopi bevarer en nøgle til beholderen. Hvis brugeren derefter slår iCloud-sikkerhedskopi fra, udskiftes beholderens nøgle, den nye nøgle lagres kun i iCloud-nøglering (Apple og tredjeparter har ikke adgang til den) og nye data, der skrives til beholderen, kan ikke afkrypteres med den gamle beholdernøgle.

Når der oprettes arkiver i databeskyttelsesklasser, der ikke er adgang til, når enheden er låst, krypteres deres arkivnøgler med klassenøglerne fra nøglesamlingen iCloud-sikkerhedskopi. Arkiver sikkerhedskopieres til iCloud i deres oprindelige, krypterede form. Arkiver i databeskyttelses-klassen Ingen beskyttelse krypteres under transport.

Nøglesamlingen iCloud-sikkerhedskopi indeholder asymmetriske (Curve25519) nøgler til hver databeskyttelsesklasse, som bruges til at kryptere arkivnøglerne. Der er flere oplysninger om indholdet af nøglesamlingen til sikkerhedskopiering og nøglesamlingen iCloud-sikkerhedskopi under "Beskyttelse af data i nøglering" i afsnittet Kryptering og databeskyttelse i dette dokument.

Sikkerhedskopisættet arkiveres i brugerens iCloud-konto og består af en kopi af brugerens arkiver og nøglesamlingen iCloud-sikkerhedskopi. Nøglesamlingen iCloud-sikkerhedskopi beskyttes med en tilfældig nøgle, som også arkiveres sammen med sikkerhedskopisættet. (Brugerens iCloud-adgangskode benyttes ikke til kryptering, så eksisterende sikkerhedskopier bliver ikke ugyldige, selvom iCloud-adgangskoden skiftes).

Så længe brugerens nøgleringsdatabase er sikkerhedskopieret til iCloud, beskyttes den med en nøgle afledt af UID. Det betyder, at nøgleringen kun kan gendannes på den enhed, den stammer fra, og at ingen andre, heller ikke Apple, kan læse emnerne i brugerens nøglering.

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

iCloud-nøglering

Integration mellem Safari og iCloud-nøglering
Safari kan automatisk generere kryptografisk stærke tilfældige strenge til adgangskoder til websteder, som opbevares i nøgleringen og synkroniseres med 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.

Med iCloud-nøglering kan brugerne synkronisere deres adgangskoder sikkert mellem iOS-enheder og 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.

Synkronisering af nøgleringen

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

Den signerede synkroniseringskæde placeres i brugeres iCloud-lagringsområde til nøgleværdier. Den kan ikke læses, hvis brugerens iCloud-adgangskode ikke er kendt, og den kan ikke ændres på en gyldig måde uden den private nøgle til medlemmets synkroniseringsidentitet.

Hvis brugeren slår iCloud-nøglering til på en anden enhed, registrerer den, at brugeren tidligere har etableret en synkroniseringskæde i iCloud, som den ikke er medlem af. Enheden danner nøgleparret til sin synkroniseringsidentitet og opretter derefter en programbillet for at anmode om medlemskab af kæden. Billetten består af den offentlige nøgle til enhedens synkroniseringsidentitet, og brugeren bliver bedt om at legitimere sig med sin iCloud-adgangskode. Parametrene til generering af den elliptiske nøgle hentes fra iCloud og genererer en nøgle, der bruges til at signere programbilletten. Til sidst placeres programbilletten i iCloud.

Når den første enhed ser, at der er ankommet en programbillet, viser den en besked om, at brugeren skal bekræfte, at en ny enhed har anmodet om at blive medlem af synkroniseringskæden. Brugeren indtaster sin iCloud-adgangskode, og programbilletten bekræftes som signeret af en matchende privat nøgle. Derved fastlægges, at den person, som oprettede anmodningen om at blive medlem af kæden, indtastede brugerens iCloud-adgangskode på det tidspunkt, hvor anmodningen blev oprettet.

Når brugeren har godkendt, at den nye enhed må føjes til kæden, tilføjer den første enhed det nye medlems offentlige nøgle til synkroniseringskæden og signerer den igen med både dens 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.

Der er nu to medlemmer af signeringskæden, og hvert medlem har det andet medlems offentlige nøgle. De kan nu begynde at udveksle enkeltemner i nøgleringen via iCloud-lagringsområdet til nøgleværdier eller arkivere dem i CloudKit. Hvis begge medlemmer af kæden har samme emne, vil emnet med den nyeste ændringsdato blive synkroniseret. Et emne springes over, hvis det andet medlem også har emnet, og ændringsdatoerne er ens. Et emne, der synkroniseres, krypteres, så det kun kan afkrypteres af en enhed i brugerens godkendelseskæde. Det kan ikke afkrypteres af nogen anden enhed eller Apple.

Processen gentages, når nye enheder bliver medlem af synkroniserings-kæden. Når en tredje enhed bliver medlem, vises bekræftelsen således på begge den anden brugers enheder. Brugeren kan enten godkende det nye medlem fra den ene eller den anden enhed. Når der tilføjes nye enheder, synkroniseres hver enhed med de nye for at sikre, at alle medlemmer har samme emner i nøgleringen.

Hele nøgleringen synkroniseres dog ikke. Nogle emner gælder kun en enhed, f.eks. VPN-identiteter, og må ikke forlade enheden. Kun emner med attributten `kSecAttrSynchronizable` synkroniseres. Apple har indstillet denne attribut til brugerdata i Safari (herunder brugernavne, adgangskoder og kreditkortnumre) samt til Wi-Fi-adgangskoder og HomeKit-krypteringsnøgler.

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

Gendannelse af nøgleringen

Gendannelse af nøgleringen giver brugerne mulighed for at deponere deres nøglering 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, der bevirker, at data ikke mistes. Det er især vigtigt, når Safari bruges til at generere tilfældige, stærke adgangskoder til webkonti, da disse adgangskoder kun er registreret i nøgleringen.

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

Når iCloud-nøglering er slået til, bruges enhedens adgangskode til at gendanne en deponeret nøglering, hvis tofaktorgodkendelse er slået til for brugerens konto. 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 lade deres enheder oprette en kryptografisk tilfældig kode, som de selv kan registrere og opbevare.

Dernæst eksporterer iOS-enheden 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 den offentlige nøgle til den klynge i hardwaresikkerhedsmodulet (HSM), hvor kontrakten skal opbevares. Det bliver brugerens iCloud-kontraktpost.

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 kontraktpost. 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 vil modtage en sms og skal svare på den, før gendannelsen kan fortsætte.

Kontraktsikkerhed

iCloud har en sikker infrastruktur til nøgleringsdeponering, der sikrer, at kun godkendte brugere og enheder kan udføre en gendannelse. Klynger i hardwaresikkerhedsmodulet (HSM) er topografisk set placeret bag iCloud og vogter kontraktposterne. Hver af dem har en nøgle, der bruges til at kryptere de kontraktposter, som de vogter over, som beskrevet tidligere i dette dokument.

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 kontraktposten ud og sender den til brugerens enhed.

Derefter bruger enheden iCloud-sikkerhedskoden til at pakke den tilfældige nøgle ud, som er brugt til at kryptere brugerens nøglering. Med den nøgle afkrypteres nøgleringen, der er hentet fra iCloud-lagringsområdet til nøgleværdier, og gendannes på enheden. Der må 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 kontrakten, 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 kontraktpost er gået tabt. De kan derefter vælge at tilmelde sig igen.

Siri

Brugerne kan få Siri til at sende beskeder, planlægge møder, foretage telefonopkald og meget mere blot ved at tale naturligt. Siri bruger talegenkendelse, tekst til tale og en klientservermodel til at svare på en lang række anmodninger. De opgaver, som Siri understøtter, er designet med henblik på at sikre, at der bruges et absolut minimum af personlige oplysninger, og at de er fuldt beskyttet.

Når Siri slås til, opretter enheden tilfældige id'er til brug sammen med talegenkendelse og Siri-serverne. Id'erne bruges kun til Siri og bruges til at forbedre tjenesten. Hvis Siri derefter slås fra, genererer enheden et nyt tilfældigt id, der skal bruges, hvis Siri slås til igen.

