Apple-alustojen tietoturva

Toukokuu 2022

Sisällysluettelo

Apple-alustojen tietoturva

Johdanto Apple-alustojen tietoturvaan

Apple suunnittelee suojauksen alustojensa ytimeen. Maailman edistyksellisimmän mobiilikäyttöjärjestelmän luomisesta saamiensa kokemusten päälle rakentaen Apple on kehittänyt suojausarkkitehtuureja, jotka vastaavat mobiililaitteiden, kellojen, pöytäkoneiden ja kotien ainutlaatuisiin vaatimuksiin.

Jokaisen Apple-laitteen *laitteisto*, *ohjelmisto* ja *palvelut* on suunniteltu toimimaan yhdessä, jotta voidaan saavuttaa paras mahdollinen suojaus ja läpinäkyvä käyttökokemus ja samalla pitää henkilökohtaiset tiedot turvattuina. Esimerkiksi Applen suunnittelema siru ja tietoturvalaitteisto ovat kriittisten suojausominaisuuksien perustana, ja ohjelmiston suojaukset pitävät käyttöjärjestelmän ja muiden valmistajien apit suojattuina. Lisäksi palvelut tarjoavat turvallisia ohjelmistopäivityksiä oikea-aikaisesti, muodostavat pohjan suojatulle appien ekosysteemille ja helpottavat turvallista viestintää ja maksamista. Tämän ansiosta Applen laitteet suojaavat itse laitetta ja sen tietoja sekä koko ekosysteemiä, mukaan lukien kaiken, mitä käyttäjät tekevät paikallisesti, verkoissa ja keskeisissä internet-palveluissa.

Suunnittelemme tuotteemme yksinkertaisiksi, intuitiivisiksi, suorituskykyisiksi ja turvallisiksi. Keskeisiä suojausominaisuuksia, kuten laitteistopohjaista laitesalausta, ei voida vahingossa laittaa pois päältä. Toiset ominaisuudet, kuten Face ID ja Touch ID, parantavat käyttökokemusta tekemällä laitteen suojaamisesta yksinkertaisempaa ja intuitiivisempaa. Koska monet näistä ominaisuuksista ovat oletusarvoisesti päällä, käyttäjien tai IT-osastojen ei tarvitse suorittaa mittavia määrityksiä.

Tässä dokumentaatiossa kerrotaan, miten suojausteknologia ja -ominaisuudet on toteutettu Applen alustoissa. Se myös auttaa organisaatioita yhdistämään Apple-alustojen tietoturvateknologiaa ja -ominaisuuksia omiin käytäntöihinsä omien tietoturvatarpeidensa täyttämiseksi.

Sisältö on jaoteltu seuraaviin aihealueisiin:

- **Laitteiston suojaus ja biometriset tiedot:** Siru ja laitteisto, jotka muodostavat suojauksen perustan Applen laitteissa, mukaan lukien Apple silicon, Secure Enclave, salausmoottorit, Touch ID ja Face ID.
- **Järjestelmän suojaus:** Integroidut laitteisto- ja ohjelmistotoiminnot, jotka mahdollistavat vikasietokäynnistyksen, päivityksen ja Applen käyttöjärjestelmien jatkuvan toiminnan.
- **Salaus ja tietojen suojaus:** Arkkitehtuuri ja suunnitteluratkaisut, jotka suojaavat käyttäjän tietoja, jos laite katoaa tai varastetaan tai jos valtuuttamaton henkilö tai prosessi yrittää käyttää tai muokata sitä.

- **Appien suojaus:** Ohjelmisto ja palvelut, jotka tarjoavat turvallisen appien ekosysteemin ja mahdollistavat appien turvallisen toiminnan siten, ettei alustan eheys ole vaarassa.
- **Palveluiden suojaus:** Applen palvelut tunnistautumista, salasanojen hallintaa, maksuja, viestintää ja kadonneiden laitteiden löytämistä varten.
- **Verkon suojaus:** Vakiintuneiden standardien mukaiset verkkoprotokollat, jotka mahdollistavat suojatun todentamisen ja siirrettävien tietojen salaamisen.
- **Kehittäjäpaketin suojaus:** Sovelluskehyksien ”paketteja” kodin ja terveyden suojattuun yksityiseen hallitsemiseen sekä Applen laitteiden ja palveluiden ominaisuuksien laajentamiseen muiden valmistajien appeihin.
- **Suojattu laitehallinta:** Menetelmiä, jotka mahdollistavat Applen laitteiden hallinnan sekä etätyhjennyksen, jos laite katoaa tai varastetaan, ja auttavat estämään valtuuttamattoman käytön.

Sitoumus suojaukseen

Apple on sitoutunut edistämään asiakkaiden suojaa johtavien yksityisyys- ja suojausteknologioiden avulla, jotka on suunniteltu pitämään henkilötiedot turvassa, ja käyttämään kattavia menetelmiä yritysten tietojen suojaamiseen. Apple palkitsee tutkijoita Apple Security Bounty -palkkiolla työstä, jota he tekevät haavoittuvuuksien löytämiseksi. Tietoja ohjelmasta ja palkkiokategorioista löytyy osoitteesta https://developer.apple.com/security-bounty/.

Meillä on erillinen tietoturvatiimi, joka tukee kaikkia Applen tuotteita. Tiimi tarjoaa tietoturvan tarkistusta ja testausta sekä kehitysvaiheessa oleville että julkistetuille tuotteille. Applen tiimi tarjoaa myös tietoturvatyökaluja ja koulutusta sekä tarkkailee aktiivisesti mahdollisia uhkia ja raportteja uusista tietoturvaongelmista. Apple on Forum of Incident Response and Security Teams (FIRST) -foorumin jäsen.

Apple laajentaa jatkuvasti tietoturvan ja yksityisyyden suojauksen mahdollisuuksia. Koko tuotevalikoimassa Apple Watchista iPhoneen ja iPadiin sekä Macin T2 Security -siruun ja Apple siliconiin käytetään räätälöityä sirua, joka on merkittävä paitsi laitteiden laskentatehon niin myös niiden tietoturvan kannalta. Apple silicon esimerkiksi muodostaa perustan suojatulle käynnistykselle, Face ID:lle ja Touch ID:lle sekä tietojen suojaukselle. Lisäksi Apple siliconia käyttävien laitteiden suojausominaisuudet – kuten kernelin eheyden suojaus, PAC-koodit ja nopeat luparajoitukset – auttavat estämään yleisiä kyberhyökkäystyyppejä. Niinpä vaikka hyökkäyskoodin suorittaminen jollakin keinolla onnistuisi, se pystyy aiheuttamaan olennaisesti vähemmän vahinkoa.

Jotta alustojemme kattavista sisäisistä suojausominaisuuksista saadaan kaikki irti, organisaatioita rohkaistaan käymään läpi IT- ja suojauskäytäntönsä ja siten varmistamaan, että näiden alustojen suojausteknologian eri tasoja hyödynnetään kokonaisvaltaisesti.

Jos haluat lisätietoja ongelmien raportoimisesta Applelle ja suojausilmoitusten tilaamisesta, katso Tietoturva- tai tietosuojahaavoittuvuudesta ilmoittaminen.

Apple uskoo, että yksityisyys on perustavanlaatuinen ihmisoikeus. Siksi Applen tuotteissa on lukuisia sisäänrakennettuja säätimiä ja valintoja, joiden avulla käyttäjät voivat päättää, miten ja milloin apit käyttävät heidän tietojaan sekä sen, mitä tietoja ne käyttävät. Lisätietoja Applen lähestymistavasta tietosuojaan, Apple-laitteiden tietosuojan säätimistä ja Applen tietosuojakäytännöstä on osoitteessa https://www.apple.com/fi/privacy.

Huomaa: Ellei toisin ole mainittu, tämä dokumentaatio kattaa seuraavat käyttöjärjestelmäversiot: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 ja watchOS 8.5.

Laitteiston suojaus ja biometriset tiedot

Laitteiston suojauksen yleiskatsaus

Jotta ohjelmisto olisi suojassa, sen täytyy olla suojatuksi rakennetussa laitteistossa. Siksi Applen iOS-, iPadOS-, macOS-, tvOS- ja watchOS-laitteissa on suojausominaisuuksia aivan laitteistotasolla. Näihin ominaisuuksiin kuuluvat prosessori, joka mahdollistaa järjestelmän suojausominaisuudet, sekä suojaustoiminnoille dedikoitu lisäsiru. Suojaukseen keskittyvissä laitteistokomponenteissa on periaatteena, että ne tukevat vain rajoitettuja ja erikseen määriteltyjä toimintoja hyökkäysmahdollisuuksien vähentämiseksi. Näitä komponentteja ovat Boot ROM, joka on laitteiston luottamuksen perusta suojatussa käynnistyksessä, turvalliseen salaukseen ja salauksen purkuun varatut AES-komponentit sekä Secure Enclave. *Secure Enclave* on järjestelmäpiiri (SoC), joka sisältyy kaikkiin uudempiin iPhone-, iPad-, Apple Watch-, Apple TV- ja HomePod-laitteisiin sekä Apple siliconilla tai Apple T2 Security -sirulla varustettuun Maciin. Itse Secure Enclave on suunniteltu samalla periaatteella kuin järjestelmäpiiri; sillä on oma erillinen Boot ROM ja AES-komponentti. Secure Enclave on myös perusta levossa olevan datan salaamisessa tarvittavien avainten suojatulle muodostamiselle ja tallennukselle, ja se suojaa ja arvioi biometriset tiedot Face ID:tä ja Touch ID:tä varten.

Tallennettujen tietojen salauksen on oltava nopeaa ja tehokasta. Samalla kuitenkin on tärkeää, että se ei paljasta tietoja (tai *avainmateriaalia*), joita se käyttää kryptografisten avainsuhteiden muodostamiseen. AES-laitteistokomponentti ratkaisee tämän ongelman nopealla salauksella ja salauksen purkamisella *tiedostoja kirjoitettaessa tai luettaessa*. AES-komponentti saa tarvitsemansa avainmateriaalin Secure Enclavelta erityistä kanavaa pitkin siten, ettei se voi paljastua appeja suorittavalle prosessorille (tai keskusprosessorille) tai käyttöjärjestelmälle. Tämä auttaa varmistamaan, että Applen tietojen suojaus- ja FileVault-teknologiat suojaavat käyttäjien tiedostoja paljastamatta pitkäaikaisia salausavaimia.

Apple on suunnitellut suojatun käynnistyksen suojaamaan ohjelmiston alimpia tasoja peukaloinnilta ja sallimaan vain Applen luotettu käyttöjärjestelmäohjelmisto latautumisen käynnistyksessä. Suojattu käynnistys alkaa muuttumattomasta koodista nimeltä Boot ROM, joka asennetaan Applen järjestelmäsiruun sen valmistuksen aikana. Tämä *laitetason RoT-koodi (Root of Trust)* on ehdottoman luotettava. Mac-tietokoneissa, joissa on T2-siru, macOS:n suojatun käynnistyksen luottamus alkaa T2:sta. (Sekä T2-siru että Secure Enclave suorittavat myös omat suojatut käynnistysprosessinsa käyttäen omaa erillistä Boot ROM -koodiaan. Tämä vastaa täsmälleen A-sarjan ja M1-siruperheen suojattua käynnistystä.)

Secure Enclave prosessoi myös Face ID:n sekä Touch ID:n tunnistinten kasvo- ja sormenjälkidatan Applen laitteissa. Tämä mahdollistaa suojatun todennuksen pitäen samalla käyttäjän biometriset tiedot yksityisinä ja suojattuina. Lisäksi käyttäjät pääsevät hyötymään pidempien ja monimutkaisempien pääsykoodien ja salasanojen tarjoamasta suojauksesta voiden samalla monissa tilanteissa nauttia kätevästä ja sujuvasta todentamisesta pääsyä tai ostoja varten.

Applen järjestelmäpiirin suojaus

Applen suunnittelema siru muodostaa yhteisen arkkitehtuurin kaikkiin Applen tuotteisiin ja on nyt iPhonen, iPadin, Apple TV:n ja Apple Watchin lisäksi myös Macissa. Applen maailmanluokan sirusuunnittelutiimi on tehnyt ja hionut Applen järjestelmäpiirejä (SoC) yli kymmenen vuotta. Tuloksena on suojausominaisuuksiltaan alansa kärkeä edustava skaalautuva arkkitehtuuri kaikille laitteille. Tämä yhteinen perusta suojausominaisuuksille on mahdollinen vain yritykselle, joka suunnittelee oman sirunsa toimimaan oman ohjelmistonsa kanssa.

Apple silicon on suunniteltu ja valmistettu erityisesti mahdollistamaan alla käsitellyt järjestelmän suojausominaisuudet.

Ominaisuus	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	M1-perhe
Kernelin eheyden suojaus	✓	✓	✓	✓	✓	✓
Nopeat luparajoitukset		✓	✓	✓	✓	✓
Järjestelmän lisäprosessorin eheyden suojaus			✓	✓	✓	✓
PAC-koodit			✓	✓	✓	✓
Page Protection Layer (PPL)		✓	✓	✓	✓	Katso huomautus alla.

Huomaa: Page Protection Layer (PPL) vaatii, että alusta suorittaa *ainoastaan* allekirjoitettua ja luotettua koodia. Tämä suojausmalli ei ole käytössä macOS:ssä.

Lisäksi juuri Applen suunnittelema siru mahdollistaa alla käsitellyt tietojen suojausominaisuudet.

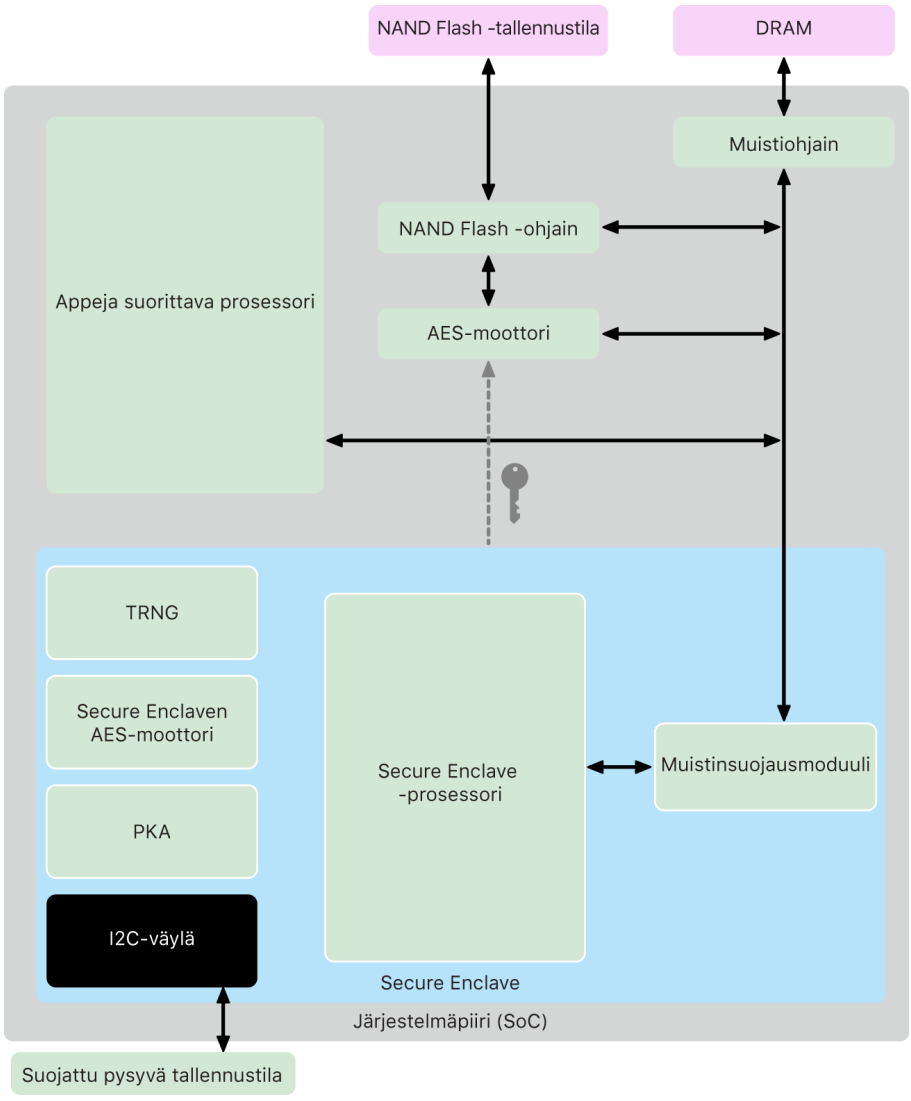
Ominaisuus	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1-perhe
Sinetöity avaimen suojaus (Sealed Key Protection, SKP)	✓	✓	✓	✓	✓
recoveryOS – kaikki tietojen suojausluokat suojataan	✓	✓	✓	✓	✓
Vaihtoehtoiset käynnistykset DFU:lle, vianmääritykselle ja päivitykselle – luokkien A, B ja C tiedot suojataan			✓	✓	✓

Secure Enclave -alue

Secure Enclave on erityinen suojattu alijärjestelmä uusimmissa iPhonen, iPadin, iPod touchin, Macin, Apple TV:n, Apple Watchin ja HomePodin versioissa.

