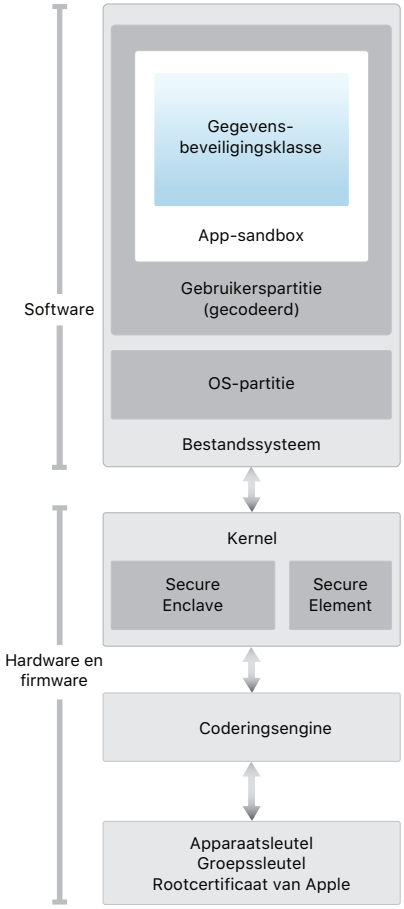
iOS-beveiliging

iOS 11

Januari 2018

Inhoud

Inleiding



Schematisch overzicht van de beveiligingsarchitectuur van iOS met de verschillende technologieën die in dit document aan bod komen.

Bij de ontwikkeling van het Apple iOS-platform heeft veiligheid centraal gestaan. In ons streven om het best mogelijke platform voor mobiele apparaten te bouwen, hebben we op basis van onze jarenlange ervaring een compleet nieuwe architectuur ontwikkeld. In verband met de veiligheidsrisico's van de desktopomgeving is in het ontwerp van iOS een nieuwe beveiligingsaanpak geïntroduceerd. Ook hebben we innovatieve functies ontworpen en geïmplementeerd die voor een nog betere mobiele beveiliging zorgen en die standaard het volledige systeem beschermen. Het eindresultaat is dat iOS een veel betere beveiliging voor mobiele apparaten biedt.

Op elk iOS-apparaat wordt gebruikgemaakt van software, hardware en voorzieningen die gezamenlijk een maximale beveiliging en een transparante gebruikerservaring bieden. iOS beveiligt niet alleen het apparaat en de bijbehorende gegevens wanneer daar niet mee wordt gewerkt; de beveiliging geldt voor het volledige ecosysteem, dus voor alles wat gebruikers lokaal, op netwerken en met belangrijke internetvoorzieningen doen.

iOS en iOS-apparaten bieden geavanceerde beveiligingsvoorzieningen, maar zijn toch heel gebruiksvriendelijk. Veel van deze voorzieningen zijn standaard ingeschakeld, zodat IT-afdelingen geen kostbare tijd kwijt zijn aan uitgebreide configuraties. Daarnaast zijn belangrijke beveiligingsvoorzieningen zoals apparaatcodering niet aanpasbaar, om te voorkomen dat ze per ongeluk worden uitgeschakeld door gebruikers. Andere voorzieningen, zoals Face ID, zorgen voor een betere gebruikerservaring, doordat het apparaat eenvoudiger en intuïtiever kan worden beveiligd.

In dit document wordt beschreven welke beveiligingstechnologieën en -voorzieningen in het iOS-platform zijn geïntegreerd. Ook kunnen organisaties in dit document lezen hoe ze de beveiligingstechnologieën en -voorzieningen van het iOS-platform kunnen combineren met hun eigen beleid en procedures om zo in specifieke beveiligingsbehoeften te voorzien.

Dit document is onderverdeeld in de volgende onderwerpen:

- **Systeembeveiliging:** de geïntegreerde, veilige software en hardware die het platform voor de iPhone, iPad en iPod touch vormen.
- **Codering en beveiliging van gegevens:** de architectuur en het ontwerp die ervoor zorgen dat gegevens ook veilig zijn wanneer het apparaat zoekraakt of gestolen wordt, of wanneer een onbevoegde gebruiker gegevens probeert te gebruiken of te wijzigen.
- **Beveiliging van apps:** de systemen die ervoor zorgen dat apps veilig kunnen worden gebruikt zonder de integriteit van het platform in gevaar te brengen.
- **Netwerkbeveiliging:** standaardnetwerkprotocollen die ervoor zorgen dat tijdens de overdracht van gegevens een veilige identiteitscontrole plaatsvindt en dat gegevens worden gecodeerd.
- **Apple Pay:** de technologie van Apple voor veilige betalingen.
- **Internetvoorzieningen:** de netwerkinfrastructuur van Apple voor het versturen en ontvangen van berichten, het synchroniseren van gegevens en het maken van reservekopieën.
- **Apparaatbeheer:** methoden waarmee iOS-apparaten kunnen worden beheerd en beveiligd tegen ongeoorloofd gebruik en waarmee bij verlies of diefstal gegevens op een apparaat op afstand kunnen worden gewist.
- **Privacybeheer:** voorzieningen van iOS waarmee de toegang tot locatievoorzieningen en gebruikersgegevens kunnen worden beheerd.

Systeembeveiliging

De DFU-modus (Device Firmware Upgrade) activeren
Als een apparaat vanuit de DFU-modus wordt hersteld, wordt een toestand hersteld waarvan bekend is dat die goed werkt, met de zekerheid dat er alleen ongewijzigde, door Apple ondertekende code aanwezig is. De DFU-modus kan handmatig worden geactiveerd. Sluit het apparaat eerst met een USB-kabel op een computer aan.

Vervolgens:

Op iPhone X, iPhone 8 of iPhone 8 Plus: Druk kort op de knop voor Volume omhoog. Druk kort op de knop voor Volume omlaag. Houd vervolgens de zijknop ingedrukt totdat je het scherm van de herstelmodus ziet.

Op iPhone 7 of iPhone 7 Plus: Houd de zijknop en de knop voor Volume omlaag tegelijk ingedrukt. Houd de knoppen ingedrukt totdat je het scherm van de herstelmodus ziet.

Op iPhone 6s en oudere modellen, iPad of iPod touch: Houd de thuisknop en de knop aan de bovenkant (of zijkant) tegelijk ingedrukt. Houd de knoppen ingedrukt totdat je het scherm van de herstelmodus ziet.

Opmerking: Het scherm is leeg wanneer de DFU-modus actief is. Als het Apple logo verschijnt, heb je te lang op de sluimerknop gedrukt.

De systeembeveiliging is zo opgezet dat software en hardware in alle kerncomponenten van elk iOS-apparaat zijn beveiligd. Dit geldt voor het opstartproces, software-updates en Secure Enclave. Deze architectuur is essentieel voor de beveiliging in iOS, maar vormt nooit een obstakel voor de bruikbaarheid van een apparaat.

De nauwe integratie van hardware, software en voorzieningen in iOS-apparaten zorgt ervoor dat elk onderdeel van het systeem wordt vertrouwd en dat het systeem in zijn geheel wordt gevalideerd. Vanaf het moment dat het apparaat wordt opgestart tot en met het moment waarop updates voor iOS en apps van andere leveranciers worden geïnstalleerd, wordt elke stap uitvoerig geanalyseerd en gevalideerd om ervoor te zorgen dat de hardware en software optimaal samenwerken en de resources op de juiste manier wordt gebruikt.

Beveiligd opstartproces

Elke stap van het opstartproces omvat onderdelen die cryptografisch door Apple worden ondertekend om de integriteit te waarborgen. De volgende stap in het proces wordt pas uitgevoerd nadat de vertrouwensketen is geverifieerd. Het betreft hier onderdelen zoals bootloaders, de kernel, kernelextensies en baseband-firmware. Dit beveiligde opstartproces zorgt ervoor dat er niet met de software op de laagste niveaus kan worden geknoeid.

Zodra een iOS-apparaat wordt ingeschakeld, wordt meteen code uit het alleen-lezengeheugen (ook wel het "opstart-ROM" genoemd) uitgevoerd. Deze onveranderlijke code wordt vastgelegd tijdens de fabricage van de chip en wordt daardoor onvoorwaardelijk vertrouwd. De opstart-ROM-code bevat de publieke sleutel van de rootcertificaatautoriteit van Apple. Deze sleutel wordt gebruikt om te controleren of de iBoot-bootloader door Apple is ondertekend voordat de bootloader wordt geladen. Dit is de eerste stap in de vertrouwensketen. Elke stap is nodig om ervoor te zorgen dat de volgende stap in de keten door Apple wordt ondertekend. Wanneer de iBoot-taken zijn voltooid, wordt de iOS-kernel gecontroleerd en vervolgens gestart. Bij apparaten met een S1-processor of een A9-processor of lager wordt een extra LLB-fase (Low-Level Bootloader) geladen en door het opstart-ROM gecontroleerd. Vervolgens wordt hiermee iBoot geladen en gecontroleerd.

Als de LLB (in oudere apparaten) of iBoot (in nieuwere apparaten) niet door het opstart-ROM kan worden geladen, schakelt het apparaat over naar de DFU-modus. Als de LLB of iBoot niet kan worden geladen of als het volgende proces niet kan worden geverifieerd, wordt het opstartproces onderbroken en wordt het scherm 'Verbind met iTunes' op het apparaat weergegeven. Dit wordt de "herstelmodus" genoemd. In dat geval moet het apparaat via USB met iTunes worden verbonden en moeten de fabrieksinstellingen worden hersteld.

Op apparaten die toegang tot een mobiel netwerk hebben, hanteert het baseband-subsysteem ook een eigen, vergelijkbaar veilig opstartproces met ondertekende software en sleutels die door de baseband-processor zijn gecontroleerd.

Voor apparaten met een Secure Enclave gebruikt de Secure Enclave-coprocessor ook een veilig opstartproces om zijn eigen software te laten controleren en ondertekenen door Apple. Zie het gedeelte "Secure Enclave" in dit document.

Voor meer informatie over het handmatig activeren van de herstelmodus ga je naar: https://support.apple.com/nl-nl/HT1808

Autorisatie van systeemsoftware

Apple brengt regelmatig software-updates uit om nieuwe beveiligingsproblemen aan te pakken en om nieuwe functies beschikbaar te stellen. Deze updates worden voor alle ondersteunde apparaten tegelijk aangeboden. Gebruikers ontvangen op hun apparaat en via iTunes een melding voor de iOS-update. De updates worden draadloos aangeboden om ervoor te zorgen dat de meest recente beveiligingsupdates snel worden geïnstalleerd.

Het eerder beschreven opstartproces zorgt er ook voor dat alleen door Apple ondertekende code op een apparaat kan worden geïnstalleerd. Om te voorkomen dat op apparaten een downgrade wordt uitgevoerd naar oudere versies waarin niet de meest recente beveiligingsupdates zijn opgenomen, wordt in iOS het proces *Autorisatie van systeemsoftware* gebruikt. Wanneer een downgrade zou kunnen worden uitgevoerd, zou een aanvaller die het beheer van een apparaat heeft overgenomen, een oudere versie van iOS kunnen installeren en vervolgens misbruik kunnen maken van een beveiligingsrisico dat in de nieuwere versie is verholpen.

Op apparaten met Secure Enclave gebruikt de Secure Enclave-coprocessor Autorisatie van systeemsoftware om de integriteit van zijn eigen software te waarborgen en downgrades te voorkomen. Zie het gedeelte "Secure Enclave" in dit document.

Software-updates voor iOS kunnen via iTunes of draadloos op het apparaat worden geïnstalleerd. Als de update via iTunes verloopt, wordt er een volledige kopie van iOS gedownload en geïnstalleerd. Bij draadloze software-updates worden alleen de onderdelen gedownload die nodig zijn om de update uit te voeren. Omdat hierbij niet het volledige OS hoeft te worden gedownload, is dit beter voor de netwerkefficiency. Daarnaast kunnen software-updates ook worden opgeslagen in de cache van een Mac met macOS High Sierra waarbij materiaalcaching is ingeschakeld, zodat iOS-apparaten de benodigde update niet meer opnieuw via het internet hoeven te downloaden. Ze moeten nog wel contact maken met Apple servers om het updateproces te voltooien.

Tijdens een iOS-upgrade maakt iTunes (of het apparaat zelf, in het geval van een draadloze software-update) verbinding met de Apple server die autorisatie voor de installatie geeft. Daarbij wordt een lijst met cryptografische meetwaarden verstuurd voor elk onderdeel van de installatiebundel dat moet worden geïnstalleerd (zoals iBoot, de kernel en de OS-image). Ook worden een willekeurige anti-replay-waarde (nonce) en de unieke ID van het apparaat (ECID) verstuurd.

Op de autorisatieserver wordt de ontvangen lijst met meetwaarden vergeleken met de versies waarvoor installatie is toegestaan. Als er een match wordt gevonden, wordt de ECID toegevoegd aan de meetwaarde en wordt het resultaat ondertekend. De server verstuurt tijdens het upgradeproces een complete set ondertekende gegevens naar het apparaat. Het toevoegen van de ECID zorgt ervoor dat de autorisatie voor het aanvragende apparaat wordt 'gepersonaliseerd'. Aangezien de server alleen bekende meetwaarden autoriseert en ondertekent, kan op deze manier worden gegarandeerd dat de update precies wordt uitgevoerd zoals die door Apple wordt aangeboden.

Met de evaluatie van de vertrouwensketen tijdens het opstarten wordt gecontroleerd of de handtekening afkomstig is van Apple en of de meetwaarde van het onderdeel dat van schijf is geladen, in combinatie met de ECID van het apparaat, overeenkomt met de gegevens waarvoor de handtekening is verkregen.

Deze stappen garanderen dat de autorisatie is verleend voor een specifiek apparaat en dat een oude iOS-versie niet van het ene naar het andere apparaat kan worden gekopieerd. De nonce voorkomt dat een aanvaller de respons van de server kan bewaren, om deze vervolgens te gebruiken om een apparaat te manipuleren of om de systeemsoftware op een andere manier aan te passen.

Secure Enclave

De Secure Enclave is een coprocessor die is verwerkt in Apple T1-processors, Apple S2-processors, Apple S3-processors, Apple A7-processors en nieuwere processors uit de A-serie. De Secure Enclave maakt gebruik van gecodeerd geheugen en omvat een hardwarematige RNG (Random Number Generator). De Secure Enclave voert alle cryptografische bewerkingen voor het beheer van gegevensbeveiligingssleutels uit en waarborgt de integriteit van de gegevensbeveiliging, ook als de kernel is aangetast. Communicatie tussen de Secure Enclave en de hoofdprocessor vindt uitsluitend plaats via een met interrupts aangestuurde mailbox en gedeelde geheugenbuffers.

De Secure Enclave werkt met een door Apple aangepaste L4-microkernel. Deze microkernel is door Apple ondertekend, is als onderdeel van het beveiligde opstartproces van iOS geverifieerd en is bijgewerkt via een gepersonaliseerd software-updateproces.

Tijdens het opstarten van het apparaat wordt er een tijdelijke (ephemeral) sleutel aangemaakt, die wordt gecombineerd met de UID van het apparaat. Vervolgens wordt met deze sleutel het gedeelte van de geheugenruimte van het apparaat gecodeerd dat voor de Secure Enclave is gereserveerd. Behalve bij de Apple A7 wordt het geheugen van de Secure Enclave ook met de tijdelijke sleutel geverifieerd. Op de Apple A11 wordt een integriteitsstructuur gebruikt om replay van beveiligingskritisch Secure Enclave-geheugen te voorkomen. Dit geheugen wordt geverifieerd aan de hand van de tijdelijke sleutel en de nonces in het SRAM van de chip.

De gegevens die door de Secure Enclave in het bestandssysteem worden bewaard, worden bovendien gecodeerd met een sleutel die wordt gecombineerd met de UID en een anti-replay-teller. Anti-replay-voorzieningen in de Secure Enclave worden gebruikt voor het intrekken van gegevens over gebeurtenissen die anti-replay-grenzen aangeven, waaronder de volgende:

- Toegangscode wijzigen
- Touch ID of Face ID in-/uitschakelen
- Vingerafdruk toevoegen/verwijderen
- Face ID opnieuw instellen
- Apple Pay-kaart toevoegen/verwijderen
- Alle inhoud en instellingen wissen

De Secure Enclave is ook verantwoordelijk voor het verwerken van vingerafdrukgegevens en gezichtsgegevens van de Touch ID- en Face ID-sensor. Als de gegevens worden herkend, wordt er toestemming gegeven om namens de gebruiker toegang te verlenen of aankopen te doen.

Touch ID

Touch ID is het systeem voor vingerafdrukregistratie waarmee iPhone en iPad op een veilige manier sneller en gemakkelijker toegankelijk zijn. Met deze technologie kunnen onder elke hoek vingerafdrukken worden gelezen. Bij elk gebruik wordt de vingerafdrukkaart uitgebreid met aanvullende overlappende knooppunten die worden herkend, zodat de vingerafdruk van de gebruiker gaandeweg steeds beter wordt herkend.

Face ID

Je hoeft maar naar iPhone X te kijken om het apparaat veilig te ontgrendelen. Face ID biedt intuïtieve en veilige verificatie met het TrueDepth-camerasysteem dat via geavanceerde technologie de geometrische kenmerken van je gezicht nauwkeurig in kaart brengt. Face ID controleert aan de hand van je kijkrichting of je aandacht op het apparaat is gericht en gebruikt dan neurale netwerken om de kijker te herkennen en bedrog tegen te gaan. Zo kun je je iPhone met een blik op het apparaat ontgrendelen. Face ID past zich automatisch aan je uiterlijke veranderingen aan en waarborgt de privacy en veiligheid van je biometrische gegevens.

Touch ID, Face ID en toegangscodes

Voor het gebruik van Touch ID of Face ID moet je op je apparaat instellen dat er een toegangscode nodig is om het apparaat te ontgrendelen. Als je met Touch ID of Face ID wordt herkend, wordt het apparaat ontgrendeld zonder dat je een toegangscode hoeft in te voeren. Hierdoor wordt het gebruik van langere en meer complexe toegangscodes een stuk praktischer, aangezien je de toegangscode minder vaak hoeft in te toetsen. Touch ID en Face ID vervangen je toegangscode niet, maar geven eenvoudig toegang tot je apparaat – binnen weloverwogen grenzen en tijdsbeperkingen. Dit is belangrijk, omdat een sterke toegangscode de basis vormt voor de cryptografische beveiliging van je iOS-apparaat.

In plaats van Touch ID of Face ID kun je altijd de toegangscode gebruiken. In de volgende gevallen is dit zelfs noodzakelijk:

- Het apparaat is net aangezet of herstart.
- Het apparaat is meer dan 48 uur niet ontgrendeld geweest.
- Het apparaat is in de afgelopen 156 uur (zes en een halve dag) niet met de toegangscode ontgrendeld en is in de afgelopen 4 uur niet met Face ID ontgrendeld.
- Het apparaat heeft een opdracht voor ontgrendeling op afstand ontvangen.
- Er zijn vijf mislukte pogingen gedaan om het apparaat met een vingerafdruk of met gezichtsherkenning te ontgrendelen.
- De functie voor uitschakelen/versturen van een SOS-noodmelding is geïnitieerd.

Als Touch ID of Face ID is ingeschakeld, wordt het apparaat vergrendeld zodra er op de zijknop wordt gedrukt of als de sluimerstand wordt geactiveerd. Telkens wanneer het apparaat uit de sluimerstand wordt gehaald, moet de gebruiker via Touch ID of Face ID worden herkend of moet de toegangscode worden ingevoerd.

De kans dat een willekeurig persoon naar je iPhone X kijkt en deze met Face ID ontgrendelt, is circa 1 op de 1.000.000 (en 1 op de 50.000 bij Touch ID). Voor extra veiligheid zijn bij zowel Touch ID als Face ID slechts vijf mislukte pogingen toegestaan; daarna moet de toegangscode worden ingevoerd om het apparaat te ontgrendelen. Met Face ID ligt de kans op een valse overeenkomst anders voor tweelingen en broers en zussen die op jou lijken. Ook voor kinderen onder de 13 is die kans anders, omdat hun gezichtskenmerken mogelijk nog niet volledig zijn ontwikkeld. Als je je hier zorgen over maakt, wordt je aangeraden om een toegangscode te gebruiken voor verificatie.

Touch ID-beveiliging

De vingerafdruksensor is alleen actief wanneer op de capacitieve stalen ring rond de thuisknop de aanraking van een vinger wordt gedetecteerd. Op dat moment wordt de geavanceerde imaging-matrix geactiveerd om de vinger te scannen en de scan naar de Secure Enclave te sturen. De communicatie tussen de processor en de Touch ID-sensor verloopt via een SPI-bus (Serial Peripheral Interface). De processor stuurt de gegevens door naar de Secure Enclave, maar kan de gegevens niet lezen. De gegevens worden gecodeerd en geverifieerd aan de hand van een sessiesleutel die is vastgesteld op basis van de gedeelde sleutel die voor elke Touch ID-sensor en de bijbehorende Secure Enclave in de fabriek is uitgegeven. De gedeelde sleutel is sterk, willekeurig en voor elke Touch ID-sensor anders. De uitwisseling van de sessiesleutel vindt plaats via key wrapping met AES, waarbij aan beide kanten een willekeurige sleutel wordt aangeboden op basis waarvan de sessiesleutel wordt vastgesteld. Het transport wordt gecodeerd via AES-CCM.

De scan van het raster wordt tijdens de analysevectorisatie tijdelijk in het gecodeerde geheugen van de Secure Enclave opgeslagen. Daarna wordt de scan verwijderd. Bij de analyse wordt de looprichting van de papillairlijnen onder een hoek afgelezen, waarbij de typicagegevens die nodig zouden zijn om de feitelijke vingerafdruk van de gebruiker te reconstrueren, worden genegeerd. De resulterende kaart met knooppunten wordt zonder identificerende gegevens opgeslagen in een gecodeerde indeling die alleen kan worden gelezen door de Secure Enclave. De kaart wordt nooit naar Apple verstuurd of opgenomen in een reservekopie van iCloud of iTunes.

Face ID-beveiliging

Face ID signaleert of de gebruiker zijn aandacht op de telefoon richt. Het systeem biedt een robuuste verificatie met een laag foutpercentage en gaat zowel digitaal als fysiek bedrog tegen.

De TrueDepth-camera zoekt automatisch naar je gezicht wanneer je iPhone X uit de sluimerstand haalt door deze op te pakken of door op het scherm te tikken. Dit gebeurt ook als iPhone X jou als gebruiker wil verifiëren om een binnengekomen bericht weer te geven, of wanneer een ondersteunde app om Face ID-verificatie vraagt. Als een gezicht wordt gedetecteerd en de persoon zijn of haar ogen open heeft en op het apparaat heeft gericht, wordt ervan uitgegaan dat die persoon het

apparaat wil ontgrendelen. Deze functie is uitgeschakeld wanneer VoiceOver is ingeschakeld, maar de functie kan eventueel ook apart worden uitgeschakeld.

Wanneer een aandachtig gezicht is gedetecteerd, worden met de TrueDepth-camera 30.000 infraroodpunten op het gezicht geprojecteerd en vervolgens afgelezen om een dieptekaart van het gezicht en een tweedimensionaal infraroodbeeld te maken. Op basis van deze gegevens wordt een reeks 2D-beelden en dieptekaarten aangemaakt, die digitaal worden ondertekend en naar de Secure Enclave worden gestuurd. Om zowel digitaal als fysiek bedrog tegen te gaan, worden de 2D-beelden en dieptekaartregistraties door de TrueDepth-camera in willekeurige volgorde gezet en wordt er een apparaatspecifiek willekeurig patroon geprojecteerd. In een deel van de neurale engine van de bionische A11-chip (dat binnen de Secure Enclave wordt beveiligd), worden deze gegevens omgezet in een wiskundige voorstelling die met de geregistreerde gezichtsgegevens wordt vergeleken. De geregistreerde gezichtsgegevens zijn zelf ook een wiskundige voorstelling van je gezicht zoals dat in een aantal verschillende houdingen is vastgelegd.

Gezichtsherkenning wordt binnen de Secure Enclave uitgevoerd met neurale netwerken die speciaal voor dat doel zijn getraind. We hebben de neurale netwerken voor gezichtsherkenning ontwikkeld op basis van meer dan een miljard beelden, waaronder infrarood- en dieptebeelden, die met toestemming van de onderzoeksdeelnemers zijn verzameld. Apple heeft met deelnemers van over de hele wereld gewerkt, zodat een representatieve groep mensen ontstond wat betreft onder andere geslacht, leeftijd en etniciteit. Het onderzoek is waar nodig aangevuld om voor uiteenlopende gebruikers een zo hoog mogelijke nauwkeurigheid te krijgen. Face ID is zo ontworpen dat ook hoofddeksels, sjaals, brillen, contactlenzen en de meeste zonnebrillen geen probleem opleveren. Bovendien werkt het systeem zowel binnen als buiten en zelfs in totale duisternis. Een aanvullend neuraal netwerk dat is getraind om bedrog te detecteren, beschermt tegen pogingen om je iPhone X met foto's of maskers te ontgrendelen.

Face ID-gegevens, waaronder wiskundige voorstellingen van je gezicht, zijn gecodeerd en alleen voor de Secure Enclave beschikbaar. Deze gegevens verlaten het apparaat nooit. Ze worden niet naar Apple gestuurd en ook niet in reservekopieën van het apparaat opgenomen. Bij normaal gebruik worden de volgende Face ID-gegevens gecodeerd bewaard om uitsluitend door de Secure Enclave te worden gebruikt:

- De wiskundige voorstellingen van je gezicht die tijdens de registratie van je gezicht worden berekend.
- De wiskundige voorstellingen van je gezicht die tijdens bepaalde ontgrendelpogingen worden berekend als deze zinvol worden beschouwd voor toekomstige gezichtsherkenning.

Gezichtsafbeeldingen die tijdens normaal gebruik worden vastgelegd, worden niet bewaard, maar meteen verwijderd nadat de wiskundige voorstelling ten behoeve van registratie of vergelijking met de geregistreerde Face ID-gegevens is berekend.

Ontgrendeling van een iOS-apparaat door Touch ID of Face ID

Als Touch ID of Face ID is uitgeschakeld en een apparaat wordt vergrendeld, worden de sleutels voor de hoogste gegevensbeveiligingsklasse (die in de Secure Enclave worden bewaard) verwijderd. De bestanden en sleutelhangeronderdelen in die klasse zijn pas toegankelijk nadat je het apparaat hebt ontgrendeld door de toegangscode in te voeren.

Als Touch ID of Face ID is ingeschakeld, worden de sleutels niet verwijderd wanneer het apparaat wordt vergrendeld. Ze worden dan 'ingepakt' met een sleutel die wordt doorgegeven aan het subsysteem van Touch ID of Face ID binnen de Secure Enclave. Als je probeert het apparaat te ontgrendelen en je vingerafdruk of gezicht wordt herkend, wordt de sleutel voor het 'uitpakken' van de sleutels van Gegevensbeveiliging verstuurd en wordt het apparaat ontgrendeld. Dit proces biedt extra beveiliging, doordat de subsystemen voor Gegevensbeveiliging en Touch ID of Face ID moeten samenwerken om het apparaat te ontgrendelen.

Wanneer het apparaat opnieuw wordt opgestart, zijn de sleutels die voor Touch ID of Face ID nodig zijn om het apparaat te ontgrendelen niet meer aanwezig. Deze worden door de Secure Enclave verwijderd wanneer een toegangscode moet worden ingevoerd (bijvoorbeeld wanneer het apparaat meer dan 48 uur niet is ontgrendeld of als er vijf mislukte pogingen tot vingerafdruk- of gezichtsherkenning zijn gedaan).

Om het ontgrendelingsproces te verbeteren en bij te blijven met natuurlijke veranderingen in je gezicht en veranderingen in je uiterlijk, wordt de wiskundige voorstelling in de loop van de tijd door Face ID aangevuld. Na de ontgrendeling kan de nieuwe berekende wiskundige voorstelling (mits van voldoende kwaliteit) voor een beperkt aantal volgende ontgrendelingen worden bewaard voordat de gegevens worden verwijderd. Als je niet door Face ID wordt herkend, maar de kwaliteit van de match wel boven een bepaalde drempelwaarde uitkomt en je meteen daarna de toegangscode invoert, wordt er opnieuw een opname van je gezicht gemaakt en worden de geregistreerde Face ID-gegevens aangevuld met de nieuwe berekende wiskundige voorstelling. Deze nieuwe Face ID-gegevens worden verwijderd als je op basis daarvan niet meer wordt herkend en nadat een bepaald aantal ontgrendelingen is uitgevoerd. Dankzij deze aanvullingen kan Face ID je ook herkennen als er ingrijpende veranderingen in je gezichtsbeharing of make-up zijn en worden onjuiste matches tot een minimum beperkt.

Touch ID, Face ID en Apple Pay

Je kunt Touch ID en Face ID ook met Apple Pay gebruiken om eenvoudig en veilig aankopen te doen in winkels, in apps en op het internet. Lees het gedeelte "Apple Pay" in dit document voor meer informatie over Touch ID en Apple Pay.

Om een betaling in de winkel met Face ID te autoriseren, moet je eerst je betaalintentie aangeven door dubbel op de zijknop te klikken. Vervolgens laat je je identiteit verifiëren met Face ID, waarna je je iPhone X dicht bij de lezer voor contactloos betalen houdt. Als je na de Face ID-verificatie een andere Apple Pay-betalingsmethode wilt kiezen, moet je je identiteit opnieuw laten verifiëren, maar hoef je niet opnieuw dubbel op de zijknop te klikken.

Om een betaling te doen in een app of in een webwinkel, geef je je betaalintentie aan door dubbel op de zijknop te klikken en vervolgens je identiteit te laten verifiëren met Face ID om de betaling te autoriseren. Als je Apple Pay-transactie niet binnen 30 seconden na je dubbele klik is voltooid, moet je je betaalintentie opnieuw aangeven door opnieuw dubbel op de zijknop te klikken.

Face ID-diagnose

Face ID-gegevens verlaten je apparaat nooit en worden ook niet in een reservekopie in iCloud of ergens anders bewaard. Alleen wanneer jij zelf voor ondersteuningskwesties diagnostische informatie van Face ID aan AppleCare wilt verstrekken, worden deze gegevens vanaf je apparaat verzonden. Voor het inschakelen van Face ID-diagnose is een digitaal ondertekende autorisatie van Apple vereist die vergelijkbaar is met degene die voor het personaliseren van software-updates wordt gebruikt. Na autorisatie kun je Face ID-diagnose activeren en de configuratie beginnen vanuit Instellingen op je iPhone X.

Tijdens de configuratie van Face ID-diagnose wordt je bestaande Face ID-registratie verwijderd en moet je je opnieuw bij Face ID registreren. In de daaropvolgende 10 dagen legt je iPhone X tijdens verificatiepogingen Face ID-beelden vast. Daarna stopt iPhone X automatisch met het bewaren van beelden. Face ID-diagnose stuurt niet automatisch gegevens naar Apple. Je kunt diagnostische informatie van Face ID, waaronder registratie- en ontgrendelingsbeelden die tijdens de diagnostische modus worden verzameld, beoordelen en goedkeuren voordat ze naar Apple worden verstuurd. Het gaat daarbij om beelden van zowel mislukte als geslaagde pogingen. Alleen de diagnostische Face ID-beelden die door jou zijn goedgekeurd worden geüpload. Bovendien worden de gegevens voor het uploaden gecodeerd en worden ze meteen van je iPhone X verwijderd nadat het uploaden is voltooid. Beelden die je afkeurt, worden meteen verwijderd.

Als je aan het einde van de sessie van Face ID-diagnose geen afbeeldingen beoordeelt en geen goedgekeurde exemplaren uploadt, wordt Face ID-diagnose automatisch na 40 dagen beëindigd en worden alle diagnostische beelden van je iPhone X verwijderd. Je kunt Face ID-diagnose bovendien op elk moment uitschakelen. In dat geval worden alle lokale beelden meteen verwijderd en worden er geen Face ID-gegevens met Apple gedeeld.

Andere toepassingen van Touch ID en Face ID

Apps van derden kunnen door het systeem aangeleverde API's gebruiken om de gebruiker te vragen zijn of haar identiteit te laten verifiëren met Touch ID, Face ID of een toegangscode. Apps die Touch ID ondersteunen, ondersteunen automatisch ook Face ID zonder dat daarvoor aanpassingen nodig zijn. Bij gebruik van Touch ID of Face ID krijgt de app alleen bericht of de verificatie is gelukt; de app heeft geen toegang tot Touch ID, Face ID of de gegevens die betrekking hebben op de geregistreerde gebruiker. Onderdelen in de sleutelhanger kunnen ook worden beveiligd met Touch ID of Face ID, waarbij de onderdelen alleen door de Secure Enclave worden vrijgegeven als er een overeenkomst is gevonden of als de toegangscode van het apparaat wordt ingevoerd. App-ontwikkelaars hebben API's om te controleren of de gebruiker een toegangscode heeft ingesteld voordat er om Touch ID, Face ID of een toegangscode wordt gevraagd om onderdelen in de sleutelhanger te ontgrendelen. App-ontwikkelaars kunnen het volgende doen:

- Afdwingen dat API-bewerkingen voor verificatie niet kunnen worden uitgevoerd met een programmawachtwoord of de toegangscode voor een apparaat. Ze kunnen nagaan of een gebruiker is geregistreerd en toestaan dat Touch ID of Face ID als tweede factor wordt gebruikt in beveilingsgevoelige apps.
- ECC-sleutels binnen de Secure Enclave genereren en gebruiken die met Touch ID of Face ID kunnen worden beveiligd. Bewerkingen met deze sleutels vinden altijd binnen de Secure Enclave plaats nadat het gebruik door de Secure Enclave is geautoriseerd.

Je kunt Touch ID of Face ID ook configureren voor het goedkeuren van aankopen in de iTunes Store, de App Store en de iBooks Store, zodat je niet meer het wachtwoord voor je Apple ID hoeft in te voeren. Bij iOS 11 en hoger worden door Touch ID en Face ID beveiligde Secure Enclave-ECC-sleutels gebruikt om de Store-aanvraag te ondertekenen en zo een aankoop te autoriseren.

Codering en beveiliging van gegevens

Alle inhoud en instellingen wissen
Met de optie 'Wis alle inhoud en instellingen' in Instellingen worden alle sleutels in Effaceable Storage permanent gewist, waardoor alle gebruikersgegevens op het apparaat cryptografisch ontoegankelijk worden. Dit is dus een ideale manier om ervoor te zorgen dat alle persoonlijke gegevens van een apparaat zijn verwijderd voordat je het apparaat aan iemand anders geeft of opstuurt voor onderhoud.

Belangrijk: Gebruik de optie 'Wis alle inhoud en instellingen' pas nadat je een reservekopie van het apparaat hebt gemaakt. Het is namelijk niet mogelijk om de verwijderde gegevens terug te halen.

Het beveiligde opstartproces, de code-ondertekening en de beveiliging van runtimeprocessen dragen allemaal bij aan een omgeving waarin alleen vertrouwde code en apps kunnen worden uitgevoerd op een apparaat. iOS biedt aanvullende voorzieningen voor codering en gegevensbeveiliging om de gegevens van de gebruiker te beschermen, zelfs wanneer andere elementen van de beveiligingsinfrastructuur zijn gemanipuleerd (zoals op een apparaat met niet-goedgekeurde aanpassingen). Dit biedt belangrijke voordelen voor zowel gebruikers als IT-beheerders, omdat persoonlijke en bedrijfsgegevens altijd zijn beveiligd en er methoden voorhanden zijn om apparaten meteen en volledig op afstand te wissen, bijvoorbeeld wanneer een apparaat kwijt of gestolen is.