I forbindelse med Siris funktioner sendes nogle af brugerens oplysninger fra enheden til serveren. Det gælder oplysninger om musikbiblioteket (sangtitler, kunstnere og spillelister), navnene på listerne med påmindelser og navne og relationer, der er defineret i Kontakter. Al kommunikation med serveren sker via HTTPS.

Når brugeren starter en Siri-session, sendes brugerens fornavn og efternavn (fra Kontakter) sammen med en omtrentlig geografisk lokalitet til serveren. Det giver Siri mulighed for at svare med navnet eller besvare spørgsmål, der kun kræver en omtrentlig lokalitet, f.eks. spørgsmål om vejret.

Hvis der er behov for en mere præcis lokalitet, f.eks. for at finde lokaliteten af biografer i nærheden, anmoder serveren om en mere præcis lokalitet fra enheden. Det er et eksempel på, hvordan oplysninger som standard kun sendes til serveren, når det er strengt nødvendigt for at behandle brugerens anmodning. I alle tilfælde kasseres sessionsoplysninger efter 10 minutters passivitet.

Når Siri bruges fra Apple Watch, opretter uret sit eget tilfældige entydige id som beskrevet tidligere. I stedet for at sende brugerens oplysninger igen sender urets anmodninger imidlertid også Siri-id'et til den iPhone, der dannes par med, som reference til oplysningerne.

Optagelsen af brugerens talte ord sendes til Apples talegenkendelses-server. Hvis opgaven kun omfatter diktering, sendes den genkendte tekst tilbage til enheden. Ellers analyserer Siri teksten og kombinerer den om nødvendigt med oplysninger fra den beskrivelse, der er knyttet til enheden. Hvis anmodningen f.eks. er "skriv en besked til min mor", bruges de relationer og navne, der blev overført fra Kontakter. Kommandoen til den fundne handling sendes derefter tilbage til enheden for at blive udført der.

Mange Siri-funktioner udføres af enheden efter serverens anvisninger. Hvis brugeren f.eks. beder Siri om at læse en indgående besked, instruerer serveren blot enheden om at læse indholdet af dens ulæste beskeder højt. Indholdet og afsenderen af beskeden sendes ikke til serveren.

Optagelser af brugerens stemme arkiveres i seks måneder, så genkendelsessystemet kan bruge dem til at blive bedre til at forstå brugerens stemme. Efter seks måneder arkiveres en anden kopi uden kopiens id i op til to år med det formål at hjælpe Apple med at forbedre og udvikle Siri. Et lille antal optagelser, udskrifter og tilhørende data uden

id'er kan blive brugt af Apple i længere tid end to år af hensyn til den løbende forbedring og kvalitetssikring af Siri. Desuden arkiveres visse optagelser med henvisninger til musik, sportshold og sportsudøvere samt virksomheder eller interessepunkter med henblik på at forbedre Siri.

Siri kan også kaldes håndfrit via stemmeaktivering. Registreringen af stemmeudløsere foretages lokalt på enheden. Med denne funktion aktiveres Siri kun, når det indgående lydmønster ligner den angivne udløsers lydmønster tilstrækkeligt. Når udløseren registreres, sendes den tilhørende lyd og den efterfølgende Siri-kommando til Apples talegenkendelsesserver til videre behandling efter samme regler som andre optagelser af brugerens stemme, der er foretaget via Siri.

Brugerne kan også starte Siri på Apple Watch ved at holde det op til munden og sige en anmodning til Siri. Siri startes på denne måde, når følgende to forudsætninger er opfyldt:

- En maskinlæringsmodel på enheden registrerer menneskelige talemønstre i nærheden af enheden.
- En anden maskinlæringsmodel på enheden identificerer et bevægelsesmønster og en stilling for enheden, der matcher bevægelsen Løft for at tale.

Når denne kombination af bevægelse og lyd registreres, sendes den tilsvarende lyd til Apples talegenkendelsesserver til videre behandling efter samme regler som andre optagelser af brugerens stemme, der er foretaget via Siri.

Siri-forslag

Siri-forslag til apps og genveje genereres vha. maskinlæring på enheden. Ingen data sendes til Apple, bortset fra oplysninger om, hvilke signaler der var nyttige mht. at forudsige genveje eller start af apps (disse oplysninger kan ikke bruges til at identificere brugeren).

Genveje i Siri

Genveje, der føjes til Siri, synkroniseres på tværs af alle Apple-enheder, der bruger iCloud, og krypteres med CloudKit-kryptering fra start til slut. De udtryk, der er knyttet til genveje, synkroniseres til Siri-serveren med henblik på talegenkendelse og knyttes til det tilfældige Siri-id, der er beskrevet tidligere i dette afsnit. Apple modtager ikke indholdet af genvejene, som lagres lokalt i en datavault.

Appen Genveje

Specielle genveje i appen Genveje synkroniseres eventuelt på tværs af Apple-enheder vha. iCloud. Genveje kan også deles med andre brugere via iCloud.

Specielle genveje er alsidige – de ligner instrukser eller programmer. Et karantænesystem bruges til at isolere genveje, der blev hentet fra internettet. Brugerne får en advarsel, første gang de forsøger at bruge genvejen, og har mulighed for at se oplysninger om den, f.eks. hvor den stammer fra.

Specielle genveje kan også afvikle JavaScript anført af brugeren på websteder i Safari, når dette startes fra siden til delinger. Der hentes opdaterede definitioner af malware for at kunne identificere skadelige instrukser ved afvikling og beskytte brugerne mod skadeligt JavaScript, der f.eks. kan 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.

Safari-forslag, Siri-forslag i Søg, Slå op, #billeder, appen News og widgetten News i lande uden News

Safari-forslag, Siri-forslag i Søg, Slå op, #billeder, appen News og widgetten News i lande uden News viser forslag til brugerne fra andre kilder end deres enheder, f.eks. Wikipedia, iTunes Store, lokale nyheder, resultater fra Kort og App Store – endda før brugeren begynder at skrive.

Når en bruger begynder at skrive på adresselinjen i Safari, åbner eller bruger Siri-forslag i Søg, bruger Slå op, åbner #billeder, bruger Søg i appen News eller bruger widgetten News i lande uden News, sendes følgende kontekst krypteret via HTTPS til Apple for at vise relevante resultater for brugeren:

- Et id, der skifter hvert kvarter for at opretholde anonymiteten.
- Brugerens søgeforespørgsel.
- Den mest sandsynlige færdiggørelse af forespørgslen baseret på konteksten og tidligere søgninger i den lokale buffer.
- Brugerens enheds omtrentlige lokalitet, hvis Lokalitetstjenester er slået til for Lokalitetsbaserede forslag. Graden af sløring af lokaliteter afhænger af den anslåede befolkningstæthed på enhedens lokalitet, f.eks. højere sløringsgrad på landet, hvor der er større geografisk afstand mellem brugerne, end i byerne, hvor brugerne normalt befinder sig tættere på hinanden. Brugerne kan slå afsendelse af alle lokalitetsoplysninger til Apple fra ved at slå Lokalitetstjenester fra for Lokalitetsbaserede forslag. Hvis Lokalitetstjenester er slået fra, kan Apple bruge enhedens IP-adresse til at udlede en omtrentlig lokalitet.
- Enhedens type, og om søgningen foretages i Siri-forslag i Søg, Safari, Slå op, appen News eller Beskeder.
- Forbindelsens type.
- Oplysninger om de senest benyttede apps på enheden (giver yderligere søgekontekst). Kun apps, som findes på en godkendelsesliste med populære apps, der vedligeholdes af Apple, og som er benyttet inden for de sidste tre timer, inkluderes.
- En liste med populære programmer på enheden.
- Indstillinger til sprog, område og indtastningsenhed.
- Hvis brugerens enhed har adgang til abonnementstjenester til musik og video, sendes oplysninger om navnene på abonnementstjenesterne og abonnementernes type muligvis til Apple. Brugerens kontonavn, kontonummer og adgangskode sendes ikke til Apple.
- Opsummeret, samlet repræsentation af interessante emner.