Yleiskatsaus

Secure Enclave on erityinen Applen järjestelmäpiireihin (SoC) integroitu suojattu alijärjestelmä. Suojauksen parantamiseksi Secure Enclave on eristetty pääprosessorista, ja se on suunniteltu pitämään käyttäjän arkaluontoiset tiedot suojattuina myös silloin, jos appeja suorittavan prosessorin kernel vaarantuu. Sen suunnittelu noudattaa samoja periaatteita kuin järjestelmäpiirin suunnittelu: sillä on Boot ROM laitetason RoT-koodia varten, AES-komponentti tehokkaisiin ja turvallisiin salausoperaatioihin sekä suojattu muisti. Vaikka Secure Enclave ei sisällä tallennustilaa, sillä on mekanismi suojattuun tiedon tallentamiseen siihen liitetyssä tallennuslaitteessa, joka on erillinen appeja suorittavan prosessorin ja käyttöjärjestelmän käyttämästä NAND-flash-tallennustilasta.



Secure Enclave on laitteisto-ominaisuus useimmissa iPhonen, iPadin, Macin, Apple TV:n, Apple Watchin ja HomePodin versioissa eli seuraavissa:

- iPhone 5s tai uudempi
- iPad Air tai uudempi
- MacBook Pro -tietokoneet, joissa on Touch Bar (2016 ja 2017) ja Apple T1 -siru
- Intel-pohjaiset Mac-tietokoneet, joissa on Apple T2 Security -siru
- Apple siliconilla varustetut Mac-tietokoneet
- Apple TV HD tai uudempi
- Apple Watch Series 1 tai uudempi
- HomePod ja HomePod mini

Secure Enclave -prosessori

Secure Enclave -prosessori on päävastuussa Secure Enclaven laskutoimituksista. Jotta eristys olisi mahdollisimman aukoton, Secure Enclave -prosessori on varattu ainoastaan Secure Enclaven käyttöön. Tämä auttaa ehkäisemään sivukanavahyökkäyksiä, joissa haittaohjelmiston tarvitsee jakaa sama suoritinydin kuin hyökkäyksen kohdeohjelmiston.

Secure Enclave -prosessorissa toimii Applen muokkaama versio L4-mikroytimestä. Se on suunniteltu toimimaan tehokkaasti alemmalla kellotaajuudella, joka auttaa suojaamaan sitä kello- ja tehohyökkäyksiltä. A11:stä ja S4:stä alkaen Secure Enclave -prosessori sisältää muistinsuojausmoduulin ja toiston estävän salatun muistin, suojatun käynnistyksen, erityisen satunnaislukugeneraattorin ja oman AES-komponentin.

Muistinsuojausmoduuli

Secure Enclave toimii sille varatulta alueelta laitteen DRAM-muistissa. Useat suojauskerrokset eristävät Secure Enclaven suojatun muistin appeja suorittavasta prosessorista.

Kun laite käynnistyy, Secure Enclaven Boot ROM luo satunnaisen väliaikaisen muistinsuojausavaimen muistinsuojausmoduulille. Aina kun Secure Enclave kirjoittaa sille varatulle muistialueelle, muistinsuojausmoduuli salaa muistilohkon käyttäen AES-salausta Macin XEX (xor-encrypt-xor) -tilassa ja laskee muistille CMAC (Cipher-based Message Authentication Code) -todennustunnisteen. Muistinsuojausmoduuli tallentaa todennustunnisteen yhdessä salatun muistin kanssa. Kun Secure Enclave lukee muistia, muistinsuojausmoduuli tarkistaa todennustunnisteen. Jos todennustunniste täsmää, muistinsuojausmoduuli purkaa muistilohkon suojauksen. Jos tunniste ei täsmää, muistinsuojausmoduuli antaa virhesignaalin Secure Enclavelle. Jos muistin todennuksessa ilmenee virhe, Secure Enclave lakkaa hyväksymästä pyyntöjä, kunnes järjestelmä käynnistetään uudelleen.

Apple A11- ja S4-järjestelmäpiireistä alkaen muistinsuojausmoduuliin on lisätty uudelleentoistosuojaus Secure Enclaven muistille. Auttaakseen estämään suojauksen kannalta kriittisten tietojen uudelleentoistoa muistinsuojausmoduuli tallentaa muistilohkolle todennustunnuksen kanssa myös ainutkertaisen numeron, josta käytetään nimitystä *nonce*. Noncea käytetään lisänä CMAC-todennustunnuksessa. Kaikkien muistilohkojen noncet suojataan käyttäen eheyspuuta, jonka juuri on sille tarkoitetussa SRAM-muistissa Secure Enclavessa. Kirjoitettaessa muistinsuojausmoduuli *päivittää* noncen ja kunkin eheyspuun tason SRAM-muistiin asti. Luettaessa muistinsuojausmoduuli *tarkistaa* noncen ja kunkin eheyspuun tason SRAM-muistiin asti. Täsmäämättömän noncen tapaukset käsitellään samoin kuin täsmäämättömän todennustunnisteen tapaukset.

Apple A14:ssä, A15:ssä, M1-perheessä ja uudemmissa järjestelmäpiireissä muistinsuojausmoduuli tukee kahta lyhytaikaista muistinsuojausavainta. Ensimmäistä käytetään tiedoille, jotka ovat vain Secure Enclaven yksityisiä, ja toista suojatun Neural Enginen kanssa jaetuille tiedoille.

Muistinsuojausmoduuli toimii läpinäkyvästi Secure Enclaven ja muistin välissä. Secure Enclave lukee ja kirjoittaa muistia kuin se olisi tavallinen salaamaton DRAM, kun taas Secure Enclaven ulkopuolella toimiva havainnoitsija näkee vain muistin salatun ja todennetun version. Tuloksena on vahva muistin suojaus ilman haittavaikutuksia ohjelmiston suorituskykyyn tai monimutkaisuuteen.

Secure Enclaven Boot ROM

Secure Enclavessa on erillinen Secure Enclaven Boot ROM. Appeja suorittavan prosessorin Boot ROMin tavoin myös Secure Enclaven Boot ROM on muuttumatonta koodia, joka muodostaa laitteiston luottamuksen perustan (Root of Trust) Secure Enclavelle.

Kun järjestelmä käynnistetään, iBoot määrittää Secure Enclavelle sille varatun muistialueen. Ennen tämän muistialueen käyttämistä Secure Enclaven Boot ROM valmistelee muistinsuojausmoduulin salaamaan Secure Enclaven suojatun muistialueen.

Tämän jälkeen appeja suorittava prosessori lähettää sepOS-levykuvan Secure Enclaven Boot ROMille. Kun sepOS-levytiedosto on kopioitu Secure Enclaven suojattuun muistiin, Secure Enclaven Boot ROM tarkistaa levytiedoston salausavaimella luodun tiivisteen ja allekirjoituksen varmistaakseen, että sepOS on valtuutettu laitteessa suoritettavaksi. Jos sepOS-levykuva on kelvollisesti allekirjoitettu laitteessa suorittamista varten, Secure Enclaven Boot ROM siirtää hallinnan sepOS:lle. Jos allekirjoitus ei ole kelvollinen, Secure Enclaven Boot ROM on suunniteltu estämään Secure Enclaven enempi käyttö, kunnes siru seuraavan kerran nollataan.

Apple A10 -järjestelmäpiirissä ja sitä uudemmissa Secure Enclaven Boot ROM lukitsee sepOS:n tiivisteen tätä tarkoitusta varten varattuun rekisteriin. Julkisen avaimen kiihdytin käyttää tätä tiivistettä käyttöjärjestelmään sidotuille avaimille.

Secure Enclaven käynnistyksen valvonta

Apple A13- ja sitä uudemmissa järjestelmäpiireissä Secure Enclave sisältää käynnistyksen valvonnan, joka on suunniteltu varmistamaan vahvemmin käynnistetyn sepOS:n tiivisteen eheys.

Järjestelmää käynnistettäessä Secure Enclave -prosessorin järjestelmän lisäprosessorin eheyden suojauksen (SCIP) määritys auttaa estämään Secure Enclave -prosessoria suorittamasta mitään muuta koodia kuin Secure Enclaven Boot ROM -koodia. Käynnistyksen valvonta auttaa estämään Secure Enclavea muuttamasta suoraan SCIP:n määritystä. Jotta ladattu sepOS voidaan suorittaa, Secure Enclaven Boot ROM lähettää käynnistyksen valvontaan pyynnön, joka sisältää ladatun sepOS:n osoitteen ja koon. Kun käynnistyksen valvonta saa tämän pyynnön, se nollaa Secure Enclave -prosessorin, laskee tiivisteen ladatusta sepOS:stä, päivittää SCIP:n asetukset sallimaan ladatun sepOS:n suorittamisen ja käynnistää suorittamisen juuri ladatulla koodilla. Järjestelmän käynnistyksen jatkuessa samaa prosessia käytetään aina, kun uudesta koodista tehdään suoritettava. Käynnistyksen valvonta päivittää joka kerta käynnistysprosessin juoksevan tiivisteen. Käynnistyksen valvonta sisällyttää juoksevaan tiivisteeseen myös kriittiset suojausparametrit.

Kun käynnistys on valmis, käynnistyksen valvonta viimeistelee juoksevan tiivisteen ja lähettää sen julkisen avaimen kiihdyttimelle käytettäväksi käyttöjärjestelmään sidotuille avaimille. Tämä prosessi on suunniteltu siten, että avainten sitomista käyttöjärjestelmään ei voi ohittaa edes Secure Enclaven Boot ROMissa olevaa haavoittuvuutta hyödyntäen.

Aitojen satunnaislukujen generaattori

Aitojen satunnaislukujen generaattoria (TRNG) käytetään luomaan turvallista satunnaista dataa. Secure Enclave käyttää TRNG-generaattoria aina luodessaan satunnaisen salausavaimen, satunnaisen avaimen siemenen tai muuta entropiaa. TRNG perustuu CTR_DRBG:llä jälkiprosessoituihin rengasoskillaattoreihin. (CTR_DRBG on algoritmi, joka perustuu lohkosalaimiin laskuritilassa.)

Pääsalausavaimet

Secure Enclave sisältää UID (unique ID) -pääsalausavaimen. UID on jokaiselle laitteelle yksilöllinen, eikä se liity mihinkään muuhun laitteen tunnisteeseen.

Satunnaisesti luotu UID yhdistetään järjestelmäpiiriin valmistuksen aikana. A9-järjestelmäpiireistä alkaen Secure Enclaven TRNG luo UID:n valmistuksen aikana ja se kirjoitetaan suojauselementteihin käyttäen ohjelmistoprosessia, joka toimii kokonaan Secure Enclavessa. Tämä prosessi suojaa UID:tä näkymästä laitteen ulkopuolelle valmistuksen aikana, ja siksi Applella tai sen toimijoilla ei ole mahdollisuutta päästä siihen käsiksi tai tallentaa sitä.

sepOS käyttää UID:tä laitekohtaisten salaisuuksien suojaamiseen. UID:n avulla tiedot voidaan sitoa kryptografisesti tiettyyn laitteeseen. Esimerkiksi tiedostojärjestelmää suojaava avainhierarkia sisältää UID:n, joten jos sisäinen SSD-muisti siirretään fyysisesti laitteesta toiseen, tiedostoja ei voida käyttää. Muita suojattuja laitekohtaisia salaisuuksia ovat Face ID- tai Touch ID -tiedot. Macissa vain AES-komponenttiin liitetty sisäinen tallennuslaite saa tämän tason suojauksen. Esimerkiksi USB:n kautta liitettyjä ulkoisia tallennuslaitteita tai vuoden 2019 Mac Pron PCIe-pohjaista tallennustilaa ei salata tällä tavalla.

Secure Enclavella on myös laitteen ryhmätunnus (GID), joka on sama kaikille samaa järjestelmäpiiriä käyttäville laitteille (esimerkiksi kaikilla laitteilla, joissa on Apple A15 -järjestelmäpiiri, on sama GID).

UID ja GID eivät ole saatavilla Joint Test Action Group -ryhmän (JTAG) tai muiden vianmäärityskäyttöliittymien kautta.

Secure Enclaven AES-moottori

Secure Enclaven AES-moottori on laitteiston osa, jota käytetään suorittamaan symmetristä salausta AES-salausmenetelmällä. AES-moottori on suunniteltu torjumaan tietojen vuotamista ajoituksen ja staattisen tehon analyysia (Static Power Analysis, SPA) hyödyntäen. A9-järjestelmäpiiristä alkaen AES-moottori sisältää myös vastakeinoja dynaamisen tehon analyysille (Dynamic Power Analysis, DPA).

AES-moottori tukee laitteisto- ja ohjelmistoavaimia. Laitteistoavaimet muodostetaan Secure Enclaven UID:stä tai GID:stä. Nämä avaimet pysyvät AES-moottorissa eivätkä näy edes sepOS-ohjelmistolle. Vaikka ohjelmisto voi pyytää salaus- ja salauksen purkuoperaatioita laitteistoavaimilla, se ei saa avaimia.

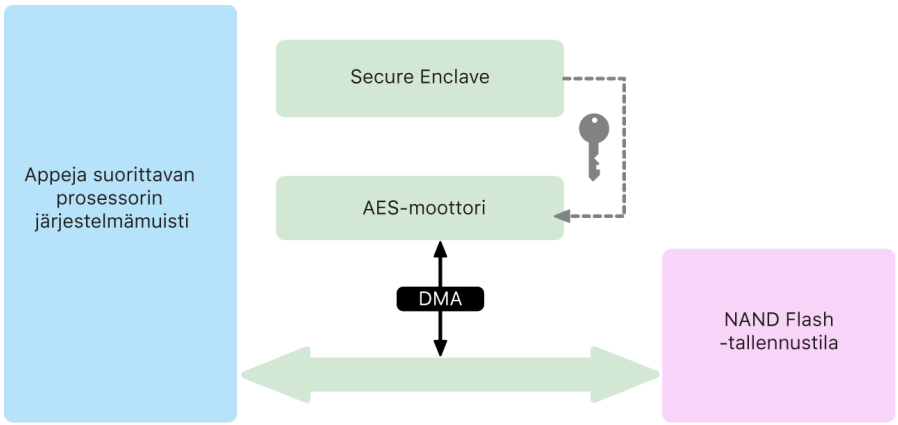
Apple A10 -järjestelmäpiirissä ja uudemmissa AES-moottori sisältää lukittavia siemenbittejä, joilla UID:stä tai GID:stä muodostetuista avaimista tehdään erilaisia. Näin laitteen toimintatila voidaan asettaa ehdoksi pääsylle tietoihin. Esimerkiksi lukittavia siemenbittejä käytetään kieltämään pääsy salasanasuojattuihin tietoihin käynnistettäessä DFU-tilasta. Jos haluat lisätietoja, katso Pääsykoodit ja salasanat.

AES-komponentti

Jokaisessa Applen laitteessa, jossa on Secure Enclave, on myös erillinen AES256-salausmoottori (”AES-moottori”), joka on sisäänrakennettuna DMA-väylään (pysyvän) NAND-flash-tallennustilan ja järjestelmämuistin välissä. Tämä tekee tiedostojen salauksesta erittäin tehokasta. A9:ssä tai uudemmissa A-sarjan prosessoreissa flash-tallennustila on eristetyllä väylällä, joka saa DMA-salausmoottorin kautta pääsyn vain muistiin, jossa ovat käyttäjän tiedot.

Käynnistyksen aikana sepOS luo väliaikaisen salausavaimen käyttäen TRNG-generaattoria. Secure Enclave toimittaa tämän avaimen AES-moottorille käyttäen tarkoitukseen varattua reittiä, joka on suunniteltu estämään mitään Secure Enclaven ulkopuolista ohjelmistoa pääsemästä siihen. Tämän jälkeen sepOS voi käyttää lyhytaikaista salausavainta appeja suorittavan prosessorin tiedostojärjestelmän ajurin käyttöön tulevien tiedostoavainten salaamiseen. Kun tiedostojärjestelmän ajuri lukee tai kirjoittaa tiedostoa, se lähettää salatun avaimen AES-moottorille, joka purkaa avaimen salauksen. AES-moottori ei koskaan paljasta salaamattomia avaimia ohjelmistolle.