Hardwarematige beveiligingsvoorzieningen

Voor mobiele apparaten zijn snelheid en een efficiënt voedingsgebruik essentieel. Cryptografische bewerkingen zijn complexe bewerkingen die de prestaties of de gebruiksduur van de accu nadelig kunnen beïnvloeden als ze zonder oog voor snelheid en voedingsefficiëntie zijn samengesteld en geïmplementeerd.

Elk iOS-apparaat heeft een speciale 256-bits AES-cryptografie-engine die is ingebouwd in het DMA-pad tussen de flash-opslag en het algemene systeemgeheugen, wat een uiterst efficiënte bestandscodering mogelijk maakt. Op A9-processors en nieuwere processors uit de A-serie bevindt het flash-opslagsubsysteem zich op een geïsoleerde bus die alleen via de DMA-cryptografie-engine toegang tot het geheugen met gebruikersgegevens heeft.

De unieke ID (UID) van het apparaat en een apparaatgroep-ID (GID) zijn 256-bits-AES-sleutels die tijdens het fabricageproces in de toepassingsprocessor en de Secure Enclave zijn aangebracht (UID) of gecompileerd (GID). De sleutels kunnen niet rechtstreeks door software of firmware worden gelezen. Het enige wat toegankelijk is, zijn de resultaten van de coderings- of decoderingsbewerkingen die worden uitgevoerd door speciale AES-engines gemaakt van silicium die de UID of GID als een sleutel gebruiken. Bovendien is het zo dat de UID en GID van de Secure Enclave alleen kunnen worden gebruikt door de AES-engine die voor de Secure Enclave is gereserveerd. De UID's en GID's zijn evenmin beschikbaar via JTAG of andere debugging-interfaces.

Op T1-, S2- en S3-processors, A9-processors en nieuwere processors uit de A-serie genereert elke Secure Enclave zijn eigen UID (unieke ID). Omdat de UID voor elk apparaat uniek is en volledig binnen de Secure Enclave wordt gegenereerd in plaats van buiten het apparaat, kan de UID niet door Apple of haar leveranciers worden opgevraagd of bewaard. Software in de Secure Enclave maakt van de UID gebruik om apparaatspecifieke geheimen te beveiligen.

Op basis van de UID kunnen gegevens cryptografisch aan een bepaald apparaat worden gekoppeld. De UID is bijvoorbeeld aanwezig in de sleutelhiërarchie die het bestandssysteem beveiligt. Dit houdt in dat de

bestanden ontoegankelijk worden als de geheugenchips fysiek van het ene apparaat naar het andere apparaat worden verplaatst. De UID staat los van andere ID's op het apparaat.

De GID is gelijk voor alle processors in apparaten van een bepaalde klasse (bijvoorbeeld alle apparaten met de Apple A8-processor).

Afgezien van de UID en GID, worden alle andere cryptografische sleutels aangemaakt door de RNG (Random Number Generator) van het systeem. Hierbij wordt gebruikgemaakt van een algoritme dat op CTR_DRBG is gebaseerd. De entropie van het systeem wordt hoofdzakelijk gegenereerd op basis van timingvariaties tijdens het opstarten en daarnaast op basis van interrupt-timing wanneer het apparaat eenmaal is opgestart. Voor de sleutels die binnen de Secure Enclave worden gegenereerd, wordt gebruikgemaakt van de hardwarematige RNG, waarbij wordt uitgegaan van meerdere ringoscillatoren die zijn nabewerkt met CTR_DRBG.

Het veilig wissen van bewaarde sleutels is net zo belangrijk als het genereren ervan. Dit geldt met name voor apparaten met flash-opslag. Wanneer op deze apparaten bijvoorbeeld gebruik wordt gemaakt van slijtagenivellering, moeten mogelijk meerdere versies van gegevens worden gewist. Hiervoor hebben iOS-apparaten een speciale voorziening, Effaceable Storage (wisbare opslag), waarmee gegevens op een veilige manier worden gewist. Deze voorziening heeft toegang tot de onderliggende opslagtechnologie (bijvoorbeeld NAND) om rechtstreeks op zeer laag niveau een klein aantal blokken te benaderen en te wissen.

Beveiliging van bestandsgegevens

Naast de hardwarematige coderingsvoorzieningen van iOS-apparaten maakt Apple gebruik van een technologie die "Gegevensbeveiliging" wordt genoemd om de gegevens die in het flash-geheugen van het apparaat worden bewaard, nog beter te beveiligen. Hierbij kan het apparaat gewoon reageren op reguliere activiteiten, zoals binnenkomende oproepen, maar is er tegelijkertijd een hoog coderingsniveau voor gebruikersgegevens mogelijk. Belangrijke systeem-apps, zoals Berichten, Mail, Agenda, Contacten en Foto's, maken standaard gebruik van Gegevensbeveiliging. Apps van andere leveranciers die onder iOS 7 of hoger worden geïnstalleerd, worden automatisch met deze technologie beschermd.

Gegevensbeveiliging wordt geïmplementeerd door een hiërarchie van sleutels samen te stellen en te beheren en bouwt voort op de technologieën voor hardwarecodering die in elk iOS-apparaat zijn ingebouwd. Gegevens-beveiliging wordt per bestand geregeld door elk bestand aan een bepaalde klasse toe te wijzen; de toegankelijkheid is afhankelijk van de ontgrendelingsstatus van de klassesleutels. Met de komst van het Apple File System (APFS) kunnen sleutels nu verder worden onderverdeeld op extentspecifieke basis (delen van een bestand kunnen afzonderlijke sleutels hebben).

Overzicht van de architectuur

Voor bestanden die op de gegevenspartitie worden aangemaakt, wordt een nieuwe 256-bits-sleutel aangemaakt (de bestandsspecifieke sleutel). Deze sleutel wordt vervolgens doorgegeven aan de AES-engine, die het bestand aan de hand van de sleutel codeert zodra het bestand in de AES CBC-modus naar het flashgeheugen wordt geschreven. (Bij apparaten met een

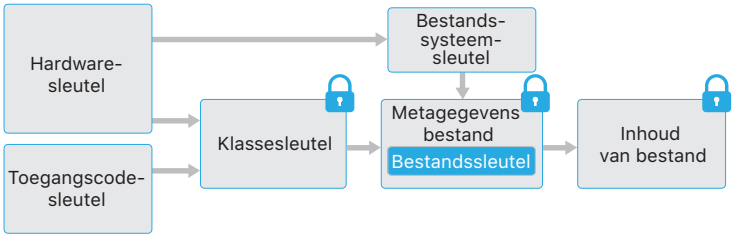
A8-processor of een nieuwere processor wordt AES-XTS gebruikt.) De initialisatievector (IV) wordt berekend met de blok-offset in het bestand, gecodeerd met de SHA-1-hash van de bestandsspecifieke sleutel.

De bestandsspecifieke (of extentspecifieke) sleutel wordt ingepakt ('wrapped') met een van de klassesleutels, afhankelijk van de omstandigheden waaronder het bestand toegankelijk moet zijn. Net als bij alle andere wrappings, wordt hiervoor NIST AES gebruikt, overeenkomstig RFC 3394. De ingepakte bestandsspecifieke sleutel wordt bewaard in de metagegevens van het bestand.

Apparaten met het Apple File System ondersteunen mogelijk het klonen van bestanden (schaduwkopieën door middel van copy-on-write-technologie). Wanneer een bestand wordt gekloond, krijgt elke helft van de kloon een nieuwe sleutel voor het accepteren van inkomende schrijfbewerkingen, zodat nieuwe gegevens met een nieuwe sleutel naar de media worden geschreven. Na verloop van tijd kan het bestand samengesteld zijn uit diverse extents (of fragmenten), elk met een andere sleutel. Alle extents die samen het bestand vormen, worden echter beveiligd met een sleutel van dezelfde klasse.

Zodra het bestand wordt geopend, worden de metagegevens gedecodeerd met de bestandssysteemsleutel, waarbij de ingepakte, bestandsspecifieke sleutel zichtbaar wordt. Ook wordt weergegeven door welke klasse het bestand wordt beveiligd. De bestandsspecifieke (of extentspecifieke) sleutel wordt uitgepakt met de klassesleutel en vervolgens doorgegeven aan de AES-engine. Deze decodeert het bestand terwijl het uit het flashgeheugen wordt gelezen. Alle verwerkingen van ingepakte bestandsspecifieke sleutels vinden plaats in de Secure Enclave. Sleutels worden nooit rechtstreeks bekend gemaakt aan de processor van het apparaat. Bij het opstarten wordt er een tijdelijke (ephemeral) sleutel overeengekomen tussen de Secure Enclave en de AES-engine. Als de Secure Enclave de sleutels van een bestand uitpakt, worden deze opnieuw ingepakt met de tijdelijke sleutel en teruggestuurd naar de processor van het apparaat.

De metagegevens van alle bestanden in het bestandssysteem worden met een willekeurige sleutel gecodeerd. Deze sleutel wordt aangemaakt op het moment dat iOS wordt geïnstalleerd of het apparaat door een gebruiker wordt gewist. Op apparaten met het Apple File System wordt de metagegevenssleutel van het bestandssysteem door de Secure Enclave UID-sleutel ingepakt voor langdurige opslag. Net als bij bestandsspecifieke of extentspecifieke sleutels wordt de metagegevenssleutel nooit rechtstreeks bekendgemaakt aan de processor van het apparaat. In plaats daarvan verstrekt de Secure Enclave een tijdelijke versie die bij elke keer opstarten anders is. Tijdens de opslag van de gecodeerde bestandssysteemsleutel wordt de sleutel extra ingepakt met een 'effaceable-sleutel' die in de Effaceable Storage wordt bewaard. Deze sleutel biedt geen extra vertrouwelijkheid voor de gegevens. De sleutel is juist bedoeld om snel op verzoek te kunnen worden gewist. De sleutel kan door een gebruiker worden gewist met de optie 'Wis alle inhoud en instellingen', maar kan ook worden gewist door een gebruiker of beheerder die via een MDM-oplossing, Exchange ActiveSync of iCloud op afstand een opdracht verstuurt om het apparaat te wissen. Wanneer de sleutel op deze manier wordt gewist, worden alle bestanden cryptografisch ontoegankelijk.



De inhoud van een bestand wordt gecodeerd met een of meer bestandsspecifieke (of extentspecifieke) sleutels, die worden ingepakt met een klassesleutel en opgeslagen in de metagegevens van het bestand. Deze metagegevens zijn op hun beurt gecodeerd met de bestandssysteemsleutel. De klassesleutel wordt beveiligd met de hardware-UID en (voor bepaalde klassen) met de toegangscode van de gebruiker. Deze hiërarchie biedt zowel flexibiliteit als hoge prestaties. Als bijvoorbeeld de klasse van een bestand moet worden gewijzigd, hoeft alleen de bestandsspecifieke sleutel opnieuw te worden ingepakt; als de toegangscode wordt gewijzigd, hoeft alleen de klassesleutel opnieuw te worden ingepakt.

Toegangscodes

Tip voor toegangscodes
Als een lange toegangscode wordt ingevoerd die alleen uit cijfers bestaat, wordt het numerieke toetsenblok in het toegangsscherm weergegeven in plaats van het toetsenbord. Een langere numerieke toegangscode is meestal eenvoudiger in te voeren dan een kortere alfanumerieke toegangscode, maar biedt dezelfde mate van bescherming.

Als een gebruiker een toegangscode instelt voor een apparaat, wordt automatisch de voorziening Gegevensbeveiliging ingeschakeld. iOS ondersteunt toegangscodes met zes of vier cijfers en alfanumerieke toegangscodes met een willekeurige lengte. Een toegangscode kan niet alleen worden gebruikt voor het ontgrendelen van het apparaat, maar biedt ook entropie voor bepaalde coderingssleutels. Dit houdt in dat een hacker die de besturing van een apparaat heeft overgenomen, zonder de toegangscode geen toegang tot de gegevens in die beveiligingsklassen heeft.

De toegangscode wordt gecombineerd met de UID van het apparaat, zodat hackers brute-force-aanvallen moeten uitvoeren. Om dit soort methoden tegen te gaan, is er een extra vertraging ingebouwd. De vertraging is zodanig ingesteld dat één poging circa 80 milliseconden duurt. Dit houdt in dat het meer dan 5,5 jaar zou duren om alle combinaties uit te proberen van een alfanumerieke toegangscode van zes tekens met kleine letters en cijfers.

Vertraging invoerpogingen toegangscodes

Pogingen	Vertraging
1-4	geen
5	1 minuut
6	5 minuten
7-8	15 minuten
9	1 uur

Hoe sterker de toegangscode, des te sterker de coderingssleutel. Met Touch ID en Face ID kan de beveiliging nog verder worden verhoogd, omdat de gebruiker een toegangscode kan instellen die veel sterker is dan anders praktisch mogelijk zou zijn. Dit resulteert in een hogere mate van daadwerkelijke entropie voor de bescherming van de coderingssleutels die worden gebruikt voor Gegevensbeveiliging, zonder dat de gebruiker diverse keren per dag zijn of haar iOS-apparaat hoeft te ontgrendelen.

Om brute-force-aanvallen verder te ontmoedigen, worden er vertragingen van toenemende lengte afgedwongen nadat in het toegangsscherm een ongeldige toegangscode is ingevoerd. Als Instellingen > 'Touch ID en toegangscode' > 'Wis gegevens' is ingeschakeld, wordt het apparaat automatisch gewist als tien keer achter elkaar een onjuiste toegangscode wordt ingevoerd. Dit kan ook als beleidsregel worden ingesteld via MDM en Exchange ActiveSync. Ook is het mogelijk om een lagere drempel in te stellen.

Op apparaten met Secure Enclave worden de vertragingen afgedwongen door de Secure Enclave-coprocessor. Als het apparaat opnieuw wordt opgestart tijdens een vertraging, blijft de vertraging van kracht en begint de tijdsduur opnieuw voor de huidige periode.

Gegevensbeveiligingsklassen

Wanneer op een iOS-apparaat een nieuw bestand wordt aangemaakt, wordt een klasse aan het bestand toegewezen door de app waarmee het bestand is aangemaakt. Elke klasse gebruikt een ander beleid om te bepalen wanneer de gegevens toegankelijk zijn. Hieronder worden de belangrijkste klassen en beleidsregels beschreven.

Volledige beveiliging

(`NSFileProtectionComplete`): Deze klassesleutel wordt beveiligd met een sleutel die is afgeleid van de toegangscode van de gebruiker en de UID van het apparaat. Kort nadat de gebruiker het apparaat heeft vergrendeld (tien seconden, als de optie 'Vraag om wachtwoord' is ingesteld op 'Meteen'), wordt de gedecodeerde klassesleutel verwijderd. Hierdoor zijn alle gegevens in deze klasse ontoegankelijk totdat de gebruiker de toegangscode opnieuw invoert of het apparaat ontgrendelt via Touch ID of Face ID.

Beveiligd tenzij geopend

(`NSFileProtectionCompleteUnlessOpen`): Sommige bestanden moeten worden weggeschreven terwijl het apparaat is vergrendeld. Een goed voorbeeld hiervan is een e-mailbijlage die op de achtergrond wordt gedownload. Dit wordt gerealiseerd door het gebruik van asymmetrische elliptische curve-cryptografie (ECDH over Curve25519). De gebruikelijke bestandsspecifieke sleutel wordt beveiligd met een sleutel die wordt afgeleid met behulp van de One-Pass Diffie-Hellman-sleutelovereenkomst (zoals beschreven in NIST SP 800-56A).

De tijdelijke publieke sleutel voor de overeenkomst wordt samen met de ingepakte, bestandsspecifieke sleutel opgeslagen. De KDF is Concatenation Key Derivation Function (Approved Alternative 1), zoals beschreven in deel 5.8.1 van NIST SP 800-56A. AlgorithmID wordt weggelaten. PartyUInfo en PartyVInfo zijn respectievelijk de tijdelijke en de statische publieke sleutels. SHA-256 wordt gebruikt als de hashing-functie. Zodra het bestand is gesloten, wordt de bestandsspecifieke sleutel uit het geheugen verwijderd. Om het bestand opnieuw te openen, wordt het gedeelde geheim (shared secret) opnieuw aangemaakt via de private sleutel van de klasse 'Beveiligd tenzij geopend' en de tijdelijke publieke sleutel van het bestand. Deze worden gebruikt om de bestandsspecifieke sleutel uit te pakken, waarmee vervolgens het bestand wordt gedecodeerd.

Beveiligd tot eerste identiteitscontrole van gebruiker

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): Deze klasse werkt op dezelfde manier als 'Volledige beveiliging', behalve dat de gedecodeerde klassesleutel niet uit het geheugen wordt verwijderd wanneer het apparaat wordt vergrendeld. De beveiliging in deze klasse heeft overeenkomsten met de codering voor complete volumes van desktopcomputers en beschermt gegevens tegen aanvallen waarvoor

het apparaat moet worden herstart. Dit is de standaardklasse voor gegevens van alle apps van andere leveranciers die niet aan een andere gegevensbeveiligingsklasse zijn toegewezen.

Geen beveiliging

(`NSFileProtectionNone`): Deze klassesleutel wordt alleen beveiligd met de UID, en wordt bewaard in Effaceable Storage. Aangezien alle sleutels die voor het decoderen van bestanden in deze klasse nodig zijn op het apparaat worden opgeslagen, biedt de codering alleen het voordeel dat het apparaat snel op afstand kan worden gewist. Als er geen gegevensbeveiligingsklasse aan een bestand is toegewezen, wordt het bestand toch gecodeerd bewaard (net als alle andere gegevens op een iOS-apparaat).

Klassesleutel gegevensbeveiliging

Klasse A	Volledige beveiliging	(NSFileProtectionComplete)
Klasse B	Beveiligd tenzij geopend	(NSFileProtectionCompleteUnlessOpen)
Klasse C	Beveiligd tot eerste identiteitscontrole van gebruiker	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Klasse D	Geen beveiliging	(NSFileProtectionNone)

Gegevensbeveiliging via de sleutelhanger

Voor veel apps zijn wachtwoorden en andere kleine, gevoelige stukjes gegevens, zoals sleutels en inlogtokens, nodig. Al deze gegevens kunnen veilig worden bewaard in de sleutelhanger van iOS.

De sleutelhanger is in feite een SQLite-database die is opgeslagen in het bestandssysteem. Er is slechts één database en de securityd-daemon bepaalt tot welke sleutelhangeronderdelen een proces of app toegang heeft. API's voor sleutelhangertoegang versturen verzoeken naar de daemon, die vervolgens de rechten (entitlements) 'Keychain-access-groups', 'application-identifier' en 'application-group' van de app opvraagt. In plaats van de toegang tot een bepaald proces te beperken, wordt er met toegangsgroepen voor gezorgd dat sleutelhangeronderdelen tussen apps kunnen worden uitgewisseld.

Sleutelhangeronderdelen kunnen uitsluitend tussen apps van dezelfde ontwikkelaar worden uitgewisseld. Apps van andere leveranciers moeten namelijk gebruikmaken van toegangsgroepen met een prefix dat via het Apple Developer Program via programmagroepen aan hen is toegewezen. De vereiste prefix en unieke programmagroepen worden afgedwongen via code-ondertekening, voorzieningenprofielen en het Apple Developer Program.

Sleutelhangergegevens worden beveiligd met een klassestructuur die lijkt op de structuur die wordt gebruikt voor de gegevensbeveiliging van bestanden. Deze klassen werken op ongeveer dezelfde manier als de gegevensbeveiligingsklassen voor bestanden. Ze maken echter gebruik van kenmerkende sleutels en zijn onderdeel van API's die een andere naam hebben.

Elementen van een sleutelhanger-onderdeel

Naast de toegangsgroep, bevat elk sleutelhangeronderdeel administratieve metagegevens (zoals tijdstempels voor de aanmaakdatum en de datum van de laatste wijziging).

Daarnaast bevat elk onderdeel SHA-1-hashes van de kenmerken die worden gebruikt om het onderdeel (zoals de account- en servernaam) op te vragen, om zo opzoekacties mogelijk te maken zonder dat daarvoor elk onderdeel hoeft te worden gedecodeerd. Ten slotte bevat een sleutelhangeronderdeel nog de coderingsgegevens, waaronder:

- Versienummer
- Gegevens van toegangsbeheerlijsten (ACL's)
- Een waarde die de beveiligingsklasse van het onderdeel aangeeft
- Onderdeelspecifieke sleutel ingepakt met de sleutel van de beveiligingsklasse
- Lijst met kenmerken die het onderdeel beschrijven (zoals doorgegeven aan SecItemAdd), gecodeerd als een binaire plist en versleuteld met de onderdeelspecifieke sleutel

De codering is AES 128 in GCM (Galois/Counter Mode); de toegangsgroep wordt opgenomen in de kenmerken en beveiligd met de GMAC-tag die tijdens de codering is berekend.

Beschikbaarheid	Beveiliging van bestandsgegevens	Gegevensbeveiliging via de sleutelhanger
Indien ontgrendeld	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Indien vergrendeld	NSFileProtectionCompleteUnlessOpen	N.v.t.
Na eerste ontgrendeling	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Altijd	NSFileProtectionNone	kSecAttrAccessibleAlways
Toegangscode ingeschakeld	N.v.t.	kSecAttrAccessible WhenPasscodeSetThisDeviceOnly

Apps die gebruikmaken van voorzieningen waarmee op de achtergrond gegevens worden vernieuwd, kunnen `kSecAttrAccessibleAfterFirstUnlock` gebruiken voor sleutelhangeronderdelen die tijdens updates op de achtergrond toegankelijk moeten zijn.

De klasse `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` werkt op dezelfde manier als `kSecAttrAccessibleWhenUnlocked`, maar is alleen beschikbaar wanneer het apparaat is geconfigureerd met een toegangscode. Deze klasse bestaat alleen in de system-sleutelverzameling (keybag) en wordt niet gesynchroniseerd met de iCloud-sleutelhanger, niet opgenomen in reservekopieën en niet toegevoegd aan escrow-sleutelverzamelingen. Als de toegangscode wordt verwijderd of gereset, zijn de onderdelen niet meer bruikbaar, omdat de klassesleutels dan ook worden verwijderd.

Andere sleutelhangerklassen hebben een tegenhanger die alleen voor het desbetreffende apparaat geldt en die altijd met de UID wordt beveiligd wanneer deze tijdens het maken van een reservekopie wordt gekopieerd. Dit maakt het onderdeel onbruikbaar als het op een ander apparaat wordt hersteld.

Apple heeft een zorgvuldige afweging gemaakt tussen veiligheid en bruikbaarheid door sleutelhangerklassen te kiezen die afhankelijk zijn van het type gegevens dat wordt beveiligd en het moment waarop iOS deze nodig heeft. Zo moet een VPN-certificaat bijvoorbeeld altijd beschikbaar zijn, zodat het apparaat continu verbinding heeft. Het certificaat krijgt echter de classificatie 'geen migratie' en kan dus niet naar een ander apparaat worden verplaatst.

De volgende klassebeveiligingen worden afgedwongen voor sleutelhanger-onderdelen die door iOS zijn aangemaakt:

Onderdeel	Toegankelijk
Wifiwachtwoorden	Na eerste ontgrendeling
Mail-accounts	Na eerste ontgrendeling
Exchange-accounts	Na eerste ontgrendeling
VPN-wachtwoorden	Na eerste ontgrendeling
LDAP, CalDAV, CardDAV	Na eerste ontgrendeling
Tokens voor accounts voor sociale netwerken	Na eerste ontgrendeling
Coderingssleutels voor Handoff-aankondigingen	Na eerste ontgrendeling
iCloud-token	Na eerste ontgrendeling
Wachtwoord voor thuisdeling	Indien ontgrendeld
Token voor Zoek mijn iPhone	Altijd

Voicemail	Altijd
Reservekopie van iTunes	Indien ontgrendeld, geen migratie
Safari-wachtwoorden	Indien ontgrendeld
Safari-bladwijzers	Indien ontgrendeld
VPN-certificaten	Altijd, geen migratie
Bluetooth®-sleutels	Altijd, geen migratie
Token voor Apple Push Notification Service	Altijd, geen migratie
iCloud-certificaten en private sleutel	Altijd, geen migratie
iMessage-sleutels	Altijd, geen migratie
Certificaten en private sleutels geïnstalleerd door een configuratieprofiel	Altijd, geen migratie
Pincode voor sim	Altijd, geen migratie

Toegangsbeheer via de sleutelhanger

Sleutelhangers kunnen worden gecombineerd met toegangsbeheerlijsten (ACL's) om beleidsregels in te stellen die ervoor moeten zorgen dat aan de vereisten voor toegankelijkheid en identiteitscontrole wordt voldaan. Het is mogelijk dat onderdelen in sleutelhangers alleen toegankelijk zijn als de gebruiker fysiek aanwezig is. Zo kan bijvoorbeeld worden opgegeven dat de identiteit van de gebruiker moet worden gecontroleerd via Touch ID, Face ID of de invoer van de toegangscode van het apparaat. De toegang tot een onderdeel kan ook worden beperkt door op te geven dat de Touch ID- of Face ID-registratie niet mag zijn gewijzigd sinds het onderdeel is toegevoegd. Hiermee wordt voorkomen dat een aanvaller zelf een vingerafdruk toevoegt om zo toegang tot een sleutelhangeronderdeel te krijgen. ACL's worden binnen de Secure Enclave geëvalueerd en worden alleen vrijgegeven aan de kernel als aan de opgegeven voorwaarden wordt voldaan.

Toegang tot in Safari bewaarde wachtwoorden

iOS-apps kunnen via de volgende twee API's toegang krijgen tot sleutelhangeronderdelen die in Safari zijn bewaard voor het automatisch invullen van wachtwoorden:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

Er wordt alleen toegang verleend als zowel de ontwikkelaar van de app als de beheerder van de website goedkeuring heeft verleend en de gebruiker toestemming heeft gegeven. App-ontwikkelaars geven aan dat ze toegang tot in Safari bewaarde wachtwoorden willen hebben door in hun app een recht op te nemen. Dit recht bevat de volledig gekwalificeerde domeinnamen (FQDN) van de desbetreffende websites. De websites moeten een bestand op hun server plaatsen met daarin de unieke app-ID's van de apps die ze hebben goedgekeurd. Als een app wordt geïnstalleerd met het recht 'com.apple.developer.associated-domains', verstuurt iOS naar elke vermelde website een TLS-verzoek om het bestand '/apple-app-site-association' op te vragen. Als het bestand de app-ID bevat van de app die wordt geïnstalleerd, wordt in iOS opgenomen dat de website en de app een vertrouwde relatie hebben. Alleen als er een vertrouwde relatie

is, resulteren de oproepen van deze twee API's in een prompt voor de gebruiker, die dan toestemming moet geven voordat wachtwoorden aan de app worden vrijgegeven of worden bijgewerkt of verwijderd.

In iOS kunnen gebruikers bewaarde gebruikersnamen en wachtwoorden in ID-velden in apps invoeren door op een sleutelsymbool in de QuickType-balk van het iOS-toetsenbord te tikken. Hiervoor wordt gebruikgemaakt van hetzelfde apple-app-site-associatiemechanisme voor een sterke koppeling van apps en websites. Deze interface geeft geen ID-gerelateerde gegevens aan de app door, tenzij de gebruiker hiervoor toestemming geeft. Als in iOS is aangegeven dat een bepaalde website en app een vertrouwde relatie hebben, zal de QuickType-balk ook rechtstreeks ID-gegevens voorstellen om in de app in te vullen. Hierdoor kunnen gebruikers ID-gegevens die in Safari zijn bewaard aan apps bekendmaken zonder dat die apps daarvoor een API nodig hebben.

Sleutelverzamelingen

De sleutels voor de gegevensbeveiligingsklassen voor zowel bestanden als sleutelhangers worden verzameld en beheerd in sleutelverzamelingen (keybags). iOS gebruikt de volgende sleutelverzamelingen: user, device, backup, escrow en iCloud Backup.

User-sleutelverzameling: Hierin worden de ingepakte klassesleutels opgeslagen die tijdens normale bewerkingen op het apparaat worden gebruikt. Als er bijvoorbeeld een toegangscode wordt ingevoerd, wordt de sleutel `NSFileProtectionComplete` uit de user-sleutelverzameling geladen en uitgepakt. Het is een binaire plist die wordt opgeslagen in de klasse 'Geen beveiliging', maar waarvan de inhoud wordt gecodeerd met een sleutel die in Effaceable Storage wordt bewaard. Om forward secrecy te garanderen voor sleutelverzamelingen, wordt deze sleutel gewist en opnieuw gegenereerd als gebruikers hun toegangscode wijzigen. De kernelextensie `AppleKeyStore` verzorgt het beheer van de user-sleutelverzameling en kan worden gevraagd naar de vergrendelingsstatus van een apparaat. Er wordt pas gemeld dat het apparaat is ontgrendeld als alle klassesleutels in de user-sleutelverzameling toegankelijk zijn en zonder problemen zijn uitgepakt.

Device-sleutelverzameling: Hierin worden de ingepakte klassesleutels opgeslagen die voor bewerkingen van apparaatspecifieke gegevens worden gebruikt. iOS-apparaten die voor gedeeld gebruik zijn geconfigureerd, hebben soms al toegang tot inloggegevens nodig voordat een gebruiker heeft ingelogd. Daarom is een sleutelverzameling nodig die niet met de toegangscode van de gebruiker is beveiligd. iOS ondersteunt geen cryptografische scheiding van gebruikersspecifieke bestandssysteemgegevens; dit houdt in dat het systeem klassesleutels uit de device-sleutelverzameling gebruikt om bestandsspecifieke sleutels in te pakken. De sleutelhanger gebruikt echter klassesleutels uit de user-sleutelverzameling om onderdelen in de sleutelhanger van de gebruiker te beveiligen. Bij iOS-apparaten die geconfigureerd zijn voor gebruik door één gebruiker (de standaardconfiguratie), is de device-sleutelverzameling tegelijk ook de user-sleutelverzameling. Deze is beveiligd met de toegangscode van de gebruiker.

Backup-sleutelverzameling: Deze sleutelverzameling wordt aangemaakt wanneer met iTunes een gecodeerde reservekopie wordt gemaakt en deze reservekopie wordt opgeslagen op de computer waarop een reservekopie van het apparaat wordt gemaakt. Er wordt een nieuwe sleutelverzameling aangemaakt met een nieuwe set sleutels. De gegevens in de reservekopie

worden opnieuw gecodeerd met behulp van deze nieuwe sleutels. Zoals eerder uitgelegd, blijven sleutelhangeronderdelen met de classificatie 'geen migratie' ingepakt met de sleutel die van de UID is afgeleid. Hierdoor kunnen ze worden teruggezet naar het apparaat waarop de reservekopie is gemaakt, maar zijn ze ontoegankelijk op een ander apparaat.

De sleutelverzameling wordt beveiligd met het wachtwoord dat in iTunes is ingesteld, waarop 10 miljoen keer PBKDF2 is toegepast. Ondanks dit grote aantal iteraties, is er geen koppeling met een specifiek apparaat en is het in theorie mogelijk om via een brute-force-aanval vanaf een groot aantal computers tegelijk de backup-sleutelverzameling te manipuleren. Deze bedreiging kan echter worden weggenomen door een wachtwoord te gebruiken dat voldoende sterk is.

Als een gebruiker ervoor kiest om een reservekopie van iTunes niet te coderen, worden de reservekopiebestanden niet gecodeerd, ongeacht hun gegevensbeveiligingsklasse. De sleutelhanger blijft echter wel beveiligd met een sleutel die van de UID is afgeleid. Om die reden worden sleutelhangeronderdelen alleen overgezet naar een nieuw apparaat als er een wachtwoord voor de reservekopie is ingesteld.

Escrow-sleutelverzameling: Deze sleutelverzameling wordt gebruikt voor iTunes-synchronisatie en MDM. Met behulp van deze sleutelverzameling kan iTunes reservekopieën maken en gegevens synchroniseren zonder dat de gebruiker een toegangscode hoeft in te voeren. Daarnaast kan een MDM-oplossing via deze sleutelverzameling de toegangscode van een gebruiker op afstand wissen. De sleutelverzameling wordt bewaard op de computer die voor de synchronisatie met iTunes wordt gebruikt of in de MDM-oplossing waarmee het apparaat wordt beheerd.

De escrow-sleutelverzameling zorgt voor een betere gebruikerservaring tijdens de apparaatsynchronisatie, waarbij in principe toegang tot alle gegevensklassen nodig is. Als een met een toegangscode vergrendeld apparaat voor het eerst wordt verbonden met iTunes, wordt de gebruiker gevraagd om de toegangscode in te voeren. Op het apparaat wordt vervolgens een escrow-sleutelverzameling aangemaakt met daarin de klassesleutels die op het apparaat worden gebruikt; deze sleutelverzameling wordt beveiligd met een nieuw gegenereerde sleutel. De escrow-sleutelverzameling en de sleutel waarmee de sleutelverzameling wordt beveiligd, worden verdeeld over het apparaat en de host of server, waarbij de gegevens op het apparaat worden toegewezen aan de klasse 'Beveiligd tot eerste identiteitscontrole van gebruiker'. Om die reden moet de toegangscode van het apparaat worden ingevoerd wanneer de gebruiker voor het eerst na een herstart een reservekopie wil maken met iTunes.

In het geval van een draadloze software-update moet de gebruiker de toegangscode invoeren wanneer hij of zij de update start. Deze code wordt gebruikt om op een veilige manier een ontgrendelingstoken voor eenmalig gebruik aan te maken waarmee de user-sleutelverzameling na de update wordt ontgrendeld. Dit token kan alleen worden gegenereerd nadat de toegangscode van de gebruiker is ingevoerd. Eerder gegenereerde tokens worden ongeldig wanneer de toegangscode van de gebruiker wordt gewijzigd.

Ontgrendelingstokens voor eenmalig gebruik zijn geschikt voor een begeleide of onbegeleide installatie van een software-update. De tokens worden gecodeerd met een sleutel die wordt afgeleid van de huidige waarde van een monotone teller in de Secure Enclave, de UUID van de sleutelverzameling en de UID van de Secure Enclave.

Wanneer de teller voor het ontgrendelingstoken voor eenmalig gebruik in de Secure Enclave wordt opgehoogd, wordt een eventueel bestaand token ongeldig. De teller wordt in de volgende gevallen opgehoogd: wanneer een token wordt gebruikt, na de eerste ontgrendeling van een opnieuw opgestart apparaat, wanneer een software-update wordt geannuleerd (door de gebruiker of het systeem) en wanneer de tijd van de beleidstimer voor een token is verstreken.

Bij begeleide software-updates vervalt het ontgrendelingstoken voor eenmalig gebruik na 20 minuten. Dit token wordt geëxporteerd uit de Secure Enclave en wordt weggeschreven naar Effaceable Storage. Een beleidstimer zorgt ervoor dat de teller wordt opgehoogd als het apparaat niet binnen 20 minuten opnieuw is opgestart.

Bij een onbegeleide software-update (waarvan sprake is als de gebruiker 'Installeer later' in een updatemelding kiest), kan het ontgrendelingstoken voor eenmalig gebruik maximaal acht uur beschikbaar worden gehouden in de Secure Enclave. Daarna wordt de teller via een beleidstimer opgehoogd.

iCloud Backup-sleutelverzameling: Deze is vergelijkbaar met de backup-sleutelverzameling. Alle klassesleutels in deze sleutelverzameling zijn asymmetrisch (op basis van Curve25519, net zoals de klasse 'Beveiligd tenzij geopend'), wat inhoudt dat iCloud-reservekopieën op de achtergrond kunnen worden gemaakt. Voor alle gegevensbeveiligingsklassen behalve 'Geen beveiliging' geldt dat de gecodeerde gegevens worden gelezen van het apparaat en naar iCloud worden verstuurd. De corresponderende klassesleutels worden beveiligd met iCloud-sleutels. De klassesleutels voor de sleutelhanger worden ingepakt met een sleutel die van de UID is afgeleid, op dezelfde manier als bij een niet-gecodeerde reservekopie van iTunes. Er wordt ook een asymmetrische sleutelverzameling gebruikt voor de reservekopie als de inhoud van de iCloud-sleutelhanger wordt teruggezet.