Når en bruger vælger et resultat eller slutter appen uden at have valgt et resultat, sendes nogle oplysninger, der bidrager til at forbedre kvaliteten af fremtidige resultater, til Apple. Oplysningerne er kun knyttet til sessions-id'et med en varighed på 15 minutter, ikke til en bestemt bruger. Feedback omfatter nogle af de tidligere beskrevne kontekstoplysninger og oplysninger om interaktion, f.eks.:

- Målinger af tiden mellem interaktioner og søgeforespørgsler på netværket.
- Forslagenes rangering og rækkefølge i oversigten.
- Resultatets id og den valgte handling, hvis resultatet ikke er lokalt, eller det valgte resultats kategori, hvis resultatet er lokalt.
- Et flag, der viser, om brugeren har valgt resultatet.

Apple opbevarer logarkiver med forespørgsler, kontekst og feedback i forbindelse med Forslag i 18 måneder. En delmængde af logarkiver opbevares i op til fem år, f.eks. forespørgsler, sprogområde, domæne, omtrentlig placering og de samlede målinger.

I nogle tilfælde vil Forslag måske videresende forespørgsler om almindelige ord og vendinger til en autoriseret partner for at modtage og vise partnerens søgeresultater. Apple benytter proxyer til forespørgslerne, så partnerne ikke modtager IP-adresser eller søgefeedback. Kommunikationen med partneren krypteres med HTTPS. I tilfælde af forespørgsler, der ofte afsendes, leverer Apple lokalitet på byniveau, enhedstype og klientsprog som søgekontekst til partneren for at forbedre ydeevnen ved søgning.

Følgende oplysninger logges uden et sessions-id for at øge forståelsen af og ydeevnen i forskellige geografiske områder og på forskellige typer netværk:

- En del af IP-adressen (uden den sidste oktet ved IPv4-adresser og uden de sidste 80 bit ved IPv6-adresser)
- Omtrentlig lokalitet
- Cirkatidspunkt for forespørgslen
- Latenstid/overførselshastighed
- Størrelse på svar
- Forbindelsestype
- Sprogområde
- Enhedstype og den app, der sender anmodningen

Intelligent beskyttelse mod sporing i Safari

Intelligent beskyttelse mod sporing (Intelligent Tracking Prevention – ITP) er en del af Safaris standardpolitik for cookies og data fra websteder, der beskytter din anonymitet. Det kan forhindre sporing mellem websteder ved at begrænse adgangen til cookies og andre data fra websteder.

ITP indsamler statistik om indlæsning af ressourcer (billeder, instrukser osv.) og brugerhandlinger, f.eks. tryk og indtastning af tekst. En maskinlæringsmodel bruges til klassificering på enheden af, hvilke domænenavne der kan spore brugeren mellem websteder baseret på den indsamlede statistik.

Når et domæne er klassificeret til at have sporingsfunktioner, partitionerer ITP med det samme domænets cookies, hvis brugeren tidligere har interageret med det domæne som en førstepart, og ITP blokerer med det samme cookies for klassificerede domæner, som en bruger ikke har interageret med. For eksempel:

- video.example tilbyder en reklamefri abonnementstjeneste og har mange af deres videoer integreret på andre websteder.
- En bruger logger ind på video.example og derefter på andre websteder, der indeholder integreret indhold fra video.example.

- ITP klassificerer video.example til at have sporingsfunktioner og partitionerer derfor cookies.
- Når en bruger besøger newspaper.example, og det indeholder integreret indhold fra video.example, er cookies, der leveres til video.example, partitionerede cookies, der er specifikke for video.example på newspaper.example.

Integreret indhold fra tredjeparter anmoder muligvis en bruger om adgang til dennes førsteparts cookies med Storage Access API. Når en bruger trykker eller klikker på integreret indhold fra en tredjepart, der bruger Storage Access API, viser Safari en besked, der spørger, om brugeren vil give tredjeparten adgang til dennes cookies og webstedsdata, hvilket gør det muligt for tredjeparten at spore brugeren på førstepartsdomænet. Hvis en bruger vælger Tillad, kan det integrerede indhold fra tredjepart få adgang til dennes førstepartscookies, så længe brugeren besøger webstedet, og ved efterfølgende besøg kan det integrerede indhold fra tredjepart få adgang til brugerens førstepartscookies, efter at brugeren interagerer med det integrerede indhold, og indholdet kalder Storage Acccess API. Og fordi brugeren tidligere gav tilladelse, bliver brugeren ikke spurgt igen. Brugerens beslutning bevares for kombinationen af første- og tredjeparter og ryddes, når en bruger rydder sin historik i Safari.

Eksisterende cookies fra domæner, der er klassificeret til at have sporingsfunktioner, slettes, hvis en bruger ikke har interageret med domænet – direkte eller via Storage Access API – i 30 dage med aktiv brug af Safari. Efter 30 dage uden interaktion kan et domæne, der er klassificeret til at have sporingsfunktioner, heller ikke oprette nye cookies. Safari tillader aldrig adgang til andre førsteparts webstedsdata i tredjeparts sammenhænge.

ITP kan forhindre brug af cookies og webstedsdata, hvor formålet er sporing på tværs af websteder, ved at isolere data fra førstepart og trejdepart. Apple har ingen adgang til, hvilke domænenavne en enhed har indsamlet statistik om eller klassificeret til at have sporingsfunktioner.

Ud over at blokere cookies fra tredjeparter på domæner, der er klassificeret til at have sporingsfunktioner, beskærer ITP også oplysningerne i HTTP-henviser, som sendes til tredjepartsdomæner, der er klassificeret til at have sporingsfunktioner, til kun at udgøre sidens oprindelse.

Administration af brugeradgangskode

iOS indeholder en række funktioner, der betyder, at brugere sikkert og nemt kan godkendes i apps fra tredjeparter og websteder, der bruger adgangskoder til godkendelse. Adgangskoder gemmes i den særlige nøglering Autoudfyld adgangskode, som kontrolleres af brugeren og kan administreres i Indstillinger > Adgangskoder & konti > Koder til websteder og apps. Apps kan ikke få adgang til nøgleringen Autoudfyld adgangskode uden brugerens tilladelse. Godkendelsesoplysninger, der gemmes i nøgleringen Autoudfyld adgangskode, synkroniseres på tværs af enheder vha. iCloud-nøglering, når dette er slået til.

Adgangskodeadministratoren til iCloud-nøglering og Autoudfyld adgangskode indeholder følgende funktioner:

- Udfyldning 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.

App-adgang til arkiverede adgangskoder

API til delte webgodkendelsesoplysninger

iOS-apps kan bruge følgende to API'er til at interagere med nøgleringen Autoudfyld adgangskode:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

Adgangen tillades kun til iOS-apps, hvis både appudvikleren og webstedsadministratoren har godkendt den, og brugeren har givet sit samtykke. Appudviklere viser deres intention om at få adgang til adgangskoder, som er arkiveret 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 en TLS-anmodning til hvert af webstederne på listen med en anmodning om en af følgende filer:

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

Hvis arkivet indeholder app-id'et på den app, der skal installeres, definerer iOS 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.

Autoudfyld adgangskode for apps

iOS giver brugerne mulighed for at indsætte arkiverede brugernavne og adgangskoder i felter til godkendelsesoplysninger i apps ved at trykke på et nøgleelement på iOS-tastaturets QuickType-linje. Det benytter den samme mekanisme til tilknytning mellem app og websted, som håndteres af arkivet apple-app-site-association, til at danne en tæt forbindelse mellem apps og websteder. Denne grænseflade viser ingen godkendelsesoplysninger til appen, før en bruger giver sit samtykke til at frigive godkendelsesoplysninger. Når iOS har defineret en godkendt relation mellem et websted og en app, foreslår QuickType-linjen straks godkendelsesoplysninger, der kan indsættes i appen. Det giver brugerne mulighed for at vælge at vise godkendelsesoplysninger, der er arkiveret i Safari, til apps med samme sikkerhedsegenskaber, uden at apps skal implementere et API.

Når en app og et websted har en godkendt relation, og en bruger skriver godkendelsesoplysninger i en app, foreslår iOS muligvis brugeren at arkivere godkendelsesoplysningerne i nøgleringen Autoudfyld adgangskode til senere brug.

Automatiske stærke adgangskoder

Når iCloud-nøglering er slået til, opretter iOS stærke, tilfældige, entydige adgangskoder, når brugere tilmelder sig eller ændrer adgangskoder i en app eller på et websted i Safari. Brugerne skal fravælge at bruge stærke adgangskoder. Genererede adgangskoder arkiveres i nøgleringen og synkroniseres på tværs af enheder med iCloud-nøglering, når dette er slået til.