Huomaa: AES-moottori on sekä Secure Enclavesta että Secure Enclaven AES-moottorista erillinen komponentti, mutta sen toiminta on tiiviisti sidoksissa Secure Enclaveen, kuten alla olevasta kuvasta käy ilmi.



Julkisen avaimen kiihdytin

Julkisen avaimen kiihdytin (Public Key Accelerator, PKA) on laitteiston osa, jota käytetään epäsymmetristen salausoperaatioiden suorittamiseen. PKA tukee RSA-allekirjoitus- ja salausalgoritmeja sekä elliptisen käyrän (ECC) allekirjoitus- ja salausalgoritmeja. PKA on suunniteltu torjumaan tietojen vuotamista ajoitus- ja sivukanavahyökkäyksissä kuten SPA ja DPA.

PKA tukee ohjelmisto- ja laitteistoavaimia. Laitteistoavaimet muodostetaan Secure Enclaven UID:stä tai GID:stä. Nämä avaimet pysyvät PKA:ssa eivätkä näy edes sepOS-ohjelmistolle.

A13-järjestelmäpiireistä alkaen PKA:n salaukset on todistettu matemaattisesti oikeiksi formaalin verifioinnin tekniikoita käyttäen.

Apple A10 -järjestelmäpiirissä ja uudemmissa PKA tukee käyttöjärjestelmään sidottuja avaimia, mistä käytetään myös nimitystä sinetöity avaimen suojaus. Nämä avaimet luodaan käyttäen yhdistelmää laitteen UID:stä ja laitteessa toimivan sepOS:n tiivisteestä. Tiiviste saadaan Secure Enclaven Boot ROMilta tai Secure Enclaven käynnistyksen valvonnalta Apple A13 -järjestelmäpiirissä ja uudemmissa. Näitä avaimia käytetään myös sepOS:n version tarkistamiseen tiettyjä Applen palveluita pyydettäessä sekä pääsykoodisuojattujen tietojen suojauksen parantamiseen, sillä avaimet auttavat estämään pääsyä avainmateriaaliin, jos järjestelmään tehdään kriittisiä muutoksia ilman käyttäjän valtuutusta.

Suojattu pysyvä tallennustila

Secure Enclavella on erityinen tallennuslaite suojattuun pysyvään tallennukseen. Suojattu pysyvä tallennustila on yhdistetty Secure Enclaveen käyttäen tähän tarkoitukseen varattua I2C-väylää, jotta ainoastaan Secure Enclave pääsee siihen. Kaikkien käyttäjän tietojen salausavainten juuri on entropiassa, joka on tallennettu Secure Enclaven pysyvään tallennustilaan.

Laitteissa, joissa on A12-, S4- tai uudempi järjestelmäpiiri, Secure Enclavesta on muodostettu pari Secure Storage -komponentin kanssa entropian tallennusta varten. Itse Secure Storage -komponentissa on muuttumaton ROM-koodi, laitteiston satunnaislukugeneraattori, laitekohtainen yksilöllinen salausavain, salausohjelmat ja fyysisen peukaloinnin tunnistin. Secure Enclave ja Secure Storage -komponentti viestivät käyttäen salattua ja todennettua protokollaa, joka antaa vain niille pääsyn entropiaan.

Syksyllä 2020 tai myöhemmin julkaistuissa laitteissa on toisen sukupolven Secure Storage -komponentti. Toisen sukupolven Secure Storage -komponentti lisää kokonaisuuteen laskurilliset turvatalletuspaikat. Kuhunkin laskurilliseen turvatalletuspaikkaan on tallennettu 128-bittinen suola, 128-bittinen pääsykoodin tarkistusarvo, 8-bittinen laskuri ja 8-bittinen yritysten enimmäismäärän arvo. Pääsyssä laskurillisiin turvatalletuspaikkoihin käytetään salattua ja todennettua protokollaa.

Laskurillisissa turvatalletuspaikoissa on entropia, jota tarvitaan pääsykoodilla suojattujen käyttäjän tietojen lukituksen avaamiseen. Päästäkseen käyttäjän tietoihin parina olevan Secure Enclaven on muodostettava oikea pääsykoodin entropia-arvo käyttäjän pääsykoodista ja Secure Enclaven UID:stä. Käyttäjän pääsykoodia ei voi selvittää käyttäen lukituksen avausyrityksiä, jotka on lähetetty muusta lähteestä kuin parina olevasta Secure Enclavesta. Jos pääsykoodiyritysten raja ylittyy (esimerkiksi kymmenen yritystä iPhonessa), Secure Storage -komponentti hävittää pääsykoodilla suojatut tiedot kokonaan.

Secure Enclave lähettää Secure Storage -komponentille laskurillisen turvatalletuspaikan luomista varten pääsykoodin entropia-arvon ja yritysten enimmäismäärän arvon. Secure Storage -komponentti luo suola-arvon käyttäen satunnaislukugeneraattoriaan. Sitten se muodostaa pääsykoodin tarkistusarvon ja turvatalletuspaikan entropia-arvon saamastaan pääsykoodin entropiasta, Secure Storage -komponentin yksilöllisestä salausavaimesta ja suola-arvosta. Secure Storage -komponentti valmistelee laskurillisen turvatalletuspaikan arvolla 0, annetulla yritysten enimmäisarvolla, muodostetulla pääsykoodin tarkistusarvolla ja suola-arvolla. Sitten Secure Storage -komponentti palauttaa luomansa turvatalletuspaikan entropia-arvon Secure Enclavelle.

Saadakseen turvatalletuspaikan entropia-arvon laskurillisesta turvatalletuspaikasta myöhemmin Secure Enclave lähettää Secure Storage -komponentille pääsykoodin entropian. Secure Storage -komponentti lisää ensin laskurillisen turvatalletuspaikan laskurin arvoa. Jos laskuri lisäyksen jälkeen ylittää yritysten enimmäisarvon, Secure Storage-komponentti poistaa kokonaan laskurillisen turvatalletuspaikan. Jos yritysten enimmäismäärä ei ole vielä täyttynyt, Secure Storage -komponentti yrittää muodostaa pääsykoodin tarkistusarvon ja turvatalletuspaikan entropia-arvon samalla algoritmilla, jota käytettiin laskurillisen turvatalletuspaikan luomiseen. Jos muodostettu pääsykoodin tarkistusarvo vastaa tallennettua pääsykoodin tarkistusarvoa, Secure Storage -komponentti palauttaa turvatalletuspaikan entropia-arvon Secure Enclavelle ja nollaa laskurin.

Salasanasuojattujen tietojen käyttöön tarvittavien avainten juuri on laskurillisiin turvatalletuspaikkoihin tallennetussa entropiassa. Jos haluat lisätietoja, katso Tietojen suojauksen yleiskatsaus.

Suojattua pysyvää tallennustilaa käytetään kaikkiin Secure Enclaven toistonestopalveluihin. Secure Enclaven toistonestopalveluita käytetään tietojen kumoamiseen sellaisten tapahtumien yhteydessä, jotka merkitsevät toistonestorajoja, mukaan lukien muun muassa seuraavat:

- Pääsykoodin vaihtaminen
- Face ID:n tai Touch ID:n ottaminen käyttöön tai pois käytöstä
- Face ID -kasvojen tai Touch ID -sormenjäljen lisääminen tai poistaminen
- Face ID:n tai Touch ID:n nollaaminen
- Apple Pay -kortin lisääminen tai poistaminen
- Kaiken sisällön ja kaikkien asetusten poistaminen

Niissä arkkitehtuureissa, joihin ei sisälly Secure Storage -komponenttia, Secure Enclaven suojatun tallennuksen palveluita varten käytetään EEPROM-muistia. Secure Storage -komponenttien tavoin EEPROM on liitetty Secure Enclaveen ja on ainoastaan sen käytettävissä, mutta sillä ei ole erityisiä laitteiston suojausominaisuuksia eikä se takaa yksinoikeudellista pääsyä entropiaan (muuten kuin fyysisen liittämisen osalta) eikä sillä ole laskurillisia turvatalletuspaikkoja.

Suojattu Neural Engine

Laitteissa, joissa on Face ID, suojattu Neural Engine muuntaa kaksiulotteiset kuvat ja syvyyskartat matemaattiseksi esitykseksi käyttäjän kasvoista.

Järjestelmäpiireissä A11:stä A13:een suojattu Neural Engine on integroitu Secure Enclaveen. Tehokkaan suorituskyvyn saavuttamiseksi suojattu Neural Engine käyttää suoraa muistin käyttöä (DMA). sepOS:n kernelin hallinnan alainen I/O-muistinhallintayksikkö (IOMMU) rajoittaa tämän suoran muistihaun valtuutetuille muistialueille.

A14:stä ja M1-perheestä alkaen suojattu Neural Engine on toteutettu suojattuna toimintona appeja suorittavan prosessorin Neural Enginessä. Erityinen laitteiston suojausohjain vaihtaa appeja suorittavan prosessorin ja Secure Enclaven tehtävien välillä ja nollaa Neural Enginen tilan kunkin siirtymisen yhteydessä Face ID:n tietojen suojaamiseksi. Muistin salauksesta, todennuksesta ja pääsynhallinnasta huolehtii tähän tarkoitukseen varattu komponentti. Samalla se käyttää erillistä salausavainta ja muistiväliä suojatun Neural Enginen rajoittamiseen valtuutetuille muistialueille.

Tehon ja kellon valvonta

Kaikki elektroniikka on suunniteltu toimimaan rajatulla jännite- ja taajuusalueella. Näiden rajojen ulkopuolella käytettynä elektroniikka voi toimia virheellisesti, ja tällöin suojauksia on ehkä mahdollista ohittaa. Secure Enclaveen on suunniteltu valvontapiirit auttamaan varmistamaan, että jännite ja taajuus pysyvät turvallisissa rajoissa. Nämä valvontapiirit on suunniteltu siten, että niiden turvallinen toiminta-alue on paljon laajempi kuin muiden Secure Enclaven osien. Jos valvonta havaitsee kielletyn toimintapisteen, Secure Enclaven kellot pysähtyvät automaattisesti eivätkä käynnisty uudelleen ennen kuin järjestelmäpiiri nollataan seuraavan kerran.

Secure Enclaven ominaisuuksien yhteenveto

Huomaa: A12-, A13-, S4- ja S5-tuotteilla, jotka on julkaistu syksyllä 2020, on toisen sukupolven Secure Storage -komponentti, kun taas aikaisemmilla näihin järjestelmäpiireihin perustuvilla tuotteilla on ensimmäisen sukupolven Secure Storage -komponentti.

Järjestelmäpiiri	Muistinsuojausmoduuli	Suojattu tallennus	AES-komponentti	PKA
A8	Salaus ja todennus	EEPROM	Kyllä	Ei
A9	Salaus ja todennus	EEPROM	DPA-suojaus	Kyllä
A10	Salaus ja todennus	EEPROM	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
A11	Salaus, todennus ja uudelleentoiston esto	EEPROM	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
A12 (ennen syksyä 2020 julkaistut Applen laitteet)	Salaus, todennus ja uudelleentoiston esto	1. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
A12 (syksyn 2020 jälkeen julkaistut Applen laitteet)	Salaus, todennus ja uudelleentoiston esto	2. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
A13 (ennen syksyä 2020 julkaistut Applen laitteet)	Salaus, todennus ja uudelleentoiston esto	1. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet ja käynnistyksen valvonta
A13 (syksyn 2020 jälkeen julkaistut Applen laitteet)	Salaus, todennus ja uudelleentoiston esto	2. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet ja käynnistyksen valvonta
A14, A15	Salaus, todennus ja uudelleentoiston esto	2. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet ja käynnistyksen valvonta
S3	Salaus ja todennus	EEPROM	DPA-suojaus ja lukittavat siemenbitit	Kyllä
S4	Salaus, todennus ja uudelleentoiston esto	1. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
S5 (ennen syksyä 2020 julkaistut Applen laitteet)	Salaus, todennus ja uudelleentoiston esto	1. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
S5 (syksyn 2020 jälkeen julkaistut Applen laitteet)	Salaus, todennus ja uudelleentoiston esto	2. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
S6, S7	Salaus, todennus ja uudelleentoiston esto	2. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
T2	Salaus ja todennus	EEPROM	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet
M1-perhe	Salaus, todennus ja uudelleentoiston esto	2. sukupolven Secure Storage -komponentti	DPA-suojaus ja lukittavat siemenbitit	Käyttöjärjestelmään sidotut avaimet ja käynnistyksen valvonta

Face ID ja Touch ID

Face ID:n ja Touch ID:n suojaus

Pääsykoodit ja salasanat ovat olennainen osa Applen laitteiden suojausta. Samalla kuitenkin käyttäjien tarvitsee päästä laitteilleen vaivattomasti, usein yli satakin kertaa päivässä. Biometrinen todennus tarjoaa keinon saada vahvan pääsykoodin suojaus (tai jopa vahvistaa pääsykoodia tai salasanaa, koska sitä ei tarvitse syöttää käsin) samalla, kun lukituksen avaaminen onnistuu vaivattomasti sormella tai vilkaisulla. Face ID ja Touch ID eivät korvaa pääsykoodia tai salasanaa, mutta ne nopeuttavat ja helpottavat käyttöä useimmissa tilanteissa.

Applen biometrinen suojausarkkitehtuuri nojaa biometrisen tunnistimen ja Secure Enclaven vastuiden tiukkaan erottamiseen ja näiden kahden väliseen suojattuun yhteyteen. Tunnistin ottaa biometrisen kuvan ja toimittaa sen suojatusti Secure Enclavelle. Rekisteröinnin aikana Secure Enclave prosessoi, salaa ja tallentaa vastaavat Face ID:n ja Touch ID:n mallitiedot. Vastaavuutta tarkistaessaan Secure Enclave vertaa biometriselta tunnistimelta saapuvia tietoja tallennettuihin malleihin ja ratkaisee sen perusteella, avataanko laite tai onko tunnistus hyväksyttävä (käytettäessä Apple Payta, apeissa sekä muissa Face ID:n ja Touch ID:n käyttötilanteissa). Arkkitehtuuri tukee laitteita, joissa on sekä tunnistin että Secure Enclave (kuten iPhone, iPad ja monet Mac-järjestelmät), ja myös mahdollisuutta käyttää fyysisesti erillään olevaa tunnistinta oheislaitteessa, josta on muodostettu suojatusti laitepari Apple siliconilla varustetun Macin Secure Enclavelle.

Face ID:n suojaus

Face ID avaa tuettujen Apple-laitteiden lukituksen suojatusti pelkän vilkaisun avulla. Se tarjoaa intuitiivisen ja turvallisen todentamisen TrueDepth-kamerajärjestelmän avulla, joka kuvaa edistyksellisten teknologioiden avulla tarkasti käyttäjän kasvojen muodot. Face ID käyttää neuroverkkoja katsekontaktin ja vastaavuuden määrittämiseen ja huijausyritysten hylkäämiseen, jotta käyttäjä voi avata puhelimen pelkällä vilkaisulla – jopa maski kasvoillaan, jos hän käyttää tuettua laitetta. Face ID mukautuu automaattisesti ulkonäön muutoksiin ja suojaa tarkasti käyttäjän biometristen tietojen yksityisyyttä ja turvallisuutta.

Face ID on suunniteltu varmistamaan käyttäjän katsekontaktin, tarjoamaan varman todentamisen, jossa vääriä tunnistamisia on vain vähän, ja estämään sekä digitaalista että fyysistä huijaamista.

TrueDepth-kamera etsii automaattisesti käyttäjän kasvoja, kun käyttäjä herättää Face ID:llä varustetun Apple-laitteen (nostamalla sen tai napauttamalla sen näyttöä), sekä silloin kun laitteet yrittävät todentaa käyttäjän näyttääkseen saapuneen ilmoituksen tai kun tuettu appi pyytää Face ID -todentamista. Kun kasvot havaitaan, Face ID varmistaa katsekontaktin ja avausyrityksen tunnistamalla, että käyttäjän silmät ovat auki ja katse on suunnattu laitteeseen. Kun VoiceOver on aktivoitu, Face ID:n katsekontaktin tarkistaminen on käyttöapusyistä pois päältä, ja sen voi tarvittaessa poistaa käytöstä erikseen. Kun Face ID:tä käytetään maskin kanssa, katsekontaktin tarkistaminen vaaditaan.

Kun TrueDepth-kamera on vahvistanut katsekontaktin, se heijastaa ja lukee tuhansia infrapunapisteitä ja muodostaa kasvoista syvyysmallinnuksen sekä kaksiulotteisen infrapunakuvan. Näiden tietojen avulla luodaan sarja kaksiulotteisia kuvia ja syvyysmallinnuksia, jotka allekirjoitetaan digitaalisesti ja lähetetään Secure Enclaveen. TrueDepth-kamera vastaa digitaalisiin ja fyysisiin huijausyrityksiin satunnaistamalla kaksiulotteisten kuvien ja syvyysmallinnuskuvien järjestyksen ja projisoimalla laitekohtaisen satunnaisen kuvion. Suojatun Neural Enginen osio, joka on suojattuna Secure Enclaven sisällä, muuntaa nämä tiedot matemaattiseksi esitykseksi ja vertaa esitystä rekisteröityihin kasvotietoihin. Nämä rekisteröidyt tiedot ovat itsessään matemaattinen esitys käyttäjän kasvoista, jotka on kuvattu eri asennoissa.