Beveiligingscertificeringen en -programma's

Opmerking: Voor actuele informatie over certificeringen, validaties en richtlijnen op het gebied van iOS-beveiliging ga je naar: https://support.apple.com/nl-nl/HT202739.

ISO 27001- en 27018-certificering

Apple heeft ISO 27001- en ISO 27018-certificering gekregen voor haar beheersysteem voor gegevensbeveiliging (Information Security Management System, ISMS) voor de infrastructuur, ontwikkeling en activiteiten die ondersteuning bieden voor de volgende producten en diensten: Apple School Manager, iCloud, iMessage, FaceTime, beheerde Apple ID's en iTunes U, conform de Statement of Applicability v2.1 van dinsdag 11 juli 2017. Apple's compliance met de ISO-standaard is gecertificeerd door de British Standards Institution. Op de BSI-website staan certificeringen voor ISO 27001 en ISO 27018. Je kunt deze certificeringen bekijken op:

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

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

Cryptografische validatie (FIPS 140-2)

De cryptografische modules in iOS zijn vanaf iOS 6 herhaaldelijk gecontroleerd op naleving van de Amerikaanse Federal Information Processing Standards (FIPS) 140-2 Level 1. Net als bij elke grote release laat Apple de modules door het CMVP hervalideren wanneer een nieuw iOS-besturingssysteem wordt uitgebracht. Deze aanpak garandeert de integriteit van cryptografische bewerkingen in apps van Apple en andere leveranciers die op de juiste manier gebruikmaken van de cryptografische voorzieningen en goedgekeurde algoritmen van iOS.

Common Criteria Certification (ISO 15408)

Sinds iOS 9 heeft Apple voor elke grote iOS-release iOS-certificeringen volgens het Common Criteria Certification-programma behaald voor:

- Mobile Device Fundamental Protection Profile
- VPN IPSec Client Protection Profile
- Extended Package for Mobile Device Management Agents
- Extended Package for Wireless LAN Clients

iOS 11 omvat daarnaast certificeringen voor:

- Application Software Protection Profile
- Extended Package for Email Clients
- Extended Package for Web Browsers

Apple wil dit voor elke volgende grote iOS-release doen. Apple speelt binnen de ITC (International Technical Community) een actieve rol bij de ontwikkeling van nieuwe Collaborative Protection Profiles (cPP's) die zijn gericht op de evaluatie van belangrijke technologie op het gebied van mobiele beveiliging. Apple gaat door met het evalueren en verkrijgen van certificeringen voor de nieuwe en bijgewerkte versies van de cPP's die op dit moment beschikbaar zijn.

Commercial Solutions for Classified (CSfC)

Waar van toepassing heeft Apple het iOS-platform en diverse voorzieningen ook aangeboden voor opname in de Commercial Solutions for Classified (CSfC) Program Components List. Terwijl platforms en voorzieningen van Apple worden getest voor naleving van de Common Criteria Certifications, worden ze ook aangeboden voor opname in de CSfC Program Components List.

De laatst opgenomen componenten kun je vinden op: https://www.nsa.gov/resources/everyone/csfc/components-list/.

Richtlijnen voor configuratie van beveiliging

Apple heeft wereldwijd met overheidsinstanties samengewerkt om richtlijnen op te stellen met instructies en aanbevelingen voor het behoud van een beter beveiligde omgeving, ook wel "apparaatversterking ('device

hardening') voor risicovolle omgevingen" genoemd. Deze richtlijnen bieden duidelijk omschreven en geverifieerde informatie over hoe ingebouwde iOS-functies kunnen worden geconfigureerd en gebruikt om voor een betere beveiliging te zorgen.

Beveiliging van apps

Apps spelen een zeer belangrijke rol in een moderne beveiligings-architectuur voor mobiele apparaten. Hoewel apps enorme productiviteits-voordelen opleveren voor gebruikers, kunnen zij ook negatieve gevolgen hebben voor de veiligheid en stabiliteit van het systeem en voor de gegevens van gebruikers als er niet goed mee wordt omgegaan.

Om die redenen is de beveiliging van iOS verdeeld over lagen, om ervoor te zorgen dat apps altijd worden ondertekend en gecontroleerd en in een sandbox worden uitgevoerd om de gebruikersgegevens te beschermen. Deze elementen staan garant voor een stabiel, veilig platform voor apps, waardoor duizenden ontwikkelaars de mogelijkheid hebben om honderdduizenden apps voor iOS aan te bieden zonder dat dit gevolgen heeft voor de integriteit van het systeem. Voor gebruikers betekent dit dat ze op hun iOS-apparaat met deze apps kunnen werken zonder overdreven bang te hoeven zijn voor virussen, malware of aanvallen.

Ondertekening van app-code

Als de kernel van iOS is gestart, bepaalt de kernel welke gebruikers-processen en apps kunnen worden uitgevoerd. Om er zeker van te zijn dat alle apps afkomstig zijn van een bekende en goedgekeurde bron en niet zijn gemanipuleerd, moet in iOS alle uitvoerbare code worden ondertekend met een door Apple uitgegeven certificaat. Apps die standaard bij het apparaat worden geleverd, zoals Mail en Safari, zijn ondertekend door Apple. Apps van andere leveranciers moeten ook worden gevalideerd en ondertekend met een door Apple uitgegeven certificaat. Door de verplichte code-ondertekening omvat de vertrouwensketen niet alleen het besturingssysteem, maar ook apps, om te voorkomen dat apps van andere leveranciers niet-ondertekende code-resources laden of zelfwijzigende code gebruiken.

Ontwikkelaars die apps willen ontwikkelen en op iOS-apparaten willen installeren, moeten zich bij Apple registreren en zich aanmelden voor het Apple Developer Program. Apple controleert de identiteit van de ontwikkelaars (zowel personen als bedrijven) voordat er een certificaat wordt afgegeven. Met dit certificaat kunnen ontwikkelaars apps ondertekenen en voor distributie aanbieden bij de App Store. Het resultaat is dat voor alle apps in de App Store bekend is welke persoon of organisatie ze heeft ingediend, wat kwaadwillenden ervan zal weerhouden schadelijke apps te ontwikkelen. Daarnaast zijn de apps door Apple gecontroleerd om ervoor te zorgen dat hun werking overeenkomt met de beschrijving en ze geen grote bugs of andere problemen bevatten. Naast de eerder besproken technologie geeft dit controleproces klanten vertrouwen in de kwaliteit van de apps die ze kopen.

iOS biedt ontwikkelaars de gelegenheid frameworks in te sluiten in hun apps, die vervolgens kunnen worden gebruikt door de app zelf of door eventuele extensies die in de app zijn ingesloten. Om te voorkomen dat binnen de adresruimte van het systeem en andere apps code van

derden wordt geladen, wordt de code-ondertekening gecontroleerd voor alle dynamische bibliotheken waaraan bij het starten van de apps een proces wordt gekoppeld. Deze controle vindt plaats aan de hand van de team-ID, die wordt geëxtraheerd uit een door Apple afgegeven certificaat. Een team-ID bestaat uit een alfanumerieke reeks van tien tekens, zoals 1A2B3C4D5F. Een programma kan worden gekoppeld aan elke platformbibliotheek die bij het systeem wordt meegeleverd en aan alle bibliotheken die dezelfde team-ID in de codehandtekening hebben als het uitvoerbare hoofdbestand. Aangezien de uitvoerbare bestanden die standaard deel uitmaken van het systeem geen team-ID hebben, kunnen ze alleen worden gekoppeld aan bibliotheken die standaard bij het systeem worden geleverd.

Bedrijven hebben ook de mogelijkheid om intern apps te schrijven voor gebruik binnen hun organisatie en deze apps te distribueren naar hun medewerkers. Bedrijven en organisaties kunnen zich met een D-U-N-S-nummer aanmelden voor het Apple Developer Enterprise Program (ADEP). Aanmeldingen worden goedgekeurd nadat Apple een identiteitscontrole heeft uitgevoerd en heeft gecontroleerd of aan de deelnamevoorwaarden wordt voldaan. Nadat een organisatie bij het ADEP is geregistreerd, kan de organisatie een voorzieningenprofiel aanvragen om intern apps te kunnen uitvoeren op geautoriseerde apparaten. Gebruikers moeten het voorzieningenprofiel installeren om de interne apps te kunnen uitvoeren. Op deze manier kunnen alleen de beoogde gebruikers van de organisatie de apps op hun iOS-apparaten laden. Apps die via een MDM-oplossing worden geïnstalleerd, worden impliciet vertrouwd, omdat er al een relatie bestaat tussen de organisatie en het apparaat. In alle andere gevallen moeten gebruikers het voorzieningenprofiel van de app goedkeuren in Instellingen. Organisaties kunnen beperkingen instellen om te voorkomen dat gebruikers apps van onbekende ontwikkelaars goedkeuren. Als een bedrijfs-app voor het eerst wordt gestart, moet het apparaat een positieve bevestiging ontvangen van Apple dat de app mag worden uitgevoerd.

Anders dan op andere mobiele platforms, kunnen gebruikers in iOS geen potentieel schadelijke, niet-ondertekende apps vanaf websites installeren en kunnen ze evenmin niet-vertrouwde code uitvoeren. Op het moment dat de app wordt gestart en de geheugenpagina's worden geladen, worden de codehandtekeningen gecontroleerd om er zeker van te zijn dat een app sinds de installatie of de laatste update niet is gewijzigd.

Beveiliging van runtimeprocessen

Als is vastgesteld dat een app afkomstig is van een goedgekeurde bron, worden er door iOS veiligheidsmaatregelen afgedwongen om te voorkomen dat de app andere apps of de rest van het systeem in gevaar brengt.

Alle apps van andere leveranciers worden in een sandbox geplaatst, waardoor ze beperkt toegang hebben tot bestanden die door andere apps zijn opgeslagen en ze geen aanpassingen op het apparaat kunnen aanbrengen. Op deze manier wordt voorkomen dat apps gegevens kunnen verzamelen of wijzigen die door andere apps zijn opgeslagen. Elke app heeft een unieke basismap voor de eigen bestanden. Deze map wordt willekeurig toegewezen op het moment dat de app wordt geïnstalleerd. Als een app van een andere leverancier toegang nodig heeft tot externe gegevens, kan dit alleen via voorzieningen die expliciet door iOS worden aangeboden.

Bestanden en resources van het systeem worden ook afgeschermd van de apps van de gebruiker. De meeste onderdelen van iOS worden, net als alle apps van andere leveranciers, uitgevoerd als de onbevoegde gebruiker 'mobile'. De volledige OS-partitie wordt als alleen-lezen gekoppeld. Overbodige tools, zoals voorzieningen voor extern inloggen, maken geen deel uit van de systeemsoftware; ook kunnen apps niet via API's hun eigen bevoegdheden verhogen om andere apps of het iOS zelf te wijzigen.

De toegang die apps van andere leveranciers hebben tot gebruikersgegevens en voorzieningen zoals iCloud en uitbreidbaarheid wordt geregeld via gedeclareerde rechten. Rechten zijn sleutel-waardeparen die bij een app worden geregistreerd en die identiteitscontrole mogelijk maken op andere momenten dan tijdens de runtime, zoals een UNIX-gebruikers-ID. Aangezien rechten digitaal worden ondertekend, kunnen ze niet worden gewijzigd. Rechten worden veel gebruikt door systeemapps en daemons om bepaalde bewerkingen met bevoegdheden uit te voeren waarvoor anders de root-gebruiker nodig zou zijn geweest. Hierdoor is de kans veel kleiner dat bevoegdheden worden verhoogd door gemanipuleerde systeem-apps of daemons.

Bovendien kunnen apps enkel aan verwerking op de achtergrond doen met API's die via het systeem worden aangeleverd. Dit houdt in dat apps kunnen blijven werken zonder dat dit ten koste gaat van de prestaties of de gebruiksduur van de batterij.

ASLR (Address Space Layout Randomization) biedt bescherming tegen misbruik van geheugenbugs. Ingebouwde apps maken gebruik van ASLR om ervoor te zorgen dat alle geheugengebieden bij het starten van de app willekeurig worden gerangschikt. Doordat de geheugenadressen van uitvoerbare code, systeembibliotheken en gerelateerde programmeerconstructies willekeurig worden gerangschikt, wordt de kans op aanvallen beperkt. Bij een "return-to-libc"-aanval wordt bijvoorbeeld geprobeerd het apparaat schadelijke code te laten uitvoeren door de geheugenadressen van de stack en systeembibliotheken te manipuleren. De willekeurige rangschikking van de geheugenadressen maakt het voor hackers veel lastiger om gerichte aanvallen uit te voeren, met name op meerdere apparaten. In Xcode, de ontwikkelomgeving van iOS, wordt ASLR-ondersteuning automatisch ingeschakeld wanneer programma's van andere leveranciers worden gecompileerd.

iOS biedt nog meer beveiliging via de functie Execute Never (XN) van ARM, waarmee geheugenpagina's als niet-uitvoerbaar worden gemarkeerd. Geheugenpagina's die als zowel beschrijfbaar als uitvoerbaar zijn aangemerkt, kunnen alleen onder strikt gereguleerde omstandigheden door apps worden gebruikt: De kernel controleert of het dynamische code-ondertekeningsrecht, dat alleen voor Apple beschikbaar is, aanwezig is. Zelfs dan kan er maar één mmap-oproep worden verstuurd voor het opvragen van een uitvoerbare en beschrijfbare pagina, die een willekeurig adres krijgt. Safari gebruikt deze functionaliteit voor de eigen JavaScript JIT-compiler.

Extensies

iOS biedt apps de mogelijkheid om functionaliteit aan andere apps aan te bieden via zogeheten extensies. Extensies zijn ondertekende, uitvoerbare binaire bestanden met een speciaal doel die in een app zijn opgenomen.

Extensies worden automatisch door het systeem herkend op het moment dat ze worden geïnstalleerd en worden via een matching-systeem beschikbaar gesteld aan andere apps.

Een systeemgebied dat ondersteuning biedt voor extensies, wordt een extensiepunt genoemd. Elk extensiepunt beschikt over API's en dwingt beleidsregels voor dat gebied af. Het systeem bepaalt welke extensies beschikbaar zijn op basis van de specifieke matching-regels die voor elk extensiepunt gelden. Het systeem start zo nodig automatisch extensieprocessen en regelt de duur van deze processen. Met behulp van rechten kan de beschikbaarheid van extensies worden beperkt tot bepaalde systeem-apps. Zo wordt de widget Vandaag alleen in Berichtencentrum weergegeven en is een extensie voor delen alleen beschikbaar via het paneel 'Delen'. De extensiepunten zijn 'Today', 'Share', 'Custom Actions', 'Photo Editing', 'Document Provider' en 'Custom Keyboard'.

Extensies worden in hun eigen adresruimte uitgevoerd. De communicatie tussen de extensie en de app van waaruit de extensie is geactiveerd, bestaat uit berichten tussen processen die via het systeemframework worden uitgewisseld. De extensies en apps hebben geen toegang tot elkaars bestanden of geheugenruimte. Extensies worden zo ontworpen dat ze niet alleen van elkaar zijn gescheiden, maar ook van de apps waarin ze zijn opgenomen en van de apps waardoor ze worden gebruikt. Net als alle andere apps van derden worden ze in een sandbox geplaatst en hebben ze een container die losstaat van de container van de app waarin ze zijn opgenomen. Ze hebben echter wel dezelfde toegang tot de privacybeheerfuncties als de app waarvan ze deel uitmaken. Dit houdt in dat als een gebruiker een app toegang geeft tot Contacten, deze toegang ook wordt verleend aan de extensies die in de app zijn ingebed, maar niet aan de extensies die door de app worden geactiveerd.

Custom Keyboard (Aangepast toetsenbord) is een speciaal type extensie, aangezien deze door de gebruiker voor het volledige systeem wordt ingeschakeld. Als een toetsenbordextensie is ingeschakeld, wordt deze gebruikt voor elk tekstveld, behalve bij de invoer van wachtwoorden en in weergaven met beveiligde tekst. Om de overdracht van gebruikersgegevens te beperken, worden aangepaste toetsenborden standaard uitgevoerd in een sandbox die veel beperkingen kent: er is geen toegang tot het netwerk, geen toegang tot voorzieningen waarmee namens een proces netwerkbewerkingen worden uitgevoerd en er is evenmin toegang tot API's waarmee de extensie getypte gegevens zou kunnen onderscheppen. Ontwikkelaars van aangepaste toetsenborden kunnen voor hun extensie Open Access aanvragen, wat inhoudt dat de extensie na toestemming van de gebruiker in de standaard-sandbox kan worden uitgevoerd.

Op apparaten die bij een MDM-oplossing zijn ingeschreven, volgen document- en toetsenbordextensies de regels van Managed Open In. De MDM-oplossing kan bijvoorbeeld voorkomen dat een gebruiker een document vanuit een beheerde app exporteert naar een onbeheerde Document Provider, of dat een onbeheerd toetsenbord wordt gebruikt met een beheerde app. Daarnaast kunnen app-ontwikkelaars instellen dat toetsenbordextensies van andere leveranciers niet binnen hun app kunnen worden gebruikt.

App-groepen

Apps en extensies die het eigendom zijn van een bepaalde ontwikkelaars-account, kunnen inhoud delen wanneer ze als onderdeel van een app-groep zijn geconfigureerd. Het is de taak van de ontwikkelaar om de juiste groepen aan te maken in de Apple Developer Portal en om de gewenste set apps en extensies toe te voegen. Wanneer apps deel uitmaken van een app-groep, hebben ze toegang tot de volgende onderdelen:

- Een gedeelde container op een volume voor opslagdoeleinden, die op het apparaat beschikbaar blijft zolang er ten minste één app uit de groep is geïnstalleerd
- Gedeelde voorkeuren
- Gedeelde sleutelhangeronderdelen

De Apple Developer Portal zorgt ervoor dat alle app-groepen een unieke ID hebben binnen het ecosysteem van apps.

Gegevensbeveiliging in apps

De iOS Software Development Kit (SDK) bevat een compleet pakket met API's waarmee interne en externe ontwikkelaars Gegevensbeveiliging kunnen implementeren om zo de hoogst mogelijke mate van beveiliging in hun apps te garanderen. Gegevensbeveiliging is beschikbaar voor bestands- en database-API's, waaronder NSFileManager, CoreData, NSData en SQLite.

De Mail-appdatabase (inclusief bijlagen), beheerde boeken, Safari-bladwijzers, opstartafbeeldingen voor apps en locatiegegevens worden ook gecodeerd opgeslagen met sleutels die zijn beveiligd met de toegangscode van de gebruiker op zijn of haar apparaat. Agenda (zonder bijlagen), Contacten, Herinneringen, Notities, Berichten en Foto's gebruiken de klasse 'Beveiligd tot eerste identiteitscontrole van gebruiker'.

Door gebruikers geïnstalleerde apps waarvoor geen specifieke gegevensbeveiligingsklasse is opgegeven, worden standaard gekoppeld aan de klasse 'Beveiligd tot eerste identiteitscontrole van gebruiker'.

Accessoires

Het licentieprogramma Made for iPhone, iPad en iPod touch (MFi) geeft geverifieerde leveranciers van accessoires toegang tot het iPod Accessories Protocol (iAP) en de benodigde ondersteunende hardwarecomponenten.

Als een MFi-accessoire via een Lightning-connector of via Bluetooth communiceert met een iOS-apparaat, moet het accessoire op verzoek van het apparaat aantonen dat het door Apple is geautoriseerd. Dit kan door te reageren met een door Apple uitgegeven certificaat, dat vervolgens wordt gecontroleerd door het apparaat. Het apparaat verstuurt dan een challenge, waarop het accessoire een ondertekende reactie moet geven. Dit proces wordt volledig afgehandeld door een aangepaste geïntegreerde schakeling (integrated circuit, IC) die door Apple aan goedgekeurde leveranciers van accessoires wordt geleverd en die transparant is voor het accessoire zelf.

Accessoires kunnen toegang aanvragen voor verschillende transport-methoden en functies, zoals toegang tot digitale audiostreams via de Lightning-kabel of locatiegegevens die via Bluetooth worden aanboden. Een identiteitscontroleschakeling zorgt ervoor dat alleen goedgekeurde

accessoires volledige toegang tot het apparaat krijgen. Als een accessoire geen identiteitscontrole ondersteunt, wordt de toegang beperkt tot analoge audio en enkele seriële audioafspeelregelaars (UART).

AirPlay gebruikt de identiteitscontroleschakeling om te controleren of ontvangers zijn goedgekeurd door Apple. Streams met AirPlay-audio en CarPlay-video maken gebruik van MFi-SAP (Secure Association Protocol), waarbij de communicatie tussen het accessoire en het apparaat wordt gecodeerd met AES-128 in de CTR-modus. Tijdelijke (ephemeral) sleutels worden uitgewisseld via ECDH (Curve25519) en ondertekend met de 1024-bits-RSA-sleutel van de identiteitscontroleschakeling als onderdeel van het STS-protocol (Station-to-Station).

HomeKit

HomeKit biedt een domotica-infrastructuur waarbij met behulp van iCloud en iOS-beveiliging persoonlijke gegevens worden beveiligd en gesynchroniseerd zonder dat Apple toegang tot de gegevens heeft.

HomeKit-identiteit

De identiteit en beveiliging van HomeKit zijn gebaseerd op publieke/private Ed25519-sleutelparen. Op het iOS-apparaat wordt een Ed25519-sleutelpaar gegenereerd voor iedere HomeKit-gebruiker. Dit sleutelpaar vormt de HomeKit-identiteit van die gebruiker. De HomeKit-identiteit wordt gebruikt om de communicatie tussen iOS-apparaten onderling en tussen iOS-apparaten en accessoires te verifiëren.

De sleutels worden opgeslagen in de sleutelhanger en worden alleen in gecodeerde reservekopieën van de sleutelhanger opgenomen. De sleutels worden via de iCloud-sleutelhanger gesynchroniseerd tussen apparaten.

Communicatie met HomeKit-accessoires

HomeKit-accessoires genereren hun eigen Ed25519-sleutelpaar voor gebruik tijdens de communicatie met iOS-apparaten. Als het accessoire wordt teruggezet op de fabrieksinstellingen, wordt een nieuw sleutelpaar gegenereerd.

Om een relatie tot stand te brengen tussen een iOS-apparaat en een HomeKit-accessoire, worden er sleutels uitgewisseld via het Secure Remote Password-protocol (3072-bits). Hierbij wordt een code van acht cijfers gebruikt die door de fabrikant van het accessoire wordt aangeleverd, op het iOS-apparaat door de gebruiker wordt ingevoerd en vervolgens wordt gecodeerd met ChaCha20-Poly1305 AEAD en van HKDF-SHA-512 afgeleide sleutels. De MFi-certificering van het accessoire wordt ook gecontroleerd tijdens de configuratie.

Als het iOS-apparaat en het HomeKit-accessoire tijdens gebruik met elkaar communiceren, verifiëren ze elkaar met behulp van de sleutels die in het bovenstaande proces zijn uitgewisseld. Elke sessie wordt tot stand gebracht via het Station-to-Station-protocol en wordt gecodeerd met sleutels die zijn afgeleid van HKDF-SHA-512 op basis van sessiegebonden Curve25519-sleutels. Dit geldt zowel voor op IP gebaseerde accessoires als voor Bluetooth Low Energy-accessoires.

Lokale opslag van gegevens

Gegevens met betrekking tot woningen, accessoires, scènes en gebruikers worden door HomeKit bewaard op het iOS-apparaat van de gebruiker. Deze opgeslagen gegevens worden gecodeerd met sleutels die worden

afgeleid van de HomeKit-identiteitssleutels van de gebruiker, plus een willekeurige nonce. HomeKit-gegevens worden bovendien beveiligd met de klasse 'Beveiligd tot eerste identiteitscontrole van gebruiker'. HomeKit-gegevens worden alleen in gecodeerde reservekopieën opgenomen. Dit houdt in dat bijvoorbeeld ongecodeerde reservekopieën van iTunes geen HomeKit-gegevens bevatten.

Gegevenssynchronisatie tussen apparaten en gebruikers

HomeKit-gegevens kunnen via iCloud en de iCloud-sleutelhanger worden gesynchroniseerd tussen de iOS-apparaten van een gebruiker. De HomeKit-gegevens worden tijdens de synchronisatie gecodeerd met sleutels die worden afgeleid van de HomeKit-identiteit van de gebruiker en een willekeurige nonce. Deze gegevens worden tijdens de synchronisatie als een Opaque Binary Blob (OBB) behandeld. De meest recente blob wordt in iCloud opgeslagen om synchronisatie mogelijk te maken, maar wordt niet voor andere doeleinden gebruikt. Aangezien de blob wordt gecodeerd met sleutels die alleen beschikbaar zijn op de iOS-apparaten van de gebruiker, is de inhoud ervan niet toegankelijk wanneer die wordt overgedragen of in iCloud is opgeslagen.

HomeKit-gegevens worden ook gesynchroniseerd tussen verschillende gebruikers van dezelfde woning. De identiteitscontrole en codering die bij dit proces worden gebruikt, zijn dezelfde als die tussen een iOS-apparaat en een HomeKit-accessoire worden gebruikt. De identiteitscontrole is gebaseerd op publieke Ed25519-sleutels die tussen de apparaten worden uitgewisseld wanneer een gebruiker aan een woning wordt toegevoegd. Nadat een nieuwe gebruiker aan een woning is toegevoegd, wordt alle verdere communicatie geverifieerd en gecodeerd met het Station-to-Station-protocol en sessiegebonden sleutels.

De gebruiker die als eerste de woning in HomeKit heeft geconfigureerd, of een andere gebruiker met wijzigingsbevoegdheden, kan nieuwe gebruikers toevoegen. Op het apparaat van de eigenaar worden de accessoires geconfigureerd met de publieke sleutel van de nieuwe gebruiker, zodat het accessoire opdrachten van de nieuwe gebruiker kan verifiëren en accepteren. Als een gebruiker met wijzigingsbevoegdheden een nieuwe gebruiker toevoegt, wordt het proces voor afronding naar een woninghub doorgestuurd.

Apple TV wordt automatisch gereedgemaakt voor gebruik met HomeKit wanneer de gebruiker inlogt bij iCloud. Voor de iCloud-account moet twee-factor-authenticatie zijn ingeschakeld. Apple TV en het apparaat van de eigenaar wisselen tijdelijke publieke Ed25519-sleutels uit via iCloud. Als het apparaat van de eigenaar en de Apple TV zich in hetzelfde lokale netwerk bevinden, wordt met de tijdelijke sleutels een beveiligde verbinding via het lokale netwerk tot stand gebracht; voor deze verbinding wordt gebruikgemaakt van het Station-to-Station-protocol en sessiegebonden sleutels. De identiteitscontrole en codering die bij dit proces worden gebruikt, zijn dezelfde als die tussen een iOS-apparaat en een HomeKit-accessoire worden gebruikt. Het apparaat van de eigenaar verstuurt via deze beveiligde lokale verbinding de publieke/private Ed25519-sleutelparen van de gebruiker naar de Apple TV. Met deze sleutels wordt vervolgens de communicatie tussen de Apple TV en de HomeKit-accessoires beveiligd, evenals de communicatie tussen de Apple TV en andere iOS-apparaten die deel uitmaken van de HomeKit-woning.

Als een gebruiker maar één apparaat heeft en geen andere gebruikers toegang tot de woning geeft, worden er geen HomeKit-gegevens gesynchroniseerd met iCloud.

Woninggegevens en apps

De toegang van apps tot gegevens met betrekking tot de woning wordt geregeld via de privacy-instellingen van de gebruiker. Gebruikers wordt gevraagd om toegang te geven op het moment dat apps gegevens met betrekking tot de woning opvragen (vergelijkbaar met Contacten, Foto's en andere iOS-gegevensbronnen). Als de gebruiker daarvoor toestemming geeft, krijgen apps informatie over de namen van de kamers, de namen van de accessoires en de kamers waarin de accessoires zich bevinden, plus de informatie die in de HomeKit-documentatie voor ontwikkelaars wordt beschreven. Deze documentatie is te vinden op: https://developer.apple.com/homekit/.

HomeKit en Siri

Siri kan worden gebruikt om accessoires te bevragen en aan te sturen, en om scènes te activeren. Siri krijgt anoniem minimale informatie over de configuratie van de woning aangeboden. Deze informatie bestaat uit namen van kamers, accessoires en scènes die nodig zijn voor opdrachtherkenning. Audio die naar Siri wordt gestuurd, kan specifieke accessoires of commando's omvatten; deze Siri-gegevens worden echter niet gebruikt voor andere voorzieningen van Apple, zoals HomeKit. Zie "Siri" in het gedeelte "Internetvoorzieningen" van dit document voor meer informatie.

HomeKit IP-camera's

IP-camera's in HomeKit sturen video- en audiostreams rechtstreeks naar het iOS-apparaat in het lokale netwerk dat de stream gebruikt. De streams worden gecodeerd met willekeurig gegenereerde sleutels op het iOS-apparaat en de IP-camera, die via de beveiligde HomeKit-sessie met de camera worden uitgewisseld. Als het iOS-apparaat zich niet in het lokale netwerk bevindt, worden de gecodeerde streams via de woninghub naar het iOS-apparaat gestuurd. De streams worden in de woninghub niet gedecodeerd; de woninghub fungeert slechts als schakelbord tussen het iOS-apparaat en de IP-camera. Als een app de videoweergave van de HomeKit IP-camera aan de gebruiker laat zien, worden de videobeelden vanuit een apart systeemproces gerenderd, zodat de videostream niet door de app kan worden benaderd of bewaard. Bovendien mogen apps geen schermafbeeldingen van deze stream maken.

Externe toegang via iCloud voor HomeKit-accessoires

HomeKit-accessoires kunnen rechtstreeks verbinding maken met iCloud om iOS-apparaten in staat te stellen het accessoire te besturen wanneer Bluetooth- of wificommunicatie niet beschikbaar is.

De voorziening voor externe toegang via iCloud is zo ontworpen dat accessoires kunnen worden bediend en meldingen kunnen worden verstuurd zonder dat Apple weet om welke accessoires het gaat en welke commando's of meldingen worden verstuurd. HomeKit verstuurt bij externe toegang via iCloud geen informatie over de woning.

Als een gebruiker een commando verstuurt via externe toegang via iCloud, wordt zowel het accessoire als het iOS-apparaat geverifieerd en worden gegevens gecodeerd met dezelfde procedure die in deze handleiding voor lokale verbindingen wordt beschreven. De inhoud van

de gegevensuitwisseling wordt gecodeerd en is niet zichtbaar voor Apple. De adressering via iCloud is gebaseerd op de iCloud-ID's die tijdens de configuratie zijn geregistreerd.

Accessoires die externe toegang via iCloud ondersteunen, worden tijdens de configuratie van het accessoire toegevoegd. Dit proces omvat enkele stappen, met als eerste stap het inloggen van de gebruiker bij iCloud. Vervolgens vraagt het iOS-apparaat aan het accessoire om een challenge te ondertekenen via de Apple Authentication Coprocessor, die is ingebouwd in alle accessoires die de aanduiding "Built for HomeKit" hebben. Het accessoire genereert ook elliptische-curvesleutels van het type prime256v1; de openbare sleutel wordt verstuurd naar het iOS-apparaat, samen met de ondertekende challenge en het X.509-certificaat van de Authentication Coprocessor. Aan de hand van deze gegevens wordt een certificaat voor het accessoire aangevraagd bij de voorzieningenserver van iCloud. Het certificaat wordt opgeslagen door het accessoire, maar bevat geen identificerende gegevens over het HomeKit-accessoire; in het certificaat wordt alleen vermeld dat er toestemming is verleend voor externe toegang via iCloud. Het iOS-apparaat waarmee het accessoire wordt toegevoegd, verstuurt ook een verzameling met daarin de URL's en andere gegevens die nodig zijn voor de verbinding met de iCloud-server voor externe toegang. Deze gegevens zijn niet specifiek aan een gebruiker of accessoire gekoppeld.

Elk accessoire registreert een lijst met toegestane gebruikers bij de server voor externe toegang via iCloud. Deze gebruikers hebben van de persoon die het accessoire in de woning heeft geïnstalleerd toestemming gekregen om het accessoire te bedienen. Gebruikers ontvangen een ID van de iCloud-server en kunnen worden gekoppeld aan een iCloud-account om de ontvangst van meldingen en terugkoppelingen van de accessoires mogelijk te maken. Ook accessoires krijgen een unieke ID toegewezen door de iCloud-server, maar deze ID's zijn ondoorzichtig en geven geen informatie over het accessoire zelf.

Als een accessoire verbinding maakt met de iCloud-server voor externe toegang voor het HomeKit-systeem, worden het certificaat van het accessoire en een pas gepresenteerd. De pas wordt opgevraagd bij een andere iCloud-server en is niet uniek voor elk accessoire. Als een accessoire een pas aanvraagt, wordt in de aanvraag de fabrikant, het model en de firmwareversie van het accessoire vermeld. Er worden geen gegevens meegestuurd waaruit de gebruiker of de woning kan worden afgeleid. Om de privacy te beschermen, wordt de verbinding met de pas-server niet geverifieerd.

Accessoires maken via HTTP/2 verbinding met de iCloud-server voor externe toegang, waarbij de verbinding wordt beveiligd door middel van TLS v1.2 met AES-128-GCM en SHA-256. Het accessoire houdt de verbinding met de iCloud-server voor externe toegang open, zodat binnenkomende berichten kunnen worden ontvangen en terugkoppelingen en meldingen kunnen worden verstuurd naar iOS-apparaten.

SiriKit

Voor de communicatie tussen Siri en apps van derden wordt gebruik-gemaakt van het iOS-extensiemechanisme. Hoewel Siri toegang heeft tot iOS-contactpersonen en de locatiegegevens van het apparaat, wordt gecontroleerd of de app die de extensie bevat toegangsrechten heeft voor gebruikersgegevens die zijn beschermd binnen iOS voordat die gegevens

worden doorgegeven. Hierbij wordt door Siri alleen het relevante fragment van de oorspronkelijke gebruikersvraag naar de extensie doorgestuurd. Als de app bijvoorbeeld geen toegang tot iOS-contactpersonen heeft, zal Siri een relatie in een gebruikersvraag zoals "Stuur mijn moeder 10 euro via Betaal-app" niet herleiden. In dit geval zou de app van de extensie alleen 'moeder' zien in het ruwe vraagfragment dat de app ontvangt. Als de app echter wel toegang tot iOS-contactpersonen heeft, zou de app de iOS-contactgegevens van de moeder van de gebruiker krijgen. Als in de berichttekst een contactpersoon wordt genoemd, zoals in "Vertel mijn moeder via Berichten-app: Mijn broer is fantastisch", zou Siri "mijn broer" niet herleiden, ongeacht de TCC's van de app. Inhoud die door de app wordt gepresenteerd, kan naar de server worden verstuurd om Siri woorden te leren die een gebruiker in de app zou kunnen gebruiken.