Adgangskoder, der genereres af iOS, 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 bits af entropi.

iOS genererer adgangskoder i apps og i Safari baseret på heuristik, der bestemmer en adgangskodeproces som værende til adgangskode-oprettelse. Hvis heuristikken ikke genkender en adgangskodekontekst som værende til adgangskodeoprettelse, kan appudviklere bruge UITextContentType.newPassword i deres tekstfelt, og webudviklere kan bruge autocomplete=”new-password” i deres <input>-elementer.

Apps og websteder kan angive regler til iOS, der sikrer, at genererede adgangskoder er kompatible med den relevante tjeneste. iOS vil generere den stærkest mulige adgangskode, der samtidig opfylder disse regler. Udviklere angiver disse regler ved at bruge UITextInputPasswordRules eller attributten passwordrules i deres <input> elementer.

Afsendelse af adgangskoder til andre personer eller enheder

AirDrop

Når AirDrop er slået til, kan brugere via AirDrop sende arkiverede godkendelsesoplysninger, inklusive de websteder, de er arkiveret på, brugernavnet og adgangskoden, til en anden enhed. Når der sendes godkendelsesoplysninger via AirDrop, bruges funktionen Kun kontakter altid uanset brugerens indstillinger. (Se flere oplysninger i afsnittet "AirDrop-sikkerhed"). Når brugeren har givet sit samtykke, gemmes godkendelsesoplysningerne på modtagerens enhed i nøgleringen Autoudfyld adgangskode.

Apple TV

Autoudfyld adgangskode kan bruges til at udfylde godkendelses-oplysninger 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 i nærheden viser en besked, der inviterer brugeren til at dele godkendelsesoplysninger med Apple TV. En iPhone og en Apple TV-enhed, der bruger den samme iCloud-konto, krypterer kommunikationen mellem de to enheder under denne proces. Hvis iPhone er logget ind på en anden iCloud-konto end Apple TV:

- Der bruges en PIN-kode til at oprette en krypteret forbindelse.
- iPhone skal være låst op og tæt på den Siri Remote, der er parret med Apple TV, for at modtage beskeden.

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

Udvidelser til levering af sikkerhedsoplysninger

Brugere kan anføre et kompatibelt program fra tredjepart til at levere godkendelsesoplysninger til Autoudfyld i indstillingerne til Adgangskoder & konti. Denne mekanisme bygger på udvidelser. Udvidelser til levering af godkendelsesoplysninger skal vise en mulighed for at vælge godkendelsesoplysninger og kan eventuelt levere iOS-metadata om gemte godkendelsesoplysninger, så de kan vises direkte i QuickType-linjen. Disse metadata inkluderer webstedet, hvor godkendelsesoplysningerne bruges, og det tilknyttede brugernavn, men ikke adgangskoden. iOS kommunikerer med udvidelsen for at få adgangskoden, når brugeren vælger at udfylde den i en app eller på et websted i Safari. Metadata for godkendelsesoplysninger lagres i et isoleret miljø (sandbox) hos leverandøren af godkendelsesoplysningerne og fjernes automatisk, når en app fjernes.

Styring af enheder

iOS understøtter fleksible sikkerhedspolitikker og -konfigurationer, der er nemme at håndhæve og administrere. På den måde kan organisationerne beskytte virksomhedens oplysninger og 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, konfigurationsbeskrivelser, ekstern sletning og MDM-løsninger 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 iOS-enheder.

Adgangskodebeskyttelse

Brugerens adgangskode defineres som standard som en PIN-kode. På enheder med Touch ID eller Face ID er den minimale længde på adgangskoden fire cifre. Brugerne kan angive en længere alfanumerisk adgangskode ved at vælge Speciel alfanumerisk kode under Indstillinger til adgangskode i Indstillinger > Adgangskode. Det anbefales at bruge længere og mere komplekse koder, som er sværere at gætte eller angribe.

Administratorer kan gennemtvinge krav om komplekse adgangskoder og andre politikker via MDM eller Exchange ActiveSync eller ved at kræve, at brugerne manuelt installerer konfigurationsbeskrivelser. Der findes følgende adgangskodepolitikker:

- Tillad simpel værdi
- Kræv alfanumerisk værdi
- Minimumslængde på adgangskode
- Mindste antal komplekse tegn
- Maksimumsalder på adgangskode
- Adgangskodehistorik
- Tidspunkt for automatisk lås
- Frist inden låsning af enhed
- Maksimalt antal forsøg med forkert adgangskode
- Tillad Touch ID eller Face ID

Der er flere oplysninger til administratorer om hver politik her: https://support.apple.com/guide/mdm/

Der er flere oplysninger til udviklere om hver politik her: https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf

Model for pardannelse i iOS

iOS 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 bruger denne godkendelse til at slå yderligere funktionalitet til for den tilsluttede vært, f.eks. datasynkronisering.

I iOS 9 kan tjenester, der kræver pardannelse, ikke startes, før brugeren har låst enheden op.

I iOS 10 og nyere versioner kræver visse tjenester, f.eks. synkronisering af fotos, at enheden er låst op, før de kan startes.

I iOS 11 og nyere versioner starter tjenester ikke, medmindre enheden er blevet låst op for nylig.

Under pardannelsesprocessen skal brugeren låse enheden op og acceptere anmodningen om pardannelse fra værten. I iOS 11 og nyere versioner skal brugeren også indtaste sin adgangskode. Når brugeren har gjort det, udveksler og arkiverer værten og enheden offentlige 2048-bit RSA-nøgler. Værten får derefter en 256 bit nøgle, der kan låse en nøglesamling af typen Depot op, som er arkiveret på enheden (se "Nøglesamlingen Depot" i afsnittet Nøglesamlinger i dette dokument). De udvekslede nøgler bruges så til at starte en krypteret SSL-session, som skal være åbnet, før enheden vil sende beskyttede data til værten eller starte en tjeneste (iTunes-synkronisering, arkivoverførsler, Xcode-udvikling osv.). Brug af den krypterede session til al kommunikation forudsætter forbindelser mellem enheden og værten via Wi-Fi, så pardannelsen skal være sket forinden via USB. Ved pardannelsen slås desuden flere muligheder for diagnosticering til. I iOS 9 udløber en pardannelsesoptegnelse, hvis den ikke har været brugt i seks måneder. Dette tidsrum afkortes til 30 dage i iOS 11 og nyere versioner.

Du kan få flere oplysninger her:
https://support.apple.com/HT203034

Visse tjenester, herunder com.apple.pcapd, er begrænset, så de kun fungerer via USB. Tjenesten com.apple.file_relay kræver desuden, at der installeres en konfigurationsbeskrivelse, 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 med godkendte værter med indstillingen "Nulstil netværksindstillinger" eller "Nulstil lokalitet & anonymitet".

Du kan få flere oplysninger her:
https://support.apple.com/HT202778

Krævet konfiguration

En konfigurationsbeskrivelse er et XML-arkiv, der sætter en administrator i stand til at distribuere konfigurationsoplysninger til iOS-enheder. Brugeren kan ikke ændre indstillinger, der er defineret i en installeret konfigurationsbeskrivelse. Hvis brugeren sletter en konfigurationsbeskrivelse, fjernes alle de indstillinger, der er defineret i beskrivelsen. Administratorer kan således gennemtvinge indstillinger ved at kæde politikker sammen med Wi-Fi- og dataadgang. En konfigurationsbeskrivelse med en e-mailkonfiguration kan f.eks. også

indeholde en politik for adgangskoder til enheder. Brugerne vil ikke kunne åbne deres e-mail, medmindre deres adgangskode opfylder administratorens krav.