Touch ID:n suojaus

Touch ID on sormenjälkien tunnistusjärjestelmä, joka tekee tuettujen Apple-laitteiden turvallisesta käytöstä nopeampaa ja helpompaa. Tämä teknologia lukee sormenjälkien tietoja mistä tahansa kulmasta ja oppii ajan myötä lisää käyttäjän sormenjäljestä. Tunnistimen avulla se laajentaa sormenjälkikarttaa, kun jokaisella käyttökerralla tunnistetaan lisää päällekkäisiä solmuja.

Touch ID:llä varustettujen Apple-laitteiden lukitus voidaan avata sormenjälkeä käyttämällä. Touch ID ei poista laitteen pääsykoodin tai käyttäjän salasanan tarvetta. Se vaaditaan edelleen laitteen käynnistyksen ja uudelleenkäynnistyksen jälkeen sekä siitä uloskirjautumisen jälkeen (Macissa). Joissakin apeissa Touch ID:tä voidaan myös käyttää laitteen pääsykoodin tai käyttäjän salasanan sijasta. Sitä voidaan käyttää esimerkiksi salasanasuojattujen muistiinpanojen avaamiseen Muistiinpanot-apissa, avainnipulla suojattujen verkkosivustojen avaamiseen ja tuettujen appien salasanojen avaamiseen. Laitteen pääsykoodi tai käyttäjän salasana vaaditaan kuitenkin joka kerta tietyissä tilanteissa (esimerkiksi laitteen olemassa olevan pääsykoodin tai käyttäjän salasanan muuttamiseen, rekisteröityjen sormenjälkien poistamiseen tai uusien sormenjälkien rekisteröimiseen).

Kun sormenjälkitunnistin tunnistaa sormen kosketuksen, se käynnistää edistyksellisen kuvantamisryhmän, joka skannaa sormen ja lähettää skannaustiedot Secure Enclaveen. Tämän yhteyden suojaamiseen käytettävä kanava vaihtelee riippuen siitä, onko Touch ID -tunnistin samassa laitteessa kuin Secure Enclave vai onko se erillisessä oheislaitteessa.

Kun sormenjäljen skannausta vektoroidaan analysointia varten, rasteriskannaus tallennetaan väliaikaisesti salattuun muistiin Secure Enclavessa, ja sitten se poistetaan. Analyysi käyttää ihonalaisten kohoumien kulman kuvausta. Se on häviöllinen prosessi, jossa poistetaan ”sormenjäljen erikoiskohtatiedot”, joita tarvittaisiin käyttäjän oikean sormenjäljen muodostamiseen uudelleen. Rekisteröinnin aikana tulokseksi saatu solmukartta tallennetaan ilman tunnistetietoja vain Secure Enclaven luettavissa olevassa salatussa muodossa malliksi, johon vastaavuutta myöhemmin verrataan. Tiedot eivät koskaan poistu laitteesta. Niitä ei lähetetä Applelle eikä niitä sisällytetä laitteiden varmuuskopioihin.

Sisäänrakennetun Touch ID:n kanavan suojaus

Secure Enclaven ja sisäänrakennetun Touch ID -tunnistimen välinen kommunikaatio tapahtuu SPI-väylällä (Serial Peripheral Interface). Prosessori välittää tiedot Secure Enclavelle, mutta ei voi lukea niitä. Tiedot salataan ja todennetaan istuntoavaimella, joka sovitaan jaetulla avaimella, joka on jo tehtaalla valmisteltu jokaiselle Touch ID -tunnistimelle ja sen vastaavalle Secure Enclavelle. Jokaisen Touch ID -tunnistimen jaettu avain on vahva, satunnainen ja erilainen. Istunnon avaimenvaihto käyttää AES-avainsalausta, johon molemmat osapuolet tarjoavat satunnaisen avaimen, joka muodostaa istuntoavaimen ja käyttää siirtosalausta, johon sisältyvät sekä todennus että luottamuksellisuus (AES-CCM).

Touch ID:llä varustettu Magic Keyboard

Touch ID:llä varustettu Magic Keyboard (sekä Touch ID:llä ja numeronäppäimistöllä varustettu Magic Keyboard) tarjoaa Touch ID -tunnistimen ulkoisessa näppäimistössä, jota voidaan käyttää minkä tahansa Apple siliconilla varustetun Macin kanssa. Touch ID:llä varustettu Magic Keyboard toimii biometrisen tunnistimen roolissa. Se ei tallenna biometrisia malleja, ei vertaa biometristen tietojen vastaavuutta eikä vaadi tietoturvakäytäntöjen noudattamista (esimerkiksi salasanan syöttämistä, kun lukitusta ei ole avattu 48 tunnin kuluessa). Touch ID:llä varustetun Magic Keyboardin Touch ID -tunnistin on liitettävä suojatusti Macin Secure Enclaven laitepariksi ennen kuin sitä voidaan käyttää, ja sen jälkeen Secure Enclave suorittaa rekisteröinnin ja vastaavuuden vertaamisen ja vaatii tietoturvakäytäntöjen noudattamista samalla tavoin, kuin jos kyseessä olisi samaan laitteeseen sisältyvä Touch ID -tunnistin. Apple suorittaa tehtaalla laiteparin muodostusprosessin sellaiselle Touch ID:llä varustetulle Magic Keyboardille, joka toimitetaan Macin mukana. Myös käyttäjä voi tarvittaessa muodostaa laiteparin. Touch ID:llä varustetulla Magic Keyboardilla voi olla suojattu pariliitäntä vain yhden Macin kanssa kerrallaan, mutta Macilla voi olla suojattu pariliitäntä jopa viiden erillisen Touch ID:llä varustetun Magic Keyboard -näppäimistön kanssa.

Touch ID:llä varustettu Magic Keyboard ja sisäänrakennetut Touch ID -tunnistimet ovat yhteensopivia. Jos Macin sisäänrakennetulla Touch ID -tunnistimella rekisteröity sormi esitetään Touch ID:llä varustetulle Magic Keyboardille, tai toisin päin, vastaavuuden prosessoiminen onnistuu Macin Secure Enclavessa.

Suojatun laiteparin muodostamisen ja sen myötä Macin Secure Enclaven ja Touch ID:llä varustetun Magic Keyboardin välisen viestinnän tukemista varten näppäimistössä on julkisen avaimen kiihdytin (PKA) vahvistusta varten sekä laitteistopohjaiset avaimet tarvittavia kryptografisia prosesseja varten.

Suojattu laiteparin muodostaminen

Ennen kuin Touch ID:llä varustettua Magic Keyboardia voidaan käyttää Touch ID -operaatioihin, se on liitettävä suojatusti Macin laitepariksi. Parinmuodostusta varten Macin Secure Enclave ja Touch ID:llä varustetun Magic Keyboardin PKA-osa vaihtavat keskenään julkiset avaimet, jotka ovat lähtöisin luotetulta Applen varmentajalta, ja ne käyttävät laitteistossa olevia vahvistamisavaimia ja lyhytaikaista ECDH:ta identiteettinsä turvalliseen vahvistamiseen. Macissa näitä tietoja suojaa Secure Enclave, ja Touch ID:llä varustetussa Magic Keyboardissa näitä tietoja suojaa sen PKA-osa. Suojatun parinmuodostuksen jälkeen kaikki Touch ID -tiedon siirtäminen Macin ja Touch ID:llä varustetun Magic Keyboardin välillä salataan AES-GCM-salauksella, jossa avaimen pituus on 256 bittiä, käyttäen tallennettuihin identiteetteihin perustuvia lyhytaikaisia ECDH-avaimia NIST P-256 -käyrällä. (Tavallisten näppäinten painallusten tiedonsiirrossa käytetään Bluetoothin suojausta samoin kuten muillakin Bluetooth-näppäimistöillä.)

Aikomus muodostaa pari luotettavasti

Suorittaessaan joitakin Touch ID -operaatioita ensimmäisen kerran (esimerkiksi rekisteröidessään uuden sormenjäljen) käyttäjän on fyysisesti vahvistettava aikeensa käyttää Touch ID:llä varustettua Magic Keyboardia Macin kanssa. Aikeen vahvistaminen fyysisesti tapahtuu painamalla kahdesti Macin virtapainiketta, kun käyttäjä saa siihen kehotuksen käyttöliittymältä, tai käyttämällä onnistuneesti aikaisemmin Maciin rekisteröityä sormenjälkeä. Jos haluat lisätietoja, katso Aikomus muodostaa pari luotettavasti ja yhteydet Secure Enclaveen.

Apple Pay -maksutapahtumat voidaan valtuuttaa Touch ID -tunnistuksella tai syöttämällä macOS:n käyttäjän salasana ja painamalla kahdesti Touch ID:llä varustetun Magic Keyboardin Touch ID -painiketta. Jälkimmäinen mahdollistaa käyttäjälle fyysisen aikeen vahvistamisen ilman Touch ID -tunnistuksen käyttämistä.

Touch ID:llä varustetun Magic Keyboardin kanavan suojaus

Osana Touch ID:llä varustetun Magic Keyboardin Touch ID -tunnistimen ja laitepariksi asetetun Macin Secure Enclaven välisen tiedonsiirtokanavan suojauspyrkimyksiä tarvitaan seuraavia:

- Edellä kuvattu suojattu parinmuodostus Touch ID:llä varustetun Magic Keyboardin PKA-osan ja Secure Enclaven välillä
- Suojattu kanava Touch ID:llä varustetun Magic Keyboardin tunnistimen ja sen PKA-osan välillä

Suojattu kanava Touch ID:llä varustetun Magic Keyboardin tunnistimen ja sen PKA-osan välillä muodostetaan tehtaalla käyttämällä näiden kahden jakamaa yksilöllistä avainta. (Tekniikka on sama kuin luotaessa suojattu kanava Macin Secure Enclaven ja sen sisäänrakennetun tunnistimen välille sellaisissa Mac-tietokoneissa, joissa on sisäänrakennettu Touch ID.)

Face ID, Touch ID, pääsykoodit ja salasanat

Jotta Face ID:tä tai Touch ID:tä voidaan käyttää, käyttäjän täytyy asettaa laitteensa vaatimaan pääsykoodia tai salasanaa sen avaamiseen. Kun Face ID tai Touch ID havaitsee täsmäävän vastaavuuden, käyttäjän laite avautuu ilman laitteen pääsykoodin tai salasanan kysymistä. Siksi pidemmän ja monimutkaisemman pääsykoodin tai salasanan käyttö on huomattavasti käytännöllisempää, sillä käyttäjän ei tarvitse syöttää sitä niin usein. Face ID ja Touch ID eivät korvaa käyttäjän pääsykoodia tai salasanaa, vaan ne tekevät laitteen käytöstä helppoa harkittujen rajoitusten ja aikarajojen puitteissa. Tämä on tärkeää, koska vahva pääsykoodi tai salasana muodostaa perustan sille, miten käyttäjän iPhone, iPad, Mac tai Apple Watch suojaa kryptografisesti kyseisen käyttäjän tietoja.

Milloin laitteen pääsykoodia tai salasanaa vaaditaan

Käyttäjät voivat käyttää pääsykoodiaan tai salasanaansa milloin vain Face ID:n tai Touch ID:n sijaan, mutta on tilanteita, joissa biometrista tunnistautumista ei sallita. Seuraavissa suojauksen kannalta tärkeissä toiminnoissa vaaditaan pääsykoodin tai salasanan syöttäminen:

- Ohjelmiston päivittäminen
- Laitteen tyhjentäminen
- Pääsykoodin asetusten katsominen tai muuttaminen
- Asetusprofiilien asentaminen
- Macin Järjestelmäasetusten Suojaus ja yksityisyys -osion lukituksen avaaminen
- Macin Järjestelmäasetusten Käyttäjät ja ryhmät -osion lukituksen avaaminen (jos FileVault on päällä)

Pääsykoodi tai salasana vaaditaan myös, jos laite on jossakin seuraavista tiloista:

- Laite on juuri laitettu päälle tai käynnistetty uudelleen.
- Käyttäjä on kirjautunut ulos Mac-tililtä (tai ei ole vielä kirjautunut sisään).
- Käyttäjä ei ole avannut laitteen lukitusta yli 48 tuntiin.
- Käyttäjä ei ole käyttänyt pääsykoodiaan tai salasanaansa laitteen lukituksen avaamiseen 156 tunnin aikana (eli kuuteen ja puoleen vuorokauteen), ja käyttäjä ei ole käyttänyt biometrista tunnistautumista lukituksen avaamiseen neljään tuntiin.
- Laite on saanut etälukituskomennon.
- Kun käyttäjä on poistunut Virta pois päältä/Hätätila SOS -tilasta pitämällä jompaakumpaa äänenvoimakkuuspainiketta ja nukkumispainiketta samaan aikaan painettuina 2 sekunnin ajan ja napauttamalla sitten Kumoa.
- Kun biometrinen tunnistautumisyritys on epäonnistunut viisi kertaa (tosin käytettävyyden parantamiseksi laite voi tarjota pääsykoodin tai salasanan syöttämistä biometristen tietojen sijaan jo vähäisemmän yritysmäärän jälkeen).

Kun Face ID otetaan käyttöön iPhonessa maskin kanssa, se on käytettävissä seuraavat 6,5 tuntia sen jälkeen, kun käyttäjä on tehnyt jonkin seuraavista:

- Onnistunut Face ID -tunnistautumisyritys (maskin kanssa tai ilman)
- Vahvistus laitteen pääsykoodilla
- Laitteen avaaminen Apple Watchilla

Minkä tahansa näiden toimintojen suorittaminen lisää käyttöaikaa 6,5 tunnilla suorittamishetkestä.

Kun Face ID tai Touch ID on käytössä iPhonessa tai iPadissa, laite lukittuu välittömästi, kun nukkumispainiketta painetaan. Laite lukittuu myös aina, kun se menee nukkumaan. Face ID ja Touch ID vaativat onnistuneen todentautumisen (tai vaihtoehtoisesti pääsykoodin käyttämistä) joka kerta, kun laite herää.

Todennäköisyys, että satunnainen henkilö voisi avata käyttäjän iPhonen tai iPadin Face ID:llä on alle yksi 1 000 000:sta – silloinkin kuin Face ID:tä käytetään maskin kanssa. Touch ID:llä varustetun tai Magic Keyboardin pariksi asetetun iPhonen, iPadin ja Macin kohdalla todennäköisyys on alle yksi 50 000:stä. Tämä todennäköisyys kasvaa, kun rekisteröityjä sormenjälkiä on enemmän (jopa yksi 10 000:sta viidellä sormenjäljellä) tai kun Face ID -otoksia on enemmän (jopa yksi 500 000:sta kahdella otoksella). Suojauksen lisäämiseksi sekä Face ID että Touch ID sallivat vain viisi epäonnistunutta todentautumisyritystä, ennen kuin pääsykoodi tai salasana vaaditaan käyttäjän laitteen tai tilin käyttämiseen. Väärän vastaavuuden todennäköisyys Face ID:llä on suurempi seuraaville:

- Kaksoset ja sisarukset, jotka muistuttavat käyttäjää
- Alle 13-vuotiaat lapset (koska heidän kasvonpiirteensä eivät ole vielä välttämättä täysin kehittyneet)

Näissä tapauksissa Face ID:n käyttäminen maskin kanssa kasvattaa väärän vastaavuuden todennäköisyyttä lisää. Jos käyttäjä on huolissaan väärästä vastaavuudesta, Apple suosittelee pääsykoodin käyttämistä todennukseen.