Bij verzoeken als "Zoek vervoer naar het huis van mijn moeder met <app-naam>", waarvoor locatiegegevens moeten worden opgehaald uit de Contacten-app van de gebruiker, worden de locatiegegevens door Siri aan de extensie van de app verstrekt. Dit gebeurt uitsluitend voor het verzoek in kwestie en ongeacht of de app toegang heeft tot locatiegegevens of Contacten.

Tijdens de uitvoering staat Siri de SiriKit-app toe om een reeks specifieke woorden aan te leveren voor die specifieke programma-instantie. Deze specifieke woorden zijn gekoppeld aan de willekeurige ID die in het Siri-gedeelte van dit document wordt besproken en hebben dezelfde levensduur.

HealthKit

Met HealthKit worden met toestemming van de gebruiker gegevens van gezondheids- en conditieapps bewaard en verzameld. HealthKit werkt ook rechtstreeks met gezondheids- en fitnessapparaten, zoals compatibele Bluetooth LE-hartslagmeters en de bewegingscoprocessor die in veel iOS-apparaten is ingebouwd.

Gezondheidsgegevens

HealthKit verzamelt gezondheidsgegevens van de gebruiker, zoals lengte, gewicht, afgelegde afstand en bloeddruk. Deze gegevens worden opgeslagen met de gegevensbeveiligingsklasse 'Volledige beveiliging', waardoor de gegevens pas toegankelijk zijn nadat een gebruiker zijn of haar toegangscode heeft ingevoerd of het apparaat heeft ontgrendeld via Touch ID of Face ID.

HealthKit verzamelt ook beheergegevens, zoals toegangsbevoegdheden voor apps, namen van apparaten die met HealthKit zijn verbonden en planningsgegevens voor het starten van apps wanneer er nieuwe gegevens beschikbaar zijn. Deze gegevens worden beveiligd met de klasse 'Beveiligd tot eerste identiteitscontrole van gebruiker'.

Tijdelijke dagboekbestanden bevatten gezondheidsgegevens die worden gegenereerd wanneer het apparaat is vergrendeld, bijvoorbeeld wanneer de gebruiker aan het sporten is. Deze bestanden worden beveiligd met de klasse 'Beveiligd tenzij geopend'. Als het apparaat is ontgrendeld, worden de tijdelijke dagboekbestanden geïmporteerd in de primaire gezondheidsdatabases en verwijderd nadat de gegevens zijn samengevoegd.

Gezondheidsgegevens kunnen in iCloud worden bewaard. Als is ingesteld dat gezondheidsgegevens in iCloud moeten worden bewaard, worden de gegevens tussen apparaten gesynchroniseerd en door codering beveiligd. Zo zijn de gegevens zowel tijdens de overdracht als tijdens de opslag beveiligd. Gezondheidsgegevens worden alleen in gecodeerde iTunes-reservekopieën opgenomen. Ze worden niet opgenomen in ongecodeerde iTunes-reservekopieën of in iCloud-reservekopie.

Integriteit van gegevens

In de database worden ook metagegevens opgeslagen om de herkomst van elke gegevensrecord te traceren. Deze metagegevens bevatten een app-ID die aangeeft door welke app de record is opgeslagen. Daarnaast kan een optioneel metagegevensonderdeel een digitaal ondertekende kopie van de record bevatten. Dit onderdeel is bedoeld om gegevensintegriteit te bieden voor records die door een vertrouwd apparaat zijn gegenereerd. De digitale handtekening heeft de CMS-indeling (Cryptographic Message Syntax), zoals vastgelegd in IETF RFC 5652.

Toegang door apps van andere leveranciers

De toegang tot de API van HealthKit wordt geregeld door middel van rechten, en apps moeten voldoen aan de gebruiksvoorwaarden die voor de gegevens gelden. Zo mogen gezondheidsgegevens niet worden gebruikt voor advertentiedoeleinden. Daarnaast moet aan gebruikers een privacybeleid worden aangeboden waarin wordt uitgelegd hoe hun gezondheidsgegevens door de app worden gebruikt.

De toegang van apps tot gezondheidsgegevens wordt geregeld door de privacy-instellingen van de gebruiker. Gebruikers wordt gevraagd om toegang te geven op het moment dat apps gezondheidsgegevens opvragen (vergelijkbaar met Contacten, Foto's en andere iOS-gegevensbronnen). In het geval van gezondheidsgegevens krijgen apps echter niet alleen afzonderlijke toegang voor het lezen en schrijven van gegevens, maar ook afzonderlijke toegang voor elk type gezondheidsgegevens. Gebruikers kunnen via de tab 'Bronnen' van de app Gezondheid de machtigingen bekijken (en intrekken) die ze hebben verleend voor het opvragen van gezondheidsgegevens.

Als toestemming is gegeven voor het wegschrijven van gegevens, kunnen apps de weggeschreven gegevens ook lezen. Als toestemming is gegeven voor het lezen van gegevens, kunnen apps de gegevens lezen die door alle bronnen zijn weggeschreven. Apps kunnen echter niet bepalen welke toegang aan andere apps wordt verleend. Bovendien kunnen apps niet met zekerheid vaststellen of ze leestoegang voor gezondheidsgegevens hebben gekregen. Als een app geen leestoegang heeft, worden er nooit gegevens geretourneerd. De respons is hetzelfde als bij een query op een lege database. Op deze manier wordt voorkomen dat apps de gezondheid van een gebruiker afleiden aan de hand van de soorten gegevens die door de gebruiker worden bijgehouden.

Medische ID

De app Gezondheid geeft gebruikers de mogelijkheid om een soort medisch paspoort aan te maken, met informatie die van belang kan zijn tijdens een medische noodsituatie. Deze informatie moet handmatig worden ingevoerd of bijgewerkt en wordt niet gesynchroniseerd met de informatie in de gezondheidsdatabases.

De informatie in het medische paspoort kan worden weergegeven door in het toegangsscherm op de knop 'Noodgeval' te tikken. De informatie wordt op het apparaat opgeslagen in de klasse 'Geen beveiliging' en is dus toegankelijk zonder dat de toegangscode van het apparaat hoeft te worden ingevoerd. Medische ID is een optionele voorziening die gebruikers in staat stelt de juiste balans te vinden tussen veiligheid en privacy.

ReplayKit

ReplayKit is een framework waarmee ontwikkelaars voorzieningen voor het maken van opnamen en voor live-uitzendingen in hun apps kunnen opnemen. Daarnaast kunnen gebruikers hiermee annotaties toevoegen aan hun opnamen en uitzendingen met behulp van de camera aan de voorzijde van het apparaat en de microfoon.

Films opnemen

Voor het opnemen van een film zijn verscheidene beveiligingslagen ingebouwd:

- **Dialoogvenster voor toestemming:** Voordat de opname begint, wordt de gebruiker gevraagd om te bevestigen dat hij of zij het scherm wil opnemen en opnamen wil maken met de microfoon en de camera aan de voorkant. Dit bericht wordt één keer per app-proces getoond en wordt opnieuw weergegeven als de app langer dan acht minuten op de achtergrond staat.
- **Scherm- en audio-opnamen:** Scherm- en audio-opnamen vinden plaats buiten het proces van de app in de ReplayKit-daemon replayd. Hierdoor heeft het app-proces nooit toegang tot het opgenomen materiaal.
- **Films maken en bewaren:** Het filmbestand wordt naar een directory geschreven die alleen voor de subsystemen van ReplayKit toegankelijk is en die nooit voor apps toegankelijk is. Zo wordt voorkomen dat opnamen zonder toestemming van de gebruiker door derden kunnen worden gebruikt.
- **Voorvertoning en delen door eindgebruiker:** De gebruiker kan via een interface van ReplayKit een voorvertoning van de film bekijken en de film delen. De interface wordt buiten het proces om via de extensie-infrastructuur van iOS beschikbaar gesteld en heeft toegang tot het gegenereerde filmbestand.

Uitzenden

- **Scherm- en audio-opnamen:** Het opnamemechanisme voor scherm-inhoud en audio tijdens uitzendingen is identiek aan het mechanisme bij filmopnamen en vindt plaats in replayd.
- **Uitzendingsextensies:** Als diensten van derden aan uitzendingen via ReplayKit willen deelnemen, moeten ze twee nieuwe extensies aanmaken die zijn geconfigureerd met het endpoint com.apple.broadcast-services:
  - Een interface-extensie waarmee de gebruiker zijn of haar uitzending kan configureren
  - Een uploadextensie waarmee het uploaden van video en audio naar de back-endservers van de dienst wordt geregeld

Door de speciale architectuur hebben hosting-apps geen bevoegdheden met betrekking tot het uitgezonden video- en audiomateriaal. Alleen ReplayKit en de desbetreffende uitzendingsextensies hebben toegang.

Uitzendingskiezer: Om een uitzendingsdienst te selecteren, biedt ReplayKit een weergaveregelaar (vergelijkbaar met UIActivityViewController) die de ontwikkelaar in zijn of haar app kan aanbieden. De weergaveregelaar wordt geïmplementeerd met de SPI UIRemoteViewController en is een extensie die zich binnen het ReplayKit-framework bevindt. De hostingapp heeft er geen procestoegang toe.

- **Uploadextensie:** De uploadextensie die door uitzendingsdiensten van derden wordt geïmplementeerd voor de verwerking van video en audio tijdens uitzendingen, kan materiaal op twee manieren ontvangen:
  - Als kleine, gecodeerde MP4-fragmenten
  - Als ruwe, ongecodeerde samplebuffers
    - **Verwerking van MP4-fragmenten:** Bij deze verwerkingsmodus worden de kleine, gecodeerde MP4-fragmenten door replayd gecodeerd en bewaard op een privélocatie die alleen voor de subsystemen van ReplayKit toegankelijk is. Nadat een filmfragment is gegenereerd, wordt de locatie ervan door replayd aan de uploadextensie van derden doorgegeven via de SPI voor het NSExtension-verzoek (op basis van XPC). replayd genereert daarnaast een eenmalig sandbox-token dat ook aan de uploadextensie wordt doorgegeven en waarmee de extensie voor de duur van het extensieverzoek toegang tot het filmfragment krijgt.
    - **Verwerking van de samplebuffer:** Bij deze verwerkingsmodus worden video en audio in realtime geserialiseerd en via een rechtstreekse XPC-verbinding aan de uploadextensie van derden doorgegeven. Video wordt gecodeerd door het IOSurface-object uit de videosamplebuffer te halen en dit beveiligd te coderen als XPC-object. Vervolgens wordt het via XPC naar de extensie van derden verstuurd en weer beveiligd gedecodeerd tot een IOSurface-object.

Vergrendelde notities

De app Notities bevat een functie waarmee gebruikers de inhoud van specifieke notities kunnen afschermen. Vergrendelde notities zijn gecodeerd met een door de gebruiker opgegeven wachtwoord. Dit wachtwoord is nodig om de notities in iOS, macOS en op de iCloud-website te kunnen bekijken.

Wanneer een gebruiker een notitie vergrendelt, wordt met PBKDF2 en SHA256 een sleutel van 16 bytes gegenereerd op basis van het wachtwoord van de gebruiker. De inhoud van de notitie wordt gecodeerd met AES-GCM. In Core Data en CloudKit worden nieuwe records aangemaakt waarin de gecodeerde notitie, de tag en de initialisatievector worden opgeslagen. De records van de oorspronkelijke notitie worden verwijderd; de gecodeerde gegevens worden niet weggeschreven. Eventuele bijlagen worden op dezelfde manier gecodeerd. Dit kunnen afbeeldingen, tekeningen, tabellen, kaarten of websites zijn. Notities met andere typen bijlagen kunnen niet worden gecodeerd. Als een notitie al vergrendeld is, kunnen niet-ondersteunde bijlagen er niet aan worden toegevoegd.

Wanneer een gebruiker een vergrendelde notitie wil bekijken of aanmaken en het juiste wachtwoord invoert, wordt in Notities een beveiligde sessie geopend. Tijdens deze sessie hoeft de gebruiker het wachtwoord niet opnieuw in te voeren (of Touch ID of Face ID te gebruiken) om andere

notities te bekijken of te vergrendelen. Notities die met een ander wachtwoord zijn vergrendeld, kunnen echter niet in dezelfde beveiligde sessie worden bekeken. De beveiligde sessie wordt gesloten als:

- De gebruiker op de knop 'Vergrendel nu' in Notities tikt
- Notities langer dan 3 minuten op de achtergrond staat
- Het apparaat wordt vergrendeld

Als gebruikers hun wachtwoord niet meer weten, kunnen ze vergrendelde notities nog wel bekijken of andere notities vergrendelen als ze Touch ID of Face ID op hun apparaat hebben ingeschakeld. In Notities verschijnt bovendien een door de gebruiker opgegeven wachtwoordaanwijzing wanneer drie keer een onjuist wachtwoord is ingevoerd. De gebruiker kan het huidige wachtwoord alleen wijzigen door eerst dat wachtwoord in te voeren.

Gebruikers kunnen een wachtwoord opnieuw instellen als ze het huidige wachtwoord niet meer weten. Ze kunnen dan met het nieuwe wachtwoord nieuwe vergrendelde notities aanmaken. Ze kunnen echter geen notities bekijken die met het oude wachtwoord zijn vergrendeld. Daarvoor is het oude wachtwoord nodig. Voor het opnieuw instellen van het wachtwoord is het wachtwoord van de iCloud-account van de gebruiker vereist.

Gedeelde notities

Notities kunnen met anderen worden gedeeld. Gedeelde notities hebben geen end-to-end-codering. Apple gebruikt het gecodeerde gegevenstype van CloudKit voor elke tekst of bijlage die de gebruiker in een notitie zet. Assets worden altijd gecodeerd met een sleutel die in de CKRecord is gecodeerd. Metagegevens, zoals de aanmaakdatum en wijzigingsdatum, worden niet gecodeerd. CloudKit beheert het proces waarmee deelnemers elkaars gegevens kunnen coderen en decoderen.

Apple Watch

Apple Watch maakt gebruik van de beveiligingsvoorzieningen en -technologieën die voor iOS zijn ontwikkeld om gegevens op het apparaat te beschermen. De communicatie met de gekoppelde iPhone en het internet wordt ook op deze manier beveiligd. Het gaat hier om technologieën zoals Gegevensbeveiliging en toegangsbeheer via sleutelhangers. Daarnaast wordt de toegangscode van de gebruiker gecombineerd met de UID van het apparaat om coderingssleutels aan te maken.

De koppeling tussen Apple Watch en iPhone wordt beveiligd via een OOB-proces (Out-Of-Band) om publieke sleutels uit te wisselen, waarna via de BTLE-verbinding een gedeeld geheim wordt uitgewisseld. Op de Apple Watch wordt een bewegend patroon weergegeven, dat wordt vastgelegd door de camera van de iPhone. Het patroon bevat een gecodeerd geheim dat wordt gebruikt voor de OOB-koppeling via BTLE 4.1. Indien nodig kunnen de apparaten ook nog worden gekoppeld door op de reguliere manier een BTLE-toegangscode in te voeren.

Zodra de BTLE-sessie tot stand is gebracht, worden er tussen Apple Watch en iPhone sleutels uitgewisseld via een proces dat is afgeleid van IDS (zie het gedeelte "iMessage" in dit document). Nadat de sleutels zijn uitgewisseld, wordt de sleutel voor de Bluetooth-sessie vernietigd en wordt alle communicatie tussen Apple Watch en iPhone gecodeerd met behulp

van IDS. De gecodeerde Bluetooth-, wifi- en mobiele verbindingen vormen hierbij een secundaire coderingslaag. De sleutel wordt elke 15 minuten gewijzigd om de blootstellingstijd van de gegevens te beperken.

Voor apps die gegevens moeten streamen, zijn de coderingsmethoden beschikbaar die worden beschreven onder "FaceTime" in het gedeelte "Internetvoorzieningen" van dit document. Hierbij wordt ofwel de IDS-voorziening gebruikt die door de gekoppelde iPhone wordt aangeboden, ofwel een rechtstreekse internetverbinding.

Apple Watch maakt gebruik van hardwarematig gecodeerde opslag en op klassen gebaseerde gegevensbeveiliging voor bestanden en sleutelhangeronderdelen. Dit wordt beschreven in het gedeelte "Codering en beveiliging van gegevens" van dit document. Voor sleutelhangeronderdelen worden ook sleutelverzamelingen met toegangsbeheer gebruikt. De sleutels die voor de communicatie tussen het horloge en de iPhone worden gebruikt, worden ook beschermd met op klassen gebaseerde gegevensbeveiliging.

Als Apple Watch zich buiten het Bluetooth-bereik bevindt, kan wifi of een mobiel netwerk worden gebruikt. De Apple Watch maakt alleen verbinding met wifinetwerken als de daarvoor benodigde referenties al aanwezig zijn op de gekoppelde iPhone. Deze referenties moeten daarvoor al eerder met de Apple Watch zijn gesynchroniseerd. Als de Apple Watch zich buiten het bereik van de iPhone bevindt, zijn eventuele nieuwe netwerkreferenties die op de iPhone aanwezig zijn, niet op de Apple Watch aanwezig.

De Apple Watch kan handmatig worden vergrendeld door de knop aan de zijkant een paar seconden ingedrukt te houden. Daarnaast wordt gebruikgemaakt van bewegingsheuristiek om te proberen het apparaat automatisch te vergrendelen kort nadat het horloge van de pols is verwijderd. Als Apple Watch is vergrendeld, kan Apple Pay alleen worden gebruikt wanneer de toegangscode van de Apple Watch wordt ingevoerd. Draagdetectie kan worden uitgeschakeld met de Apple Watch-app op de iPhone. Deze instelling kan ook worden afgedwongen via een MDM-oplossing.

Het horloge kan ook worden ontgrendeld via de gekoppelde iPhone, maar alleen als het horloge wordt gedragen. Hiervoor moet een verbinding tot stand worden gebracht die is geverifieerd via de sleutels die tijdens de koppeling zijn aangemaakt. De iPhone verstuurt de sleutel waarmee vervolgens de gegevensbeveiligingssleutels op het horloge worden ontgrendeld. De toegangscode van de Apple Watch is niet bekend op de iPhone en wordt ook niet verstuurd. Deze functie kan worden uitgeschakeld met de Apple Watch-app op de iPhone.

Een Apple Watch kan met één iPhone tegelijk worden gekoppeld. Als iPhone wordt losgekoppeld van de Apple Watch, geeft iPhone instructies om alle gegevens van de Apple Watch te wissen.

Wanneer Zoek mijn iPhone op de gekoppelde iPhone wordt ingeschakeld, wordt ook op de Apple Watch het gebruik van het activeringsslot toegestaan. Hierdoor wordt het moeilijker voor iemand om een gevonden of gestolen Apple Watch te gebruiken of te verkopen. Als het activeringsslot is ingeschakeld, zijn de Apple ID en het wachtwoord van de gebruiker nodig om een Apple Watch los te koppelen, te wissen of opnieuw te activeren.

Netwerkbeveiliging

In aanvulling op de ingebouwde veiligheidsmechanismen die Apple gebruikt voor de beveiliging van gegevens die op iOS-apparaten worden opgeslagen, zijn er allerlei maatregelen die organisaties kunnen nemen om hun netwerk te beveiligen en om hun gegevens te beschermen terwijl die met een iOS-apparaat worden uitgewisseld.

Mobiele gebruikers moeten overal ter wereld toegang hebben tot het netwerk van hun bedrijf. Het is daarom belangrijk dat zij de juiste toegangsrechten hebben en dat hun gegevens tijdens de overdracht worden beveiligd. iOS gebruikt standaard-netwerkprotocollen voor geverifieerde, bevoegde en gecodeerde communicatie en geeft ook ontwikkelaars toegang tot deze protocollen. Om deze beveiligingsdoelstellingen te realiseren, zijn in iOS bewezen technologieën en de nieuwste standaarden geïntegreerd voor wifiverbindingen en verbindingen via mobieledatanetwerken.

Op andere platforms is firewallsoftware nodig om open communicatie-poorten te beschermen tegen indringers. Aangezien in iOS het potentiële 'aanvalsgebied' is verkleind, doordat het aantal luisterpoorten is beperkt en overbodige netwerkprogramma's, zoals telnet, shells of een webserver, zijn weggelaten, is op iOS-apparaten geen aanvullende firewallsoftware nodig.

TLS

iOS ondersteunt Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) en DTLS. Het ondersteunt zowel AES-128 als AES-256 en geeft de voorkeur aan versleutelingssuites met 'perfect forward-secrecy'. Dit protocol wordt automatisch door Safari, Agenda, Mail en andere internet-apps gestart, waardoor er een gecodeerd communicatiekanaal ontstaat tussen het apparaat en de netwerkvoorzieningen. Hoog-niveau API's (zoals CFNetwork) maken het voor ontwikkelaars eenvoudig om TLS in hun apps toe te passen, terwijl laag-niveau API's (SecureTransport) fijnmazige controle bieden. SSLv3 wordt door CFNetwork niet toegestaan en apps die WebKit gebruiken (zoals Safari) kunnen geen SSLv3-verbinding tot stand brengen.

Vanaf iOS 11 en macOS High Sierra zijn SHA-1-certificaten niet meer toegestaan voor TLS-verbindingen, tenzij ze door de gebruiker worden vertrouwd. Certificaten met RSA-sleutels van minder dan 2048 bits zijn ook niet meer toegestaan. De symmetrische RC4-versleutelingssuite wordt in iOS 10 en macOS Sierra niet meer ondersteund. Standaard zijn bij TLS-clients of -servers waarop SecureTransport-API's zijn geïmplementeerd geen RC4-versleutelingssuites ingeschakeld en kunnen deze geen verbinding maken wanneer RC4 de enige beschikbare versleutelingssuite is. Voor een betere beveiliging moeten diensten of apps die RC4 nodig hebben, worden geüpgraded zodat ze veilige versleutelingssuites kunnen gebruiken.

App Transport Security

Met behulp van App Transport Security worden standaardvereisten voor verbindingen afgedwongen, om ervoor te zorgen dat de optimale werkwijzen voor veilige verbindingen worden gevolgd wanneer apps

gebruikmaken van de API's NSURLConnection, CFURL of NSURLSession. Standaard wordt versleutelingsselectie door App Transport Security beperkt tot alleen die suites die forward-secrecy bieden, namelijk ECDHE_ECDSA_AES en ECDHE_RSA_AES in GCM- of CBC-modus. Apps kunnen per domein de vereiste van forward-secrecy uitschakelen, waarna RSA_AES aan de reeks beschikbare versleutelingen wordt toegevoegd.

Servers moeten ondersteuning bieden voor TLS v1.2 en forward-secrecy, en certificaten moeten geldig zijn en zijn ondertekend met SHA-256 of beter met minimaal een 2048-bits RSA-sleutel of een 256-bits elliptische-curvesleutel.

Netwerkverbindingen die niet aan deze vereisten voldoen, mislukken, tenzij de app App Transport Security omzeilt. Bij ongeldige certificaten treedt altijd een onherstelbare fout op en wordt er geen verbinding gemaakt. App Transport Security wordt automatisch toegepast op apps die voor iOS 9 of hoger zijn gecompileerd.

VPN

Beveiligde netwerkvoorzieningen zoals een VPN zijn meestal snel te configureren voor gebruik met iOS-apparaten. iOS-apparaten werken met VPN-servers die de volgende protocollen en verificatiemethoden ondersteunen:

- IKEv2/IPSec met verificatie via een gedeeld geheim, RSA-certificaten, ECDSA-certificaten, EAP-MSCHAPv2 of EAP-TLS
- SSL-VPN met de desbetreffende client-app uit de App Store
- Cisco IPSec met gebruikersverificatie via een wachtwoord, RSA SecurID of CRYPTOCard, en apparaatverificatie via een gedeeld geheim en certificaten
- L2TP/IPSec met gebruikersverificatie via een MS-CHAPV2-wachtwoord, RSA SecurID of CRYPTOCard, en apparaatverificatie via een gedeeld geheim.

iOS biedt ondersteuning voor:

- **VPN op aanvraag** voor netwerken waarin verificatie aan de hand van certificaten plaatsvindt. IT-beleidsregels bepalen via een VPN-configuratieprofiel voor welke domeinen een VPN-verbinding nodig is.
- **VPN per app**, waardoor het aanbieden van VPN-verbindingen veel zorgvuldiger kan worden geregeld. In een MDM-oplossing kan een verbinding worden ingesteld voor elke beheerde app en specifieke domeinen in Safari. Zo wordt ervoor gezorgd dat beveiligde gegevens altijd van en naar het bedrijfsnetwerk worden gestuurd en gescheiden blijven van de persoonlijke gegevens van de gebruiker.
- **Altijd actieve VPN**. Deze voorziening kan worden geconfigureerd voor apparaten die via MDM worden beheerd en die via Apple Configurator 2, het Device Enrollment Program of Apple School Manager onder supervisie staan. Hierdoor hoeven gebruikers niet steeds VPN in te schakelen om hun verkeer te beveiligen als ze verbinding met mobiele en wifinetwerken maken. Met Altijd actieve VPN heeft een organisatie de volledige controle over het apparaatverkeer, doordat al het IP-verkeer via een tunnel naar de organisatie wordt geleid. Door het standaardprotocol voor tunnels, IKEv2, wordt het verkeer beveiligd met gegevenscodering. De organisatie kan het verkeer van en naar de eigen apparaten bewaken en filteren, gegevens binnen het netwerk beveiligen en de toegang van apparaten tot het internet beperken.

Wifi

iOS ondersteunt industriestandaard wifiprotocollen, waaronder WPA2 Enterprise, om geverifieerde toegang tot draadloze bedrijfsnetwerken te bieden. WPA2 Enterprise maakt gebruik van 128-bits-AES-codering, waardoor gebruikers de hoogst mogelijke zekerheid hebben dat hun gegevens beschermd blijven wanneer zij gegevens via een wifinetwerkverbinding uitwisselen. Dankzij de ondersteuning voor 802.1X kunnen iOS-apparaten in uiteenlopende RADIUS-verificatieomgevingen worden geïntegreerd. iPhone en iPad ondersteunen verschillende methoden voor draadloze identiteitscontrole via 802.1X, zoals EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1 en LEAP.

WPA2-beveiliging wordt in iOS niet alleen gebruikt voor gegevens-bescherming, maar ook voor unicast- en multicastmanagementframes via de Protected Management Frame-service die in 802.11w wordt genoemd. PMF-ondersteuning is beschikbaar op iPhone 6 en iPad Air 2 en nieuwere modellen.

iOS maakt tijdens wifiscans gebruik van een willekeurig MAC-adres (Media Access Control) wanneer er geen verbinding met een wifinetwerk is. Deze scans kunnen worden uitgevoerd om een voorkeurs-wifinetwerk te vinden en daarmee verbinding te maken, of voor locatievoorzieningen voor apps die met geozones ("geofences") werken, zoals locatiegebonden herinneringen of het vastleggen van een locatie in Apple Kaarten. Houd er rekening mee dat wifiscans die plaatsvinden terwijl de iPhone verbinding probeert te maken met een voorkeurs-wifinetwerk, niet willekeurig zijn.

iOS gebruikt ook een willekeurig gekozen MAC-adres voor het uitvoeren van ePNO-scans (enhanced Preferred Network Offload) wanneer een apparaat niet aan een wifinetwerk is gekoppeld of als de processor van het apparaat in de sluimerstand staat. ePNO-scans worden uitgevoerd wanneer op een apparaat locatievoorzieningen worden gebruikt voor apps die met geozones werken, zoals locatiegebonden herinneringen waarvoor wordt vastgesteld of het apparaat zich in de buurt van een specifieke locatie bevindt.

Aangezien het MAC-adres van een apparaat nu verandert wanneer er geen verbinding met een wifinetwerk is, is het niet mogelijk om via passieve observatie van het wifiverkeer een apparaat te volgen, zelfs niet wanneer het apparaat is verbonden met een mobiel netwerk. Apple heeft wififabrikanten laten weten dat in wifiscans van iOS een willekeurig MAC-adres wordt gebruikt, en dat noch Apple noch de fabrikanten deze willekeurig gekozen MAC-adressen kunnen voorspellen. De willekeurige selectie van wifi-MAC-adressen wordt niet ondersteund op iPhone 4s en oudere modellen.

Op iPhone 6s en nieuwere modellen is de verborgen eigenschap van een bekend wifinetwerk bekend en wordt deze automatisch bijgewerkt. Als de Service Set Identifier (SSID) van een wifinetwerk wordt uitgezonden, zal het iOS-apparaat geen sonde versturen waarbij de SSID in het verzoek is opgenomen. Zo wordt voorkomen dat het apparaat de netwerknaam van niet-verborgen netwerken uitzendt.

Om het apparaat te beveiligen tegen kwetsbaarheden in de firmware van netwerkprocessors, hebben netwerkinterfaces waaronder wifi en baseband slechts beperkt toegang tot het geheugen van de hoofdprocessor. Als USB of SDIO wordt gebruikt voor communicatie met de netwerkprocessor, kan

de netwerkprocessor geen DMA-transacties (Direct Memory Access) naar de hoofdprocessor in gang zetten. Als PCIe wordt gebruikt, bevindt elke netwerkprocessor zich op zijn eigen geïsoleerde PCIe-bus. Een IOMMU op elke PCIe-bus beperkt de DMA-toegang van de netwerkprocessor tot geheugenpagina's met netwerkpakketten of netwerkcontrolestructuren van de netwerkprocessor.

Bluetooth

De Bluetooth-ondersteuning in iOS biedt bruikbare functionaliteit zonder dat persoonlijke gegevens onnodig toegankelijk zijn. iOS-apparaten ondersteunen verbindingen via Encryption Mode 3, Security Mode 4 en Service Level 1. iOS ondersteunt de volgende Bluetooth-profielen:

- Hands-Free Profile (HFP 1.5)
- Phone Book Access Profile (PBAP)
- Message Access Profile (MAP)
- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Personal Area Network-profiel (PAN)
- Human Interface Device-profiel (HID)
- De ondersteuning voor deze profielen verschilt per apparaat.

Voor meer informatie ga je naar:
https://support.apple.com/nl-nl/HT204387.

Eenmalige aanmelding

iOS ondersteunt identiteitscontrole bij bedrijfsnetwerken via eenmalige aanmelding (Single Sign-on, SSO). Bij eenmalige aanmelding wordt gewerkt met op Kerberos gebaseerde netwerken om de identiteit van gebruikers te controleren voor voorzieningen die zij mogen gebruiken. Eenmalige aanmelding kan worden gebruikt voor allerlei netwerkactiviteiten, variërend van beveiligde Safari-sessies tot en met apps van andere leveranciers. Identiteitscontrole op basis van certificaten (PKINIT) wordt ook ondersteund.

Voor de eenmalige aanmelding in iOS worden SPNEGO-tokens en het HTTP Negotiate-protocol gebruikt om samen te werken met op Kerberos gebaseerde verificatiegateways en Windows Integrated Authentication-systemen die Kerberos-tickets ondersteunen. De ondersteuning van eenmalige aanmelding is gebaseerd op het open-source Heimdal-project.

De volgende typen coderingen worden ondersteund:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari ondersteunt eenmalige aanmelding, en apps van andere leveranciers die standaard-netwerk-API's van iOS gebruiken, kunnen ook worden geconfigureerd voor het gebruik van eenmalige aanmelding. De configuratie van eenmalige aanmelding onder iOS verloopt via een configuratieprofiel met behulp waarvan MDM-oplossingen de benodigde instellingen naar het apparaat kunnen pushen.Het gaat hierbij onder andere om het instellen van de principal-naam van de gebruiker (de

gebruikersaccount in Active Directory), het opgeven van Kerberos-realm-instellingen en het configureren van de apps en URL's in Safari waarvoor eenmalige aanmelding mag worden gebruikt.

AirDrop-beveiliging

iOS-apparaten die AirDrop ondersteunen, gebruiken Bluetooth Low Energy (BLE) en door Apple ontwikkelde peer-to-peer-wifitechnologie om bestanden en gegevens naar apparaten in de buurt te versturen, waaronder AirDrop-compatibele Mac-computers met OS X 10.11 of hoger. De wifiradio wordt gebruikt voor rechtstreekse communicatie tussen apparaten, zonder dat daarvoor een internetverbinding of wifitoegangspunt nodig is.

Als een gebruiker AirDrop inschakelt, wordt er een 2048-bits-RSA-identiteit opgeslagen op het apparaat. Daarnaast wordt er een hash voor de AirDrop-identiteit aangemaakt die is gebaseerd op de e-mailadressen en telefoonnummers die aan de Apple ID van de gebruiker zijn gekoppeld.

Als een gebruiker een onderdeel via AirDrop deelt, verstuurt het apparaat een AirDrop-signaal via Bluetooth Low Energy. Andere apparaten in de buurt die niet in de sluimerstand staan en waarop AirDrop ook is ingeschakeld, herkennen het signaal en reageren met een verkorte versie van de hash van de identiteit van hun eigenaar.

AirDrop deelt standaard alleen gegevens met contacten. Gebruikers kunnen er ook voor kiezen om via AirDrop gegevens met iedereen te delen. Een derde mogelijkheid is om de functie helemaal uit te schakelen. In de modus 'Alleen contacten' worden de ontvangen identiteits-hashes vergeleken met de hashes van personen in de app Contacten van de initiator. Als er een match wordt gevonden, wordt er door het verzendende apparaat een peer-to-peer-wifinetwerk tot stand gebracht en wordt er via Bonjour een AirDrop-verbinding aangekondigd. De ontvangende apparaten versturen via deze verbinding hun volledige identiteits-hashes naar de initiator. Als de volledige hash nog steeds overeenkomt met een hash uit de app Contacten, worden de voornaam en foto van de ontvanger (indien aanwezig in Contacten) weergegeven in het AirDrop-venster voor het delen van bestanden.

Bij gebruik van AirDrop bepaalt de verzendende gebruiker met wie hij gegevens wil delen. Het verzendende apparaat zet een (via TLS) gecodeerde verbinding op met het ontvangende apparaat, waarna de iCloud-identiteitscertificaten worden uitgewisseld. De identiteit in de certificaten wordt gecontroleerd aan de hand van de gegevens in de app Contacten van de gebruikers. Daarna wordt de ontvangende gebruiker gevraagd of hij of zij de binnenkomende overdracht van de geïdentificeerde persoon of het geïdentificeerde apparaat wil accepteren. Als meerdere ontvangers zijn geselecteerd, wordt dit proces voor elke bestemming herhaald.

In de modus 'Iedereen' wordt hetzelfde proces gebruikt, maar als er geen match wordt gevonden in Contacten, worden de ontvangende apparaten met een silhouet en de naam van het apparaat weergegeven in het AirDrop-venster voor het versturen van bestanden, zoals is opgegeven via Instellingen > 'Algemeen' > 'Over' > 'Naam'.

Organisaties kunnen het gebruik van AirDrop beperken voor apparaten of apps die met een MDM-oplossing worden beheerd.

Wifiwachtwoorden delen

iOS-apparaten die het delen van wifiwachtwoorden ondersteunen, gebruiken een AirDrop-achtig mechanisme om een wifiwachtwoord van het ene apparaat naar het andere te versturen.

Als een gebruiker een wifinetwerk selecteert (de aanvrager) en wordt gevraagd om het wifiwachtwoord op te geven, start het Apple apparaat een Bluetooth Low Energy-aankondiging waarin om het wifiwachtwoord wordt gevraagd. Andere Apple apparaten in de buurt die actief zijn en die het wachtwoord voor het geselecteerde wifinetwerk hebben, maken via Bluetooth Low Energy verbinding met het aanvragende apparaat.

Het apparaat dat het wifiwachtwoord heeft (de verstrekker) vraagt vervolgens om de contactgegevens van de aanvrager, en deze moet via een AirDrop-achtig mechanisme zijn identiteit aantonen. Wanneer de identiteit is aangetoond, stuurt de verstrekker de uit 64 tekens bestaande PSK, die kan worden gebruikt om verbinding met het netwerk te maken.