En iOS-konfigurationsbeskrivelse indeholder et antal indstillinger, der kan angives, herunder:

- Politikker til adgangskoder
- Begrænsning af funktioner på enheden (slå kameraet fra f.eks.)
- Wi-Fi-indstillinger
- VPN-indstillinger
- Indstillinger til postserveren
- Exchange-indstillinger
- Indstillinger til LDAP-bibliotekstjenesten
- Indstillinger til CalDAV-kalendertjenesten
- Webklip
- Godkendelsesoplysninger og nøgler
- Avancerede indstillinger til mobilnetværket

Administratorer kan se en aktuel liste her:
https://support.apple.com/guide/mdm/mdm5370d089

Udviklere kan se en aktuel liste her:
https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf

Konfigurationsbeskrivelser kan signeres og krypteres med henblik på at bekræfte deres oprindelse, bevare deres integritet og beskytte deres indhold. Konfigurationsbeskrivelser krypteres ved hjælp af CMS (RFC 3852), der understøtter 3DES og AES-128.

Konfigurationsbeskrivelser kan desuden fastlåses på en enhed, så de ikke kan slettes eller kun kan slettes med en adgangskode. Da mange brugere i virksomheder selv ejer deres iOS-enhed, kan konfigurationsbeskrivelser, der binder en enhed til en MDM-løsning, fjernes, men hvis de fjernes, fjernes også alle administrerede konfigurationsoplysninger, data og apps.

Brugerne kan installere konfigurationsbeskrivelser direkte på deres enheder ved at bruge Apple Configurator 2, eller de kan hente dem via Safari, få dem tilsendt i en e-mail eller overføre dem trådløst fra en MDM-løsning. Når en bruger indstiller en enhed i Apple School Manager eller Apple Business Manager, henter og installerer enheden en beskrivelse til tilmelding til MDM.

MDM (Mobile Device Management)

Understøttelse af MDM i iOS sætter virksomheder i stand til at konfigurere og administrere skalerede implementeringer af iPhone, iPad, Apple TV og Mac på en sikker måde i hele organisationen. MDM-funktionerne bygger på eksisterende iOS-teknologier som konfigurationsbeskrivelser, 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. Der overføres ingen fortrolige oplysninger eller oplysninger ejet af virksomheden via APNs.

Med MDM kan it-afdelinger indlemme iOS-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.

Du kan få flere oplysninger om MDM her:

- https://www.apple.com/dk/iphone/business/it/management.html
- https://help.apple.com/deployment/ios/#/ior07301dd60
- https://support.apple.com/guide/mdm/mdmbf9e668

Delt iPad

Delt iPad er en flerbrugerfunktion til brug i iPad-implementeringer i uddannelsesinstitutioner. Funktionen sætter studerende i stand til at dele en iPad uden at dele dokumenter og data. Hver studerende får sin egen hjemmemappe, som oprettes som en APFS-enhed, der beskyttes af brugerens godkendelsesoplysninger. Delt iPad forudsætter brug af administrerede Apple-id'er, der udstedes og ejes af skolen. Med delt iPad kan en studerende logge på en hvilken som helst enhed, der ejes af organisationen og er indstillet til at blive brugt af flere studerende. De studerendes data opbevares i særskilte hjemmemapper, der har hver sit databeskyttelsesdomæne og både beskyttes med UNIX-tilladelser og brug af et isoleret miljø (“sandbox”).

Log ind på Delt iPad

Når en studerende logger ind, godkendes det administrerede Apple-id af Apples identitetsservere ved hjælp af SRP-protokollen. Hvis brugeren kan logge ind, udstedes et midlertidigt adgangstoken specielt til enheden. Hvis den studerende har brugt enheden før, har vedkommende allerede en lokal brugerkonto, der låses op med samme godkendelsesoplysninger.

Hvis den studerende ikke har brugt enheden før, oprettes et nyt UNIX-bruger-id, en APFS-enhed med brugerens hjemmemappe og en logisk nøglering. Hvis enheden ikke har forbindelse til internettet (f.eks. fordi den studerende er på studietur), 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, logge ind. Når den begrænsede tid er gået, skal de studerende godkendes på nettet, selvom de allerede har en lokal konto.

Når den studerendes 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 den studerendes indstillinger, og vedkommendes dokumenter og data synkroniseres fra iCloud.

Så længe den studerendes session er aktiv, og enheden har forbindelse til internettet, arkiveres oprettede og ændrede dokumenter og data i iCloud. En synkroniseringsfunktion i baggrunden sørger for, at ændringer overføres til iCloud, efter den studerende er logget ud. Når synkronisering i baggrunden for brugeren er færdig, gøres brugerens APFS-enhed passiv, og den kan ikke gøres aktiv igen uden brugerens godkendelsesoplysninger.

Log ud af Delt iPad

Når en studerende logger ud af Delt iPad, låses nøglesamlingen Bruger for den studerende med det samme, og alle apps lukkes ned. Systemet udskyder nogle almindelige log ud-handlinger midlertidigt for at gøre processen hurtigere, når en ny studerende logger ind, og viser et Log ind-vindue til den nye studerende. Hvis en studerende logger ind i dette tidsrum (ca. 30 sekunder), udfører Delt iPad den udsatte oprydning som

en del af processen, når den nye studerende logger ind. Hvis Delt iPad forbliver passiv, startes den udsatte oprydning. Log ind-vinduet genstartes under oprydningsprocessen, som hvis der var blevet logget ud igen.

Opgraderinger af Delt iPad

Når en Delt iPad opgraderes fra en version før iOS 10.3 til version 10.3 eller en nyere version, foretages en engangskonvertering af arkivsystemet, der konverterer HFS+-datapartitionen til en APFS-enhed. Hvis der på det tidspunkt findes nogen hjemmemapper til brugere på systemet, bevares de på den primære dataenhed i stedet for at blive konverteret til individuelle APFS-enheder.

Når flere studerende logger ind, anbringes deres hjemmemapper også på den primære dataenhed. Nye brugerkonti oprettes ikke med deres egen APFS-enhed som beskrevet tidligere, før alle brugerkonti på den primære dataenhed er blevet slettet. For at sikre at brugerne får den ekstra beskyttelse og de kvoter, som APFS giver, skal iPad opgraderes til 10.3 eller en nyere version, ved at enheden først slettes, hvorefter den nye version installeres, eller også skal alle brugerkonti på enheden slettes med MDM Slet bruger.

Du kan få flere oplysninger om Delt iPad her:
https://support.apple.com/guide/mdm/cad7e2e0cf56

Apple School Manager

Apple School Manager er en tjeneste, som gør det muligt for uddannelsesinstitutioner at købe indhold, konfigurere automatisk tilmelding af enheder i MDM-løsninger, oprette konti til studerende og personale og indstille iTunes U-kurser. Apple School Manager er tilgængeligt på internettet og designet til teknologiledere, it-administratorer, personale og lærere.

Der er flere oplysninger om Apple School Manager her:
https://help.apple.com/schoolmanager/

Apple Business Manager

Apple Business Manager er en enkel, webbaseret portal til IT-administratorer beregnet til implementering af iOS-, macOS- og tvOS-enheder fra et samlet sted. Når den bruges med din MDM-løsning, kan du konfigurere enhedsindstillinger og købe og distribuere apps og bøger. Apple School Manager er tilgængeligt på internettet og er designet til IT-administratorer.

Der er flere oplysninger om Apple School Manager her:
https://help.apple.com/businessmanager/

Tilmelding af enheder

Apple School Manager og Apple Business Manager gør det muligt at implementere iOS-enheder, som en organisation har købt direkte fra Apple eller via autoriserede Apple-forhandlere eller -udbydere, der deltager i programmet, på en hurtig og strømlinet måde. Enheder med iOS 11 eller en nyere version og tvOS 10.2 eller en nyere version kan også føjes til Apple School Manager og Apple Business Manager efter købstidspunktet ved hjælp af Apple Configurator 2.

Organisationer kan tilmelde enheder automatisk i MDM uden at røre eller klargøre enhederne fysisk, før brugerne får dem. Når administratorerne har tilmeldt sig et af programmerne, logger de ind på programmets websted og knytter programmet til deres MDM-løsning. De enheder, de har købt, kan derefter tildeles til brugerne via MDM. Under konfigurering af enheden kan sikkerheden for følsomme data øges ved at sikre, at de rette sikkerhedsforanstaltninger er på plads. For eksempel:

- Få brugerne til at godkende som en del af den første indstillingsprocedure i Apple-enhedens Indstillingsassistent under aktivering.
- Sørg for at have en foreløbig konfiguration med begrænset adgang, og kræv yderligere enhedskonfiguration, før der gives adgang til følsomme data.