Kasvojen tunnistuksen suojaus

Kasvojen tunnistus tehdään Secure Enclavessa neuroverkoilla, jotka on koulutettu nimenomaan tähän tarkoitukseen. Apple kehitti kasvojen tunnistuksen neuroverkot käyttäen yli miljardia kuvaa, mukaan lukien infrapuna- ja syvyyskuvia, jotka kerättiin osallistujien tietoisella suostumuksella tehdyissä tutkimuksissa. Tämän jälkeen Apple työskenteli osallistujien kanssa ympäri maailman ja otti mukaan edustavan ryhmän osallistujia, joissa oli eri sukupuolten, ikien, etnisyyksien ja muiden tekijöiden edustajia. Tutkimuksia täydennettiin tarpeen mukaan, jotta erilaisia käyttäjiä tunnistettaisiin mahdollisimman tarkasti. Face ID on suunniteltu toimimaan hattujen, huivien, silmälasien, piilolinssien ja monentyyppisten aurinkolasien kanssa. Face ID tukee lukituksen avaamista myös maski kasvoilla iPhone-laitteissa iPhone 12:sta alkaen ja iOS 15.4:llä tai uudemmilla. Lisäksi se on suunniteltu toimimaan sisällä, ulkona ja jopa täydellisessä pimeydessä. Huijauksia tunnistava ja estävä lisäneuroverkko suojaa yrityksiltä avata laite valokuvien tai naamioiden avulla. Face ID -tiedot, mukaan lukien käyttäjän kasvojen matemaattiset esitykset, on salattu, ja ne ovat vain Secure Enclaven käytettävissä. Tiedot eivät koskaan poistu laitteesta. Niitä ei lähetetä Applelle eikä niitä sisällytetä laitteiden varmuuskopioihin. Seuraavat Face ID -tiedot tallennetaan ja salataan vain Secure Enclaven käytettäväksi normaalin toiminnan aikana:

- Rekisteröitymisen yhteydessä lasketut käyttäjän kasvojen matemaattiset esitykset
- Avausyritysten aikana lasketut käyttäjän kasvojen matemaattiset esitykset, jos Face ID määrittää ne hyödyllisiksi parantaakseen tulevia tunnistuksia

Normaalissa käytössä kuvattuja kasvokuvia ei tallenneta, vaan ne poistetaan välittömästi, kun matemaattinen esitys on laskettu joko rekisteröintiä tai aiemmin rekisteröityjen Face ID -tietojen vertailua varten.

Face ID -tunnistuksen parantaminen

Jotta Face ID voi parantaa tunnistusta ja pysyä mukana kasvojen ja ulkonäön luonnollisissa muutoksissa, se lisää tallennettuja matemaattisia esityksiä ajan myötä. Kun tunnistus onnistuu, Face ID voi tunnistaa uudella lasketulla matemaattisella esityksellä (jos se on riittävän laadukas) rajallisen määrän kertoja, ennen kuin tiedot poistetaan. Jos taas Face ID ei onnistu tunnistamaan kasvoja, mutta vastaavuuden laatu on korkeampi kuin tietty raja-arvo ja käyttäjä syöttää välittömästi epäonnistuneen tunnistuksen jälkeen pääsykoodinsa, Face ID ottaa toisen kuvan ja lisää sen rekisteröityihin Face ID -tietoihin uuden lasketun matemaattisen esityksen kanssa. Nämä uudet Face ID -tiedot poistetaan, jos käyttäjän kuva ei enää vastaa niitä. Tiedot poistetaan myös tietyn tunnistusmäärän jälkeen. Uudet tiedot voidaan myös poistaa valitsemalla Face ID:n nollaaminen. Näiden lisäysprosessien ansiosta Face ID pystyy mukautumaan käyttäjän kasvojen karvoituksen tai meikin käytön merkittäviin muutoksiin samalla, kun se minimoi väärät tunnistukset.

Face ID:n ja Touch ID:n käyttötarkoitukset

Laitteen tai käyttäjätilin lukituksen avaaminen

Kun Face ID tai Touch ID on pois käytöstä ja laite tai tili lukittuu, suurimman tietojen suojausluokan avaimet, joita säilytetään Secure Enclavessa, poistetaan. Tämän luokan tiedostoja ja avainnipun kohteita ei voida käyttää ennen kuin käyttäjä avaa laitteen tai tilin syöttämällä pääsykoodinsa tai salasanansa.

Kun Face ID tai Touch ID on käytössä, avaimia ei poisteta, kun laite tai tili lukittuu. Sen sijaan ne salataan avaimella, joka annetaan Face ID:n tai Touch ID:n alijärjestelmälle Secure Enclavessa. Kun käyttäjä yrittää avata laitteen tai tilin ja jos laite havaitsee onnistuneen tunnistuksen, se antaa avaimen tietojen suojausavaimien salauksen purkamiseen, ja laite tai tili avataan. Tämä prosessi tarjoaa lisäsuojausta, sillä se edellyttää laitteen avaamista varten yhteistyötä tietojen suojauksen ja Face ID:n tai Touch ID:n alijärjestelmien välillä.

Kun laite käynnistyy uudelleen, laitteen tai tilin avaamiseen tarvittavat Face ID- tai Touch ID -avaimet katoavat. Secure Enclave hävittää ne, kun mikä tahansa ehto, joka vaatii pääsykoodin tai salasanan syötön, täyttyy.

Ostojen varmistaminen Apple Paylla

Käyttäjä voi käyttää Face ID:tä ja Touch ID:tä myös Apple Payn kanssa helppoon ja turvalliseen ostojen tekemiseen myymälöissä, apeissa ja verkossa:

- *Face ID:n käyttäminen myymälöissä:* Jotta käyttäjä voi valtuuttaa maksun myymälässä Face ID:llä, käyttäjän täytyy ensin vahvistaa ostoaie kaksoispainamalla sivupainiketta. Tämä kaksoispainallus välittää käyttäjän aikeen Secure Enclaveen suoraan yhdistetyn fyysisen eleen avulla ja estää haitallisten prosessien väärennösyrityksiä. Sitten käyttäjä todentautuu Face ID:llä ennen kuin asettaa laitteen lähelle lähimaksulukijaa. Face ID -todentamisen jälkeen voidaan valita toinen Apple Pay -maksutapa. Tämä vaatii uuden todentamisen, mutta käyttäjän ei kuitenkaan tarvitse kaksoispainaa sivupainiketta uudelleen.
- *Face ID:n käyttäminen apeissa ja verkossa:* Jos käyttäjä haluaa tehdä oston apeissa tai verkossa, hän vahvistaa ostoaikeen kaksoispainamalla sivupainiketta ja valtuuttaa oston todentautumalla Face ID:llä. Jos Apple Pay -tapahtumaa ei suoriteta 60 sekunnin kuluessa siitä, kun sivupainiketta painetaan kahdesti, käyttäjän täytyy vahvistaa ostoaie uudelleen painamalla sitä uudelleen kaksi kertaa.
- *Touch ID:n käyttäminen:* Touch ID:llä ostoaie vahvistetaan käyttämällä Touch ID:n tunnistimen aktivoimiselettä ja käyttäjän sormenjäljen onnistunutta tunnistamista.

Järjestelmän tarjoamien API-rajapintojen käyttäminen

Muiden valmistajien apit voivat pyytää järjestelmän tarjoamien API:en avulla käyttäjää todentautumaan Face ID:llä, Touch ID:llä, pääsykoodilla tai salasanalla. Touch ID:tä tukevat apit tukevat automaattisesti Face ID:tä ilman mitään muutoksia. Kun käytetään Face ID:tä tai Touch ID:tä, apille ilmoitetaan vain, onnistuiko todennus. Se ei pääse käsiksi Face ID:hen, Touch ID:hen tai rekisteröityyn käyttäjään liitettyihin tietoihin.

Avainnipun kohteiden suojaaminen

Face ID:llä tai Touch ID:llä voidaan myös suojata avainnipun kohteita. Secure Enclave vapauttaa ne vain, kun tunnistautuminen onnistuu tai laitteen pääsykoodi tai tilin salasana syötetään. Appien kehittäjillä on API-rajapintoja, joilla varmistetaan, että käyttäjä on asettanut pääsykoodin tai salasanan, ennen kuin Face ID, Touch ID, pääsykoodi tai salasana vaaditaan avainnipun kohteiden avaamiseksi. Appien kehittäjät voivat tehdä kaikkia seuraavia:

- Vaatia, että todentamisrajapintojen toiminnot eivät perustu apin salasanaan tai laitteen pääsykoodiin. Ne voivat kysellä, onko käyttäjä rekisteröity, jolloin Face ID:tä tai Touch ID:tä voidaan käyttää toisena tunnistautumisosana suojauksen kannalta tärkeissä apeissa.
- Muodostaa ja käyttää Secure Enclaven sisällä elliptisen käyrän salausmenetelmään (ECC) perustuvia avaimia, jotka voidaan suojata Face ID:llä tai Touch ID:llä. Toiminnot näillä avaimilla suoritetaan aina Secure Enclaven sisällä sen jälkeen, kun se valtuuttaa niiden käytön.

Ostojen tekeminen ja hyväksyminen

Käyttäjät voivat asettaa Face ID:n tai Touch ID:n hyväksymään ostoja iTunes Storesta, App Storesta, Apple Booksista ja muualta, jotta käyttäjän ei tarvitse syöttää Apple ID -salasanaansa. Kun tehdään ostoja, Secure Enclave tarkistaa, että biometrinen valtuutus on suoritettu, ja vapauttaa sitten ECC-avaimet, joita käytetään kaupan pyynnön allekirjoittamiseen.

Aikomus muodostaa pari luotettavasti ja yhteydet Secure Enclaveen

Aikomus muodostaa pari luotettavasti on keino varmistua käyttäjän aikeesta ilman vuorovaikutusta käyttöjärjestelmän tai appeja suorittavan prosessorin kanssa. Yhteytenä toimii fyysinen yhteys fyysisestä painikkeesta Secure Enclaveen, ja ominaisuus on käytettävissä seuraavissa laitteissa:

- iPhone X tai uudempi
- Apple Watch Series 1 tai uudempi
- iPad Pro (kaikki mallit)
- iPad Air (2020)
- Apple siliconilla varustetut Mac-tietokoneet

Tämän yhteyden avulla käyttäjät voivat vahvistaa aikeensa toiminnon suorittamiseen tavalla, joka on suunniteltu siten, ettei edes root-oikeuksilla tai kernelissä toimiva ohjelmisto voi huijata sitä.

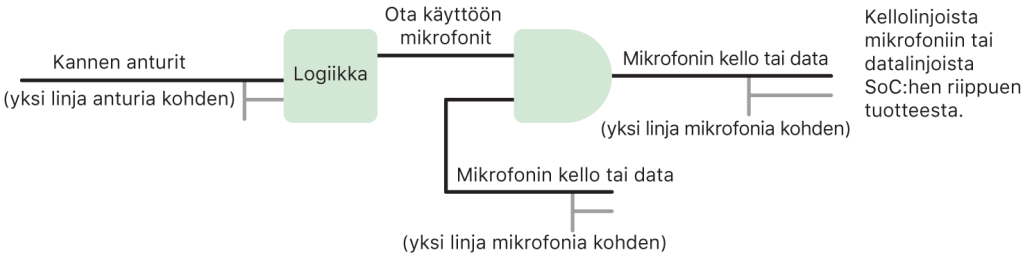
Tätä ominaisuutta käytetään käyttäjän aikeen vahvistamiseen Apple Pay -maksutapahtumissa tai viimeisteltäessä Touch ID:llä varustetun Magic Keyboardin asettamista Apple siliconilla varustetun Macin laitepariksi. Käyttäjän aie vahvistetaan siten, että saatuaan kehotuksen käyttöliittymältä käyttäjä painaa kahdesti toimintoon käytettävää painiketta (Face ID:lle) tai sormenjäljen lukijaa (Touch ID:lle). Jos haluat lisätietoja, katso Ostojen varmistaminen Apple Paylla. Samankaltaista mekanismia – joka perustuu Secure Enclaveen ja T2-laiteohjelmistoon – tuetaan sellaisissa MacBook-malleissa, joissa on Apple T2 Security -siru mutta ei Touch Baria.

Mikrofonin laitteistopohjainen poiskytkentä

Kaikissa Apple silicon -pohjaisissa Mac-kannettavissa sekä Intel-pohjaisissa Mac-kannettavissa, joissa on Apple T2 Security -siru, on laitteistopohjainen poiskytkentä, joka estää mikrofonin toiminnan, kun kansi on suljettuna. Kaikissa T2-sirulla varustetuissa 13-tuumaisissa MacBook Pro- ja MacBook Air -kannettavissa, kaikissa T2-sirulla varustetuissa loppuvuoden 2019 tai uudemmissa MacBook-kannettavissa sekä Apple siliconilla varustetuissa Mac-kannettavissa tämä poiskytkentä on toteutettu kokonaan laitteistossa. Poiskytkentä on suunniteltu estämään ohjelmistoa (jopa T2-sirun ohjelmistoa tai muuta laiteohjelmistoa) käyttämästä mikrofonia kannen ollessa suljettuna silloinkin, kun sillä on macOS:n root- tai kernel-oikeudet. (Kameraa ei poisteta käytöstä laitteistossa, koska sen näkymä on täysin peitetty, kun kansi on suljettuna.)

Vuoden 2020 iPad-malleista alkaen myös iPadin mikrofonissa on laitteistopohjainen poiskytkentä. Kun MFi-vaatimukset täyttävä kotelo (mukaan lukien Applen myymät kotelot) kiinnitetään iPadiin ja suljetaan, mikrofoni poistetaan käytöstä laitetasolla. Tämä on suunniteltu estämään sitä, että mikään ohjelmisto (vaikka sillä olisi iPadOS:n root- tai kernel-oikeudet) tai mikään laiteohjelmisto pystyisi käyttämään mikrofonin äänidataa.

Tämän osion suojaukset on toteutettu suoraan laitteiston logiikassa seuraavan piirikaavion mukaisesti:



Kaikissa tuotteissa, joissa on mikrofonin laitteistopohjainen poiskytkentä, yksi tai useampi kannen anturi tunnistaa kannen tai kotelon sulkemisen fyysisen toiminnan jonkin fyysisen ominaisuuden perusteella (esimerkiksi Hall-ilmiön anturi tai saranan kulman anturi). Niille antureille, jotka tarvitsevat kalibrointia, asetetaan parametrit laitteen valmistuksen aikana ja kalibrointiprosessiin kuuluu peruuttamaton laitteiston lukitseminen myöhemmiltä muutoksilta anturin arkaluontoisiin parametreihin. Nämä anturit lähettävät suoran laitteistosignaalin, joka kulkee läpi yksinkertaisesta ei-uudelleenohjelmoitavasta laitteistologiikan sarjasta. Tämä logiikka tuottaa kosketinvärähtelyn eston, hystereesin ja/tai enimmillään 500 ms:n viiveen ennen mikrofonin poistamista käytöstä. Tuotteesta riippuen tämä signaali voidaan toteuttaa joko estämällä toiminta mikrofonin ja järjestelmäpiirin (SoC) välillä tietoa siirtävissä linjoissa tai estämällä yksi mikrofonimoduulin tulolinja, joka mahdollistaa sen aktiivisuuden (kuten kellolinja), tai vastaavalla tehokkaalla tavalla.

ExpressCard-kortit virransäästöllä

Jos iOS ei toimi, koska iPhone täytyy ladata, akussa voi silti olla tarpeeksi virtaa ExpressCard-toimintojen tukemiseen. Tuetut iPhone-laitteet tukevat tätä ominaisuutta automaattisesti seuraavien kanssa:

- Maksu- tai matkakortti, joka on määritelty pikamatkakortiksi
- Opiskelijakortit, joissa on pikatila päällä
- Auton avaimet, joissa on pikatila päällä
- Kotiavaimet, joissa on pikatila päällä
- Majoitusliikkeiden ja yritysten kulkukortit, joissa on pikatila päällä

Sivupainikkeen (tai Koti-painikkeen 2. sukupolven iPhone SE:ssä) painaminen tuo näkyviin akun alhaisen tason kuvakkeen sekä tekstin, jossa ilmoitetaan, että ExpressCard-kortit ovat käytettävissä. NFC-ohjain suorittaa ExpressCard-toiminnot samoilla ehdoilla kuin iOS:n ollessa päällä, mutta toiminnoista ilmoitetaan vain tuntopalautteella (näkyvää ilmoitusta ei näytetä). 2. sukupolven iPhone SE:ssä suoritettujen maksutapahtumien näkymiseen näytöllä voi kulua muutama sekunti. Tämä ominaisuus ei ole käytettävissä, kun käyttäjä sammuttaa laitteen tavalliseen tapaan.

Järjestelmän suojaus

Järjestelmän suojauksen yleiskatsaus

Applen laitteiston ainutlaatuisten ominaisuuksien pohjalle rakennettu järjestelmän suojaus vastaa pääsynhallinnasta järjestelmän resursseihin Applen laitteissa käytettävyydestä tinkimättä. Järjestelmän suojaus kattaa käynnistysprosessin, ohjelmistopäivitykset ja tietokoneen järjestelmäresurssien kuten prosessorin, muistin, levyn, ohjelmien ja tallennettujen tietojen suojaamisen.