Organisaties kunnen het delen van wifiwachtwoorden beperken voor apparaten of apps die met een MDM-oplossing worden beheerd.

Apple Pay

Met Apple Pay kunnen gebruikers vanaf een ondersteund iOS-apparaat gemakkelijk, veilig en privé betalingen uitvoeren in winkels, apps en op het web in Safari. Het is eenvoudig in het gebruik en de beveiligingsfuncties zijn in zowel de hardware als de software geïntegreerd.

Bij het ontwerp van Apple Pay is ook rekening gehouden met de bescherming van de persoonlijke gegevens van de gebruiker. Met Apple Pay worden geen transactiegegevens verzameld waarmee de identiteit van de gebruiker kan worden vastgesteld. Betalingstransacties vinden plaats tussen de gebruiker, de verkoper en de kaartverstrekker.

Onderdelen van Apple Pay

Secure Element: Het Secure Element is een industriestandaard, gecertificeerde chip waarop het Java Card-platform wordt uitgevoerd en die voldoet aan de eisen die door de financiële sector aan elektronische betalingen worden gesteld.

NFC-controller: De NFC-controller is verantwoordelijk voor de afhandeling van Near Field Communication-protocollen en de routering van de communicatie tussen de processor van het apparaat en het Secure Element, en van de communicatie tussen het Secure Element en de POS-terminal.

Wallet: Wallet wordt gebruikt om creditcards, pinpassen, beloningskaarten en winkelkaarten toe te voegen en te beheren en om betalingen te verrichten met Apple Pay. Gebruikers kunnen in Wallet onder andere hun kaarten, het privacybeleid en aanvullende gegevens van de kaart-verstrekker, en recente transacties bekijken. Gebruikers kunnen ook via de configuratie-assistent en Instellingen kaarten toevoegen aan Apple Pay.

Secure Enclave: Op iPhone, iPad en Apple Watch beheert de Secure Enclave het verificatieproces en zorgt het ervoor dat een betalingstransactie kan worden uitgevoerd.

In het geval van een Apple Watch moet het apparaat zijn ontgrendeld en moet de gebruiker twee keer de knop aan de zijkant indrukken. Deze knopindrukken worden geregistreerd en rechtstreeks – buiten de processor om – doorgegeven aan het Secure Element (of de Secure Enclave, indien beschikbaar).

Apple Pay-servers: De Apple Pay-servers beheren de configuratie en aanlevering van creditcards en pinpassen in Wallet en de apparaat-rekeningnummers die in het Secure Element worden bewaard. De servers communiceren met het apparaat en met de servers in het betaalnetwerk. De Apple Pay-servers zijn ook verantwoordelijk voor het opnieuw coderen van betalingsreferenties voor betalingen binnen apps.

De functie van het Secure Element voor Apple Pay

Het Secure Element omvat een speciaal ontworpen applet om Apple Pay te beheren. Daarnaast bevat de chip betaal-applets die door de betaalnetwerken zijn gecertificeerd. De gegevens van creditcards, pinpassen en prepaidkaarten worden vanuit het betaalnetwerk of door

de kaartverstrekker gecodeerd verstuurd naar deze betaal-applets. Voor de codering worden sleutels gebruikt die alleen bekend zijn bij het betaalnetwerk en het beveiligingsdomein van de betaal-applets. Deze gegevens worden binnen deze betaal-applets opgeslagen en beschermd met de beveiligingsvoorzieningen van het Secure Element. Tijdens een transactie communiceert de terminal door middel van de NFC-controller (Near Field Communication) rechtstreeks met het Secure Element. Deze communicatie verloopt via een gereserveerde hardwarebus.

De functie van de NFC-controller in Apple Pay

De NFC-controller fungeert als gateway naar het Secure Element en zorgt ervoor dat alle contactloze betalingstransacties worden uitgevoerd via een POS-terminal die zich dicht in de buurt van het apparaat bevindt. Alleen betalingsaanvragen die binnenkomen van een terminal die zich binnen het bereik bevindt (in-field), worden door de NFC-controller gemarkeerd als contactloze transacties.

Nadat de kaarthouder de betaling door middel van Touch ID of een toegangscode via de Secure Enclave heeft geautoriseerd (of de betaling heeft geautoriseerd door op een ontgrendelde Apple Watch twee keer op de zijknop te drukken), worden contactloze reacties die binnen het Secure Element door de betaal-applets zijn opgesteld, exclusief door de controller naar het NFC-veld gerouteerd. Dit houdt in dat de autorisatiegegevens van contactloze betalingstransacties beperkt blijven tot het lokale NFC-veld en nooit zichtbaar zijn voor de processor van het apparaat. De autorisatiegegevens van betalingen binnen apps en op het web worden echter gerouteerd naar de processor van het apparaat, maar dit gebeurt pas nadat de gegevens door het Secure Element gecodeerd naar de Apple Pay-server zijn gestuurd.

Creditcards, pinpassen en prepaidkaarten toevoegen

Als een gebruiker een creditcard, pinpas of prepaidkaart (bijvoorbeeld winkelkaarten) toevoegt aan Apple Pay, worden de kaartgegevens op een veilige manier door Apple naar de kaartverstrekker (of de geautoriseerde dienstverlener van de kaartverstrekker) verstuurd. Tegelijkertijd worden ook andere gegevens van het profiel en het apparaat van de gebruiker verstuurd. Op basis van deze gegevens bepaalt de kaartverstrekker of de kaart kan worden gebruikt voor Apple Pay.

Apple Pay gebruikt tijdens het toevoegen van een betaalkaart drie aanroepen aan de serverkant om te communiceren met de kaartverstrekker of het netwerk: "Required Fields", "Check Card" en "Link and Provision". De kaartverstrekker of het netwerk gebruikt deze aanroepen om kaarten te controleren, goed te keuren en toe te voegen aan Apple Pay. Deze client-serversessies worden gecodeerd via TLS v1.2.

De feitelijke nummers van de kaart of pas worden niet op het apparaat of op Apple servers bewaard. In plaats daarvan wordt er een uniek apparaatrekeningnummer aangemaakt, dat vervolgens gecodeerd wordt opgeslagen in het Secure Element. Dit nummer wordt zo gecodeerd dat Apple geen toegang tot het nummer heeft. Het apparaatrekeningnummer is uniek en anders dan het nummer van reguliere creditcards of pinpassen. Het is mogelijk dat de kaartverstrekker niet toestaat om het nummer te gebruiken voor betalingen via een magneetstrip, via de telefoon of

op websites. Het apparaatrekeningnummer in het Secure Element is afgeschermd van iOS en watchOS, wordt nooit opgeslagen op servers van Apple en wordt nooit opgenomen in reservekopieën van iCloud.

Kaarten voor gebruik met Apple Watch worden voorbereid voor Apple Pay via de Apple Watch-app op iPhone. Het voorbereiden van een kaart voor Apple Watch is alleen mogelijk als het horloge zich binnen het Bluetooth-communicatiebereik bevindt. Kaarten worden specifiek geregistreerd voor gebruik met Apple Watch en hebben een eigen apparaatrekeningnummer, dat wordt opgeslagen binnen het Secure Element op de Apple Watch. Er zijn drie manieren om een creditcard, pinpas of prepaidkaart toe te voegen aan Apple Pay:

- Een kaart handmatig toevoegen aan Apple Pay
- Een creditcard of pinpas vanuit een iTunes Store-account toevoegen aan Apple Pay
- Een kaart toevoegen vanuit de app van de kaartverstrekker

Een creditcard of pinpas handmatig toevoegen aan Apple Pay

Om een betaalkaart (of andere kaart) handmatig toe te voegen, zijn de volgende gegevens nodig: de naam van de kaarthouder, het kaartnummer, de vervaldatum en de CVV-code. Gebruikers kunnen die gegevens vanuit Instellingen, de Wallet-app of de Apple Watch-app zelf invoeren of overbrengen via de camera op het apparaat. Als de kaart- of pasgegevens met de camera worden vastgelegd, wordt automatisch geprobeerd de naam, het nummer en de vervaldatum in te vullen. De foto wordt nooit opgeslagen op het apparaat of bewaard in de fotobibliotheek. Zodra alle velden zijn ingevuld, worden alle velden (behalve de CVV-code) geverifieerd tijdens het proces 'Check Card'. De gegevens worden vervolgens gecodeerd en naar de Apple Pay-server verstuurd.

Als tijdens het proces 'Check Card' een voorwaarden-ID wordt geretourneerd, worden de voorwaarden van de desbetreffende kaartverstrekker gedownload en weergegeven voor de gebruiker. Als de gebruiker akkoord gaat met de voorwaarden, verstuurt Apple de ID van de geaccepteerde voorwaarden, samen met de CVV-code, naar het proces 'Link and Provision'. Tijdens het proces 'Link and Provision' deelt Apple ook gegevens van het apparaat met de kaartverstrekker of het netwerk. Het betreft hier informatie over je iTunes- en App Store-account (bijvoorbeeld of je via iTunes veel transacties tot stand hebt gebracht) en informatie over je apparaat (zoals je telefoonnummer en naam en het model van je apparaat, plus een eventueel aanvullend iOS-apparaat dat nodig is om Apple Pay in te stellen). Daarnaast wordt vastgelegd waar je je bij benadering bevindt op het moment dat je de kaart toevoegt (dit gebeurt echter alleen als Locatievoorzieningen is ingeschakeld). Op basis van deze gegevens bepaalt de kaartverstrekker of de kaart kan worden gebruikt voor Apple Pay.

Als het proces 'Link and Provision' is voltooid, worden er twee bewerkingen gestart:

- Het Wallet-pasbestand voor de creditcard of betaalkaart wordt gedownload.
- De kaart wordt gekoppeld aan het Secure Element.

Het pasbestand bevat URL's voor het downloaden van illustraties voor de kaart of pas, metagegevens van de kaart of pas (zoals contactgegevens), de app van de verstrekker, en ondersteunde voorzieningen. Daarnaast bevat het bestand de status van de pas. Er kan bijvoorbeeld worden aangegeven of de personalisatie van het Secure Element is afgerond, of de kaart momenteel door de kaartverstrekker is geblokkeerd en of er aanvullende verificatie nodig is voordat de kaart kan worden gebruikt voor betalingen met Apple Pay.

Een creditcard of pinpas vanuit een iTunes Store-account toevoegen aan Apple Pay

Als een creditcard of pinpas wordt toegevoegd die bij iTunes is geregistreerd, kan de gebruiker worden gevraagd om het wachtwoord van de Apple ID opnieuw in te voeren. Het kaartnummer wordt vervolgens opgehaald uit iTunes, waarna het proces 'Check Card' wordt gestart. Als de kaart geschikt is voor Apple Pay, worden automatisch de voorwaarden gedownload en weergegeven, waarna de voorwaarden-ID en de CVV-code naar het proces 'Link and Provision' worden verstuurd. Er kan aanvullende verificatie plaatsvinden voor kaarten die in een iTunes-account zijn geregistreerd.

Een creditcard of pinpas toevoegen vanuit de app van de kaartverstrekker

Als de app wordt geregistreerd voor gebruik met Apple Pay, worden er sleutels gegenereerd voor de app en voor de server van de verkoper. Deze sleutels worden gebruikt om de kaartgegevens te coderen die naar de verkoper worden verstuurd. Op deze manier wordt voorkomen dat de gegevens worden gelezen door het iOS-apparaat. De werkwijze is vergelijkbaar met de werkwijze voor het handmatig toevoegen van kaarten (zoals hiervoor is beschreven), behalve dat er eenmalige wachtwoorden worden gebruikt in plaats van een CVV-code.

Aanvullende verificatie

De kaartverstrekker kan besluiten dat voor een creditcard of pinpas aanvullende verificatie nodig is. De kaartverstrekker kan verschillende mogelijkheden voor aanvullende verificatie bieden, zoals verificatie via sms, e-mail, de klantenservice of een app van een externe partij. Bij aanvullende verificatie via een sms of e-mail kiest de gebruiker de contactgegevens die bij de verstrekker zijn geregistreerd. Vervolgens wordt een code verstuurd, die de gebruiker moet invoeren in Wallet, Instellingen of de Apple Watch-app. Als de gebruiker kiest voor verificatie via de klantenservice of verificatie via een externe app, bepaalt de verstrekker het communicatieproces.

Autorisatie van betalingen

Op apparaten met een Secure Enclave wordt een betaling pas door het Secure Element toegestaan nadat er toestemming van de Secure Enclave is ontvangen. Op iPhone of iPad betekent dit dat er wordt gecontroleerd of de gebruiker zich heeft gelegitimeerd via Touch ID, Face ID of de toegangscode van het apparaat. Touch ID of Face ID (indien beschikbaar) is de standaardmethode, maar in plaats daarvan kan altijd de toegangscode worden gebruikt. De mogelijkheid om een toegangscode in te voeren, wordt automatisch aangeboden na drie mislukte pogingen met

Touch ID of twee mislukte pogingen met Face ID. Na vijf mislukte pogingen moet de toegangscode worden ingevoerd. Een toegangscode is ook verplicht wanneer Touch ID of Face ID niet is geconfigureerd of niet is ingeschakeld voor Apple Pay. In het geval van een Apple Watch moet het apparaat zijn ontgrendeld met een toegangscode en moet de gebruiker twee keer de knop aan de zijkant indrukken om een betaling te kunnen doen.

De communicatie tussen de Secure Enclave en het Secure Element verloopt via een seriële interface, waarbij het Secure Element wordt verbonden met de NFC-controller, die op zijn beurt is verbonden met de processor van het apparaat. Hoewel de Secure Enclave en het Secure Element niet rechtstreeks met elkaar zijn verbonden, kunnen ze veilig met elkaar communiceren via een gedeelde koppelingssleutel die tijdens de productie is verstrekt. De codering en verificatie van de communicatie zijn gebaseerd op AES, waarbij aan beide zijden cryptografische nonces worden gebruikt als bescherming tegen replay-aanvallen. Deze sleutel wordt binnen de Secure Enclave gegenereerd aan de hand van de UID-sleutel van de Enclave en de unieke ID van het Secure Element. De sleutel wordt vervolgens in de fabriek beveiligd overgebracht van de Secure Enclave naar een HSM (Hardware Security Module), waarna de sleutel hardwarematig wordt vastgelegd in het Secure Element.

Wanneer de gebruiker een transactie autoriseert, verstuurt de Secure Enclave ondertekende informatie over het type verificatie en informatie over het type transactie (contactloos of binnen apps) naar het Secure Element, gekoppeld aan een AR-waarde (Authorization Random). De AR wordt in de Secure Enclave gegenereerd op het moment dat een gebruiker voor het eerst een creditcard toevoegt en blijft aanwezig zolang Apple Pay is ingeschakeld. De waarde wordt beveiligd met het coderings- en anti-rollbackmechanisme van de Secure Enclave. De AR wordt via de koppelingssleutel op een veilige manier overgebracht naar het Secure Element. Als door het Secure Element een nieuwe AR-waarde wordt ontvangen, worden eerder toegevoegde kaarten als verwijderd gemarkeerd.

Creditcards, pinpassen en prepaidkaarten die aan het Secure Element zijn toegevoegd, kunnen alleen worden gebruikt als het Secure Element een autorisatie ontvangt waarvoor dezelfde koppelingssleutel en AR-waarde zijn gebruikt als bij het toevoegen van de creditcard of pinpas. Dit houdt in dat iOS in de volgende situaties de Secure Enclave opdracht kan geven om kaarten onbruikbaar te maken door het exemplaar van de AR in de Enclave als ongeldig te markeren:

- Als de toegangscode is uitgeschakeld.
- Als de gebruiker uitlogt bij iCloud.
- Als de gebruiker 'Wis alle inhoud en instellingen' selecteert.
- Als het apparaat wordt teruggezet vanuit de herstelmodus.

Bij Apple Watch worden kaarten in de volgende gevallen als ongeldig aangemerkt:

- Als de toegangscode van het horloge wordt uitgeschakeld.
- Als het horloge wordt losgekoppeld van de iPhone.
- Als draagdetectie wordt uitgeschakeld.

Het Secure Element gebruikt de koppelingssleutel en het exemplaar van de huidige AR-waarde om de autorisatie te verifiëren die van de Secure Enclave is ontvangen. Nadat de autorisatie is geverifieerd, wordt de

betaal-applet vrijgegeven voor een contactloze betaling. Dit proces vindt ook plaats bij het ophalen van gecodeerde betalingsgegevens uit een betaal-applet voor transacties binnen apps.

Transactiespecifieke, dynamische beveiligingscode

Alle betalingstransacties die uit de betaal-applets afkomstig zijn, bevatten een transactiespecifieke, dynamische beveiligingscode plus een apparaatrekeningnummer. Deze eenmalige code wordt vastgesteld aan de hand van een teller die voor elke nieuwe transactie wordt opgehoogd en een sleutel die tijdens de personalisatie in de betaal-applet wordt gegenereerd en die bekend is bij het betaalnetwerk en/of de kaartverstrekker. Afhankelijk van het betalingsschema kunnen er nog andere gegevens worden meegenomen bij de vaststelling van deze codes, zoals:

- Een willekeurig getal dat door de betaal-applet wordt gegenereerd
- Een ander willekeurig getal dat door de terminal wordt gegenereerd (bij NFC-transacties)

  of

- Een ander willekeurig getal dat door de server wordt gegenereerd (bij transacties binnen apps)

Deze beveiligingscodes worden aangeboden aan het betaalnetwerk en de kaartverstrekker, zodat transacties kunnen worden geverifieerd. De lengte van deze beveiligingscodes kan per type transactie variëren.

Contactloze betalingen met Apple Pay

Als de iPhone is ingeschakeld en een NFC-veld detecteert, verschijnt de relevante creditcard, pinpas of prepaidkaart, of de kaart die als standaardbetaalmiddel is opgegeven (via Instellingen). De gebruiker kan ook naar de app Wallet gaan en een creditcard of pinpas kiezen. Als het apparaat is vergrendeld, moet de gebruiker twee keer op de thuisknop drukken.

Vervolgens moet de gebruiker zich identificeren via Touch ID of Face ID of de toegangscode van het apparaat invoeren voordat de betalingsgegevens worden verstuurd. Als Apple Watch is ontgrendeld, drukt de gebruiker twee keer op de zijknop om de standaardkaart voor betaling te activeren. Er worden geen betalingsgegevens verstuurd als de gebruiker zich niet heeft geïdentificeerd. Nadat de identificatie is afgerond, wordt de betaling verwerkt aan de hand van het apparaatrekeningnummer en een transactiespecifieke, dynamische beveiligingscode. Het volledige nummer van een creditcard of pinpas wordt nooit door Apple of het apparaat van een gebruiker naar een verkoper verstuurd. Apple ontvangt mogelijk wel anonieme transactiegegevens, zoals de globale tijd en locatie van de transactie. Deze gegevens worden alleen gebruikt om Apple Pay en andere producten en diensten van Apple verder te verbeteren.

Betaling met Apple Pay binnen apps

Apple Pay kan ook worden gebruikt voor betalingen in iOS-apps en in Apple Watch-apps vanaf watchOS 3. Als gebruikers in apps met Apple Pay betalen, ontvangt Apple gecodeerde transactiegegevens, die vervolgens met een sleutel van de ontwikkelaar opnieuw worden gecodeerd voordat ze naar de ontwikkelaar of verkoper worden verstuurd. Apple Pay bewaart bepaalde, anonieme transactiegegevens, zoals het globale aankoopbedrag. Het is niet mogelijk om aan de hand van deze gegevens de identiteit van de gebruiker vast te stellen. Er wordt ook nooit geregistreerd wat de gebruiker heeft gekocht.

Als vanuit een app een betalingstransactie via Apple Pay wordt gestart, ontvangen de Apple Pay-servers de gecodeerde transactie van het apparaat voordat de verkoper deze ontvangt. De transactie wordt vervolgens met een sleutel van de verkoper opnieuw gecodeerd door de Apple Pay-servers, waarna de transactie wordt doorgestuurd naar de verkoper.

Als vanuit een app een betaling wordt aangevraagd, wordt een API aangeroepen om te controleren of het apparaat Apple Pay ondersteunt en of de gebruiker een creditcard of pinpas heeft waarmee betalingen kunnen worden uitgevoerd in een betaalnetwerk dat door de verkoper wordt geaccepteerd. De app vraagt welke gegevens nodig zijn om de transactie te verwerken en uit te voeren. Dit kunnen gegevens zijn zoals het factuuradres, het afleveradres en contactgegevens. De app verstuurt vervolgens een verzoek naar iOS om het venster van Apple Pay weer te geven, waarin wordt gevraagd om gegevens voor de app, evenals andere noodzakelijke informatie, zoals de kaart die moet worden gebruikt.

Op dit moment worden de woonplaats, provincie en postcode aan de app doorgegeven, zodat de definitieve verzendkosten kunnen worden berekend. De volledige set aangevraagde gegevens wordt pas aan de app aangeboden nadat de gebruiker de betaling heeft geautoriseerd via Touch ID of Face ID of door de toegangscode van het apparaat in te voeren. Na autorisatie van de betaling worden de gegevens in het venster van Apple Pay naar de verkoper verstuurd.

Wanneer de gebruiker de betaling autoriseert, wordt een aanroep naar de Apple Pay-servers verzonden om een cryptografische nonce op te vragen. Deze nonce is vergelijkbaar met de waarde die door de NFC-terminal wordt geretourneerd voor transacties in de winkel. De nonce wordt samen met andere transactiegegevens doorgegeven aan het Secure Element, zodat er een betalingsreferentie kan worden gegenereerd die vervolgens met een sleutel van Apple wordt gecodeerd. De gecodeerde betalingsreferentie wordt vanuit het Secure Element doorgegeven aan de Apple Pay-servers. Hier vinden nu de volgende bewerkingen plaats: de referentie wordt gedecodeerd, de nonce in de referentie wordt vergeleken met de nonce die door het Secure Element is verstuurd en de betalingsreferentie wordt opnieuw gecodeerd, nu met de speciale sleutel die aan de ID van de verkoper is gekoppeld. De referentie wordt vervolgens teruggestuurd naar

het apparaat, die de referentie via de API retourneert aan de app. De app stuurt de referentie ter verwerking door naar het transactiesysteem van de verkoper. Daar kan de betalingsreferentie worden gedecodeerd met de eigen private sleutel van de verkoper. Aan de hand van dit proces en de handtekening van de servers van Apple kan de verkoper controleren of de transactie inderdaad voor hem is bedoeld.

De API's hebben een recht nodig waarin de ondersteunde verkoper-ID's worden vermeld. Een app kan ook aanvullende gegevens meesturen om deze door het Secure Element te laten ondertekenen, zoals een ordernummer of klantidentiteit, om te voorkomen dat de transactie naar een andere klant wordt omgeleid. Dit moet door de ontwikkelaar van de app worden ingesteld. Deze kan hiertoe 'applicationData' opgeven in het PKPaymentRequest. Een hash van deze gegevens wordt opgenomen in de gecodeerde betalingsgegevens. Het is vervolgens de verantwoordelijkheid van de verkoper om te controleren of hun hash van applicationData overeenkomt met de hash in de betalingsgegevens.

Betaling met Apple Pay op het web of via Handoff

Met Apple Pay kunnen gebruikers op websites betalen. Onder iOS 10 of hoger kunnen op iPhone en iPad Apple Pay-transacties op het web worden uitgevoerd. Bovendien kunnen Apple Pay-transacties in macOS Sierra of hoger op een Mac worden gestart en op een iPhone of Apple Watch worden voltooid. Voorwaarde is wel dat die apparaten Apple Pay ondersteunen en dat daarop dezelfde iCloud-account wordt gebruikt.

Voor Apple Pay op het web moeten alle deelnemende websites zich bij Apple registreren. De Apple servers voeren een domeinnaamvalidatie uit en verstrekken een TLS-clientcertificaat. Websites die Apple Pay ondersteunen, zijn verplicht hun inhoud via HTTPS aan te bieden. Voor elke betaaltransactie moeten websites een beveiligde en unieke handelaarssessie met een Apple server instellen met het door Apple verstrekte TLS-clientcertificaat. De gegevens van een handelaarssessie worden door Apple ondertekend. Nadat een handtekening van een handelaarssessie is gecontroleerd, kan een website vragen of de gebruiker een apparaat heeft dat Apple Pay ondersteunt en of er een creditcard, pinpas of prepaidkaart op het apparaat is geactiveerd. Er worden geen andere gegevens gedeeld. Als de gebruiker deze gegevens niet wil delen, kunnen in macOS en iOS Apple Pay-vragen worden uitgeschakeld in de privacy-instellingen van Safari.

Wanneer een handelaarssessie is gevalideerd, zijn alle beveiligings- en privacymaatregelen hetzelfde als wanneer een gebruiker binnen een app betaalt.

Bij Handoff van Mac naar iPhone of Apple Watch gebruikt Apple Pay het IDS-protocol met end-to-end-codering om betalingsgegevens tussen de Mac van de gebruiker en het geautoriseerde apparaat uit te wisselen. De gegevens worden door IDS met de sleutels van het apparaat van de gebruiker gecodeerd, zodat deze gegevens door geen enkel ander apparaat kunnen worden gedecodeerd. De sleutels zijn ook niet beschikbaar voor Apple. Bij apparaatdetectie voor Apple Pay-handoff wordt gebruikgemaakt van het type en de unieke ID's van de creditcards

van de gebruiker, plus bepaalde metagegevens. Het apparaatgebonden rekeningnummer van de kaart van de gebruiker wordt niet gedeeld en blijft veilig bewaard op de iPhone of Apple Watch van de gebruiker. Apple brengt ook de recent gebruikte correspondentie-, verzend- en factuuradressen van de gebruiker op beveiligde wijze over via de iCloud-sleutelhanger.

Wanneer de gebruiker de betaling goedkeurt met Touch ID of Face ID, door op iPhone zijn of haar toegangscode in te voeren of door dubbel op de zijknop van Apple Watch te klikken, wordt een betalingstoken met een unieke codering voor het handelaarscertificaat van de desbetreffende website op veilige wijze van de iPhone of Apple Watch van de gebruiker naar zijn of haar Mac verzonden en vervolgens naar de website van de handelaar overgebracht.

Alleen apparaten die bij elkaar in de buurt zijn, kunnen betalingsverzoeken doen of betalingen uitvoeren. Deze nabijheid wordt bepaald via Bluetooth Low Energy-aankondigingen.

Beloningskaarten

In iOS 9 en hoger biedt Apple Pay ondersteuning voor het VAS-protocol (Value Added Service) voor het versturen van beloningskaarten van verkopers naar compatibele NFC-terminals. Het VAS-protocol kan worden geïmplementeerd op terminals van verkopers en gebruikt NFC om te communiceren met ondersteunde Apple apparaten. Het VAS-protocol werkt over een korte afstand en wordt gebruikt om als onderdeel van een Apple Pay-transactie aanvullende voorzieningen aan te bieden, zoals het versturen van gegevens van een beloningskaart.

De NFC-terminal start de ontvangst van de kaartgegevens door een verzoek om een kaart te versturen. Als de gebruiker een kaart met de winkel-ID heeft, wordt de gebruiker gevraagd om toestemming te geven voor het gebruik van de kaart. Als de verkoper codering ondersteunt, wordt er een coderingssleutel afgeleid voor de kaartgegevens die naar de terminal wordt verstuurd. Deze sleutel wordt vastgesteld aan de hand van de kaartgegevens, een tijdstempel en een willekeurige ECDH P-256-sleutel voor eenmalig gebruik, in combinatie met de openbare sleutel van de verkoper. Als de verkoper geen codering ondersteunt, wordt de gebruiker gevraagd om het apparaat opnieuw aan de terminal aan te bieden voordat de gegevens van de beloningskaart worden verstuurd.

Apple Pay Cash

Vanaf iOS 11.2 en watchOS 4.2 kan op een iPhone, iPad of Apple Watch met Apple Pay geld naar en van andere gebruikers worden verstuurd en ontvangen en kunnen geldverzoeken naar andere gebruikers worden verstuurd. Wanneer een gebruiker geld ontvangt, wordt dit toegevoegd aan een Apple Pay Cash-account. Deze account is toegankelijk in Wallet of via 'Instellingen' > 'Wallet & Apple Pay' op alle daarvoor in aanmerking komende apparaten waarop de gebruiker met zijn of haar Apple ID is aangemeld.

Voor betalingen tussen personen en voor Apple Pay Cash moet de gebruiker op een apparaat dat met Apple Pay Cash compatibel is bij zijn of haar iCloud-account zijn aangemeld en in de iCloud-account twee-factor-authenticatie hebben geconfigureerd.

Wanneer je Apple Pay Cash configureert, kan dezelfde informatie als bij het toevoegen van een creditcard of betaalkaart worden gedeeld met onze partnerbank Green Dot Bank en met Apple Payments Inc. Dit laatste bedrijf

is een volledige dochter van Apple die speciaal is opgezet om je privacy te beschermen: informatie wordt los van de rest van Apple en op een manier die de rest van Apple niet kent opgeslagen en verwerkt. Deze gegevens worden uitsluitend gebruikt voor het oplossen van problemen, voor het voorkomen van fraude en voor het naleven van de regelgeving.

Verzoeken om geld en overboekingen tussen gebruikers worden gestart vanuit de Berichten-app of door Siri hierom te vragen. Wanneer een gebruiker probeert om geld te versturen, wordt in iMessage het Apple Pay-venster weergegeven. Het Apple Pay Cash-saldo wordt altijd als eerste gebruikt. Indien nodig wordt het bedrag aangevuld met geld van een tweede creditcard of betaalkaart die de gebruiker aan Wallet heeft toegevoegd.

Met de Apple Pay Cash-kaart in Wallet kunnen betalingen worden gedaan in winkels, in apps en op het web. Geld in de Apple Pay Cash-account kan ook naar een bankrekening worden overgemaakt. Je kunt niet alleen geld van een andere gebruiker ontvangen, maar ook geld aan de Apple Pay Cash-account toevoegen vanaf een betaalkaart of prepaidkaart in Wallet.

Nadat een transactie is voltooid, worden de transactiegegevens door Apple Payments Inc. bewaard en indien nodig gebruikt voor het oplossen van problemen, het voorkomen van fraude en het naleven van de regelgeving. De rest van Apple weet niet naar wie jij geld hebt gestuurd, van wie je geld hebt ontvangen of waar je met je Apple Pay Cash-kaart iets hebt gekocht.

Wanneer de gebruiker met Apple Pay geld stuurt, geld aan een Apple Pay Cash-account toevoegt of geld naar een bankrekening overmaakt, gaat er een verzoek naar de Apple Pay-servers om een cryptografische nonce. Deze nonce is vergelijkbaar met de waarde die voor Apple Pay binnen apps wordt geretourneerd. De nonce wordt samen met andere transactiegegevens doorgegeven aan het Secure Element, zodat er een betalingshandtekening kan worden gegenereerd. Wanneer de betalingshandtekening het Secure Element verlaat, wordt die aan de Apple Pay-servers doorgegeven. De authenticatie, integriteit en juistheid van de transactie worden aan de hand van de betalingshandtekening en de nonce door de Apple Pay-servers geverifieerd. Vervolgens wordt het geld overgemaakt en wordt de gebruiker op de hoogte gesteld zodra de transactie is voltooid.

Als de transactie plaatsvindt met een creditcard of betaalkaart om:

- Geld aan Apple Pay Cash toe te voegen, of
- Geld naar een andere gebruiker te sturen, of
- Geld bij te storten als het Apple Pay Cash-saldo onvoldoende is,

wordt er naast de eerder beschreven overdrachtshandtekening ook een gecodeerde betalings-ID gegenereerd en naar de Apple Pay-servers gestuurd. Deze betalings-ID is vergelijkbaar met de ID die in apps en op websites voor Apple Pay wordt gebruikt.

Als het saldo van de Apple Pay Cash-account boven een bepaald bedrag komt, of als er ongebruikelijke activiteit wordt waargenomen, wordt de gebruiker gevraagd om zijn of haar identiteit te laten verifiëren. Gegevens die worden verstrekt om de identiteit van de gebruiker aan te tonen, zoals het burgerservicenummer of antwoorden op vragen (bijvoorbeeld in

welke straat je vroeger hebt gewoond), worden op veilige wijze naar de partner van Apple gestuurd en met zijn sleutel gecodeerd. Apple kan deze gegevens niet decoderen.

Suica Cards

In Japan kunnen gebruikers een Suica Card aan Apple Pay Wallet toevoegen op iPhone- en Apple Watch-modellen die dit ondersteunen. Hiervoor kunnen ze de waarde en forenzenpas van een fysieke kaart overbrengen naar de digitale versie daarvan in Wallet of een nieuwe Suica Card vanuit de Suica-app in Wallet opnemen. Nadat een Suica Card aan Wallet is toegevoegd, kunnen gebruikers in winkels betalen of van het openbaar vervoer gebruikmaken met hun anonieme Suica Card, hun MySuica Card of een kaart met een forenzenpas.

Toegevoegde Suica Cards worden aan de iCloud-account van de gebruiker gekoppeld. Als de gebruiker meerdere kaarten aan Wallet toevoegt, kunnen de persoonsgegevens van de gebruiker en de bijbehorende accountgegevens door Apple of de uitgever van de ov-kaart aan elkaar worden gekoppeld. Zo kunnen bijvoorbeeld MySuica Cards aan anonieme Suica Cards worden gekoppeld. Suica Cards en transacties worden met een aantal hiërarchische cryptografische sleutels beveiligd.

Als het saldo van een fysieke kaart naar Wallet wordt overgebracht terwijl het om een anonieme Suica Card gaat, moeten gebruikers de laatste vier cijfers van het serienummer van de kaart invoeren. Als het gaat om een MySuica Card of een kaart met een forenzenpas, moeten gebruikers ook hun geboortedatum opgeven als bewijs dat ze de kaart daadwerkelijk in hun bezit hebben. Om passen van een iPhone naar een Apple Watch te kunnen overbrengen, moeten beide apparaten tijdens de overdracht online zijn.

Het saldo kan via Wallet of vanuit de Suica-app met creditcards en prepaidkaarten worden opgeladen. Hoe de beveiliging is geregeld wanneer het saldo met Apple Pay wordt opgeladen, wordt beschreven in het gedeelte "Betaling met Apple Pay binnen apps" in dit document.

Hoe de Suica Card vanuit de Suica-app kan worden toegevoegd, wordt beschreven in het gedeelte "Een creditcard of pinpas toevoegen vanuit de app van de kaartverstrekker" in dit document.

De uitgever van de ov-kaart beschikt over de cryptografische sleutels die nodig zijn om de echtheid van de fysieke kaart te controleren en de door de gebruiker ingevoerde gegevens te verifiëren. Na verificatie kan een Device Account Number voor het Secure Element worden aangemaakt en kan de toegevoegde pas met het overgebrachte saldo in Wallet worden geactiveerd. Zodra de virtuele kaart is toegevoegd, wordt de fysieke kaart uitgeschakeld.

Ongeacht hoe de kaart wordt toegevoegd, wordt het Suica-saldo na de toevoeging van de kaart gecodeerd en bewaard in een speciale applet in het Secure Element. Het ov-bedrijf beschikt over de sleutels die nodig zijn om voor saldotransacties cryptografische bewerkingen op de kaartgegevens uit te voeren.

Gebruikers genieten standaard van de naadloze Express Transit-ervaring waarbij ze zonder Touch ID, Face ID of een toegangscode met het ov kunnen reizen. Informatie zoals onlangs bezochte stations, transactiegeschiedenis en extra kaartjes is toegankelijk via elke contactloze kaartlezer in de buurt wanneer de Express Mode is

ingeschakeld. Gebruikers kunnen verplichte autorisatie met Touch ID, Face ID of een toegangscode inschakelen in de instellingen van Wallet & Apple Pay door Express Transit uit te schakelen.