Når der er tildelt en bruger, installeres automatisk alle konfigurationer, begrænsninger eller betjeningsmuligheder, der er angivet i MDM. Al kommunikation mellem enheder og Apple-servere krypteres under overførsel ved hjælp af HTTPS (SSL).

Indstillingen til brugerne kan forenkles yderligere, ved at bestemte trin i Indstillingsassistenten fjernes for iOS, tvOS og MacOS, så brugerne hurtigt kommer i gang. Administratorerne kan også styre, om brugeren må fjerne MDM-beskrivelsen fra enheden, og de kan sikre, at enhedsbegrænsningerne er defineret helt fra starten. Når enheden er pakket ud og aktiveret, kan den tilmeldes organisationens MDM-løsning, og alle administrationsindstillinger, apps og bøger installeres.

Apple Configurator 2

Ud over MDM gør Apple Configurator 2 til macOS det nemt at indstille og konfigurere iOS- og Apple TV-enheder på forhånd, inden de udleveres til brugerne. Med Apple Configurator 2 kan enheder hurtigt konfigureres på forhånd med apps, data, begrænsninger og indstillinger.

Med Apple Configurator 2 kan du bruge Apple School Manager eller Apple Business Manager til at tilmelde enheder i en MDM-løsning, så brugerne ikke behøver at bruge Indstillingsassistent. Apple Configurator 2 kan også bruges til at føje iOS- og Apple TV-enheder til Apple School Manager eller Apple Business Manager efter købstidspunktet.

Du kan få flere oplysninger om Apple Configurator 2 her:
https://support.apple.com/guide/apple-configurator-2/

Tilsyn

Under indstillingen af en enhed kan en organisation konfigurere enheden til at være under tilsyn. Tilsyn betyder, at enheden ejes af organisationen, og dette giver mulighed for yderligere styring af enhedens konfiguration og begrænsninger. Med Apple School Manager eller Apple Business Manager kan tilsyn slås trådløst til på enheden som en del af MDM-tilmeldingsprocessen eller slås manuelt til ved hjælp af Apple Configurator 2. Før der kan føres tilsyn med en enhed, skal enheden slettes, og operativsystemet skal installeres igen.

Der er flere oplysninger om konfiguration og administration af iOS- og Apple TV-enheder med MDM eller Apple Configurator 2 her:
https://help.apple.com/deployment/ios/

Begrænsninger

Administratorer kan slå begrænsninger til og i nogle tilfælde slå dem fra for at forhindre brugerne i at få adgang til et program, en app, en tjeneste eller en funktion på enheden. Begrænsninger sendes til enheder i begrænsningsdata, som knyttes til en konfigurationsbeskrivelse. Begrænsninger kan anvendes på iOS-, tvOS- og macOS-enheder. Visse begrænsninger på en administreret iPhone kan blive dubleret på et parret Apple Watch.

IT-ledere kan se en aktuel liste her:
https://support.apple.com/guide/mdm/mdm0f7dd3d8

Ekstern sletning

iOS-enheder kan slettes eksternt af en administrator eller bruger. Øjeblikkelig ekstern sletning foretages ved, at krypteringsnøglen til bloklagringsplads slettes i Effaceable Storage på en sikker måde, hvorved alle data bliver ulæselige.
Kommandoen til ekstern sletning kan aktiveres af MDM, Exchange eller iCloud.

Når en kommando til ekstern sletning udløses af MDM eller iCloud, sender enheden en bekræftelse og udfører sletningen. I tilfælde af ekstern sletning via Exchange udfører enheden en kontrol på Exchange-serveren, inden den udfører sletningen.

Brugerne kan også slette de enheder, de råder over, ved at bruge appen Indstillinger. Som beskrevet tidligere kan enheder også indstilles, så de automatisk slettes efter en række mislykkede adgangskodeforsøg.

Funktionen Mistet

Hvis en enhed mistes eller bliver stjålet, kan en MDM-administrator eksternt slå funktionen Mistet fra på en enhed under tilsyn med iOS 9.3 eller en nyere version. Når funktionen Mistet 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. Når funktionen Mistet slås til på enheden, kan administratoren få enheden til at sende sin nuværende lokalitet og eventuelt afspille en lyd. Funktionen Mistet kan kun afsluttes, ved at en administrator slår den fra. Når det sker, får brugeren vist en besked på den låste skærm eller en advarsel på hjemmeskærmen.

Aktiveringslås

Når Find min iPhone er slået til, kan enheden kun gøres aktiv igen, ved at godkendelsesoplysningerne til ejerens Apple-id eller enhedens tidligere adgangskode indtastes.

Det er en god ide at føre tilsyn med enheder, der ejes af en organisation, så Aktiveringslås kan administreres af organisationen i stedet for, at de enkelte brugere skal indtaste godkendelsesoplysningerne til deres Apple-id for at gøre enheder aktive igen.

På enheder under tilsyn kan MDM-løsningen arkivere en tilsidesættelses-kode, når Aktiveringslås slås til, eller senere bruge denne kode til automatisk at slå Aktiveringslås fra, når enheden skal slettes og tildeles en ny bruger.

Aktiveringslås er som standard aldrig slået til på enheder under tilsyn, selvom brugeren har slået Find min iPhone til. En MDM-løsning kan imidlertid hente en tilsidesættelseskode og tillade, at Aktiveringslås slås til på enheden. Hvis Find min iPhone er slået til, når MDM-løsningen slår Aktiveringslås til, aktiveres låsen på dette tidspunkt. Hvis Find min iPhone er slået fra, når MDM-løsningen slår Aktiveringslås til, aktiveres låsen, næste gang brugeren aktiverer Find min iPhone.

På enheder, der bruges til uddannelse med et administreret Apple-id, som er oprettet via Apple School Manager, kan Aktiveringslås knyttes til en administrators Apple-id i stedet for brugerens Apple-id eller slås fra ved hjælp af enhedens tilsidesættelseskode.

Skærmtid

Skærmtid er en funktion i iOS 12, der giver en bruger mulighed for at forstå og kontrollere deres eget eller deres børns brug af apps og websteder. Brugerne kan:

- Se brugsdata
- Indstille begrænsninger for brug af apps eller websteder
- Konfigurere Skærmfri tid
- Gennemtvinge yderligere begrænsninger

Hvis en bruger administrerer deres egen enhed, kan betjeningsmuligheder for Skærmtid og brugsdata synkroniseres på tværs af enheder, der er knyttet til den samme iCloud-konto vha. CloudKit-kryptering fra start til slut. Det kræver, at tofaktorgodkendelse er slået til i brugerens konto (synkronisering er som standard slået fra). Skærmtid erstatter funktionen Begrænsninger i tidligere versioner af iOS.

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-enheder til at forstå og kontrollere deres børns brug. Hvis en forælder er familiearrangør (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 eget brug. Når forældre slår Skærmtid til for deres børn, kan de indstille en adgangskode, så børnene ikke kan foretage nogen ændringer. Når børnene fylder 18 år (afhængigt af land og område), kan de slå denne overvågning fra.

Brugsdata og konfigurationsindstillinger overføres mellem forælderens og barnets enhed vha. en forbindelse til IDS, der er krypteret fra start til slut. Krypterede data lagres muligvis midlertidigt på IDS-servere, indtil de læses af den modtagende enhed (f.eks. så snart iPhone/iPad 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
- Er Skærmtid slået til

- Er Skærmfri tid slået til
- Antal gange der blev anmodet om mere tid
- Antal af apptidsgrænser

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 appsymbolerne hentet direkte fra App Store, og de indeholder ikke nogen data fra disse anmodninger.

Håndtering af Anonymitet

Apple lægger vægt på at beskytte kunders identitet og har utallige indbyggede betjeningsmuligheder og indstillinger, som iOS-brugerne kan benytte til at bestemme, hvordan og hvornår apps må bruge deres oplysninger, og hvilke oplysninger der må bruges.