Applen käyttöjärjestelmien uusimmat versiot ovat kaikista turvallisimmat. *Suojattu käynnistys* on tärkeä osa Applen tietoturvaa. Se suojaa järjestelmää haittaohjelmatartunnalta käynnistettäessä. Suojattu käynnistys alkaa laitteistosta ja kehittää ohjelmistoon luottamusketjun, jossa jokainen vaihe on suunniteltu varmistamaan, että seuraava vaihe toimii kunnolla, ennen kuin hallinta siirretään seuraavalle. Tämä suojausmalli tukee Apple-laitteiden oletuskäynnistyksen lisäksi eri käynnistystiloja Apple-laitteiden palautukseen ja ajoittaiseen päivittämiseen. Lisäksi alikomponentit kuten T2-siru ja Secure Enclave suorittavat oman suojatun käynnistyksensä sen varmistamiseksi, että ne käynnistävät ainoastaan hyväksi tunnettua Applen koodia. Päivitysjärjestelmä on suunniteltu estämään heikennyshyökkäyksiä, jotta laitteita ei voitaisi palauttaa käyttöjärjestelmän vanhaan versioon (jonka hyökkääjä kykenee vaarantamaan) käyttäjän tietojen varastamista varten.

Apple-laitteet sisältävät myös käynnistyksen ja ajonaikaisen suojauksen, jotta ne säilyttävät eheytensä jatkuvan toiminnan aikana. Applen suunnittelema siru iPhonessa, iPadissa, Apple Watchissa, Apple TV:ssä, HomePodissa ja Apple siliconilla varustetussa Macissa tarjoaa yhteisen arkkitehtuurin käyttöjärjestelmän eheyden suojausta varten. macOS:ssä on lisäksi laajennettu ja muokattava joukko suojausominaisuuksia sen erilaista tietojenkäsittelymallia varten sekä kaikilla Mac-laitteistoalustoilla tuettuja ominaisuuksia.

Suojattu käynnistys

iOS- ja iPadOS-laitteiden käynnistysprosessi

Käynnistysprosessin jokainen vaihe sisältää elementtejä, jotka Apple on allekirjoittanut kryptografisesti eheyden tarkistuksen mahdollistamiseksi, ja käynnistys etenee vasta luottamusketjun tarkistamisen jälkeen. Näitä elementtejä ovat käynnistyslataajat, kernel, kernelin laajennukset ja mobiiliyhteyden kantataajuusalijärjestelmän laiteohjelmisto. Suojattu käynnistysketju on suunniteltu varmistamaan, että ohjelmiston alimpia tasoja ei ole peukaloitu.

Kun iOS- tai iPadOS-laite käynnistetään, sen appeja suorittava prosessori suorittaa välittömästi ROM-muistissa olevan Boot ROM -koodin. Siruun asennetaan valmistuksen aikana muuttumatonta *laitetason RoT (Root of Trust) -koodia*, johon luotetaan implisiittisesti. Boot ROM -koodi sisältää Applen juurivarmentajan julkisen avaimen, jolla varmistetaan, että iBoot-käynnistyslataaja on Applen allekirjoittama, ennen kuin sen lataaminen sallitaan. Tämä on ensimmäinen vaihe luottamusketjussa, jonka jokainen vaihe tarkistaa, että seuraava on Applen allekirjoittama. Kun iBoot päättää tehtävänsä, se varmistaa ja suorittaa iOS- tai iPadOS-kernelin. Laitteissa, joissa on A9 tai aiempi A-sarjan prosessori, Boot ROM lataa ja varmistaa ylimääräisen Low-Level Bootloader (LLB) -tason, ja se puolestaan lataa ja varmistaa iBootin.

Seuraavien vaiheiden lataamisen tai varmentamisen virhe käsitellään eri tavalla laitteistosta riippuen:

- *Boot ROM ei pysty lataamaan LLB:tä (vanhemmat laitteet):* DFU-tila
- *LLB tai iBoot:* Palautustila

Kummassakin tapauksessa laite täytyy yhdistää Finderiin (macOS 10.15:ssä tai uudemmissa) tai iTunesiin (macOS 10.14 tai aiemmissa) USB:llä, ja se täytyy palauttaa tehdasoletusasetuksiin.

Secure Enclave käyttää käynnistymisen edistymisrekisteriä (Boot Progress Register, BPR) rajoittamaan pääsyä käyttäjätietoihin eri tiloissa, ja se päivitetään ennen siirtymistä seuraaviin tiloihin:

- *DFU-tila:* Boot ROM asettaa laitteissa, joissa on Apple A12 tai uudempi järjestelmäpiiri.
- *Palautustila:* iBoot asettaa laitteissa, joissa on Apple A10, S2 tai uudempi järjestelmäpiiri.

Laitteissa, joissa on mobiiliyhteys, sen kantataajuusalijärjestelmä suorittaa lisäksi suojatun käynnistyksen, jossa käytetään kantataajuusprosessorin varmistamia allekirjoitettuja ohjelmistoa ja avaimia.

Secure Enclave suorittaa myös suojatun käynnistyksen, joka tarkistaa, että sen ohjelmisto (sepOS) on Applen tarkistama ja allekirjoittama.

Muistiturvallinen iBoot

iOS 14:ssä ja iPadOS 14:ssä Apple on muokannut iBoot-käynnistyslataajan rakentamiseen käytettävää C-kääntäjän työkaluketjua turvallisemmaksi. Muokatussa työkaluketjussa käytetään koodia, joka on suunniteltu estämään C-ohjelmille tyypillisiä muisti- ja tyyppiturvallisuusongelmia. Se esimerkiksi auttaa ehkäisemään useimmat haavoittuvuudet seuraavissa haavoittuvuusluokissa:

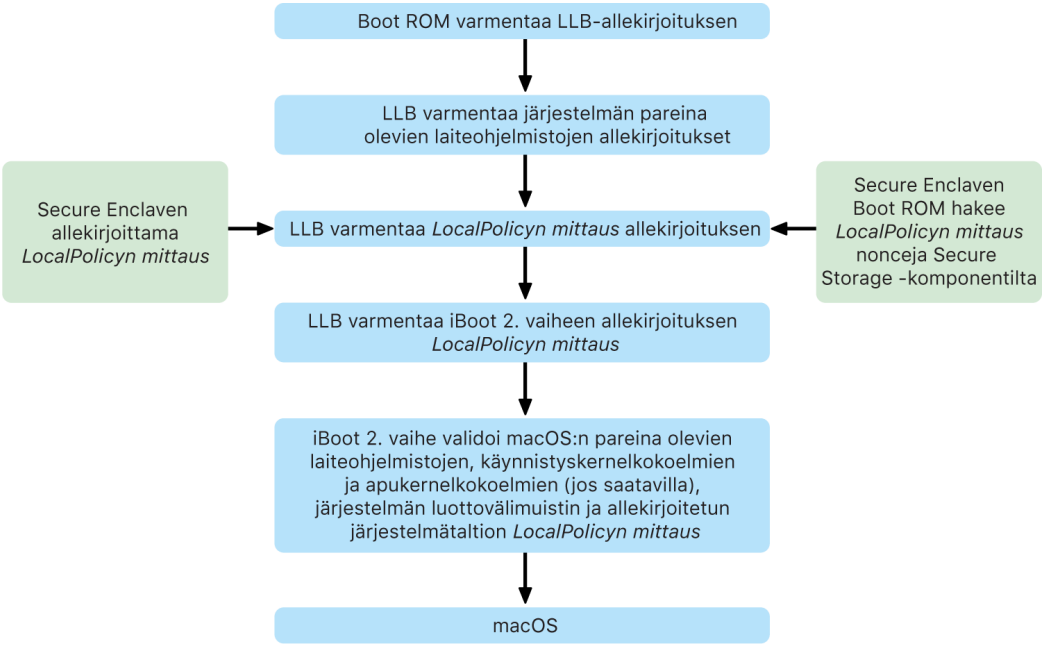
- Puskurin ylivuotovirheitä estetään varmistamalla, että kaikissa osoittimissa on tieto rajoista, joka tarkistetaan muistia käytettäessä.
- Kekojen hyväksikäyttämistä estetään erottamalla keon data sen metadatasta ja havaitsemalla täsmällisesti virhetilat kuten muistin vapauttaminen kahdesti.
- Tyypin sekaannusta estetään varmistamalla, että kaikissa osoittimissa on ajonaikainen tyyppitieto, joka tarkistetaan osoittimen tyypinmuunnosoperaatioiden yhteydessä.
- Tyypin sekaannusta, joka aiheutuu yrityksestä käyttää vapautettua muistia, estetään erottamalla kaikki dynaamiset muistivaraukset staattisella tyypillä.

Tämä teknologia on saatavilla iPhonessa, jossa on Apple A13 Bionic -siru tai uudempi, ja iPadissa, jossa on A14 Bionic -siru.

Apple siliconilla varustetut Mac-tietokoneet

Apple siliconilla varustetun Macin käynnistysprosessi

Kun Apple siliconilla varustettu Mac käynnistetään, se suorittaa käynnistysprosessin, joka on hyvin samanlainen kuin iPhonessa ja iPadissa.



Siru suorittaa luottamusketjun ensimmäisessä vaiheessa koodin Boot ROMista. macOS:n suojattu käynnistys Apple siliconilla varustetussa Macissa tarkistaa itse käyttöjärjestelmän koodin lisäksi myös valtuutettujen käyttäjien määrittämät suojauskäytännöt ja kernelin laajennukset (joita tuetaan mutta ei suositella).

Kun LLB (lyhennetty sanoista Low Level Bootstrap) käynnistetään, se tarkistaa allekirjoitukset ja lataa järjestelmän parina olevan laiteohjelmiston järjestelmäpiirin sisäisille ytimille kuten tallennustilan-, näytön-, järjestelmän hallinnan- ja Thunderbolt-ohjaimille. LLB vastaa myös Secure Enclave -prosessorin allekirjoittaman LocalPolicy-tiedoston lataamisesta. LocalPolicy-tiedosto kuvaa määritykset, jotka käyttäjä on valinnut järjestelmän suojauskäytännöille käynnistyksen ja ajon aikana. LocalPolicylla on sama tietorakenne kuin kaikilla muillakin käynnistyskohteilla, mutta se on allekirjoitettu paikallisesti yksityisellä avaimella, joka on saatavilla vain tietyn tietokoneen Secure Enclavessa sen sijaan, että allekirjoittaminen tehtäisiin keskitetysti Applen palvelimella (kuten ohjelmistopäivityksissä).

Aikaisemman LocalPolicyn uudelleentoiston estämiseksi LLB:n täytyy tarkistaa nonce Secure Enclaveen liitetyltä Secure Storage -komponentilta. Se käyttää tähän tarkoitukseen Secure Enclaven Boot ROMia ja varmistaa, että LocalPolicyssa oleva nonce vastaa Secure Storage -komponentissa olevaa. Tämä auttaa estämään käyttämästä järjestelmälle uudelleen vanhaa, mahdollisesti alemmalle suojaustasolle määritettyä LocalPolicya sen jälkeen, kun suojausta on päivitetty. Lopputulos on, että Apple siliconilla varustetun Macin suojattu käynnistys auttaa suojautumaan sekä aikaisempien käyttöjärjestelmäversioiden palauttamiselta että suojauskäytäntöjen heikennyksiltä.

LocalPolicy-tiedosto kertoo, onko käyttöjärjestelmän suojausasetus täysi, alennettu vai salliva.

- *Täysi suojaus:* Järjestelmä käyttäytyy kuten iOS ja iPadOS ja sallii käynnistää ainoastaan ohjelmiston, jonka tiedettiin olevan viimeisin saatavilla oleva asennuksen aikana.
- *Alennettu suojaus:* LLB ohjataan luottamaan "yleisiin" allekirjoituksiin, jotka tulevat käyttöjärjestelmän mukana. Näin järjestelmässä voidaan käyttää vanhempia macOS-versioita. Koska vanhemmissa macOS-versioissa on väistämättä paikkaamattomia haavoittuvuuksia, tätä suojaustilaa kutsutaan *alennetuksi suojaukseksi*. Kernelin laajennusten käynnistyksen tukeminen edellyttää käytännön asettamista tälle tasolle.
- *Salliva suojaus:* Järjestelmä käyttäytyy kuten alennetussa suojauksessa siltä osin, että se käyttää yleisten allekirjoitusten tarkistusta iBootille ja sen jälkeen, mutta se myös käskee iBootin hyväksymään joitakin Secure Enclaven allekirjoittamia käynnistyskohteita, joiden allekirjoituksessa on käytetty samaa avainta kuin LocalPolicyn allekirjoituksessa. Tälle tasolle asetettu käytäntö tukee käyttäjiä, jotka rakentavat, allekirjoittavat ja käynnistävät omia muokattuja XNU-kerneleitä.

Jos LocalPolicy kertoo LLB:lle, että valittu käyttöjärjestelmä suoritetaan täydellä suojauksella, LLB tarkistaa yksilöllisen allekirjoituksen iBootille. Jos tasona on alennettu suojaus tai salliva suojaus, se tarkistaa yleisen allekirjoituksen. Kaikista allekirjoituksen tarkistamisen virheistä seuraa, että järjestelmä käynnistyy recoveryOS:ään korjausvaihtoehtojen tarjoamista varten.

Kun LLB on siirtänyt hallinnan iBootille, se lataa macOS:n parina olevan laiteohjelmiston muun muassa Secure Neural Enginelle ja aina päällä olevalle prosessorille sekä muut laiteohjelmistot. iBoot myös katsoo LLB:ltä saamansa LocalPolicyn tiedot. Jos LocalPolicy ilmaisee, että järjestelmässä pitäisi olla apukernelkokoelma (AuxKC), iBoot etsii sitä tiedostojärjestelmästä, tarkistaa, että se on Secure Enclaven allekirjoittama samalla avaimella kuin LocalPolicy, ja tarkistaa, että sen tiiviste vastaa LocalPolicyyn tallennettua tiivistettä. Jos apukernelkokoelma läpäisee tarkistuksen, iBoot sijoittaa sen muistiin käynnistyskernelkokoelman kanssa ennen kuin lukitsee järjestelmän lisäprosessorin eheyden suojauksella (SCIP) koko muistialueen, joka kattaa käynnistyskernelkokoelman ja apukernelkokoelman. Jos käytäntö ilmaisee, että järjestelmässä pitäisi olla apukernelkokoelma, mutta sitä ei löydy, järjestelmä jatkaa macOS:n käynnistystä ilman sitä. iBoot vastaa myös allekirjoitetun järjestelmätaltion (SSV) juuritiivisteen tarkistamisesta, jolla tarkistetaan, että kernelin näkyviin tuoman tiedostojärjestelmän eheys on täysin tarkistettu.

Apple siliconilla varustetun Macin käynnistystilat

Apple siliconilla varustetulla Macilla on alla kuvatut käynnistystilat.

Tila	Näppäinyhdistelmä	Kuvaus
macOS	Kun laite on sammutettu, paina virtapainiketta ja **vapauta** se.	1. Boot ROM siirtää hallinnan LLB:lle. 2. LLB lataa järjestelmän parina olevan laiteohjelmiston ja LocalPolicyn valitulle macOS:lle. 3. LLB lukitsee käynnistymisen edistymisrekisteriin (BPR) tiedon, että se käynnistää macOS:ään, ja siirtää hallinnan iBootille. 4. iBoot lataa macOS:n parina olevan laiteohjelmiston, staattisen luottamusvälimuistin, laitepuun ja käynnistyskernelkokoelman. 5. LocalPolicyn salliessa, iBoot lataa muiden valmistajien kernelin laajennusten apukernelkokoelman (AuxKC). 6. Jos LocalPolicy ei ole poistanut tätä toimintoa käytöstä, iBoot tarkistaa juuriallekirjoituksen tiivisteen allekirjoitetulle järjestelmätaltiolle (SSV).
Parina oleva recoveryOS	Kun laite on sammutettu, **pidä** virtapainiketta painettuna.	1. Boot ROM siirtää hallinnan LLB:lle. 2. LLB lataa järjestelmän parina olevan laiteohjelmiston ja LocalPolicyn recoveryOS:ää varten. 3. LLB lukitsee käynnistymisen edistymisrekisteriin tiedon, että se käynnistää parina olevaan recovery OS:ään, ja siirtää hallinnan parina olevan recovery OS:n iBootille. 4. iBoot lataa macOS:n parina olevan laiteohjelmiston, luottamusvälimuistin, laitepuun ja käynnistyskernelkokoelman. 5. Jos parina olevan recoveryOS:n käynnistys epäonnistuu, yritetään käynnistystä vara-recovery OS:ään. *Huomaa:* Parina olevan recoveryOS:n LocalPolicyssa ei sallita suojauksen heikennyksiä.
Vara-recoveryOS	Kun laite on sammutettu, **paina kahdesti ja pidä painettuna** virtapainiketta.	1. Boot ROM siirtää hallinnan LLB:lle. 2. LLB lataa järjestelmän parina olevan laiteohjelmiston ja LocalPolicyn recoveryOS:ää varten. 3. LLB lukitsee käynnistymisen edistymisrekisteriin tiedon, että se käynnistää parina olevaan recovery OS:ään, ja siirtää hallinnan recoveryOS:n iBootille. 4. iBoot lataa macOS:n parina olevan laiteohjelmiston, luottamusvälimuistin, laitepuun ja käynnistyskernelkokoelman. *Huomaa:* Parina olevan recoveryOS:n LocalPolicyssa ei sallita suojauksen heikennyksiä.
Vikasietotila	Käynnistä recoveryOS:ään edellä kuvatulla tavalla ja pidä sitten **vaihtonäppäintä** painettuna, kun valitset käynnistystaltion.	1. Käynnistyy recoveryOS:ään edellä kuvatulla tavalla. 2. Kun vaihtonäppäintä pidetään painettuna taltiota valittaessa, BootPicker-appi hyväksyy tavalliseen tapaan macOS:n käynnistystä varten. Lisäksi se asettaa `nvram`-muuttujan, joka käskee iBootia olemaan lataamatta apukernelkokoelmaa seuraavan käynnistyksen yhteydessä. 3. Järjestelmä käynnistyy uudelleen ja käynnistyy kohdetaltioon, mutta iBoot ei lataa apukernelkokoelmaa.