Net als bij andere Apple Pay-kaarten kunnen gebruikers Suica Cards op de volgende manieren opschorten of verwijderen:

- Door het apparaat op afstand met Zoek mijn iPhone te wissen
- Door de verloren-modus in te schakelen met Zoek mijn iPhone
- Door het apparaat op afstand te wissen met MDM
- Door alle kaarten op hun Apple ID-accountpagina te verwijderen
- Door alle kaarten uit iCloud.com te verwijderen
- Door alle kaarten uit Wallet te verwijderen

De ov-maatschappij wordt door Apple Pay-servers verzocht om de desbetreffende Suica Cards uit te schakelen. Als gebruikers hun Suica Cards proberen te verwijderen terwijl hun apparaat offline is, kunnen deze kaarten bij bepaalde terminals nog tot 12:01 AM JST de volgende dag te gebruiken zijn.

Als gebruikers hun Suica Cards verwijderen, is het saldo nog terug te halen. Ze kunnen dat de volgende dag na 5:00 AM JST weer toevoegen aan een apparaat waarop ze met dezelfde Apple ID zijn aangemeld.

Suica Cards kunnen niet worden opgeschort als je apparaat offline is.

Kaarten blokkeren, verwijderen en wissen

Gebruikers kunnen Apple Pay blokkeren op iPhone, iPad en Apple Watch met watchOS 3 door het apparaat via Zoek mijn iPhone in de verloren-modus te zetten. Daarnaast kunnen gebruikers hun kaarten uit Apple Pay verwijderen en wissen via Zoek mijn iPhone, via iCloud.com of rechtstreeks op hun apparaat met Wallet. Op een Apple Watch kunnen kaarten worden verwijderd via iCloud-instellingen, met de Apple Watch-app op de iPhone of rechtstreeks op de Watch. De mogelijkheid om op het apparaat met kaarten te betalen, wordt in dat geval door de kaartverstrekker of het betaalnetwerk opgeschort of uit Apple Pay verwijderd, zelfs als het apparaat offline is en niet is verbonden met een mobiel of wifinetwerk. Gebruikers kunnen ook de kaartverstrekker bellen met het verzoek om hun kaart op te schorten of uit Apple Pay te verwijderen.

Als een gebruiker het volledige apparaat wist met 'Wis alle inhoud en instellingen', via Zoek mijn iPhone of door het apparaat te herstellen via de herstelmodus, ontvangt het Secure Element opdracht van iOS om alle kaarten als verwijderd te markeren. Als gevolg hiervan worden de kaarten onmiddellijk onbruikbaar gemaakt, totdat contact kan worden opgenomen met de Apple Pay-servers om de kaarten in het Secure Element volledig te wissen. Los daarvan wordt de AR in de Secure Enclave als ongeldig gemarkeerd, zodat verdere betalingsautorisaties voor eerder geregistreerde kaarten niet meer mogelijk zijn. Als het apparaat online is, wordt er geprobeerd contact op te nemen met de Apple Pay-servers om er zeker van te zijn dat alle kaarten in het Secure Element zijn gewist.

Internetvoorzieningen

Sterke wachtwoorden voor Apple ID's
Apple ID's worden gebruikt om verbinding te maken met een aantal voorzieningen, waaronder iCloud, FaceTime en iMessage. Sterke wachtwoorden voor accounts hebben de volgende kenmerken:

- Minimaal acht tekens
- Minimaal één letter
- Minimaal één hoofdletter
- Minimaal één cijfer
- Niet meer dan drie opeenvolgende, identieke tekens
- Niet hetzelfde als de accountnaam

Apple heeft een uitgebreide reeks voorzieningen ontwikkeld om gebruikers nog meer gebruiksmogelijkheden te geven. Het betreft hier voorzieningen zoals iMessage, FaceTime, Siri-suggesties, iCloud, iCloud-reservekopie en de iCloud-sleutelhanger.

Deze internetvoorzieningen zijn ontwikkeld vanuit dezelfde beveiligingsdoelstellingen als voor de overige onderdelen van het iOS-platform gelden. Deze doelstellingen zijn onder meer een veilige verwerking van gegevens (tijdens opslag op het apparaat en tijdens overdracht via draadloze netwerken), bescherming van de persoonlijke gegevens van de gebruikers, en het voorkomen van toegang tot informatie en voorzieningen door kwaadwillenden of onbevoegden. Elke voorziening maakt gebruik van een eigen, krachtige beveiligingsarchitectuur zonder dat dit ten koste gaat van de gebruiksvriendelijkheid van iOS.

Apple ID

Een Apple ID is de account die wordt gebruikt om in te loggen bij Apple voorzieningen zoals iCloud, iMessage, FaceTime, de iTunes Store, de iBooks Store en de App Store. Het is belangrijk dat gebruikers hun Apple ID geheimhouden, om zo onbevoegde toegang tot hun accounts te voorkomen. Om dit gemakkelijker te maken, verlangt Apple sterke wachtwoorden die uit minimaal acht tekens bestaan, die letters en cijfers bevatten, waarin niet drie tekens achter elkaar hetzelfde zijn en die niet uit veelgebruikte woorden bestaan. Gebruikers wordt aangeraden om nog verder te gaan dan deze richtlijnen en extra tekens en leestekens toe te voegen om zo hun wachtwoorden nog sterker te maken. Gebruikers moeten daarnaast drie beveiligingsvragen instellen. Hiermee kan de identiteit van een gebruiker worden geverifieerd als deze wijzigingen aanbrengt in de accountgegevens of een vergeten wachtwoord opnieuw wil instellen.

Apple stuurt ook e-mail- en push-meldingen naar gebruikers als er belangrijke wijzigingen zijn in hun account, bijvoorbeeld als een wachtwoord of factureringsinformatie is gewijzigd, of als de Apple ID is gebruikt om in te loggen op een nieuw apparaat. Als iets er niet vertrouwd uitziet, wordt gebruikers gevraagd om het wachtwoord voor hun Apple ID meteen te wijzigen.

Apple hanteert daarnaast diverse beleidsregels en procedures die erop gericht zijn om gebruikersaccounts te beschermen. Zo geldt er een beperking voor het aantal pogingen om in te loggen of om een wachtwoord opnieuw te instellen en wordt met actieve fraudecontrole geprobeerd om eventuele aanvallen tijdig op te sporen. De beleidsregels worden regelmatig herzien om in te spelen op nieuwe ontwikkelingen die impact hebben op de beveiliging van gebruikers.

Twee-factor-authenticatie

Met *twee-factor-authenticatie* biedt Apple gebruikers een extra methode om hun account te beveiligen. Dit dient als extra beveiligingslaag voor Apple ID's en zorgt ervoor dat alleen de eigenaar van een account toegang heeft tot die account, zelfs als iemand anders het wachtwoord kent.

Met twee-factor-authenticatie is een gebruikersaccount alleen toegankelijk op apparaten die de gebruiker als vertrouwd heeft aangemerkt, zoals zijn of haar iPhone, iPad of Mac. Een gebruiker die voor het eerst inlogt op een nieuw apparaat, moet het wachtwoord van de Apple ID opgeven en een zescijferige verificatiecode die automatisch op de vertrouwde apparaten van de gebruiker wordt weergegeven of naar een vertrouwd telefoonnummer wordt verstuurd. Door de code in te voeren bevestigt de gebruiker dat het nieuwe apparaat wordt vertrouwd en dat het veilig is om in te loggen. Deze twee-factor-authenticatie, waarbij een gebruikersaccount niet meer alleen met een wachtwoord toegankelijk is, zorgt voor een betere beveiliging van Apple ID's en alle persoonlijke informatie die een gebruiker bij Apple bewaart. Deze functionaliteit is rechtstreeks in iOS, macOS, tvOS en watchOS geïntegreerd, en tevens in de verificatiesystemen die op de websites van Apple worden gebruikt.

Voor meer informatie over twee-factor-authenticatie ga je naar: https://support.apple.com/nl-nl/HT204915.

Twee-staps-verificatie

Apple biedt sinds 2013 een vergelijkbare beveiligingsmethode die *twee-staps-verificatie* wordt genoemd. Als twee-staps-verificatie is ingeschakeld, moet voor bepaalde acties de identiteit van de gebruiker worden geverifieerd via een tijdelijke code die naar een van de vertrouwde apparaten van de gebruiker wordt verstuurd. Bij deze acties gaat het om het wijzigen van de accountgegevens van de Apple ID van de gebruiker, het inloggen bij iCloud, iMessage, FaceTime of Game Center, en het doen van aankopen bij de iTunes Store, iBooks Store of App Store vanaf een nieuw apparaat. Gebruikers krijgen ook een herstelcode van 14 tekens die ze op een veilige plaats moeten bewaren en die ze kunnen gebruiken als ze hun wachtwoord zijn vergeten of geen toegang meer hebben tot hun vertrouwde apparaten. Hoewel de meeste nieuwe gebruikers worden aangemoedigd om twee-factor-authenticatie te gebruiken, zijn er nog steeds situaties waarin twee-staps-verificatie wordt aangeraden.

Voor meer informatie over twee-staps-verificatie voor Apple ID's ga je naar: https://support.apple.com/nl-nl/HT204152

Beheerde Apple ID's

Beheerde Apple ID's lijken op gewone Apple ID's, maar zijn het eigendom van een onderwijsinstelling die ook de controle over de ID's heeft. De onderwijsinstelling kan wachtwoorden opnieuw instellen en beperkingen instellen voor het doen van aankopen en voor communicatievoorzieningen zoals FaceTime en Berichten. Ook kan de instelling bevoegdheden op basis van rollen instellen voor docenten, leerlingen en ondersteunend personeel.

Sommige voorzieningen van Apple zijn uitgeschakeld voor beheerde Apple ID's, zoals Apple Pay, de iCloud-sleutelhanger, HomeKit en Zoek mijn iPhone.

Voor meer informatie over beheerde Apple ID's ga je naar: https://help.apple.com/schoolmanager/

Apple ID's inspecteren

Beheerde Apple ID's kunnen worden geïnspecteerd, zodat instellingen kunnen nagaan of ze aan wettelijke en privacyrichtlijnen voldoen. Aan de accounts van beheerders, managers en docenten kunnen inspectiebevoegdheden worden toegekend voor specifieke beheerde Apple ID's. Inspecteurs kunnen alleen accounts controleren die in de

hiërarchie van de school onder hen staan. Docenten kunnen dus leerlingen inspecteren, managers kunnen docenten en leerlingen inspecteren en beheerders kunnen managers, docenten en leerlingen inspecteren.

Wanneer via Apple School Manager identiteitsgegevens voor inspectie worden aangevraagd, wordt een speciale account verstrekt die alleen toegang geeft tot de beheerde Apple ID waarvoor inspectie is aangevraagd. De inspectiebevoegdheden zijn zeven dagen lang geldig. In die zeven dagen kan de inspecteur het gebruikers-materiaal lezen en wijzigen dat in iCloud of in CloudKit-apps is opgeslagen. Elk verzoek om inspectietoegang wordt in Apple School Manager in een logbestand geregistreerd. Daarbij wordt de naam van de inspecteur vermeld, de beheerde Apple ID waarvoor toegang is aangevraagd, het tijdstip van het verzoek en of de inspectie is uitgevoerd.

Beheerde Apple ID's en persoonlijke apparaten

Beheerde Apple ID's kunnen ook worden gebruikt voor iOS-apparaten en Mac-computers die in privébezit zijn. Leerlingen loggen dan in bij iCloud met de beheerde Apple ID die door de instelling is verstrekt, en met een extra wachtwoord voor thuisgebruik dat als tweede factor fungeert in de twee-factor-authenticatie van de Apple ID. Als een beheerde Apple ID op een persoonlijk apparaat wordt gebruikt, is de iCloud-sleutelhanger niet beschikbaar. Ook is het mogelijk dat de instelling beperkingen heeft ingesteld voor andere voorzieningen, zoals FaceTime en Berichten. Alle iCloud-documenten die leerlingen aanmaken terwijl ze ingelogd zijn, kunnen worden geïnspecteerd (zie hierboven).

iMessage

Apple iMessage is een berichtenvoorziening voor iOS-apparaten, Apple Watch en Mac-computers. iMessage ondersteunt tekst en bijlagen, zoals foto's, contacten en locaties. Berichten worden weergegeven op alle geregistreerde apparaten van een gebruiker, zodat een gesprek op elk van die apparaten kan worden voortgezet. iMessage maakt uitgebreid gebruik van de Apple Push Notification Service (APNS). De inhoud van berichten en bijlagen worden niet opgeslagen door Apple; deze worden beveiligd met end-to-end-codering, zodat ze alleen toegankelijk zijn voor de afzender en de ontvanger. De gegevens kunnen niet door Apple worden gedecodeerd.

Als een gebruiker iMessage inschakelt op een apparaat, worden er twee sleutelparen gegenereerd voor de voorziening: een 1280-bits-RSA-sleutel voor codering en een 256-bits-ECDSA-sleutel in de NIST P-256-curve voor ondertekening. De private sleutels voor beide sleutelparen worden bewaard in de sleutelhanger van het apparaat, terwijl de publieke sleutels worden verstuurd naar de adreslijstvoorziening van Apple (IDS), waar ze, samen met het APNS-adres van het apparaat, worden gekoppeld aan het telefoonnummer of e-mailadres van de gebruiker.

Als gebruikers extra apparaten inschakelen voor iMessage, worden de publieke coderings- en ondertekeningssleutels van die apparaten toegevoegd aan de adreslijstvoorziening, evenals de APNS-adressen en bijbehorende telefoonnummers. Gebruikers kunnen ook meer e-mailadressen toevoegen, die via een bevestigingskoppeling worden geverifieerd. Telefoonnummers worden geverifieerd door de

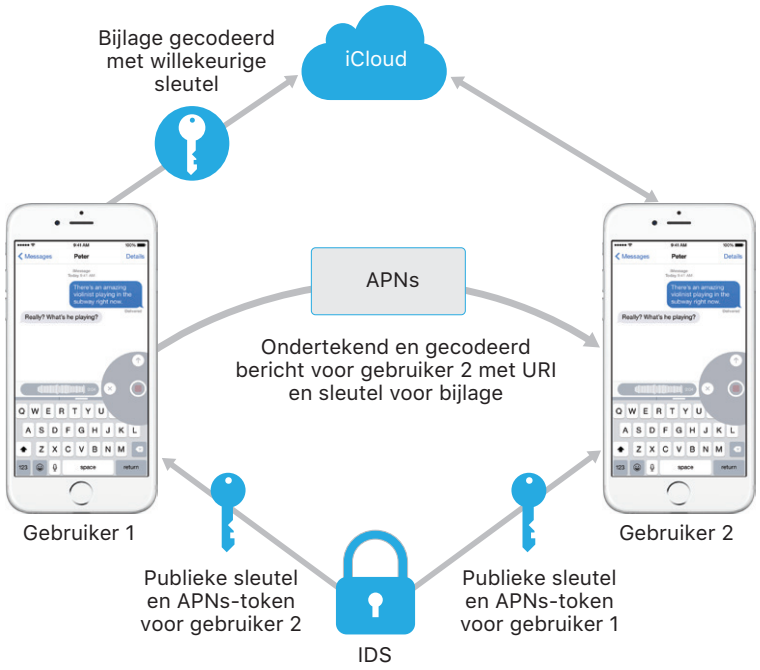
telefoonaanbieder en de sim. Bij bepaalde netwerken gebeurt dit per sms. (Als de sms niet gratis is, verschijnt eerst een dialoogvenster waarin de gebruiker de sms kan accepteren of weigeren.) Verificatie van het telefoonnummer kan ook nodig zijn voor andere systeemvoorzieningen dan iMessage, zoals FaceTime en iCloud. Er wordt op alle geregistreerde apparaten van de gebruiker een waarschuwing weergegeven wanneer een nieuw apparaat, telefoonnummer of e-mailadres wordt toegevoegd.

Berichten versturen en ontvangen met iMessage

Gebruikers starten een nieuw iMessage-gesprek door een adres of naam in te voeren. Als ze een telefoonnummer of e-mailadres invoeren, maakt het apparaat verbinding met de IDS om de publieke sleutels en APNS-adressen op te halen voor alle apparaten die aan de geadresseerde zijn gekoppeld. Als de gebruiker een naam invoert, worden eerst uit de app Contacten van de gebruiker de telefoonnummers en e-mailadressen opgehaald die aan die naam zijn gekoppeld. Vervolgens worden de publieke sleutels en APNS-adressen opgehaald uit IDS.

Het uitgaande bericht van de gebruiker wordt afzonderlijk gecodeerd voor elk van de apparaten van de ontvanger. De publieke RSA-coderingssleutels van de ontvangende apparaten worden opgehaald uit IDS. Het versturende apparaat genereert voor elk ontvangend apparaat een willekeurige 88-bits waarde en gebruikt deze als HMAC-SHA256-sleutel om een 40-bits waarde te genereren die is afgeleid van de publieke sleutel van de afzender en de ontvanger en van de platte tekst van het bericht. Uit de 88-bits waarde en de 40-bits waarde ontstaat een 128-bits sleutel, waarmee het bericht met AES in CTR-modus wordt gecodeerd. De 40-bits waarde wordt aan de ontvangende kant gebruikt om de integriteit van de gedecodeerde platte tekst te verifiëren. Deze berichtspecifieke AES-sleutel wordt via RSA-OAEP gecodeerd naar de publieke sleutel van het ontvangende apparaat. De combinatie van de gecodeerde berichttekst en de gecodeerde berichtsleutel wordt vervolgens via SHA-1 omgezet in een hash, die daarna wordt ondertekend met ECDSA en de private ondertekeningssleutel van het verzendende apparaat. De resulterende berichten (één voor elk ontvangend apparaat) bestaan uit de gecodeerde berichttekst, de gecodeerde berichtsleutel en de digitale handtekening van de afzender. De berichten worden voor bezorging afgeleverd bij de APNS. Metagegevens, zoals het tijdstempel en de routegegevens van de APNS, worden niet gecodeerd. De communicatie met de APNS wordt gecodeerd via een TLS-kanaal met forward-secrecy.

APNS kan alleen berichten met een maximale grootte van 4KB of 16KB doorgeven, afhankelijk van de iOS-versie. Als de berichttekst te lang is, of als er een bijlage met bijvoorbeeld een foto wordt toegevoegd, wordt de bijlage met een willekeurig gegenereerde 256-bits-sleutel gecodeerd via AES in de CTR-modus. Daarna wordt de bijlage geüpload naar iCloud. De AES-sleutel voor de bijlage, de bijbehorende URI (Uniform Resource Identifier) en een SHA-1-hash van het gecodeerde exemplaar worden vervolgens als de inhoud van een iMessage-bericht naar de ontvanger verstuurd. De vertrouwelijkheid en integriteit worden hierbij gegarandeerd via de gebruikelijke iMessage-codering, zoals hieronder schematisch wordt aangegeven.



Voor groepsgesprekken wordt dit proces herhaald voor iedere ontvanger en zijn of haar apparaten.

Op elk ontvangend apparaat komt een kopie van het bericht van de APNS binnen en wordt, indien nodig, de bijlage opgehaald uit iCloud. Het binnenkomende telefoonnummer of e-mailadres van de afzender wordt gekoppeld aan de contacten van de ontvanger, zodat er (indien mogelijk) een naam kan worden weergegeven.

Net als bij alle push-meldingen, wordt het bericht na bezorging verwijderd uit de APNS. In tegenstelling tot andere APNS-meldingen worden iMessage-berichten echter in een wachtrij geplaatst voor bezorging op offline apparaten. Op dit moment worden berichten maximaal 30 dagen bewaard.

FaceTime

FaceTime is de Apple voorziening voor video- en audiogesprekken. Net als voor iMessage-berichten wordt ook voor FaceTime-gesprekken gebruikgemaakt van de Apple Push Notification Service (APNS) om een eerste verbinding op te zetten met de geregistreerde apparaten van de gebruiker. De audio/video van FaceTime-gesprekken wordt beveiligd met end-to-end codering en is dus alleen toegankelijk voor de afzender en de ontvanger. De gegevens kunnen niet door Apple worden gedecodeerd.

De eerste FaceTime-verbinding wordt gemaakt via de Apple server-infrastructuur die gegevenspakketten tussen de geregistreerde apparaten van gebruikers doorstuurt. De apparaten maken gebruik van APNS-

meldingen en STUN-berichten (Session Traversal Utilities voor NAT) via de doorgeschakelde verbinding om hun identiteitscertificaten te verifiëren en voor elke sessie een gedeeld geheim in te stellen. Met het gedeelde geheim worden sessiesleutels opgehaald voor mediakanalen die met het Secure Real-time Transport Protocol (SRTP) worden gestreamd. SRTP-pakketten worden gecodeerd met AES-256 in Counter Mode en HMAC-SHA1. Na de eerste verbinding en beveiligingsconfiguratie maakt FaceTime gebruik van STUN en Internet Connectivity Establishment (ICE) om indien mogelijk een peer-to-peer-verbinding tussen de apparaten tot stand te brengen.

iCloud

In iCloud worden de contactpersonen, agenda's, foto's, documenten en ander materiaal van gebruikers bewaard. Dit materiaal wordt via iCloud automatisch op alle apparaten van een gebruiker up-to-date gehouden. iCloud kan ook door apps van andere leveranciers worden gebruikt om documenten en sleutelwaarden voor app-gegevens op te slaan en te synchroniseren. Gebruikers kunnen iCloud configureren door in te loggen met een Apple ID en de voorzieningen te kiezen die ze willen gebruiken. Voorzieningen van iCloud, zoals Mijn fotostream, iCloud Drive en iCloud-reservekopie, kunnen door IT-beheerders via MDM-configuratieprofielen worden uitgeschakeld. De voorziening is agnostisch over wat er wordt opgeslagen en verwerkt alle bestandsinhoud op dezelfde manier, als een verzameling bytes.

Elk bestand wordt door iCloud opgedeeld in chunks en gecodeerd met AES-128 en een sleutel die van de inhoud van een chunk wordt afgeleid en waarvoor SHA-256 wordt gebruikt. De sleutels, alsook de metagegevens van het bestand, worden door Apple opgeslagen in de iCloud-account van de gebruiker. De gecodeerde chunks van het bestand worden zonder identificerende gegevens opgeslagen via opslagvoorzieningen van derden, zoals S3 en Google Cloud Platform.

iCloud Drive

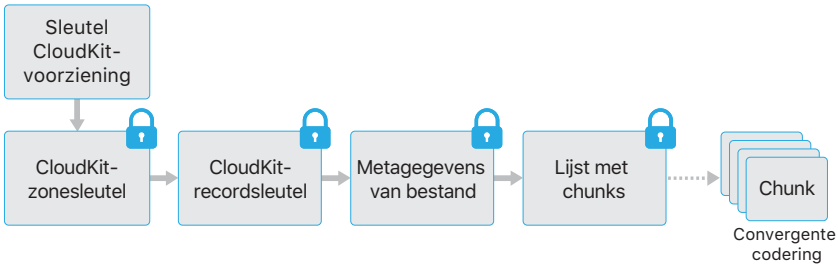
iCloud Drive voegt op accounts gebaseerde sleutels toe om in iCloud opgeslagen documenten te beveiligen. Net als bij bestaande iCloud-voorzieningen, wordt de inhoud van bestanden opgedeeld in chunks, die vervolgens worden gecodeerd en via voorzieningen van derden worden opgeslagen. De sleutels voor de bestandsinhoud worden echter ingepakt met recordsleutels die samen met de metagegevens van iCloud Drive worden opgeslagen. Deze recordsleutels worden op hun beurt beveiligd door de sleutel van de iCloud Drive-voorziening van de gebruiker, die vervolgens bij de iCloud-account van de gebruiker wordt opgeslagen. Gebruikers krijgen toegang tot de metagegevens van hun iCloud-documenten door zich te identificeren bij iCloud. Daarnaast moeten ze beschikken over de sleutel van de iCloud Drive-voorziening om de beveiligde onderdelen van de iCloud Drive-opslag te kunnen raadplegen.

CloudKit

CloudKit biedt app-ontwikkelaars de mogelijkheid om sleutelwaarde-gegevens, gestructureerde gegevens en bestanden (assets) op te slaan in iCloud. De toegang tot CloudKit wordt geregeld via app-rechten. CloudKit ondersteunt publieke en private databases. Publieke databases

worden door alle exemplaren van de app gebruikt (meestal voor algemene assets) en worden niet gecodeerd. In private databases worden de gebruikersgegevens opgeslagen.

CloudKit maakt, net als iCloud Drive, gebruik van op account gebaseerde sleutels om de informatie te beveiligen die in de private database van de gebruiker wordt bewaard. Net als bij andere iCloud-voorzieningen het geval is, worden bestanden ook opgedeeld in chunks die vervolgens worden gecodeerd en via externe voorzieningen worden opgeslagen. In CloudKit wordt een hiërarchie van sleutels gebruikt, vergelijkbaar met Gegevensbeveiliging. De bestandsspecifieke sleutels worden ingepakt met CloudKit-recordsleutels. De recordsleutels worden op hun beurt beveiligd met een zonesleutel, die weer wordt beveiligd met de gebruikerssleutel voor de CloudKit-voorziening. De sleutel voor de CloudKit-voorziening wordt opgeslagen in de iCloud-account van de gebruiker en is pas beschikbaar nadat de gebruiker zich heeft geïdentificeerd bij iCloud.



End-to-end-codering van CloudKit

Bij Apple Pay Cash, User Keywords, Siri Intelligence en Hé Siri wordt gebruikgemaakt van CloudKit end-to-end-codering met een CloudKit-voorzieningssleutel die door synchronisatie van iCloud-sleutelhanger wordt beveiligd. Voor deze CloudKit-containers heeft de sleutelhiërarchie zijn basis in iCloud-sleutelhanger, waardoor deze dezelfde beveiligings-kenmerken heeft als de iCloud-sleutelhanger: de sleutels zijn alleen beschikbaar op de vertrouwde apparaten van de gebruiker en zijn niet voor Apple of een derde partij beschikbaar. Als de toegang tot gegevens in de iCloud-sleutelhanger verloren is gegaan (zie het gedeelte "Escrow-beveiliging" verderop in dit document), worden de gegevens in CloudKit opnieuw ingesteld. Als er gegevens van het vertrouwde lokale apparaat beschikbaar zijn, worden deze opnieuw naar CloudKit geüpload.

iCloud-reservekopie

In iCloud worden ook dagelijks via wifi reservekopieën van allerlei inhoud bewaard, zoals apparaatinstellingen, app-gegevens, foto's en video's in de filmrol, en gesprekken in de Berichten-app. Deze inhoud wordt bij verzending via het internet gecodeerd en in een gecodeerde indeling opgeslagen. Bovendien worden beveiligde tokens gebruikt voor verificatie. Er worden alleen reservekopieën in iCloud gemaakt als het apparaat is vergrendeld, is aangesloten op een stopcontact en via wifi toegang heeft tot het internet. Door de codering die in iOS wordt gebruikt, is de gegevensbeveiliging gewaarborgd, terwijl er zonder tussenkomst van de gebruiker incrementele reservekopieën kunnen worden gemaakt en teruggezet.

In een reservekopie van iCloud worden de volgende onderdelen opgenomen:

- Gegevens over gekochte muziek, films, tv-programma's, apps en boeken. De iCloud-reservekopie bevat niet het gekochte materiaal zelf dat op het iOS-apparaat van de gebruiker staat, maar alleen gegevens daarover. Wanneer de gebruiker een reservekopie uit iCloud op zijn of haar apparaat terugzet, wordt het gekochte materiaal automatisch uit de iTunes Store, iBooks Store of App Store gedownload. Bepaalde typen materiaal worden niet in alle landen of regio's automatisch gedownload. Ook is het mogelijk dat eerdere aankopen niet beschikbaar zijn als het aankoopbedrag daarvoor is gerestitueerd of als ze niet meer in de desbetreffende Store staan. De volledige aankoopgeschiedenis is aan de Apple ID van de gebruiker gekoppeld.
- Foto's en video's op iOS-apparaten van een gebruiker. Houd er rekening mee dat als gebruikers iCloud-fotobibliotheek op hun iOS-apparaat (iOS 8.1 of hoger) of Mac (OS X versie 10.10.3 of hoger) inschakelen, hun foto's en video's al in iCloud worden bewaard en dus niet in de iCloud-reservekopie worden meegenomen.
- Contactgegevens, activiteiten uit Agenda, herinneringen en notities
- Apparaatinstellingen
- App-gegevens
- Oproepgeschiedenis en beltonen
- Beginscherm en rangschikking van apps
- HomeKit-configuratie
- Gegevens uit HealthKit
- iMessage-berichten, sms- en mms-berichten (hiervoor is de simkaart nodig die tijdens het maken van de reservekopie in gebruik was)
- Visual Voicemail-wachtwoord (hiervoor is de simkaart nodig die tijdens het maken van de reservekopie in gebruik was)

Wanneer bestanden worden aangemaakt in gegevensbeveiligingsklassen die niet toegankelijk zijn wanneer het apparaat is vergrendeld, worden de bijbehorende bestandsspecifieke sleutels gecodeerd met de klassesleutels uit de iCloud Backup-sleutelverzameling. Bestanden worden met hun oorspronkelijke, gecodeerde status opgenomen in de reservekopie van iCloud. Bestanden in de beveiligingsklasse 'Geen beveiliging' worden tijdens het transport gecodeerd.

De iCloud Backup-sleutelverzameling bevat voor elke gegevens-beveiligingsklasse asymmetrische sleutels (Curve25519), die worden gebruikt om de bestandsspecifieke sleutels te coderen. Zie "Gegevensbeveiliging via de sleutelhanger" in het gedeelte "Codering en beveiliging van gegevens" van dit document voor meer informatie over de inhoud van de backup-sleutelverzameling en de iCloud Backup-sleutelverzameling.

De reservekopieset wordt opgeslagen in de iCloud-account van de gebruiker en bestaat uit een kopie van de bestanden van de gebruiker en de iCloud Backup-sleutelverzameling. De iCloud Backup-sleutelverzameling wordt beveiligd met een willekeurige sleutel, die bij de reservekopieset wordt opgeslagen. (Het iCloud-wachtwoord van de

gebruiker wordt niet gebruikt voor coderingsdoeleinden, zodat bestaande reservekopieën ook na wijziging van het iCloud-wachtwoord nog steeds toegankelijk zijn.)

Hoewel er een reservekopie van de sleutelhangerdatabase van de gebruiker wordt bewaard in iCloud, blijft deze beveiligd met een sleutel die op de UID is gebaseerd. Hierdoor kan de sleutelhanger alleen worden teruggezet op het apparaat waarop de reservekopie van de sleutelhanger is gemaakt. Bovendien kunnen de sleutelhangeronderdelen van de gebruiker door niemand worden gelezen, ook niet door Apple.

In het geval van een herstelbewerking worden de bestanden in de reservekopie, de iCloud Backup-sleutelverzameling en de sleutel voor de sleutelverzameling opgehaald uit de iCloud-account van de gebruiker. De iCloud Backup-sleutelverzameling wordt met behulp van de bijbehorende sleutel gedecodeerd, waarna de bestandsspecifieke sleutels in de sleutelverzameling worden gebruikt om de bestanden in de reservekopieset te decoderen. Deze bestanden worden vervolgens als nieuwe bestanden weggeschreven naar het bestandssysteem, waardoor ze volgens de toegewezen gegevensbeveiligingsklasse opnieuw worden gecodeerd.

iCloud-sleutelhanger

Integratie van Safari met de iCloud-sleutelhanger
Safari kan automatisch cryptografisch sterke, willekeurige tekenreeksen genereren voor wachtwoorden voor websites. Deze reeksen worden opgeslagen in de sleutelhanger en worden gesynchroniseerd met andere apparaten. Sleutelhangeronderdelen worden via Apple servers uitgewisseld tussen apparaten, maar zijn zo gecodeerd dat de inhoud ervan niet door Apple en andere apparaten kan worden gelezen.

Met de iCloud-sleutelhanger kunnen gebruikers hun wachtwoorden veilig synchroniseren tussen iOS-apparaten en Mac-computers, zonder dat die informatie met Apple wordt gedeeld. Andere doelstellingen naast een hoge mate van privacy en beveiliging die een grote invloed hebben gehad op het ontwerp en de architectuur van de iCloud-sleutelhanger, waren gebruiksvriendelijkheid en de mogelijkheid om een sleutelhanger te herstellen. De iCloud-sleutelhanger bestaat uit twee componenten: synchronisatie en herstel.

Apple heeft de iCloud-sleutelhanger en sleutelhangerherstel zodanig ontworpen dat de wachtwoorden van een gebruiker ook in de volgende omstandigheden beveiligd zijn:

- Er zijn problemen met de beveiliging van de iCloud-account van een gebruiker.
- iCloud is gemanipuleerd door een externe aanvaller of een medewerker.
- Derden hebben toegang tot gebruikersaccounts.

Synchronisatie van sleutelhangers

Als een gebruiker de iCloud-sleutelhanger voor het eerst inschakelt, wordt er door het apparaat een vertrouwensketen ingesteld en een synchronisatie-ID aangemaakt. De synchronisatie-ID bestaat uit een private sleutel en een publieke sleutel. De publieke sleutel van de synchronisatie-ID wordt in de keten geplaatst en de keten wordt tweemaal ondertekend: eerst met de private sleutel van de synchronisatie-ID en vervolgens nog een keer met een asymmetrische, elliptische sleutel (via P-256) die wordt afgeleid van het wachtwoord van de iCloud-account van de gebruiker. In de vertrouwensketen worden ook de parameters (een willekeurige salt en iteraties) opgeslagen waarmee de sleutel wordt aangemaakt die op het iCloud-wachtwoord van de gebruiker is gebaseerd.

De ondertekende synchronisatieketen wordt toegevoegd aan het iCloud-opslaggebied voor sleutelwaarden van de gebruiker. De keten kan alleen worden gelezen als het iCloud-wachtwoord van de gebruiker bekend is. De private sleutel van de synchronisatie-ID van het apparaat is nodig om rechtmatig wijzigingen aan te brengen.

Als de gebruiker de iCloud-sleutelhanger inschakelt op een ander apparaat, wordt daarop vastgesteld dat de gebruiker een eerder aangemaakte vertrouwensketen in iCloud heeft waarvan het apparaat geen deel uitmaakt. Op het nieuwe apparaat wordt een sleutelpaar voor de eigen synchronisatie-ID gegenereerd en wordt vervolgens een ticket aangemaakt met het verzoek om in de keten te worden opgenomen. Het ticket bestaat uit de publieke sleutel van de synchronisatie-ID van de gebruiker, en de gebruiker wordt gevraagd zich te identificeren met zijn of haar iCloud-wachtwoord. De parameters voor het genereren van de elliptische sleutel worden opgehaald uit iCloud en worden gebruikt om een sleutel te genereren waarmee het ticket wordt ondertekend. Tot slot wordt het ticket in iCloud geplaatst.

Zodra op het eerste apparaat een ticket is ontvangen, wordt de gebruiker gevraagd of het nieuwe apparaat mag worden opgenomen in de synchronisatieketen. De gebruiker voert zijn of haar iCloud-wachtwoord in, waarna wordt geverifieerd dat het ticket door een overeenkomende private sleutel is ondertekend. Hiermee wordt bevestigd dat de persoon die het verzoek om opname in de keten heeft gegenereerd, het iCloud-wachtwoord van de gebruiker heeft ingevoerd bij het aanmaken van het verzoek.