Lokalitetstjenester

Lokalitetstjenester bruger GPS, Bluetooth og data fra brugere om placering af Wi-Fi-hotspots og mobilmaster til at bestemme brugerens omtrentlige lokalitet. Lokalitetstjenester kan slås fra med en enkelt betjeningsmulighed i Indstillinger, eller brugerne kan godkende adgangen for hver app, som bruger tjenesterne. Apps kan enten anmode om kun at modtage lokalitetsdata, når appen bruges, eller altid. Brugerne kan vælge ikke at tillade adgang, og de kan altid ændre deres valg i Indstillinger. I Indstillinger kan adgangen indstilles til Aldrig, Ved brug eller Altid, afhængigt af den brug af lokaliteten, appen har anmodet om. Hvis apps, der har fået tilladelse til altid at bruge lokaliteten, benytter tilladelsen, mens de afvikles i baggrunden, mindes brugerne om deres godkendelse og kan ændre appens adgang.

Brugerne kan desuden styre systemtjenesters brug af lokalitetsoplysninger på et detaljeret niveau. Det omfatter muligheden for at slå følgende fra: inkludering af lokalitetsoplysninger i de data, der indsamles af de analysetjenester, som Apple bruger til at forbedre iOS, lokalitetsbaserede Siri-oplysninger, lokalitetsbaseret kontekst til søgninger med Siri-forslag, lokale trafikforhold og vigtige lokaliteter, brugeren tidligere har besøgt.

Adgang til personlige data

iOS hjælper med at forhindre apps i at få adgang til en brugers personlige oplysninger uden tilladelse. Desuden kan brugerne i Indstillinger se, hvilke apps de har givet adgang til bestemte oplysninger, og tildele adgang eller tilbagekalde adgangen. Det gælder adgangen til:

- Kontakter
- Kalendere
- Påmindelser
- Fotos
- Fysisk aktivitet og fitness
- Lokalitetstjenester
- Apple Music
- Din musik- og videoaktivitet
- Mikrofon
- Kamera
- HomeKit
- Sundhed
- Talegenkendelse
- Bluetooth-deling
- Dit mediebibliotek

Hvis brugeren logger ind på iCloud, får apps som standard adgang til iCloud Drive. Brugerne kan styre hver apps adgang under iCloud i Indstillinger. iOS har desuden begrænsninger, der forhindrer, at data flyttes mellem apps og konti, der er installeret af en MDM-løsning, og dem, der er installeret af brugeren.

Politik med hensyn til beskyttelse af kunders identitet

Du kan læse Apples anonymitetspolitik her:
https://www.apple.com/legal/privacy/dk

Sikkerhedscertifikater og -programmer

Bemærk: Du finder de nyeste oplysninger om sikkerhedscertificeringer, godkendelser og vejledning til iOS i https://support.apple.com/HT202739

ISO 27001- og 27018-certificeringer

Apple har fået ISO 27001- og ISO 27018-certificeringer inden for styring af informationssikkerhed for den infrastruktur, udvikling og drift, der understøtter disse produkter og tjenester: Apple School Manager, iTunes U, iCloud, iMessage, FaceTime, Administrerede Apple-id'er, Siri og Skolearbejde i overensstemmelse med Statement of Applicability v2.1 dateret 11-07-2017. Apples overholdelse af ISO-standarder er certificeret af British Standards Institution. BSI-webstedet har certifikater, der viser overholdelse af ISO 27001 og ISO 27018. Du kan se certifikaterne her:

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Kryptografisk validering (FIPS 140-2)

De kryptografiske moduler i iOS er gentagne gange godkendt med hensyn til overholdelse af de amerikanske FIPS-standarder (Federal Information Processing Standards) 140-2 i forbindelse med frigivelsen af alle nye versioner fra og med iOS 6. Apple sender modulerne til CMVP til fornyet godkendelse, hver gang en større version af iOS-operativsystemet frigives. Dette program godkender integriteten ved kryptografiske funktioner til apps fra Apple og tredjeparter, som benytter de kryptografiske tjenester og godkendte algoritmer i iOS korrekt.

Apple har modtaget FIPS 140-2-godkendelse af det integrerede hardwaremodul kaldet **Apple Secure Enclave Processor (SEP) Secure Key Store (SKS) Cryptographic Module, hvilket muliggør godkendt brug af** SEP-genererede og -administrerede nøgler. Apple vil arbejde på at opnå godkendelse af hardwaremodulet på stadig højere niveau for hver større iOS-udgivelse, som det måtte være hensigtsmæssigt.

Common Criteria-certificering (ISO 15408)

Siden frigivelsen af iOS 9 har Apple opnået ISO-certificeringer af hver større version af iOS i henhold til Common Criteria-certificerings-programmet og har udvidet certificeringen til at dække følgende:

- Grundlæggende beskyttelsesbeskrivelse til mobile enheder
  - Udvidet pakke til administrationsagenter til mobile enheder
  - Udvidet pakke til klienter på trådløse netværk
  - PP-modul til VPN-klient
- Beskyttelsesbeskrivelse af programsoftware
  - Udvidet pakke til webbrowsere
- Apple har til hensigt at udvide certificeringen for hver større udgave af iOS.

Apple har påtaget sig en aktiv rolle i ITC (International Technical Community) med hensyn til udvikling af cPP'er (samarbejdende beskyttelsesbeskrivelser), som ikke er tilgængelige på nuværende tidspunkt, med fokus på evaluering af vigtig sikkerhedsteknologi til mobile enheder. Apple evaluerer og arbejder fortsat på at opnå certificeringer i forhold til nye og opdaterede versioner af de cPP'er, der er tilgængelige i øjeblikket og under udvikling.

CSfC (Commercial Solutions for Classified)

Hvor det er relevant, har Apple også sendt iOS-platformen og diverse tjenester til inkludering i programkomponentlisten til CSfC (Commercial Solutions for Classified). Når Apple-platforme og -tjenester er underlagt CCC-certificeringer, bliver de også sendt til inkludering under program-komponentlisten til CSfC.

Du kan se de nyeste komponenter på listen her:
https://www.nsa.gov/resources/everyone/csfc/components-list/

Vejledninger i sikkerhedskonfiguration

Apple har i samarbejde med myndigheder i hele verden udviklet vejledninger med instruktioner og anbefalinger til vedligeholdelse af et mere sikkert miljø. Dette kaldes også "device hardening" i højrisikomiljøer. Disse vejledninger indeholder definerede og godkendte oplysninger om, hvordan indbyggede funktioner i iOS kan konfigureres og bruges til at opnå bedre beskyttelse.

Apples sikkerhedsdusører

Apple belønner personer, der deler oplysninger om alvorlige problemer med Apple. Personer, der ønsker at komme i betragtning til en sikkerheds-dusør fra Apple, skal levere en tydelig rapport og et bevis på deres påstand. Sårbarheden skal berøre den senest leverede iOS-version og (hvis det er relevant) den nyeste hardware. Det beløb, der udbetales, afgøres efter Apples gennemgang. Kriterierne omfatter blandt andet, hvem der rapporterede sårbarheden først, nye funktioner, risikosandsynligheden og graden af nødvendig brugerinteraktion.

Når problemerne er delt på korrekt vis, forpligter Apple sig til at løse bekræftede problemer så hurtigt som muligt. Hvis det er relevant, vil Apple nævne anmelderens bidrag offentligt, medmindre dette ikke ønskes.

Kategori	Største betaling (i USD)
Firmwarekomponenter til sikker start	USD200.000
Udtræk af fortroligt materiale, der er beskyttet af Secure Enclave	USD100.000
Afvikling af tilfældig kode med kerneprivilegier	USD50.000
Uautoriseret adgang til iCloud-kontodata på Apple-servere	USD50.000
Adgang fra en proces i sandbox til brugerdata uden for sandbox	USD25.000

Apple matcher donationer af dusøren til kvalificerede velgørende organisationer.

Du kan få flere oplysninger om rapportering af fejl til Apple her: https://developer.apple.com/bug-reporting/

Konklusion

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 virksomhedsdata i et virksomhedsmiljø.

Sikkerheden er indbygget i iOS. Alt det, en virksomhed har brug for, er tilgængeligt på iOS-platformen, lige fra selve platformen over netværket til appene. Disse komponenter danner tilsammen sikkerheden i iOS, der er førende i branchen, uden at give køb på brugeroplevelsen.