Parina olevan recoveryOS:n rajoitukset

macOS 12.0.1:ssä tai uudemmissa jokainen uusi macOS-asennus asentaa myös parina olevan recoveryOS:n version vastaavaan APFS-taltioryhmään. Tämä malli on tuttu Intel-pohjaisten Mac-tietokoneiden käyttäjille, mutta Apple siliconilla varustetussa Macissa se varmistaa vielä paremmin suojausta ja yhteensopivuutta. Se, että jokaisella macOS-asennuksella on nyt oma parina oleva recoveryOS, auttaa varmistamaan, että vain kyseinen oma parina oleva recoveryOS voi suorittaa suojauksen tasoa laskevia toimintoja. Tämä auttaa suojaamaan uudempien macOS-versioiden asennuksia vanhemmasta macOS-versiosta aloitetulta peukaloinnilta ja päinvastoin.

Pareja koskevat rajoitukset toimivat seuraavasti:

- Kaikki macOS 11 -asennukset asetetaan recoveryOS:n pariksi. Jos jokin macOS 11 -asennus valitaan käynnistymään oletuksena, pitämällä virtapainiketta painettuna käynnistyksen aikana Apple siliconilla varustetussa Macissa käynnistetään recoveryOS. recoveryOS voi laskea suojausasetusten tasoa missä tahansa macOS 11 -asennuksissa, mutta ei missään macOS 12.0.1:n asennuksissa.
- Jos jokin macOS 12.0.1 -asennus valitaan käynnistymään oletuksena, pitämällä virtapainiketta painettuna Macin käynnistyksen aikana käynnistetään sen parina oleva recoveryOS. Parina oleva recoveryOS voi laskea suojausasetusten tasoa sen parina olevalle macOS-asennukselle, mutta ei millekään muulle macOS-asennukselle.

Käynnistäminen minkä tahansa macOS:n parina olevaan recoveryOS:ään edellyttää, että kyseinen asennus on valittu oletukseksi. Tämä tehdään Järjestelmäasetusten Käynnistyslevy-asetuksissa tai käynnistämällä mikä tahansa recoveryOS ja pitämällä optionäppäintä painettuna taltiota valittaessa.

Huomaa: Vara-recoveryOS ei voi alentaa suojaustasoa millekään macOS-asennukselle.

Käynnistyslevyn suojauskäytännön hallinta Apple siliconilla varustetussa Macissa

Yleiskatsaus

Toisin kuin Intel-pohjaisessa Macissa, Apple siliconilla varustetussa Macissa on erilliset suojauskäytännöt jokaiselle asennetulle käyttöjärjestelmälle. Tämä tarkoittaa, että samassa Macissa tuetaan useita erillisiä macOS-asennuksia, joissa voidaan käyttää eri versioita ja eri tietoturvakäytäntöjä. Tämän vuoksi Käynnistyksen suojaustyökaluun on lisätty *käyttöjärjestelmän valitsin*.

Apple siliconilla varustetussa Macissa Järjestelmän suojaustyökalu kertoo käyttäjän määrittämän macOS:n suojauksen kokonaistilan, kuten kernelin laajennusten käynnistyksen tai järjestelmän eheyden suojauksen määritykset. Mikäli suojausasetuksen muuttaminen heikentäisi suojausta merkittävästi tai helpottaisi järjestelmän vaarantumista, käyttäjien täytyy siirtyä recoveryOS:ään pitämällä virtapainiketta painettuna (jotta haittaohjelmat eivät voi antaa tätä signaalia vaan ainoastaan laitteen luona fyysisesti oleva ihminen voi tehdä sen), jotta muutoksen voi tehdä. Tämän vuoksi Apple silicon -pohjainen Mac ei myöskään vaadi (eikä tue) laiteohjelmiston salasanaa, koska kaikki kriittiset muutokset ovat jo käyttäjän valtuutuksen takana. Jos haluat lisätietoja järjestelmän eheyden suojauksesta, katso Järjestelmän eheyden suojaus.

Täysi suojaus ja Alennettu suojaus voidaan asettaa käyttäen Käynnistyksen suojaustyökalua recoveryOS:ltä. Salliva suojaus sen sijaan on käytettävissä ainoastaan komentorivityökaluilla käyttäjille, jotka hyväksyvät sen riskin, että heidän Macinsa on huomattavasti heikommin suojattu.

Täysi suojaus -käytäntö

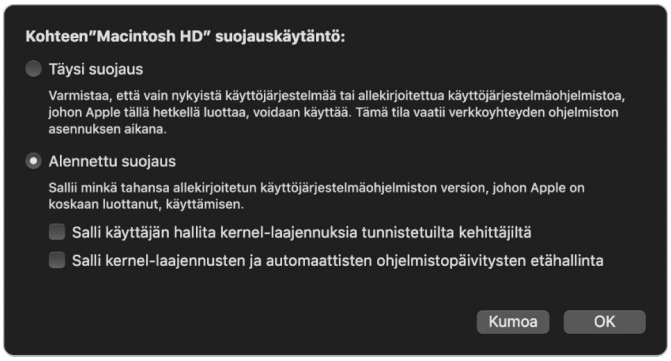
Täysi suojaus on oletuksena, ja se toimii kuin iOS ja iPadOS. Kun ohjelmisto ladataan ja sen asennusta valmistellaan, macOS ei käytä ohjelmiston mukana tulevaa yleistä allekirjoitusta, vaan se ottaa yhteyden Applen allekirjoituspalvelimeen (joka on sama kuin iOS:lle ja iPadOS:lle) ja pyytää tuoreen ”yksilöllisen” allekirjoituksen. Allekirjoitus on yksilöllinen, kun allekirjoituspyynnössä on ECID-tunniste (Exclusive Chip Identification), joka on tässä tapauksessa Applen prosessorin yksilöllinen tunnus. Allekirjoituspalvelimen takaisin antama allekirjoitus on tällöin yksilöllinen ja vain kyseisen Applen prosessorin käytettävissä. Kun Täysi suojaus -käytäntö on käytössä, Boot ROM ja LLB auttavat varmistamaan, että annettu allekirjoitus on Applen allekirjoittama ja lisäksi allekirjoitettu juuri tälle tietylle Macille, mikä sitoo macOS:n version kyseiseen Maciin.

Online-allekirjoituspalvelimen käyttö tarjoaa myös parempaa suojaa heikennyshyökkäyksiltä kuin tavalliset yleiset allekirjoitusmallit. Yleisessä allekirjoitusjärjestelmässä turvallisuusajanjakso voidaan rekisteröidä useita kertoja, mutta järjestelmä, joka ei ole koskaan nähnyt uusinta laiteohjelmistoa, ei tiedä tätä. Esimerkiksi tietokone, joka luulee, että tällä hetkellä on meneillään turvallisuusajanjakso 1, hyväksyy ohjelmistoja turvallisuusajanjaksolta 2, vaikka nykyinen turvallisuusajanjakso olisi 5. Apple siliconin online-allekirjoitusjärjestelmän ansiosta allekirjoituspalvelin voi kieltäytyä luomasta allekirjoituksia ohjelmistolle, jolla on mikä tahansa paitsi uusin turvallisuusajanjakso.

Lisäksi jos hyökkääjä huomaa haavoittuvuuden turvallisuusajanjakson muutoksen jälkeen, hän ei voi vain ottaa edellisen ajanjakson haavoittuvaista ohjelmistoa järjestelmästä A ja käyttää sitä hyökkäykseen järjestelmässä B. Koska vanhemman ajanjakson haavoittuvainen ohjelmisto oli yksilöllisesti allekirjoitettu järjestelmälle A, tämä auttaa estämään sen siirtämistä ja käyttämistä hyökkäykseen järjestelmässä B. Kaikki nämä menetelmät yhdessä takaavat paremmin sen, että hyökkääjät eivät voi tarkoituksella laittaa haavoittuvaista ohjelmistoa tietokoneeseen kiertääkseen uusimman ohjelmiston suojauksia. Käyttäjä, jolla on hallussaan Macin ylläpitäjän käyttäjänimi ja salasana, voi kuitenkin aina valita suojauskäytännön, joka toimii parhaiten hänen omissa käyttötapauksissaan.

Alennettu suojaus -käytäntö

Alennettu suojaus vastaa Keskitason suojaus -valinnan käyttäytymistä Intel-pohjaisessa T2-sirulla varustetussa Macissa. Siinä toimittaja (tässä tapauksessa Apple) luo digitaalisen allekirjoituksen koodiin osoittaakseen, että se on peräisin toimittajalta. Tämä suunnitteluratkaisu auttaa estämään hyökkääjiä syöttämästä allekirjoittamatonta koodia. Apple kutsuu tätä allekirjoitusta ”yleiseksi” allekirjoitukseksi, koska sitä voidaan käyttää kuinka kauan tahansa missä tahansa sellaisessa Macissa, jossa on sillä hetkellä asetettuna Alennettu suojaus -käytäntö. Alennettu suojaus itsessään ei suojaa heikennyshyökkäyksiltä (joskin valtuuttamattomista käyttöjärjestelmän muutoksista voi seurata, ettei käyttäjän tietoihin pääse. Jos haluat lisätietoja, katso Kernelin laajennukset Apple siliconilla varustetussa Macissa.

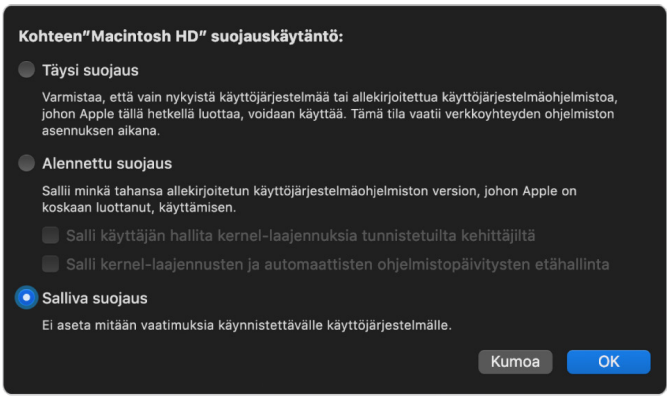


Sen lisäksi, että alennettu suojaus sallii käyttäjille vanhempien macOS-versioiden käytön, sitä tarvitaan muihin toimintoihin, jotka voivat vaarantaa käyttäjän järjestelmän suojauksen, kuten muiden valmistajien kernelin laajennusten (kext) lisäämiseen. Kernelin laajennuksilla on samat oikeudet kuin kernelillä, ja näin ollen haavoittuvuudet muiden valmistajien kernelin laajennuksissa voivat johtaa koko käyttöjärjestelmän vaarantumiseen. Tämän vuoksi kehittäjiä kannustetaan painokkaasti ottamaan käyttöön järjestelmälaajennukset ennen kuin kernelin laajennusten tuki poistetaan macOS:stä tulevissa Apple siliconilla varustetuissa Maceissa. Silloinkaan kun muiden valmistajien kernelin laajennuksia otetaan käyttöön, niitä ei voi ladata kerneliin milloin tahansa. Sen sijaan kernelin laajennukset yhdistetään apukernelkokoelmaan (AuxKC), jonka tiiviste tallennetaan LocalPolicyyn, ja näin ollen ne vaativat uudelleenkäynnistyksen. Jos haluat lisätietoja apukernelkokoelman luomisesta, katso Kernelin laajennukset macOS:ssä.

Salliva suojaus -käytäntö

Salliva suojaus on käyttäjille, jotka hyväksyvät sen riskin, että heidän Macinsa on paljon suojattomammassa tilassa. Tämä on erilainen kuin Intel-pohjaisen T2-sirulla varustetun Macin Ei suojausta -tila. Sallivaa suojausta käytettäessä allekirjoituksen tarkistus ja koko suojatun käynnistyksen ketju suoritetaan edelleen, mutta käytännön asettaminen sallivaksi kertoo iBootille, että sen tulisi hyväksyä Secure Enclaven paikallisesti allekirjoittamat käynnistyskohteet, kuten käyttäjän tuottama käynnistyskernelkokoelma, joka on tehty muokatusta XNU-kernelistä. Tällä tavoin salliva suojaus myös tarjoaa arkkitehtuurissa olevan mahdollisuuden suorittaa mitä tahansa ”täysin ei-luotetun käyttöjärjestelmän” kerneliä. Kun muokattu käynnistyskernelkokoelma tai täysin ei-luotettu käyttöjärjestelmä ladataan järjestelmässä, jotkin salauksen purkuavaimet eivät ole käytettävissä. Tämän tarkoitus on estää täysin ei-luotettuja käyttöjärjestelmiä pääsemästä luotettujen käyttöjärjestelmien tietoihin.

Tärkeää: Apple ei tarjoa muokattuja XNU-kerneleitä eikä tue niitä.



Salliva suojaus eroaa Intel-pohjaisen T2-sirulla varustetun Macin Ei suojausta -käytännöstä myös toisella tavalla. Sitä vaaditaan joihinkin suojauksen heikennyksiin, joita aikaisemmin on voinut hallita riippumattomasti. Huomattavin näistä on, että jos käyttäjä haluaa poistaa käytöstä järjestelmän eheyden suojauksen Apple siliconilla varustetussa Macissa, hänen on hyväksyttävä, että hän asettaa järjestelmän sallivan suojauksen tilaan. Tätä vaaditaan, koska järjestelmän eheyden suojauksen poistaminen käytöstä on aina asettanut järjestelmän tilaan, jossa kernel vaarantuu paljon helpommin. Erityisesti on syytä huomata, että järjestelmän eheyden suojauksen poistaminen käytöstä Apple siliconilla varustetussa Macissa estää kernelin laajennuksen allekirjoituksen vaatimisen apukernelkokoelmaa muodostettaessa, mikä mahdollistaa minkä tahansa kernelin laajennuksen lataamisen kernelmuistiin. Toinen Apple siliconilla varustetussa Macissa tehty järjestelmän eheyden suojauksen parannus on, että käytäntöjen tallennus on siirretty NVRAM-muistista LocalPolicyyn. Näin järjestelmän eheyden suojauksen poistaminen käytöstä vaatii todentamisen käyttäjältä, jolla on pääsy LocalPolicyn allekirjoitusavaimeen, ja se on tehtävä recoveryOS:ltä (johon pääsee pitämällä virtapainiketta painettuna). Tämä tekee järjestelmän eheyden suojauksen poistamisen käytöstä huomattavasti hankalammaksi vain ohjelmistoa käyttävälle hyökkääjälle tai jopa fyysisesti laitteen luona olevalle käyttäjälle.

Suojausta ei ole mahdollista laskea sallivan suojauksen tasolle Käynnistyksen suojaustyökalu -apista. Käyttäjät voivat laskea suojauksen vain suorittamalla Päätteessä recoveryOS:ssä komentorivityökaluja kuten `csrutil` (jolla poistetaan käytöstä järjestelmän eheyden suojaus). Kun käyttäjä on laskenut suojauksen, se näkyy Käynnistyksen suojaustyökalussa, joten käyttäjä voi helposti asettaa suojauksen turvallisempaan tilaan.

Huomaa: Apple siliconilla varustettu Mac ei vaadi eikä tue tiettyä tallennusvälineen käynnistyskäytäntöä, koska teknisestä näkökulmasta kaikki käynnistykset tehdään paikallisesti. Jos käyttäjä valitsee käynnistyksen ulkoiselta tallennusvälineeltä, kyseinen käyttöjärjestelmäversio on ensin tehtävä yksilöllisesti sopivaksi käyttämällä todennettua uudelleenkäynnistystä recoveryOS:stä. Tämä uudelleenkäynnistys luo sisäiseen asemaan LocalPolicy-tiedoston, jota käytetään luotetun käynnistyksen suorittamiseen ulkoiseen tallennusvälineeseen tallennetusta käyttöjärjestelmästä. Tämä tarkoittaa, että määritykset käynnistykselle ulkoiselta tallennusvälineeltä sallitaan aina nimenomaisesti käyttöjärjestelmäkohtaisesti, ja se vaatii jo käyttäjän todennuksen, joten muuta suojausratkaisua ei tarvita.