Nadat de gebruiker toestemming heeft gegeven om het nieuwe apparaat toe te voegen aan de keten, voegt het eerste apparaat de publieke sleutel van het nieuwe apparaat toe aan de synchronisatieketen. Daarna wordt de sleutels nogmaals ondertekend door zowel de synchronisatie-ID als de sleutel die van het iCloud-wachtwoord van de gebruiker is afgeleid. De nieuwe synchronisatieketen wordt opgenomen in iCloud, waar deze op de aangegeven manier wordt ondertekend door het nieuwe apparaat in de keten.

De ondertekeningsketen heeft nu twee leden, en elk lid beschikt over de publieke sleutel van het andere lid. De apparaten gaan nu via het iCloud-opslaggebied voor sleutelwaarden afzonderlijke sleutelhangeronderdelen uitwisselen of ze gaan die sleutelwaarden opslaan in CloudKit. Als op beide apparaten in de keten hetzelfde onderdeel staat, wordt het onderdeel met de meest recente wijzigingsdatum gesynchroniseerd. Onderdelen die op beide apparaten aanwezig zijn en dezelfde wijzigingsdatum hebben, worden overgeslagen. Elk onderdeel dat wordt gesynchroniseerd, wordt zodanig gecodeerd dat het alleen kan worden gedecodeerd door een apparaat dat door de gebruiker wordt vertrouwd. Het onderdeel kan niet door andere apparaten of door Apple worden gedecodeerd.

Dit proces wordt herhaald als er nog meer apparaten worden toegevoegd aan de synchronisatieketen. Als er bijvoorbeeld een derde apparaat wordt toegevoegd, verschijnt de bevestiging op de beide andere apparaten van de gebruiker. De gebruiker kan het nieuwe apparaat vanaf beide bestaande apparaten goedkeuren. Als er nieuwe apparaten worden toegevoegd, wordt elk apparaat gesynchroniseerd met het nieuwe apparaat om er zeker van te zijn dat ze allemaal dezelfde sleutelhangeronderdelen hebben.

De sleutelhanger wordt echter niet volledig gesynchroniseerd. Sommige onderdelen, zoals VPN-ID's, zijn namelijk apparaatspecifiek en mogen niet buiten het apparaat worden verspreid. Alleen onderdelen met het kenmerk `kSecAttrSynchronizable` worden gesynchroniseerd. Apple heeft dit kenmerk ingesteld voor de gegevens van Safari-gebruikers (waaronder gebruikersnamen, wachtwoorden en creditcardnummers), wifiwachtwoorden en HomeKit-coderingssleutels.

Daarnaast is het zo dat sleutelhangeronderdelen die door apps van derden zijn toegevoegd, standaard niet worden gesynchroniseerd. Ontwikkelaars moeten het kenmerk `kSecAttrSynchronizable` instellen wanneer ze onderdelen aan de sleutelhanger toevoegen.

Sleutelhangerherstel

De voorziening sleutelhangerherstel biedt gebruikers de mogelijkheid om hun sleutelhanger bij Apple in bewaring te geven, zonder dat Apple de wachtwoorden of de andere daarin opgenomen gegevens kan lezen. Zelfs als een gebruiker maar één apparaat heeft, kan sleutelhangerherstel een vangnet tegen gegevensverlies vormen. Dit is met name belangrijk als Safari wordt gebruikt voor het genereren van krachtige willekeurige wachtwoorden voor internetaccounts, aangezien deze wachtwoorden dan uitsluitend in de sleutelhanger worden bewaard.

Essentiële elementen van sleutelhangerherstel zijn een secundaire identiteitscontrole en een beveiligde bewaarvoorziening, die specifiek door Apple is ontwikkeld ter ondersteuning van deze voorziening. De sleutelhanger van de gebruiker wordt met een sterke toegangscode gecodeerd, en er wordt pas een exemplaar van de sleutelhanger uit de bewaarvoorziening afgegeven als aan een reeks strikte voorwaarden is voldaan.

Als iCloud-sleutelhanger wordt ingeschakeld en twee-factor-authenticatie voor de gebruikersaccount is ingeschakeld, wordt de toegangscode van het apparaat gebruikt om een in bewaring gegeven sleutelhanger te herstellen. Als twee-factor-authenticatie niet is geconfigureerd, wordt de gebruiker gevraagd om een beveiligingscode voor iCloud aan te maken door een zescijferige toegangscode op te geven. Zonder twee-factor-authenticatie kunnen gebruikers desgewenst ook een langere code opgeven of ze kunnen door het apparaat een willekeurige cryptografische code laten genereren die ze noteren en geheimhouden.

Vervolgens wordt vanaf het iOS-apparaat een kopie van de sleutelhanger van de gebruiker geëxporteerd, die ingepakt met sleutels in een asymmetrische sleutelverzameling wordt gecodeerd en in het iCloud-opslaggebied voor sleutelwaarden van de gebruiker wordt geplaatst. De sleutelverzameling wordt ingepakt met de iCloud-beveiligingscode van de gebruiker en de publieke sleutel van de HSM-cluster (Hardware Security Module) waarin de escrow-record wordt opgeslagen. Samen vormen deze elementen de iCloud-escrow-record van de gebruiker.

Als de gebruiker besluit om een willekeurige cryptografische beveiligingscode te accepteren in plaats van zelf een code van vier cijfers op te geven, is geen escrow-record nodig. In dat geval wordt de beveiligingscode van iCloud gebruikt om de willekeurige sleutel rechtstreeks in te pakken.

Naast het instellen van een beveiligingscode, moeten gebruikers een telefoonnummer registreren. Dit nummer wordt gebruikt voor een secundaire verificatie tijdens sleutelhangerherstel. De gebruikers ontvangen een sms die zij moeten beantwoorden om het herstelproces verder uit te voeren.

Escrow-beveiliging

iCloud biedt een beveiligde infrastructuur voor het bewaren van sleutelhangers die ervoor zorgt dat alleen bevoegde gebruikers en apparaten een herstelbewerking kunnen uitvoeren. Topografisch achter iCloud bevinden zich clusters met HSM-modules die de escrow-records

beschermen. Elke cluster heeft een sleutel voor het coderen van de escrow-records waarvoor de cluster verantwoordelijk is (zoals eerder in dit document beschreven).

Om een sleutelhanger te herstellen, moeten gebruikers zich identificeren met hun iCloud-account en het bijbehorende wachtwoord en moeten ze daarna een sms beantwoorden die naar het geregistreerde telefoonnummer is verstuurd. Als dit is gebeurd, moeten gebruikers hun beveiligingscode voor iCloud invoeren. De HSM-cluster controleert met behulp van het SRP-protocol (Secure Remote Password) of een gebruiker zijn of haar beveiligingscode van iCloud weet; de code zelf wordt niet naar Apple verstuurd. Alle leden van de cluster controleren los van elkaar of de gebruiker niet het maximale aantal toegestane pogingen heeft overschreden om zijn of haar record op te halen (zoals hierna beschreven). Als de meerderheid toestemming geeft, wordt de escrow-record door de cluster uitgepakt en naar het apparaat van de gebruiker verstuurd.

Vervolgens wordt op het apparaat de beveiligingscode van iCloud gebruikt om de willekeurige sleutel uit te pakken waarmee de sleutelhanger van de gebruiker is gecodeerd. Met die sleutel wordt dan de sleutelhanger (die inmiddels is opgehaald uit het iCloud-opslaggebied voor sleutelwaarden) gedecodeerd en hersteld op het apparaat. Er zijn slechts tien pogingen toegestaan om een escrow-record te verifiëren en op te halen. Na enkele mislukte pogingen wordt de record vergrendeld en moet de gebruiker Apple Support bellen om extra pogingen aan te vragen. Na de tiende mislukte poging wordt de escrow-record vernietigd door de HSM-cluster en kan de sleutelhanger niet meer worden hersteld. Op deze manier wordt voorkomen dat de record via een brute-force-aanval wordt opgevraagd. Het nadeel is alleen wel dat de gegevens in de sleutelhanger verloren gaan.

Deze beleidsregels zijn vastgelegd in de HSM-firmware. De toegangskaarten waarmee de firmware kan worden gewijzigd, zijn vernietigd. Een poging om de firmware aan te passen of de private sleutel in te zien, heeft tot gevolg dat de sleutel door de HSM-cluster wordt verwijderd. Als dit gebeurt, krijgt de eigenaar van elke sleutelhanger die met de cluster wordt beveiligd een bericht dat zijn of haar escrow-record verloren is gegaan. Zij kunnen er dan voor kiezen zich opnieuw in te schrijven.

Siri

Door gewoon te praten kunnen gebruikers onder andere berichten laten versturen, vergaderingen laten plannen en telefoonnummers laten kiezen door Siri. Siri gebruikt spraakherkenning, tekst-naar-spraak en een client-servermodel om op uiteenlopende verzoeken te kunnen reageren. De taken die door Siri worden ondersteund, zijn zo ontworpen dat alleen het absolute minimum aan persoonlijke gegevens wordt gebruikt en dat deze gegevens volledig beveiligd zijn.

Als Siri wordt ingeschakeld, genereert het apparaat willekeurige ID's voor gebruik met de spraakherkennings- en Siri-servers. Deze ID's worden alleen gebruikt binnen Siri en uitsluitend om de voorziening te verbeteren. Als Siri vervolgens wordt uitgeschakeld, genereert het apparaat een nieuwe willekeurige ID die wordt gebruikt als Siri weer wordt ingeschakeld.

Om de voorzieningen van Siri te kunnen gebruiken, worden sommige gebruikersgegevens op het apparaat verstuurd naar de server. Het gaat hier onder andere om gegevens van de muziekbibliotheek (namen van nummers, artiesten en afspeellijsten), de namen van lijsten met herinneringen, en namen en relaties die in Contacten zijn vastgelegd. Alle communicatie met de server verloopt via HTTPS.

Als er een Siri-sessie tot stand wordt gebracht, worden de voor- en achternaam van de gebruiker (uit Contacten) naar de server verstuurd, samen met een globale geografische locatie. Op basis van deze gegevens kan Siri de gebruiker persoonlijk aanspreken en vragen beantwoorden waarvoor een globale locatie volstaat, zoals vragen over het weer.

Als een nauwkeurige locatie nodig is, bijvoorbeeld om bioscopen in de buurt te vinden, vraagt de server het apparaat om een exactere locatie op te geven. Dit is een voorbeeld om te laten zien dat met de standaardinstellingen alleen gegevens naar de server worden verstuurd wanneer deze strikt noodzakelijk zijn voor het verwerken van het verzoek van de gebruiker. De gegevens van een sessie worden altijd na tien minuten van inactiviteit verwijderd.

Als Siri vanaf een Apple Watch wordt gebruikt, genereert het horloge een nieuwe willekeurige ID, zoals hierboven wordt beschreven. In plaats van de gegevens van de gebruiker opnieuw te versturen, bevatten de verzoeken ook de Siri-ID van de gekoppelde iPhone als verwijzing naar die gegevens.

De opname van de gesproken woorden van de gebruiker wordt naar de spraakherkenningsserver van Apple verstuurd. Als de taak alleen betrekking heeft op de dicteerfunctie, wordt de herkende tekst teruggestuurd naar het apparaat. Voor alle andere taken wordt de tekst geanalyseerd door Siri en, indien nodig, gecombineerd met gegevens uit het profiel dat aan het apparaat is gekoppeld. Als het verzoek bijvoorbeeld bestaat uit de tekst "send a message to my mom", worden de relaties en namen gebruikt die uit Contacten zijn geüpload. De opdracht voor de herkende actie wordt vervolgens teruggestuurd naar het apparaat om te worden uitgevoerd.

Veel functies van Siri worden onder aansturing van de server op het apparaat uitgevoerd. Als de gebruiker bijvoorbeeld aan Siri vraagt om een binnenkomend bericht voor te lezen, geeft de server het apparaat opdracht om de inhoud van ongelezen berichten voor te lezen. De inhoud en de afzender van het bericht worden niet naar de server verstuurd.

De opnamen van de stem van de gebruiker worden zes maanden bewaard, zodat het herkenningssysteem ze kan gebruiken om de stem van de gebruiker beter te begrijpen. Na zes maanden wordt er een andere kopie bewaard, zonder ID, die maximaal twee jaar door Apple kan worden gebruikt om Siri verder te verbeteren en te ontwikkelen. Om Siri te kunnen blijven verbeteren en de kwaliteit ervan te kunnen garanderen, kan Apple ook na die twee jaar gebruik blijven maken van een kleine selectie van de opnamen, transcripten en bijbehorende gegevens zonder ID. Daarnaast worden om dezelfde redenen nog opnamen bewaard die verwijzen naar muziek, sportteams en spelers, en bedrijven of nuttige plaatsen.

Siri kan ook handsfree worden ingeschakeld via stemactivering. De detectie van de stemactivering wordt lokaal uitgevoerd op het apparaat. In deze modus wordt Siri alleen geactiveerd wanneer het binnenkomende audiopatroon in voldoende mate overeenkomt met de geluidseigenschappen van de ingesproken activeringstekst.

Als de trigger wordt herkend, wordt de bijbehorende audio samen met de daaropvolgende Siri-opdracht ter verwerking naar de spraakherkenningsserver van Apple verstuurd. Hiervoor gelden dezelfde regels als bij andere tekstopnamen die met Siri zijn gemaakt.

Continuïteit

Continuïteit is een voorziening waarvoor gebruik wordt gemaakt van technologieën zoals iCloud, Bluetooth en wifi. Met de continuïteits-voorziening kunnen gebruikers taken van het ene apparaat overnemen op een ander apparaat, telefoneren, sms-berichten versturen en ontvangen en een mobiele internetverbinding delen.

Handoff

Met Handoff kan een gebruiker met een Mac en iOS-apparaten zijn of haar activiteiten automatisch overzetten naar het andere apparaat wanneer de apparaten zich bij elkaar in de buurt bevinden. Handoff maakt het dus mogelijk om snel te wisselen van apparaat en dan gewoon verder te werken.

Als een gebruiker vanaf een tweede Handoff-apparaat inlogt bij iCloud, worden de twee apparaten via Bluetooth Low Energy 4.0 en de APNS out-of-band gekoppeld. De afzonderlijke berichten worden op dezelfde manier gecodeerd als bij iMessage. Nadat de apparaten zijn gekoppeld, genereren ze elk een symmetrische 256-bits-AES-sleutel die wordt opgeslagen in de sleutelhanger van het apparaat. Deze sleutel wordt gebruikt voor het coderen en verifiëren van de Bluetooth Low Energy-aankondigingen waarmee de huidige activiteit van het apparaat aan andere in iCloud gekoppelde apparaten wordt doorgegeven via AES-256 in de GCM-modus. Hierbij worden ook maatregelen getroffen om replay te voorkomen. De eerste keer dat een apparaat een aankondiging ontvangt van een nieuwe sleutel, wordt er een Bluetooth Low Energy-verbinding opgezet met het eerste apparaat en worden de sleutels voor de codering van de aankondiging uitgewisseld. Deze verbinding wordt beveiligd met de gebruikelijke codering van Bluetooth Low Energy 4.0. Bovendien worden ook de afzonderlijke berichten gecodeerd, op ongeveer dezelfde manier als bij iMessage. In sommige situaties worden deze berichten verstuurd via APNS in plaats van via Bluetooth Low Energy. De payload van de activiteit wordt beveiligd en overgebracht zoals dat bij een iMessage-bericht gebeurt.

Handoff tussen native apps en websites

Via Handoff kan een native iOS-app webpagina's oppakken uit domeinen die rechtmatig worden beheerd door de ontwikkelaar van de app. Omgekeerd kunnen gebruikersactiviteiten in de native app worden voortgezet in een webbrowser.

Om te voorkomen dat native apps websites oppakken die niet door de ontwikkelaar worden beheerd, moet de app aantonen dat de webdomeinen onder het rechtmatige beheer vallen. De controle over een websitedomein wordt tot stand gebracht via het mechanisme dat voor gedeelde internetreferenties wordt gebruikt. Zie "Toegang tot in Safari bewaarde wachtwoorden" in het gedeelte "Codering en beveiliging van gegevens"

in dit document voor meer informatie. Het systeem moet controleren of een domeinnaam door een app wordt beheerd voordat de app de Handoff van gebruikersactiviteit mag accepteren.

De bron van Handoff van een webpagina kan elke browser zijn waarin de API's van Handoff zijn geïmplementeerd. Als de gebruiker een webpagina bekijkt, publiceert het systeem de domeinnaam van de webpagina in de gecodeerde bytes van de Handoff-aankondiging. Deze bytes kunnen alleen worden gedecodeerd door de andere apparaten van de gebruiker (zoals eerder in dit gedeelte is beschreven).

Op een ontvangend apparaat herkent het systeem dat een geïnstalleerde native app Handoff uit de aangekondigde domeinnaam accepteert, waarna het symbool van die native app wordt weergegeven als de Handoff-optie. Wanneer de app wordt gestart, ontvangt deze de volledige URL en de titel van de webpagina. Er worden geen andere gegevens van de browser doorgegeven aan de native app.

In omgekeerde richting kan een native app een fallback-URL opgeven voor het geval niet dezelfde native app is geïnstalleerd op een apparaat dat een Handoff ontvangt. Als dat zo is, wordt de standaardbrowser van de gebruiker weergegeven als de Handoff-app (als die browser de Handoff-API's heeft geïmplementeerd). Als Handoff wordt aangevraagd, wordt de browser gestart en ontvangt deze de fallback-URL die door de bron-app is opgegeven. De fallback-URL hoeft niet beperkt te zijn tot de domeinnamen die onder het beheer vallen van de ontwikkelaar van de native app.

Handoff van grotere hoeveelheden gegevens

Ontwikkelaars van apps hebben de mogelijkheid om naast de basis-functionaliteit van Handoff API's te implementeren die ondersteuning bieden voor het versturen van grotere hoeveelheden gegevens via door Apple ontworpen peer-to-peer-wifitechnologie (vergelijkbaar met de werking van AirDrop). De Mail-app gebruikt deze API's bijvoorbeeld om Handoff van een conceptmail te ondersteunen, die grote bijlagen kan bevatten.

Als een app deze mogelijkheid gebruikt, verloopt het proces in eerste instantie zoals hierboven is beschreven. Als echter de eerste payload is ontvangen via Bluetooth Low Energy, wordt door het ontvangende apparaat een nieuwe verbinding via wifi opgezet. Deze verbinding is gecodeerd (TLS) en is bedoeld voor de uitwisseling van de iCloud-identiteitscertificaten van de apps. De identiteit in de certificaten wordt vergeleken met de identiteit van de gebruiker. De verdere payloadgegevens worden via deze gecodeerde verbinding verstuurd totdat de overdracht is voltooid.

Universeel klembord

Universeel klembord is een voorziening waarmee de inhoud van het klembord van een gebruiker met Handoff veilig tussen zijn of haar apparaten wordt overgebracht. Zo kan de gebruiker op het ene apparaat iets kopiëren en dit vervolgens op een ander apparaat plakken. De inhoud wordt op dezelfde manier beveiligd als andere Handoff-gegevens en standaard via Universeel klembord gedeeld, tenzij de ontwikkelaar van de app ervoor kiest om delen niet toe te staan.

Nu is het zo dat apps altijd al toegang hebben tot gewone klembordgegevens, ongeacht of de gebruiker het klembord in de app heeft geplakt. Via Universeel klembord krijgen ook apps op andere apparaten van de gebruiker toegang tot deze gegevens (als de gebruiker daarop tenminste met dezelfde iCloud-account is ingelogd).

Automatische ontgrendeling

Mac-computers waarop Automatische ontgrendeling wordt ondersteund, maken gebruik van Bluetooth Low Energy en peer-to-peer-wifi om ervoor te zorgen dat de Apple Watch van de gebruiker zijn of haar Mac veilig kan ontgrendelen. Iedere compatibele Mac en Apple Watch waaraan een iCloud-account is gekoppeld, moet gebruikmaken van twee-factor-authenticatie.

Wanneer wordt ingesteld dat een Apple Watch een Mac mag ontgrendelen, wordt er met behulp van Automatische ontgrendelings-ID's een beveiligde koppeling tot stand gebracht. De Mac genereert een willekeurig, eenmalig te gebruiken ontgrendelingsgeheim en stuurt dit via deze koppeling naar de Apple Watch. Het geheim wordt op de Apple Watch bewaard en is alleen toegankelijk wanneer de Apple Watch ontgrendeld is (zie het gedeelte "Gegevensbeveiligingsklassen"). Noch de master-entropie, noch het nieuwe geheim is het wachtwoord van de gebruiker.

Tijdens een ontgrendelingsactie maakt de Mac via Bluetooth Low Energy verbinding met de Apple Watch. Vervolgens wordt er een beveiligde koppeling tussen de twee apparaten tot stand gebracht met de gedeelde sleutels die zijn gebruikt toen dit voor het eerst werd ingeschakeld. De Mac en Apple Watch bepalen vervolgens de afstand tussen de twee apparaten via peer-to-peer-wifi en een beveiligde sleutel die van de beveiligde koppeling is afgeleid. Als de apparaten binnen elkaars bereik zijn, wordt de beveiligde koppeling gebruikt om het vooraf gedeelde geheim te versturen om de Mac te ontgrendelen. Wanneer de ontgrendeling is geslaagd, wordt het huidige ontgrendelingsgeheim op de Mac vervangen door een nieuw eenmalig geheim en wordt het nieuwe ontgrendelingsgeheim via de koppeling naar de Apple Watch gestuurd.

Mobiele oproepen via iPhone

Als de Mac, iPad of iPod touch van een gebruiker zich in hetzelfde wifinetwerk bevindt als zijn of haar iPhone, kan de gebruiker op dat apparaat bellen en gebeld worden via de mobiele verbinding van de iPhone. Hiervoor moeten de apparaten met dezelfde Apple ID zijn ingelogd bij zowel iCloud als FaceTime.

Als een oproep binnenkomt, ontvangen alle geconfigureerde apparaten een melding via de Apple Push Notification Service. Voor elke melding wordt dezelfde end-to-end codering toegepast als bij iMessage. Apparaten in hetzelfde netwerk reageren door de UI voor binnenkomende oproepen weer te geven. Als de oproep wordt beantwoord, wordt de audio zonder vertraging vanaf de iPhone van de gebruiker doorgegeven via een beveiligde peer-to-peer-verbinding tussen de twee apparaten.

Wanneer een oproep op een van de apparaten wordt beantwoord, wordt het bellen van andere nabije en in iCloud gekoppelde apparaten beëindigd door een korte aankondiging via Bluetooth Low Energy 4.0. De bytes van de aankondiging worden op dezelfde manier gecodeerd als Handoff-aankondigingen.

Uitgaande oproepen worden ook aan iPhone doorgegeven via de Apple Push Notification Service, terwijl audio op dezelfde manier wordt verstuurd via de beveiligde peer-to-peer-koppeling tussen de apparaten.

Gebruikers kunnen deze functionaliteit uitschakelen op een apparaat door 'Bellen via de iPhone' uit te schakelen in de FaceTime-instellingen.

Sms-berichten doorsturen op een iPhone

Met de functie 'Stuur sms door' kunnen sms-berichten die op een iPhone binnenkomen, automatisch worden doorgestuurd naar een geregistreerde iPad, iPod touch of Mac van de gebruiker. Alle apparaten moeten wel met dezelfde Apple ID zijn ingelogd bij de iMessage-service. Wanneer de functie 'Stuur sms door' is ingeschakeld, worden door de gebruiker vertrouwde apparaten automatisch ingeschreven als twee-factor-authenticatie is ingeschakeld. In andere gevallen wordt de inschrijving van elk apparaat gecontroleerd door een code van zes willekeurige cijfers in te voeren die door iPhone wordt gegenereerd.

Nadat de apparaten zijn gekoppeld, worden de binnenkomende sms-berichten op iPhone gecodeerd en doorgestuurd naar de apparaten. Hierbij worden de methoden gebruikt die worden beschreven in het gedeelte "iMessage" in dit document. Eventuele antwoorden worden via dezelfde methode teruggestuurd naar de iPhone, waarna het antwoord als sms wordt verstuurd via het sms-overdrachtsmechanisme van de aanbieder. De functie 'Stuur sms door' kan worden uitgeschakeld in de instellingen van Berichten.

Instant Hotspot

iOS-apparaten die Instant Hotspot ondersteunen, gebruiken Bluetooth Low Energy om apparaten te detecteren die bij dezelfde iCloud-account zijn ingelogd en om met die apparaten te communiceren. Compatibele Mac-computers met OS X Yosemite of nieuwer gebruiken dezelfde technologie om iOS-apparaten met Instant Hotspot te detecteren en hiermee te communiceren.

Als een gebruiker wifi-instellingen op het iOS-apparaat invoert, verstuurt het apparaat een Bluetooth Low Energy-signaal met een ID die is overeengekomen door alle apparaten die bij dezelfde iCloud-account zijn ingelogd. De ID wordt gegenereerd op basis van een DSID (Destination Signaling Identifier) die aan de iCloud-account is gekoppeld, en wordt regelmatig gewijzigd. Als andere apparaten die bij dezelfde iCloud-account zijn ingelogd zich in de buurt van een ander apparaat bevinden en Persoonlijke hotspot ondersteunen, vangen deze het signaal op en reageren ze om hun beschikbaarheid aan te geven.

Als een gebruiker een apparaat kiest dat beschikbaar is voor Persoonlijke hotspot, wordt er een verzoek naar dat apparaat gestuurd om Persoonlijke hotspot in te schakelen. Dit verzoek wordt verstuurd via een verbinding die wordt gecodeerd met de standaardcodering van Bluetooth Low Energy. Bovendien wordt het verzoek zelf gecodeerd op een manier die te vergelijken is met iMessage-codering. Het apparaat reageert vervolgens via dezelfde Bluetooth Low Energy-verbinding, met dezelfde berichtspecifieke codering met gegevens over de verbinding via Persoonlijke hotspot.

Safari-suggesties, Siri-suggesties in Zoek, Zoek op, #beelden, News-app en News-widget in landen waarin News niet wordt ondersteund

Safari-suggesties, Siri-suggesties in Zoek, Zoek op, #beelden, News-app en News-widget in landen waarin News niet wordt ondersteund, tonen suggesties van buiten het apparaat van de gebruiker. De suggesties zijn afkomstig van bronnen zoals Wikipedia, de iTunes Store, lokale nieuwssites, resultaten uit Kaarten en de App Store. Er worden zelfs al suggesties gedaan voordat de gebruiker begint te typen.

Als een gebruiker in de adresbalk van Safari begint te typen, of Siri-suggesties opent of gebruikt in Zoek, Zoek op, #beelden, Zoek in de News-app of de News-widget in landen waarin News niet wordt ondersteund, wordt de volgende context gecodeerd via HTTPS naar Apple verstuurd om de gebruiker relevante resultaten te kunnen verstrekken:

- Een ID die uit privacyoverwegingen om de 15 minuten wordt gewijzigd
- De zoekopdracht van de gebruiker
- De meest waarschijnlijke voltooiing van de vraag op basis van context en eerdere zoekopdrachten in de cache
- De globale locatie van het apparaat, als de gebruiker locatievoorzieningen voor locatiegebonden suggesties heeft ingeschakeld. De mate van 'vervaging' is gebaseerd op de geschatte bevolkingsdichtheid op de locatie van het apparaat. Zo wordt een locatie op het platteland (met een lagere bevolkingsdichtheid) globaler aangegeven dan een locatie in het centrum van een stad, waar gebruikers doorgaans dichter op elkaar zitten. Gebruikers kunnen het versturen van locatiegegevens naar Apple uitschakelen door in Instellingen locatievoorzieningen voor locatiegebonden suggesties uit te schakelen. Als locatievoorzieningen zijn uitgeschakeld, kan Apple aan de hand van het IP-adres van het apparaat een globale locatie bepalen.
- Het apparaattype en of de zoekopdracht is gedaan in Siri-suggesties, Safari, Zoek op, de News-app of Berichten
- Het type verbinding
- Informatie over de drie apps die het laatst op het apparaat zijn gebruikt (om aanvullende zoekcontext te verstrekken). Hierbij worden alleen apps meegenomen die in een door Apple bijgehouden witte lijst van populaire apps zijn opgenomen en die in de afgelopen drie uur zijn gebruikt.
- Een lijst met populaire programma's op het apparaat
- Voorkeuren met betrekking tot taal, locaties en invoer
- Als het apparaat van de gebruiker toegang heeft tot muziek- of videoabonnementsdiensten, kunnen er gegevens zoals de naam van de abonnementsdienst en het type abonnement naar Apple worden verstuurd. De accountnaam, toegangscode of het wachtwoord van de gebruiker worden niet naar Apple verstuurd.
- Samengevatte weergave van interessante onderwerpen

Als een gebruiker een resultaat kiest of de app verlaat zonder een resultaat te hebben gekozen, worden er bepaalde gegevens naar Apple gestuurd om de kwaliteit van toekomstige zoekresultaten te verbeteren. Deze gegevens worden alleen aan dezelfde 15 minuten geldige sessie-ID gekoppeld en niet aan een bepaalde gebruiker. De feedback omvat een deel van de eerder beschreven contextuele informatie, plus interactiegegevens zoals:

- Tijdspannes tussen interacties en zoeknetwerkaanvragen
- Rangschikking en weergavevolgorde van suggesties
- De ID van het resultaat en de gekozen actie als het resultaat niet lokaal is, of de categorie als er een lokaal resultaat is gekozen
- Een markering om aan te geven of de gebruiker het resultaat heeft gekozen

De logbestanden van de suggesties, met daarin zoekacties, context en feedback, worden 18 maanden door Apple bewaard. Een deel van de loggegevens wordt maximaal vijf jaar bewaard. Hierbij gaat het bijvoorbeeld om zoekopdrachten, locatievoorkeuren, domein, globale locatie en geaggregeerde cijfers.

In sommige gevallen worden zoekopdrachten met veelvoorkomende woorden en woordgroepen doorgestuurd naar een erkende partner om de zoekresultaten van die partner te ontvangen en weer te geven. Apple laat de zoekopdrachten via een proxy lopen, zodat ook het IP-adres van de gebruiker en de zoekresultaten verborgen blijven. De communicatie met de partners wordt gecodeerd via HTTPS. Bij regelmatig terugkerende zoekopdrachten verstrekt Apple locatiegegevens op plaatsniveau, het type van het apparaat en de taal van de client als zoekcontext aan de partner. Dit heeft tot doel om de zoekresultaten te verbeteren. In iOS 11 worden zoekopdrachten van Siri-suggesties in Zoek niet naar partners gestuurd.

Omdat Apple inzicht wil krijgen in de prestaties van de suggesties op geografisch niveau en in verschillende typen netwerken, zodat Apple de suggesties kan verbeteren, worden de volgende gegevens zonder sessie-ID vastgelegd:

- Een deel van het IP-adres (zonder het laatste octet van IPv4-adressen en zonder het laatste 80-bits gedeelte van IPv6-adressen)
- Locatie (bij benadering)
- Tijd van de zoekopdracht (bij benadering)
- Latentie/overdrachtssnelheid
- Grootte van reactie
- Type verbinding
- Locatievoorkeuren
- Type apparaat en de app waaruit de zoekopdracht afkomstig is

Apparaatbeheer

iOS ondersteunt flexibele beveiligingsinstellingen en -configuraties die eenvoudig kunnen worden afgedwongen en beheerd. Hierdoor kunnen organisaties hun bedrijfsgegevens beveiligen en ervoor zorgen dat medewerkers aan de bedrijfseisen voldoen. Dit is zelfs mogelijk als ze werken met apparaten die ze zelf hebben gekocht en die ze mogen meenemen in het kader van een BYOD-programma (Bring Your Own Device).

Organisaties kunnen tools zoals wachtwoordbeveiliging, configuratie-profielen, wissen op afstand en MDM-oplossingen van derden inzetten om apparaten te beheren en de gegevens van het bedrijf te beschermen, ook wanneer medewerkers deze gegevens op hun eigen iOS-apparaten raadplegen.

Beveiliging met toegangscodes

De toegangscode van een gebruiker kan standaard bestaan uit een pincode met een aantal cijfers. Op apparaten met Touch ID of Face ID moet de toegangscode uit minimaal zes cijfers bestaan. Op andere apparaten is de minimale lengte vier cijfers. Gebruikers kunnen een langere alfanumerieke toegangscode opgeven door 'Aangepaste alfanumerieke code' te selecteren bij 'Toegangscodeopties' in Instellingen > 'Toegangs-code'. Langere en complexere toegangscodes zijn moeilijker te raden en aan te vallen en worden daarom aangeraden.

Beheerders kunnen complexe toegangscodes en andere beleidsregels afdwingen via MDM of Exchange ActiveSync. Het is ook mogelijk om gebruikers zelf configuratieprofielen te laten installeren. Dit zijn de beschikbare beleidsregels voor toegangscodes:

- Eenvoudige waarde toestaan
- Alfanumerieke waarde vereist
- Minimale lengte toegangscode
- Minimale aantal complexe tekens
- Maximale gebruiksduur toegangscode
- Geschiedenis toegangscodes
- Time-out voor automatische vergrendeling
- Maximale geldigheid toegangscode bij vergrendeling
- Maximale aantal mislukte pogingen
- Touch ID of Face ID toestaan

Voor beheerdersinformatie over elk beleid ga je naar: https://help.apple.com/deployment/ios/#/apd4D6A472A-A494-4DFD-B559-D59E63167E43

Voor ontwikkelaarsinformatie over elk beleid ga je naar: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

iOS-koppelingsmodel

In iOS wordt een koppelingsmodel gebruikt om de toegang tot een apparaat vanaf een hostcomputer te beheren. Door de koppeling wordt een vertrouwensrelatie tussen het apparaat en de daarmee verbonden host tot stand gebracht, wat blijkt uit de uitwisseling van publieke sleutels. Op basis van dit bewijs van vertrouwen worden in iOS aanvullende functies met de verbonden host beschikbaar gesteld, zoals gegevenssynchronisatie.

In iOS 9 kunnen voorzieningen waarvoor een koppeling nodig is, pas worden gestart nadat het apparaat door de gebruiker is ontgrendeld.

Bovendien moet het apparaat in iOS 10 voor bepaalde voorzieningen (zoals fotosynchronisatie) ontgrendeld zijn.

Vanaf iOS 11 kunnen voorzieningen alleen starten als het apparaat onlangs is ontgrendeld.

De koppeling komt tot stand als de gebruiker het apparaat ontgrendelt en het koppelverzoek van de host accepteert. Vanaf iOS 11 moet de gebruiker ook zijn of haar toegangscode invoeren. Als de gebruiker dit heeft gedaan, worden er 2048-bits publieke RSA-sleutels uitgewisseld en bewaard door de host en het apparaat. De host krijgt vervolgens een 256-bits sleutel waarmee een escrow-sleutelverzameling kan worden ontgrendeld die op het apparaat is opgeslagen (zie de informatie over escrow-sleutelverzamelingen in het gedeelte "Sleutelverzamelingen" in dit document). De uitgewisselde sleutels worden gebruikt voor het opzetten van een gecodeerde SSL-sessie, iets wat noodzakelijk is voordat het apparaat beveiligde gegevens naar de host stuurt of een voorziening start (iTunes-synchronisatie, bestandsoverdrachten, Xcode-ontwikkeling, enzovoort). Verbindingen met een host die via een wifinetwerk lopen, moeten voor alle communicatie gebruikmaken van deze gecodeerde sessie, wat inhoudt dat het apparaat al eerder via USB moet zijn gekoppeld. Koppeling maakt ook diagnostische mogelijkheden beschikbaar. Als in iOS 9 een koppelingsrecord langer dan zes maanden niet is gebruikt, verloopt de record. Deze periode is in iOS 11 verkort tot 30 dagen.