Apple bruger en ensartet, integreret infrastruktur til sikkerhed i hele iOS og i økosystemet med iOS-apps. Hardwarebaseret kryptering af lagrede data giver mulighed for at slette en enhed eksternt, hvis enheden mistes, og sætter brugerne i stand til at fjerne alle virksomhedsdata og personlige oplysninger helt, før en enhed sælges eller overdrages til en ny ejer. Diagnosticeringsoplysninger indsamles også anonymt.

iOS-apps fra Apple er udviklet med øget sikkerhed for øje. F.eks. krypterer iMessage og FaceTime kommunikationen mellem klienter. Når det gælder apps fra tredjeparter, giver kombinationen af krav om kodesignering, afvikling i et isoleret miljø (“sandbox”) og berettigelser brugerne en brancheførende beskyttelse mod virus, malware og andre angreb. App Store-indsendelsesprocessen beskytter brugerne yderligere mod disse risici, da alle iOS-apps gennemses, før de gøres tilgængelige.

Virksomheder 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 iOS-platformen.

Apple har et sikkerhedsteam, der udelukkende beskæftiger sig med at yde support til Apples produkter. Teamet foretager sikkerhedsrevisioner og -test af såvel produkter, der er ved at blive udviklet, som af frigivne produkter. Apples team tilbyder også sikkerhedsværktøjer og -uddannelse og overvåger løbende rapporter om nye problemer og trusler i forbindelse med sikkerhed. Apple er medlem af FIRST (Forum of Incident Response and Security Teams).

Du kan få mere at vide om, hvordan du rapporterer problemer til Apple og abonnerer på sikkerhedsmeddelelser, her:
https://support.apple.com/HT201220

Ordliste

APNs (Apple Push Notification service)	En tjeneste, som Apple tilbyder i hele verden, der sørger for push-meddelelser til iOS-enheder.
arkivnøgle	Den AES-256-bit nøgle, der bruges 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 i iOS 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. I iOS 5 og nyere versioner har alle systemapps og systembiblioteker en tilfældig placering. Det samme gælder apps fra tredjeparter, der er kompileret som positionsuafhængige programarkiver.
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 af SoC-hardwareflag, som software kan bruge til at spore de startfunktioner, som enheden har anvendt, f.eks. DFU-funktion og gendannelsesfunktion. Når først et BPR-flag er blevet sat, kan det ikke slettes. Det betyder, at efterfølgende software kan få en pålidelig indikation af systemets tilstand.
Databeskyttelse	Mekanisme til beskyttelse af arkiver og nøglering i iOS. Mekanismen kan også referere til de API'er, som apps bruger til at beskytte arkiver og emner i nøgleringen.
DFU (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 er startet, vises følgende meddelelse: "iTunes har fundet en iPad, som er indstillet til gendannelse. Du skal gendanne denne iPad, før du kan bruge den med iTunes."
ECDHE (Elliptic Curve Diffie-Hellman Exchange)	Diffie-Hellman-nøgleudveksling baseret på en elliptisk kurve med flygtige 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	En algoritme til digital signatur baseret på elliptisk kurve-kryptografi.
ECID (Exclusive Chip Identification)	Et processor-id på 64 bit, der er forskelligt på alle iOS-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 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.
Gendannelsesfunktion	Gendannelsesfunktion bruges til at gendanne en iOS- eller Apple TV-enhed, hvis: • iTunes ikke genkender din enhed eller siger, at den er i Gendannelsesfunktion. • Skærmen med Apple-logoet fryser i adskillige minutter uden nogen statuslinje. • Skærmen Opret forbindelse til iTunes vises.

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.
iBoot	Kode, der indlæser XNU som led i den sikre start. Afhængigt af SoC-generationen bliver iBoot muligvis indlæst af LLB 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.
JTAG (Joint Test Action Group)	Et standardværktøj til hardwarefejlfinding, som bruges af programmører og mikrochipudviklere.
kombination af nøgler	Den proces, hvor en brugers adgangskode omdannes til en kryptografisk nøgle og forstærkes med enhedens UID. Det sikrer, 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.
kortlægning af rillers vinkel og forløb	En matematisk gengivelse af retning og bredde på riller, der udgør en del af et fingeraftryk.
LLB (Low-Level Bootloader)	Kode, der startes af Boot ROM, og som derefter indlæser iBoot som led i den sikre start, på systemer med startarkitektur i to trin.
nøgleindpakning	Kryptering af en nøgle sammen med en anden nøgle. iOS bruger NIST AES-nøgleindpakning i henhold til RFC 3394.
Nøglering	Den infrastruktur og det sæt API'er, som bruges af iOS og apps fra tredjeparter til at arkivere og hente adgangskoder, nøgler og andre følsomme godkendelsesoplysninger.
nøglesamling	En datastruktur, hvori der opbevares en samling klassenøgler. Hver type (bruger, enhed, system, sikkerhedskopi, depot eller iCloud-sikkerhedskopi) har samme format: • En header, der indeholder: – Version (indstillet til tre i iOS 5) – Type (system, sikkerhedskopi, depot eller iCloud-sikkerhedskopi) – UUID til nøglesamling – En HMAC-kode, hvis nøglesamlingen er signeret – 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 databeskyttelsesklasse til arkiver eller nøgleringe det drejer sig om) – Indpakningstype (kun nøgle afledt af UID eller nøgle afledt af UID og nøgle afledt af adgangskode) – Indpakket klassenøgle – Offentlig nøgle til asymmetriske klasser
Programbeskrivelse	En plist (egenskabsliste) signeret af Apple, som indeholder et sæt egenskaber og berettigelser, der tillader, at apps installeres og testes på en iOS-enhed. En programbeskrivelse til udvikling indeholder en liste med de enheder, som en udvikler har valgt til ad hoc-distribution, og en programbeskrivelse til distribution indeholder id'et til en app udviklet af en virksomhed.
SCIP (System Coprocessor Integrity Protection)	Systemhjælpeprocessorer er CPU'er på samme SoC som programprocessoren.
SoC (system on chip)	Et integreret kredsløb (IC), der samler flere komponenter på en enkelt chip. Programprocessoren, 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 OS 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.
styreenhed til hukommelse	Subsystemet i SoC'en, der styrer grænsefladen mellem SoC'en og dens hovedhukommelse.
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.
XNU	Kernen i hjertet af iOS- og macOS-operativsystemerne. Den betragtes som godkendt og sørger for, at sikkerhedsforanstaltninger såsom kodesignering, afvikling i et isoleret miljø (”sandbox”), kontrol af berettigelse og ASLR overholdes.

Dokumentrevisionshistorik

Dato	Resume
Maj 2019	**Opdateret til iOS 12.3** • Understøttelse af TLS 1.3 • Revideret beskrivelse af AirDrop-sikkerhed • DFU-funktion og Gendannelsesfunktion • Adgangskodekrav 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- og gendannelsesfunktion • HomeKit TV-fjernbetjeningstilbehør • Kontaktfrie kort • Studiekort • Siri-forslag • Genveje i Siri • Appen Genveje • Administration af brugeradgangskode • Skærmtid • Sikkerhedscertifikater og programmer
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 **Opdateret til iOS 11.1** • Sikkerhedscertifikater og -programmer • Touch ID/Face ID • Delte noter • CloudKit-kryptering fra start til slut • TLS • Apple Pay, betaling med Apple Pay på internettet • Siri-forslag • Delt iPad

Dato	Resume
Juli 2017	**Opdateret til iOS 10.3** • System Enclave • Beskyttelse af arkivdata • Nøglesamlinger • Sikkerhedscertifikater og programmer • SiriKit • HealthKit • Netværkssikkerhed • Bluetooth • Delt iPad • Funktionen Mistet • Aktiveringslås • Håndtering af Anonymitet
Marts 2017	**Opdateret til iOS 10** • Systemsikkerhed • Databeskyttelsesklasser • Sikkerhedscertifikater og programmer • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Log ind en gang (Single Sign-On) • Apple Pay, betaling med Apple Pay på internettet • Anvendelse af kreditkort, debetkort og forudbetalte kort • Safari-forslag
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

Dato	Resume
September 2015	**Opdateret til iOS 9** • Aktiveringslås på Apple Watch • Politikker til adgangskoder • API-understøttelse af Touch ID • Databeskyttelse på A8 bruger AES-XTS • Nøglesamlinger til uovervåget softwareopdatering • Certificeringsopdateringer • Model for appgodkendelse 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 • Model for pardannelse i iOS • Apple Configurator 2 • Begrænsninger

Maj 2019