Voor meer informatie ga je naar:
https://support.apple.com/nl-nl/HT203034

Bepaalde voorzieningen, waaronder com.apple.pcapd, werken alleen via USB. Verder werkt de voorziening com.apple.file_relay alleen als er een door Apple ondertekend configuratieprofiel is geïnstalleerd.

In iOS 11 kan Apple TV met het Secure Remote Password-protocol draadloos een koppelingsrelatie tot stand brengen.

Een gebruiker kan de lijst met vertrouwde hosts wissen met de opties 'Herstel netwerkinstellingen' en 'Herstel locatie en privacy'.

Voor meer informatie ga je naar:
https://support.apple.com/nl-nl/HT202778

Configuratie afdwingen

Een configuratieprofiel is een XML-bestand waarmee een beheerder configuratiegegevens kan distribueren naar iOS-apparaten. Instellingen die met een geïnstalleerd configuratieprofiel worden gedefinieerd, kunnen niet door de gebruiker worden gewijzigd. Als de gebruiker een configuratieprofiel verwijdert, worden ook alle instellingen verwijderd die met het profiel zijn gedefinieerd. Op deze manier kunnen beheerders instellingen afdwingen door beleidsinstellingen te koppelen aan wifi- en gegevenstoegang. Zo kan in een configuratieprofiel met een e-mailconfiguratie ook een toegangscodebeleid voor een apparaat worden opgegeven. Gebruikers kunnen hun e-mail dan alleen raadplegen als hun toegangscode voldoet aan de vereisten die de beheerder heeft ingesteld.

Een iOS-configuratieprofiel bevat een aantal instellingen die kunnen worden opgegeven, zoals:

- Toegangscodebeleid
- Beperkingen van apparaatfuncties (bijvoorbeeld het uitschakelen van de camera)
- Wifi-instellingen
- VPN-instellingen
- Instellingen mailserver
- Exchange-instellingen
- Instellingen voor LDAP-adreslijstvoorziening
- Instellingen voor CalDAV-agendavoorziening
- Webknipsels
- Referenties en sleutels
- Geavanceerde instellingen voor mobiele netwerken

Voor een actuele lijst voor beheerders ga je naar:
https://help.apple.com/deployment/ios/#/cad5370d089

Voor een actuele lijst voor ontwikkelaars ga je naar:
https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

Configuratieprofielen kunnen worden ondertekend en gecodeerd om de oorsprong aan te tonen, de integriteit te garanderen en de inhoud te beveiligen. Configuratieprofielen worden gecodeerd met CMS (RFC 3852) en bieden ondersteuning voor 3DES en AES-128.

Configuratieprofielen kunnen ook worden gekoppeld aan een apparaat om te voorkomen dat de profielen worden verwijderd of om ervoor te zorgen dat ze alleen kunnen worden verwijderd nadat een toegangscode is ingevoerd. Aangezien veel medewerkers van een bedrijf eigenaar zijn van hun iOS-apparaat, is het wel mogelijk om configuratieprofielen te verwijderen waarmee een apparaat aan een MDM-oplossing wordt gekoppeld. Daarbij worden echter ook alle beheerde configuratiegegevens en apps verwijderd.

Gebruikers kunnen configuratieprofielen via Apple Configurator 2 rechtstreeks op hun apparaten installeren of configuratieprofielen downloaden via Safari. Configuratieprofielen kunnen ook via e-mail of draadloos via een MDM-oplossing worden verstuurd. Als een gebruiker een

apparaat configureert in het Device Enrollment Program of in Apple School Manager, wordt er op het apparaat een profiel voor MDM-inschrijving gedownload en geïnstalleerd.

Mobile Device Management (MDM)

iOS-ondersteuning voor MDM houdt in dat bedrijven op een veilige manier grote of kleine aantallen iPhones, iPads, Apple TV's en Macs binnen hun organisatie kunnen configureren en beheren. De MDM-voorzieningen zijn gebaseerd op bestaande iOS-technologieën, zoals configuratieprofielen, draadloze inschrijving en de Apple Push Notification Service (APNS). APNS wordt bijvoorbeeld gebruikt om het apparaat uit de slaapstand te halen, zodat via een beveiligde verbinding rechtstreekse communicatie met de MDM-oplossing mogelijk is. Via APNS wordt geen vertrouwelijke informatie verstuurd.

Met behulp van MDM kan de IT-afdeling iOS-apparaten op een veilige manier opnemen in de bedrijfsomgeving, de instellingen draadloos configureren en bijwerken, controleren of aan het bedrijfsbeleid wordt voldaan en zelfs op afstand de gegevens van beheerde apparaten wissen of apparaten vergrendelen.

Voor meer informatie over MDM ga je naar:
https://www.apple.com/nl/iphone/business/it/management.html

Gedeelde iPad

Gedeelde iPad maakt gedeeld gebruik van iPads mogelijk en is bedoeld voor implementaties in het onderwijs. Leerlingen kunnen een iPad delen zonder dat ze hun documenten en gegevens delen. Iedere leerling krijgt een eigen thuismap. Deze wordt als APFS-volume aangemaakt en wordt door de inloggegevens van de gebruiker beschermd. Voor Gedeelde iPad moeten beheerde Apple ID's worden gebruikt. Deze ID's worden door de school verstrekt en zijn ook eigendom van de school. Met Gedeelde iPad kan een leerling inloggen op elk apparaat van de instelling dat geconfigureerd is voor gebruik door meerdere leerlingen.

Per leerling worden de gegevens in afzonderlijke thuismappen bewaard, elk in hun eigen gegevensbeschermingsdomein. Elke map wordt beveiligd met zowel UNIX-toegangsrechten als sandboxing. Wanneer een leerling inlogt, wordt de beheerde Apple ID met behulp van het SRP-protocol gecontroleerd op de Apple servers voor identiteitscontrole. Bij een geslaagde controle wordt specifiek voor dat apparaat een toegangstoken verstrekt dat beperkte tijd geldig is. Als de leerling het apparaat eerder heeft gebruikt, is er al een lokale gebruikersaccount die met dezelfde inloggegevens wordt ontgrendeld. Als de leerling het apparaat nog niet eerder heeft gebruikt, worden een nieuwe UNIX-gebruikers-ID, een APFS-volume met de thuismap van de gebruiker en een logische sleutelhanger toegevoegd. Als het apparaat niet met het internet is verbonden (bijvoorbeeld omdat de gebruiker op een schoolreisje is), is gedurende een beperkt aantal dagen identiteitscontrole aan de hand van de lokale account mogelijk. In dat geval kunnen alleen gebruikers met reeds bestaande

lokale accounts inloggen. Wanneer de tijdslimiet is verlopen, moeten de leerlingen hun identiteit online laten verifiëren, ook als er al een lokale account aanwezig is.

Nadat de lokale account van de leerling is ontgrendeld of aangemaakt (bij een identiteitscontrole op afstand), wordt het beperkt geldige token dat door de servers van Apple is verstrekt, omgezet in een iCloud-token waarmee bij iCloud kan worden ingelogd. Vervolgens worden de instellingen van de leerling hersteld en worden de documenten en gegevens van de leerling met iCloud gesynchroniseerd.

Zolang de leerling ingelogd is en het apparaat verbonden blijft met het internet, worden alle aangemaakte of gewijzigde documenten en gegevens direct in iCloud bewaard. Daarnaast zorgt een synchronisatiemechanisme in de achtergrond ervoor dat alle wijzigingen naar iCloud worden gepusht zodra de leerling uitlogt. Nadat voor die gebruiker de synchronisatie op de achtergrond is voltooid, wordt het APFS-volume van de gebruiker losgekoppeld en kan het niet meer opnieuw worden gekoppeld zonder dat de inloggegevens van de gebruiker worden ingevoerd.

Als een Gedeelde iPad met een oudere versie dan iOS 10.3 wordt geüpgraded naar versie 10.3 of hoger, vindt er een eenmalige bestandssysteemconversie plaats om de HFS+-gegevenspartitie om te zetten in een APFS-volume. Als er op dat moment thuismappen van gebruikers op het systeem aanwezig zijn, blijven die mappen op het hoofdgegevensvolume staan in plaats van dat ze naar afzonderlijke APFS-volumes worden geconverteerd. Als er extra leerlingen inloggen, worden hun thuismappen ook op het hoofdgegevensvolume geplaatst. Zoals eerder beschreven, worden nieuwe gebruikersaccounts pas met een eigen APFS-volume aangemaakt als alle gebruikersaccounts van het hoofdgegevensvolume zijn verwijderd. Om ervoor te zorgen dat gebruikers over de extra bescherming en quota's van APFS beschikken, moet de iPad dus naar versie 10.3 of hoger worden geüpgraded (door het apparaat te wissen en de software opnieuw te installeren), of moeten alle gebruikersaccounts op het apparaat met het MDM-commando 'Verwijder gebruiker' worden verwijderd.

Apple School Manager

Apple School Manager is een voorziening waarmee onderwijsinstellingen materiaal kunnen kopen, apparaten automatisch bij een MDM-oplossing kunnen laten inschrijven, accounts voor leerlingen en personeel kunnen aanmaken, en cursussen van iTunes U kunnen opzetten. Apple School Manager is toegankelijk op het web en is bedoeld voor technologiemanagers, IT-beheerders, ondersteunend personeel en docenten.

Voor meer informatie over Apple School Manager ga je naar: https://help.apple.com/schoolmanager/

Apparaatinschrijving

Het Device Enrollment Program (DEP) is onderdeel van Apple School Manager en Apple Deployment Programs en voorziet in een snelle, gestroomlijnde manier voor het implementeren van iOS-apparaten die een organisatie rechtstreeks bij Apple of via deelnemende Apple Authorized

Resellers en providers heeft aangeschaft. iOS-apparaten met iOS 11 of hoger kunnen na aankoop met Apple Configurator 2 ook aan DEP worden toegevoegd.

Organisaties kunnen apparaten automatisch inschrijven bij MDM zonder ze fysiek in handen te hoeven hebben, of de apparaten voorbereiden voordat ze aan de gebruikers worden verstrekt. Na inschrijving bij het programma logt de beheerder in bij de programmawebsite en koppelt hij of zij het programma aan de MDM-oplossing. De gekochte apparaten kunnen vervolgens via MDM aan gebruikers worden toegewezen. Zodra een gebruiker is toegewezen, worden eventuele via MDM opgegeven configuraties, beperkingen of opties automatisch geïnstalleerd. Alle communicatie tussen apparaten en Apple servers wordt tijdens de overdracht gecodeerd via HTTPS (SSL).

Het configuratieproces voor gebruikers kan verder worden vereenvoudigd door specifieke stappen uit de configuratie-assistent te verwijderen, zodat de gebruikers snel aan de slag kunnen. Bovendien kunnen beheerders instellen of gebruikers het MDM-profiel van het apparaat kunnen verwijderen en of er meteen vanaf het begin al bepaalde beperkingen van kracht moeten zijn. Nadat het apparaat is uitgepakt en geactiveerd, kan het bij de MDM-oplossing van de organisatie worden ingeschreven en worden alle beheerinstellingen, apps en boeken geïnstalleerd.

Voor meer informatie met betrekking tot bedrijven ga je naar: https://help.apple.com/deployment/business/

Voor meer informatie met betrekking tot onderwijsinstellingen ga je naar: https://help.apple.com/schoolmanager/

Opmerking: Apparaatinschrijving is niet in alle landen mogelijk.

Apple Configurator 2

Als aanvulling op een MDM-oplossing kan Apple Configurator 2 voor macOS worden gebruikt om eenvoudig iOS-apparaten en Apple TV te configureren voordat ze aan gebruikers worden verstrekt. Met Apple Configurator 2 kunnen apparaten snel vooraf worden geconfigureerd met apps, gegevens, beperkingen en instellingen.

Apple Configurator 2 maakt het mogelijk om met Apple School Manager (voor het onderwijs) of het Device Enrollment Program (voor bedrijven) apparaten in te schrijven bij een MDM-oplossing zonder dat gebruikers de configuratie-assistent hoeven te gebruiken. Apple Configurator 2 kan ook worden gebruikt om na aankoop iOS-apparaten en Apple TV aan Apple School Manager of het Device Enrollment Program toe te voegen.

Voor meer informatie over Apple Configurator 2 ga je naar: https://help.apple.com/configurator/mac

Supervisie

Tijdens de configuratie kan het apparaat onder supervisie worden geplaatst. Bij supervisie is het apparaat eigendom van de instelling en heeft de instelling meer controle over de configuratie van het apparaat en de beperkingen die voor het apparaat gelden. Apparaten kunnen tijdens de configuratie onder supervisie worden geplaatst via Apple School Manager,

het Device Enrollment Program of Apple Configurator 2. Om een apparaat onder supervisie te kunnen stellen, moet het worden gewist en moet het besturingssysteem opnieuw worden geïnstalleerd.

Voor meer informatie over het configureren en beheren van apparaten met MDM of Apple Configurator 2 ga je naar: https://help.apple.com/deployment/ios/

Beperkingen

Beperkingen kunnen door beheerders worden ingeschakeld (of in sommige gevallen uitgeschakeld) om te voorkomen dat gebruikers toegang hebben tot een bepaalde app, voorziening of functie van het apparaat. Beperkingen worden naar apparaten gestuurd in een beperkingen-payload die bij een configuratieprofiel is gevoegd. Beperkingen kunnen worden toegepast op apparaten met iOS, tvOS en macOS. Bepaalde beperkingen op een beheerde iPhone kunnen op een gekoppelde Apple Watch worden overgenomen.

Een actuele lijst voor IT-managers kun je vinden op: https://help.apple.com/deployment/ios/#/apdbd6309354

Wissen op afstand

iOS-apparaten kunnen op afstand worden gewist door een beheerder of gebruiker. Direct op afstand wissen is mogelijk door de coderingssleutel voor blokopslag veilig te verwijderen uit Effaceable Storage, zodat alle gegevens onleesbaar worden. Een opdracht voor het op afstand wissen van een apparaat kan worden gestart door MDM, Exchange of iCloud.

Als een opdracht voor wissen op afstand wordt geactiveerd door MDM of iCloud, verstuurt het apparaat een bevestiging, waarna het apparaat wordt gewist. Als Exchange wordt gebruikt om een apparaat op afstand te wissen, wordt het apparaat ingecheckt bij Exchange Server voordat de bewerking wordt uitgevoerd.

Gebruikers kunnen apparaten waarvan ze de eigenaar zijn ook wissen via de app Instellingen. Bovendien kan er, zoals eerder besproken, worden ingesteld dat apparaten automatisch worden gewist nadat een bepaald aantal onjuiste toegangscodes is ingevoerd.

Verloren-modus

Bij verlies of diefstal van een beheerd apparaat met iOS 9.3 of hoger kan een MDM-beheerder het apparaat op afstand in de verloren-modus zetten. Wanneer de verloren-modus is ingeschakeld, wordt de huidige gebruiker uitgelogd en kan het apparaat niet worden ontgrendeld. Op het scherm verschijnt een bericht (aan te passen door de beheerder) met daarin bijvoorbeeld een telefoonnummer dat de vinder van het apparaat kan bellen. Wanneer het apparaat in de verloren-modus is gezet, kan de beheerder het apparaat zijn huidige locatie laten doorgeven en eventueel een geluidssignaal laten afspelen. Als een beheerder de verloren-modus uitschakelt, wat de enige manier is om deze modus ongedaan te maken, krijgt de gebruiker een melding op het toegangsscherm of op het beginscherm te zien.

Activeringsslot

Als de functie Zoek mijn iPhone is ingeschakeld, kan het apparaat alleen opnieuw worden geactiveerd door de Apple ID-gegevens van de eigenaar of de vorige toegangscode van het apparaat in te voeren.

Als apparaten eigendom zijn van een organisatie, is het raadzaam om ze onder supervisie te stellen. De organisatie heeft dan zelf de controle over het activeringsslot en hoeft niet te wachten tot een gebruiker zijn of haar Apple ID heeft ingevoerd om het apparaat opnieuw te activeren.

Bij apparaten onder supervisie kan een compatibele MDM-oplossing een bypass-code opslaan wanneer het activeringsslot is ingeschakeld. Deze code kan later ook worden gebruikt om het activeringsslot automatisch te verwijderen wanneer het apparaat moet worden gewist en aan een nieuwe gebruiker moet worden toegewezen.

Het activeringsslot is standaard nooit ingeschakeld op apparaten die onder supervisie staan, zelfs niet als de gebruiker Zoek mijn iPhone inschakelt. Een MDM-oplossing kan echter een bypass-code ophalen en daarmee inschakeling van het activeringsslot op het apparaat toestaan. Als Zoek mijn iPhone is ingeschakeld wanneer de MDM-oplossing het activeringsslot inschakelt, wordt het slot op dat moment ingeschakeld. Als Zoek mijn iPhone is uitgeschakeld wanneer de MDM-server het activeringsslot inschakelt, wordt het slot ingeschakeld op het moment dat de gebruiker Zoek mijn iPhone activeert.

Voor apparaten die in een onderwijsinstelling worden gebruikt en waarvoor met Apple School Manager een beheerde Apple ID is aangemaakt, kan het activeringsslot aan de Apple ID van een beheerder in plaats van een gebruiker worden gekoppeld. Het activeringsslot kan ook worden uitgeschakeld met de bypass-code van het apparaat.

Privacybeheer

Apple hecht zeer veel waarde aan de privacy van klanten en heeft dan ook een groot aantal instellingen en opties ingebouwd waarmee gebruikers van iOS kunnen bepalen welke gegevens door apps mogen worden gebruikt en hoe en wanneer deze mogen worden gebruikt.

Locatievoorzieningen

Voor locatievoorzieningen wordt gebruikgemaakt van gps, Bluetooth en openbare wifihotspots en zendmasten om de globale locatie van de gebruiker te bepalen. Locatievoorzieningen kunnen eenvoudig worden uitgeschakeld met een optie in Instellingen. Gebruikers kunnen ook toestemming geven voor elke app die van de voorziening gebruikmaakt. Apps kunnen vragen om alleen bij gebruik locatiegegevens te ontvangen of om altijd locatiegegevens toe te staan. Gebruikers kunnen ervoor kiezen deze toegang niet toe te staan en kunnen hun keuze altijd aanpassen in Instellingen. Via Instellingen kan worden opgegeven dat nooit toegang is toegestaan, dat toegang alleen is toegestaan wanneer de app in gebruik is of dat altijd toegang is toegestaan, afhankelijk van het locatiegebruik dat door de app is aangevraagd. Als voor apps is ingesteld dat ze de locatie altijd mogen gebruiken en vervolgens op de achtergrond van deze mogelijkheid gebruikmaken, worden de gebruikers aan deze instelling herinnerd en kunnen zij de toegang van de app desgewenst wijzigen.

Daarnaast kunnen gebruikers zeer gedetailleerd aangeven op welke manier systeemvoorzieningen gebruik mogen maken van locatiegegevens. Zo kunnen ze onder andere opgeven dat geen locatiegegevens mogen worden opgenomen in informatie die wordt verzameld voor de analysevoorzieningen die door Apple worden gebruikt ter verbetering van iOS. Verder kunnen ze de volgende gegevens uitsluiten: locatiegebonden informatie van Siri, locatiegebonden context voor zoekacties met Siri-suggesties, lokale verkeersinformatie en belangrijke locaties die in het verleden zijn bezocht.

Toegang tot persoonlijke gegevens

iOS helpt te voorkomen dat apps zonder voorafgaande toestemming van een gebruiker zijn of haar persoonlijke gegevens raadplegen. Bovendien kunnen gebruikers in Instellingen zien welke apps ze toestemming hebben gegeven om bepaalde informatie te raadplegen. Via de app Instellingen kan ook de toegang voor apps worden ingetrokken of juist worden verleend. Het gaat hier om toegang tot de volgende onderdelen:

- Contacten
- Agenda's
- Herinneringen
- Foto's
- Beweging en conditie
- Locatievoorzieningen
- Apple Music
- Je muziek- en videoactiviteit
- Accounts voor sociale media, zoals Twitter en Facebook
- Microfoon
- Camera
- HomeKit
- Gezondheid
- Spraakherkenning
- Delen via Bluetooth
- Je mediabibliotheek

Als de gebruiker inlogt bij iCloud, krijgen apps standaard toegang tot iCloud Drive. Gebruikers kunnen de toegang van apps regelen via het paneel 'iCloud' in Instellingen. Daarnaast kunnen in iOS beperkingen worden opgegeven om te voorkomen dat gegevens worden verplaatst tussen de apps en accounts die door een MDM-oplossing zijn geïnstalleerd en de apps en accounts die door de gebruiker zijn geïnstalleerd.

Privacybeleid

Voor het privacybeleid van Apple ga je naar https://www.apple.com/legal/privacy/nl/.

Apple beveiligingsbeloning

Apple beloont onderzoekers die kritieke problemen aan Apple melden. Om in aanmerking te komen voor een Apple beveiligingsbeloning moeten onderzoekers een duidelijk rapport en een werkend proof of concept aanleveren. Het beveiligingsrisico moet betrekking hebben op de nieuwste beschikbare iOS-versie en, indien van toepassing, de nieuwste hardware. Het exacte uit te betalen bedrag zal na beoordeling door Apple worden vastgesteld. Er wordt daarbij onder meer gelet op hoe onbekend het risico is, hoe waarschijnlijk het is dat het zich voordoet en hoeveel interactie met de gebruiker is vereist.

Zodra een probleem is gemeld en bevestigd, zal Apple het probleem zo snel mogelijk oplossen. Indien van toepassing ontvangt de melder publiekelijk erkenning, tenzij hij of zij dat niet wenst.

Categorie	**Maximale beloning (USD)**
Firmwareonderdelen veilig opstartproces	$ 200.000
Extractie van vertrouwelijk materiaal dat door de Secure Enclave wordt beveiligd	$ 100.000
Uitvoeren van willekeurige code met kernelbevoegdheden	$ 50.000
Onbevoegde toegang tot iCloud-accountgegevens op Apple servers	$ 50.000
Toegang vanuit een proces in een sandbox tot gebruikersgegevens buiten die sandbox	$ 25.000

Samenvatting

Veiligheid op de eerste plaats

Apple stelt alles in het werk om haar klanten te beschermen. Zo maakt Apple gebruik van geavanceerde privacy- en beveiligingstechnologieën om persoonlijke gegevens vertrouwelijk te houden, alsook van geavanceerde methoden om bedrijfsgegevens in een zakelijke omgeving te beveiligen.

Beveiliging is standaard ingebouwd in iOS. Alles wat een bedrijf nodig heeft, van het platform tot en met het netwerk en de apps, is beschikbaar in het iOS-platform. Deze combinatie van elementen maakt iOS marktleider op het gebied van veiligheid, zonder aan gebruiksgemak in te boeten.

Apple hanteert overal binnen iOS en het ecosysteem van iOS-apps een consistente, geïntegreerde beveiligingsinfrastructuur. Hardwarematige codering van opslag maakt het mogelijk om apparaten op afstand te wissen als ze kwijt zijn. Deze voorziening stelt gebruikers ook in staat om alle zakelijke en persoonlijke gegevens volledig en permanent van hun apparaat te verwijderen als het apparaat wordt verkocht of aan een andere medewerker wordt gegeven. Diagnostische gegevens worden ook anoniem verzameld.

De iOS-apps die door Apple zijn ontworpen, worden gekenmerkt door uitgebreide beveiligingsfuncties. iMessage en FaceTime bieden bijvoorbeeld client-to-client-codering. Voor apps van derden vormt de combinatie van verplichte code-ondertekening, sandboxing en rechten een geavanceerde beveiliging tegen virussen, malware en andere gevaren. Ook de procedure voor het publiceren van apps in de App Store draagt er toe bij dat deze risico's tot een minimum worden beperkt, doordat elke iOS-app wordt geëvalueerd voordat de app ter beschikking wordt gesteld.

Om maximaal te profiteren van de uitgebreide beveiligingsvoorzieningen die in iOS zijn ingebouwd, wordt bedrijven aangeraden hun IT- en beveiligingsbeleid door te nemen om er zeker van te zijn dat ze optimaal gebruikmaken van de verschillende beveiligingslagen die dit platform biedt.

Apple heeft een speciaal beveiligingsteam dat ondersteuning biedt voor alle Apple producten. Dit team voert beveiligingscontroles en -tests uit voor producten die nog in ontwikkeling zijn en voor producten die al zijn uitgebracht. Het Apple team biedt ook beveiligingstools en -training aan en is altijd alert op meldingen van nieuwe beveiligingsproblemen en bedreigingen. Apple is lid van het Forum of Incident Response and Security Teams (FIRST).

Voor meer informatie over het melden van problemen aan Apple en het ontvangen van beveiligingsmeldingen ga je naar: https://www.apple.com/nl/support/security.

Verklarende woordenlijst

Address space layout randomization (ASLR)	Een techniek die in iOS wordt toegepast om het voor aanvallers moeilijker te maken om misbruik te maken van bugs in de software. Door ervoor te zorgen dat geheugenadressen en offsets niet te voorspellen zijn, wordt voorkomen dat aanvallers deze waarden in hun code kunnen vastleggen. In iOS 5 of hoger wordt de positie van alle systeem-apps en -bibliotheken willekeurig bepaald, terwijl ook alle apps van derden worden gecompileerd als positie-onafhankelijke, uitvoerbare bestanden.
Apple Push Notification Service (APNS)	Een voorziening die wereldwijd door Apple wordt aangeboden en waarmee push-meldingen op iOS-apparaten worden afgeleverd.
Bestandsspecifieke sleutel	De 256-bits-AES-sleutel die wordt gebruikt om een bestand in het bestandssysteem te coderen. De bestandsspecifieke sleutel wordt ingepakt met een klassesleutel en wordt opgeslagen in de metagegevens van het bestand.
Bestandssysteemsleutel	De sleutel waarmee de metagegevens van een bestand worden gecodeerd, waaronder de klassesleutel daarvan. Deze sleutel wordt in Effaceable Storage bewaard om een apparaat snel te kunnen wissen en niet zozeer om vertrouwelijkheid te bieden.
Combineren	Het proces waarmee de toegangscode van een gebruiker wordt omgezet in een cryptografische sleutel die vervolgens wordt versterkt met de UID van het apparaat. Dit proces zorgt ervoor dat op een bepaald apparaat alleen een brute-force-aanval mogelijk is, wat het aantal beperkt en parallelle uitvoering onmogelijk maakt. Het combinatie-algoritme is PBKDF2, waarbij AES samen met de apparaat-UID als de pseudo-willekeurige functie (PRF) voor elke iteratie wordt gebruikt.
Device Firmware Upgrade (DFU)	Een modus waarin de code in het opstart-ROM van een apparaat wacht om via USB te worden hersteld. In de DFU-modus is het scherm zwart. Bij verbinding met een computer waarop iTunes wordt uitgevoerd, verschijnt het volgende bericht: "iTunes heeft een iPad aangetroffen waarvan de herstelmodus actief is. Je moet deze iPad herstellen voordat je deze kunt gebruiken met iTunes."
ECID	Een 64-bits-ID die uniek is voor de processor in elk iOS-apparaat. Wanneer een oproep op een van de apparaten wordt beantwoord, wordt het bellen van andere nabije en in iCloud gekoppelde apparaten beëindigd door een korte aankondiging via Bluetooth Low Energy 4.0. De bytes van de aankondiging worden op dezelfde manier gecodeerd als Handoff-aankondigingen. Deze ID wordt gebruikt als onderdeel van het personalisatieproces en wordt niet als geheim beschouwd.
Effaceable Storage	Een gereserveerd gebied voor NAND-opslag waarin cryptografische sleutels worden opgeslagen, dat rechtstreeks kan worden benaderd en dat veilig kan worden gewist. Hoewel dit opslaggebied geen bescherming biedt als een aanvaller de fysieke controle over het apparaat heeft, kunnen de sleutels in Effaceable Storage worden gebruikt als onderdeel van een sleutelhiërarchie om apparaten snel te wissen en forward secrecy mogelijk te maken.
Gegevensbeveiliging	Een beveiligingsmechanisme voor bestanden en sleutelhangers voor iOS. De term kan ook verwijzen naar de API's die door apps worden gebruikt om bestanden en sleutelhangeronderdelen te beveiligen.
Geïntegreerde schakeling (IC)	Wordt ook wel een microchip genoemd.
Groeps-ID (GID)	Te vergelijken met de UID, maar voor elke processor in een klasse hetzelfde.
Hardware Security Module (HSM)	Een speciale hardwaremodule die bestand is tegen manipulaties en die wordt gebruikt voor het beveiligen en beheren van digitale sleutels.
Hoekaflezing van looprichting van papillairlijnen	Een wiskundige voorstelling van de richting en breedte van de papillairlijnen die uit een deel van een vingerafdruk zijn geëxtraheerd.

iBoot	Code die als onderdeel van het veilige opstartproces wordt geladen door LLB en er dan voor zorgt dat XNU wordt geladen.
Identity Service (IDS)	De adreslijst van Apple met publieke sleutels van iMessage, APNS-adressen, en telefoonnummers en e-mailadressen die worden gebruikt voor het opzoeken van de sleutels en apparaatadressen.
Inpakken van sleutels	Het coderen van een sleutel met een andere sleutel. In iOS wordt hiervoor NIST AES conform RFC 3394 gebruikt. Wordt ook wel "inpakken" of "wrapping" genoemd.
Joint Test Action Group (JTAG)	Een standaardtool die door programmeurs en circuitontwerpers wordt gebruikt om hardware te debuggen.
Low-Level Bootloader (LLB)	Code die als onderdeel van het veilige opstartproces wordt aangeroepen door het opstart-ROM, en er dan voor zorgt dat iBoot wordt geladen.
Opstart-ROM	De allereerste code die door de processor van een apparaat wordt uitgevoerd wanneer het apparaat wordt opgestart. Omdat het opstart-ROM is geïntegreerd in de processor, kan het noch door Apple, noch door een aanvaller worden aangepast.
Sleutelhanger	De infrastructuur en een set API's die worden gebruikt door apps van iOS en derden voor het opslaan en ophalen van wachtwoorden, sleutels en andere vertrouwelijke identiteitsgegevens.
Sleutelverzameling (keybag)	Een gegevensstructuur die wordt gebruikt voor het opslaan van een verzameling klassesleutels. Elk type (user, device, system, backup, escrow en iCloud Backup) heeft dezelfde indeling: • Een header met: – Versie (ingesteld op drie in iOS 5) – Type (system, backup, escrow of iCloud Backup) – UUID van de sleutelverzameling – Een HMAC als de sleutelverzameling is ondertekend – De methode voor het inpakken van de klassesleutels: combinatie met de UID of PBKDF2, samen met de salt en iteratietelling • Een lijst met klassesleutels: – UUID van sleutel – Klasse (de gegevensbeveiligingsklasse voor het bestand of de sleutelhanger) – Manier van inpakken (alleen van UID afgeleide sleutel; van UID afgeleide sleutel en van toegangscode afgeleide sleutel) – Ingepakte klassesleutel – Publieke sleutel voor asymmetrische klassen
Smart card	Een geïntegreerd, ingebed circuit dat beveiligde identificatie, verificatie en gegevensopslag biedt.
System on a Chip (SoC)	Een geïntegreerde schakeling of circuit (IC) waarin meerdere componenten zijn gecombineerd in één chip. De Secure Enclave is een SoC in de centrale Apple A7-processor en nieuwere processormodellen.
Uniform Resource Identifier (URI)	Een reeks tekens die de identiteit van een resource op het web vormt.
Unieke ID (UID)	Een 256-bits-AES-sleutel die tijdens het fabricageproces in een processor wordt gebrand. De ID kan niet door firmware of software worden gelezen en wordt alleen gebruikt door de hardwarematige AES-engine van de processor. Een aanvaller kan de feitelijke sleutel alleen in handen krijgen door het silicium in de processor fysiek te bewerken, wat een zeer geavanceerde en kostbare aangelegenheid is. De UID houdt geen verband met de andere ID's op het apparaat, zoals de UDID.
Voorzieningenprofiel	Een door Apple ondertekende plist die een set entiteiten en rechten bevat op basis waarvan apps kunnen worden geïnstalleerd en getest op een iOS-apparaat. In een ontwikkelingsvoorzieningenprofiel worden de apparaten vermeld die de ontwikkelaar heeft uitgekozen voor ad-hocdistributie, terwijl een distributievoorzieningenprofiel de app-ID van een intern ontwikkelde app bevat.
XNU	De kernel die het hart vormt van de besturingssystemen iOS en macOS. Het is een onderdeel dat standaard wordt vertrouwd en dat diverse beveiligingsmaatregelen afdwingt, zoals code-ondertekening, sandboxing, controle van rechten en ASLR.

Revisieoverzicht

Datum	Overzicht
Januari 2018	**Bijgewerkt voor iOS 11.2** • Apple Pay Cash **Bijgewerkt voor iOS 11.1** • Beveiligingscertificeringen en -programma's • Touch ID/Face ID • Gedeelde notities • End-to-end-codering van CloudKit • TLS • Apple Pay, Betaling met Apple Pay op het web • Siri-suggesties • Gedeelde iPad • Als je meer informatie wilt over de beveiligingsaspecten van iOS 11, ga je naar: https://support.apple.com/nl-nl/HT208112
Juli 2017	**Bijgewerkt voor iOS 10.3** • Secure Enclave • Beveiliging van bestandsgegevens • Sleutelverzamelingen • Beveiligingscertificeringen en -programma's • SiriKit • HealthKit • Netwerkbeveiliging • Bluetooth • Gedeelde iPad • Verloren-modus • Activeringsslot • Privacybeheer • Als je meer informatie wilt over de beveiligingsaspecten van iOS 10.3, ga je naar: https://support.apple.com/nl-nl/HT207617
Maart 2017	**Bijgewerkt voor iOS 10** • Systeembeveiliging • Gegevensbeveiligingsklassen • Beveiligingscertificeringen en -programma's • HomeKit, ReplayKit, SiriKit • Apple Watch • Wifi, VPN • Eenmalige aanmelding • Apple Pay, Betaling met Apple Pay op het web • Creditcards, pinpassen en prepaidkaarten toevoegen • Safari-suggesties • Als je meer informatie wilt over de beveiligingsaspecten van iOS 10, ga je naar: https://support.apple.com/nl-nl/HT207143

Datum	Overzicht
Mei 2016	**Bijgewerkt voor iOS 9.3** • Beheerde Apple ID • Twee-factor-authenticatie voor Apple ID's • Sleutelverzamelingen • Beveiligingscertificeringen • Verloren-modus, Activeringsslot • Vergrendelde notities • Apple School Manager, Gedeelde iPad • Als je meer informatie wilt over de beveiligingsaspecten van iOS 9.3, ga je naar: https://support.apple.com/nl-nl/HT206166
September 2015	**Bijgewerkt voor iOS 9** • Activeringsslot voor Apple Watch • Toegangscodebeleid • API-ondersteuning Touch ID • Gegevensbeveiliging van A8 gebruikt AES-XTS • Sleutelverzamelingen voor onbegeleide software-update • Updates van certificeringen • Vertrouwensmodel voor bedrijfs-apps • Gegevensbeveiliging voor Safari-bladwijzers • App Transport Security • VPN-specificaties • Externe toegang via iCloud voor HomeKit • Beloningskaarten Apple Pay, App van kaartverstrekker voor Apple Pay • Indexering op apparaat voor Spotlight • iOS-koppelingsmodel • Apple Configurator 2 • Beperkingen • Als je meer informatie wilt over de beveiligingsaspecten van iOS 9, ga je naar: https://support.apple.com/nl-nl/HT205212

Januari 2018