LocalPolicyn allekirjoitusavaimen luominen ja hallinta

Luominen

Kun macOS asennetaan ensi kertaa tehtaalla tai kun suoritetaan yhdistetty tyhjennys ja asennus, Mac suorittaa koodin tilapäiseltä palautus-RAM-levyltä oletustilan alustamista varten. Tämän prosessin aikana palautusympäristö luo uuden julkisen ja yksityisen avaimen parin, joka pidetään Secure Enclavessa. Yksityistä avainta kutsutaan *omistajaidentiteetin avaimeksi (Owner Identity Key, OIK)*. Jos OIK-avain on olemassa ennestään, vanha avain tuhotaan tässä prosessissa. Palautusympäristö valmistelee myös avaimen, jota käytetään aktivointilukitukseen, eli *käyttäjäidentiteetin avaimen (User Identity Key, UIK)*. Apple siliconilla varustetulle Macille ainutlaatuinen osa prosessia on, että kun UIK-avaimelle pyydetään varmennetta aktivointilukitusta varten, mukaan sisältyy joukko pyydettyjä rajoituksia, joita käytetään LocalPolicyn validoinnin aikana. Jos laite ei saa UIK-avaimelle varmennetta aktivointilukitusta varten (esimerkiksi koska laite on liitetty Etsi Macini -tiliin ja ilmoitettu kadonneeksi), se ei voi edetä ja luoda LocalPolicya. Jos laite saa *käyttäjäidentiteetin varmenteen (ucrt)*, tämä ucrt sisältää palvelimen vaatimat käytännön rajoitukset ja käyttäjän pyytämät käytännön rajoitukset X.509 v3 -laajennuksessa.

Kun aktivointilukitus/`ucrt` on saatu onnistuneesti, se tallennetaan tietokantaan palvelimen puolella ja palautetaan myös laitteeseen. Kun laitteella on ucrt, varmennepyyntö OIK-avainta vastaavalle julkiselle avaimelle lähetetään *perustodentaja (Basic Attestation Authority, BAA)* -palvelimelle. BAA tarkistaa omistajaidentiteetin avaimen varmennepyynnön käyttäen julkista avainta ucrt-varmenteelta, joka on tallennettu BAA:n saatavilla olevaan tietokantaan. Jos BAA:n tekemä varmentamisen tarkistus onnistuu, se antaa varmenteen julkiselle avaimelle palauttaen *omistajaidentiteetin varmenteen (Owner Identity Certificate, OIC)*, joka on BAA:n allekirjoittama ja sisältää ucrt:hen tallennetut rajoitukset. OIC-varmenne lähetetään takaisin Secure Enclavelle. Sen jälkeen aina kun Secure Enclave allekirjoittaa uuden LocalPolicyn, se liittää Image4-tiedostoon OIC-varmenteen. LLB:ssä on sisäänrakennettuna luottamus BAA:n juurivarmenteeseen, josta seuraa että se luottaa OIC-varmenteeseen, josta seuraa että se luottaa koko LocaPolicyn allekirjoitukseen.

RemotePolicyn rajoitukset

Paikallisten käytäntöjen lisäksi kaikki muutkin Image4-tiedostot sisältävät rajoituksia Image4-vaatimustiedoston arvioinnille. Nämä rajoitukset on koodattu käyttäen erityisiä objektitunnisteita (OID) lehtivarmenteessa. Image4:n tarkistuskirjasto etsii varmenteesta erityisen varmenteen rajoituksen objektitunnisteen allekirjoituksen arvioinnin yhteydessä ja arvioi sitten mekaanisesti siinä eritellyt rajoitukset. Rajoitukset ovat muotoa:

- X täytyy olla olemassa
- X ei saa olla olemassa
- X:llä täytyy olla tietty arvo

Esimerkiksi ”yksilöllisten” allekirjoitusten varmenteen rajoituksissa on ”ECID täytyy olla olemassa”, ja ”yleisten” allekirjoitusten varmenteen rajoituksissa on ”ECID ei saa olla olemassa”. Nämä rajoitukset on suunniteltu varmistamaan, että kaikkien tietyllä avaimella allekirjoitettujen Image4-tiedostojen on oltava tiettyjen vaatimusten mukaisia, jotta vältytään luomasta virheellisesti allekirjoitettuja Image4-vaatimustiedostoja.

Kunkin LocalPolicyn yhteydessä näihin Image4-varmennerajoituksiin viitataan nimellä *RemotePolicy*. Eri käynnistysympäristöjen LocalPolicyille voi olla eri RemotePolicy. RemotePolicya käytetään rajoittamaan recoveryOS:n LocalPolicya niin että kun recoveryOS käynnistetään, se voi käyttäytyä ainoastaan niin kuin käynnistettäessä Täysi suojaus -tilassa. Tämä lisää luottamusta recoveryOS:n käynnistysympäristön eheyteen paikkana, jossa käytäntöä voidaan muuttaa. RemotePolicy rajoittaa LocalPolicya edellyttämällä, että sen tulee sisältää sen Macin ECID, jossa LocalPolicy on luotu, ja nimenomaan kyseisen Macin Secure Storage -komponenttiin tallennettu etäkäytännön noncen tiiviste (`rpnh`). `rpnh` ja sen myötä RemotePolicy muuttuvat ainoastaan silloin, kun Etsi Macini -toiminnolle ja aktivointilukitukselle suoritetaan toimenpiteitä kuten rekisteröinti, rekisteröinnin poistaminen, etälukitus ja etätyhjennys. Etäkäytännön rajoitukset määritetään ja ne eritellään käyttäjäidentiteetin avaimen (UIK) varmenteen antamisen aikana ja ne kirjataan annettavaan käyttäjäidentiteetin varmenteeseen (ucrt). Palvelin määrittää jotkin etäkäytännön rajoitukset, kuten ECID-, ChipID- ja BoardID-tunnisteen. Tämä on suunniteltu estämään sitä, että yksi laite voisi allekirjoittaa LocalPolicy-tiedostoja toiselle laitteelle. Laite voi eritellä muita etäkäytännön rajoituksia auttaakseen estämään paikallisen käytännön suojauksen heikentämistä ilman sekä paikallista todennusta nykyisen OIK-avaimen käyttämiseksi että etätodennusta tilille, johon laite on aktivointilukittu.

Apple siliconilla varustetun Macin LocalPolicy-tiedoston sisältö

LocalPolicy on Secure Enclaven allekirjoittama Image4-tiedosto. Image4 on ASN.1 (Abstract Syntax Notation One) DER -koodattu tietorakennemuoto, jota käytetään kuvaamaan tietoja suojatun käynnistysketjun kohteista Applen alustoilla. Image4:ään perustuvassa suojatun käynnistyksen mallissa ohjelmiston asentamisen aikana allekirjoituspyyntö Applen keskitetylle allekirjoituspalvelimelle käynnistää suojauskäytäntöjen pyytämisen. Jos käytäntö on hyväksyttävä, allekirjoituspalvelin palauttaa allekirjoitetun Image4-tiedoston, jossa on erilaisia nelimerkkisiä koodeja (4CC). Ohjelmistot kuten Boot ROM tai LLB tarkistavat nämä allekirjoitetut Image4-tiedostot ja 4CC:t käynnistettäessä.

Omistajuuden antaminen käyttöjärjestelmien välillä

Pääsyä omistajaidentiteetin avaimeen (OIK) kutsutaan ”omistajuudeksi”. Omistajuutta tarvitaan, jotta käyttäjät voivat allekirjoittaa LocalPolicyn uudelleen tehtyään muutoksia käytäntöön tai ohjelmistoon. OIK-avainta suojaa sama avainhierarkia, josta kerrotaan kohdassa Sinetöity avaimen suojaus (SKP). Siinä OIK-avain on suojattu samalla avaimensalausavaimella (KEK) kuin taltion salausavain (VEK). Tämä tarkoittaa, että se on normaalisti suojattu sekä käyttäjien salasanoilla että käyttöjärjestelmän ja käytännön mittauksilla. Macissa on kaikille käyttöjärjestelmille vain yksi OIK-avain. Siksi toista käyttöjärjestelmää asennettaessa vaaditaan nimenomainen suostumus ensimmäisen käyttöjärjestelmän käyttäjiltä omistajuuden antamiseksi toisen käyttöjärjestelmän käyttäjille. Toisen käyttöjärjestelmän käyttäjiä ei kuitenkaan ole vielä olemassa, kun asentajaa suoritetaan ensimmäisestä käyttöjärjestelmästä. Käyttöjärjestelmien käyttäjiä ei normaalisti luoda ennen kuin käyttöjärjestelmä on käynnistetty ja käyttöönottoapuri suorittaa käyttöönottoa. Siksi tarvitaan kaksi uutta toimintoa asennettaessa Apple siliconilla varustettuun Maciin toista käyttöjärjestelmää:

- LocalPolicyn luominen toiselle käyttöjärjestelmälle
- ”Asennuskäyttäjän” valmisteleminen omistajuuden antamista varten

Kun asennusapuri suoritetaan ja asennus kohdistetaan tyhjälle toiselle taltiolle, kehote kysyy käyttäjältä, haluaako hän kopioida käyttäjän nykyiseltä taltiolta seuraavan taltion ensimmäiseksi käyttäjäksi. Jos käyttäjä vastaa kyllä, luotava ”asennuskäyttäjä” on tosiasiassa KEK-avain, joka muodostetaan valitun käyttäjän salasana- ja laitteistoavaimista ja jota sitten käytetään OIK-avaimen salaamiseen, kun se annetaan toiselle käyttöjärjestelmälle. Sen jälkeen se pyytää toisen käyttöjärjestelmän asennusapurista kyseisen käyttäjän salasanaa päästäkseen OIK-avaimeen uuden käyttöjärjestelmän Secure Enclavessa. Jos käyttäjä valitsee, että käyttäjää ei kopioida, asennuskäyttäjä luodaan siinäkin tapauksessa samalla tavalla, mutta käyttäjän salasanan sijasta käytetään tyhjää salasanaa. Tämä toinen tapa on olemassa tiettyjä järjestelmän ylläpitäjän skenaarioita varten. Kuitenkin käyttäjien, jotka haluavat asentaa käyttöjärjestelmiä useille taltioille ja suorittaa omistajuuden antamisen turvallisimmalla mahdollisella tavalla, tulisi aina valita käyttäjän kopioiminen ensimmäisestä käyttöjärjestelmästä toiseen käyttöjärjestelmään.

Apple siliconilla varustetun Macin LocalPolicy

Apple siliconilla varustetussa Macissa paikallisen suojauskäytännön hallinta on delegoitu Secure Enclavessa toimivalle apille. Tämä ohjelmisto voi käyttää käyttäjän tunnistetietoja ja ensisijaisen prosessorin käynnistystilaa sen määrittämiseen, kuka voi muuttaa suojauskäytäntöä ja mistä käynnistysympäristöstä. Tämä auttaa estämään haitallista ohjelmistoa käyttämästä suojauskäytännön hallintakeinoja käyttäjää vastaan niin, että se alentaisi hallintaa saadakseen lisää oikeuksia.

LocalPolicy-vaatimustiedoston ominaisuudet

LocalPolicy-tiedosto sisältää joitakin arkkitehtuuriin kuuluvia 4CC-koodeja, jotka ovat lähes kaikissa Image4-tiedostoissa, kuten levyn tai mallin tunnus (BORD), tiettyä Applen sirua ilmaiseva CHIP tai ECID (Exclusive Chip Identification). Alla olevissa 4CC-koodeissa kuitenkin keskitytään ainoastaan käyttäjien määritettävissä oleviin suojauskäytäntöihin.

Huomaa: Parina oleva One True recoveryOS (1TR) tarkoittaa fyysisesti (virtapainiketta kerran painamalla ja pitämällä) käynnistettävää parina olevaa recoveryOS:ää. Tämä eroaa tavallisesta recoveryOS-käynnistyksestä, joka tapahtuu käyttämällä NVRAM:ia tai painiketta kahdesti painamalla ja pitämällä tai joka voi tapahtua, jos käynnistyksessä ilmenee virheitä. Määrätynlainen fyysinen painikkeen painaminen lisää luotettavuutta, koska se auttaa varmistamaan, etteivät macOS:ään murtautuneet puhtaasti ohjelmistopohjaiset hyökkäykset pääse tähän käynnistysympäristöön.

LocalPolicyn noncen tiiviste (lpnh)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* `lpnh`:ta käytetään LocalPolicyn uudelleentoiston estämiseen. Tämä on SHA384-tiiviste LocalPolicyn noncesta (LPN), joka on tallennettu Secure Storage -komponentille ja johon pääsee käyttäen Secure Enclaven Boot ROMia tai Secure Enclavea. Käsittelemätön nonce ei ole koskaan näkyvillä appeja suorittavalle prosessorille vaan ainoastaan sepOS:lle. Hyökkääjän, joka haluaa uskotella LLB:lle, että hänen kaappaamansa aikaisempi LocalPolicy on kelvollinen, täytyisi sijoittaa Secure Storage -komponentille arvo, joka tiivistyy samaan `lpnh`-arvoon kuin siinä LocalPolicyssa, jonka hän haluaa uudelleentoistaa. Normaalisti järjestelmässä on yksi kelvollinen paikallisen käytännön nonce, mutta ohjelmistopäivitysten aikana kelvollisia nonceja on samanaikaisesti kaksi. Näin vanha ohjelmisto voidaan vielä käynnistää, jos päivityksessä tapahtuu virhe. Kun minkä tahansa käyttöjärjestelmän mikä tahansa LocalPolicy muuttuu, kaikki käytännöt allekirjoitetaan uudelleen uudella *lpnh*-arvolla, joka vastaa Secure Storage -komponentilta löytyvää uutta LocalPolicyn noncea. Tämä muutos tapahtuu, kun käyttäjä muuttaa suojausasetuksia tai luo uusia käyttöjärjestelmiä, joilla on kullakin uusi LocalPolicy.

Etäkäytännön noncen tiiviste (rpnh)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* `rpnh` käyttäytyy samalla tavoin kuin `lpnh`, mutta päivittyy vain kun etäkäytäntö päivittyy, esimerkiksi kun Missä on…? -rekisteröinnin tilaa muutetaan. Muutos tapahtuu, kun käyttäjä muuttaa Missä on…? -toiminnon tilaa Macissaan.

recoveryOS:n noncen tiiviste (ronh)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* `ronh` käyttäytyy kuten lpnh, mutta se löytyy ainoastaan järjestelmän recoveryOS:n LocalPolicysta. Se päivittyy, kun järjestelmän recoveryOS päivittyy, esimerkiksi ohjelmistopäivitysten yhteydessä. `lpnh`:sta ja `rpnh`:sta erillistä noncea käytetään sitä varten, että kun laitteen käyttö estetään Missä on…? -toiminnolla, olemassa olevien käyttöjärjestelmien käyttö voidaan estää (poistamalla niiden LocalPolicyn nonce ja RemotePolicyn nonce Secure Storage -komponentista), mutta järjestelmän recoveryOS voidaan edelleen käynnistää. Tällä tavoin käyttöjärjestelmät saadaan uudelleen käyttöön, kun järjestelmän omistaja todistaa hallitsevansa järjestelmää antamalla Missä on…? -tilin kanssa käyttämänsä iCloud-salasanan. Tämä muutos tapahtuu, kun käyttäjä päivittää järjestelmän recoveryOS:n tai luo uusia käyttöjärjestelmiä.

Seuraavan tason Image4-vaatimustiedoston tiiviste (nsih)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus: nsih*-kenttä edustaa SHA384-tiivistettä Image4-vaatimustiedoston tietorakenteesta, joka kuvaa käynnistetyn macOS:n. macOS:n Image4-vaatimustiedosto sisältää mittaukset kaikille käynnistyskohteille kuten iBoot, staattinen luottamusvälimuisti, laitepuu, käynnistyskernelkokoelma ja allekirjoitetun järjestelmätaltion (Signed System Volume - SSV) hajautus. Kun LLB on ohjattu käynnistämään tietty macOS, se on suunniteltu varmistamaan, että iBootiin liitetyn macOS:n Image4-vaatimustiedoston tiiviste vastaa LocalPolicyn `nsih`-kentässä olevaa. Näin `nsih` kertoo, mille käyttöjärjestelmälle käyttäjä on luonut LocalPolicyn. Käyttäjä muuttaa `nsih`-arvoa implisiittisesti päivittäessään ohjelmiston.

Apukernelkokoelman (AuxKC) käytännön tiiviste (auxp)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* macOS
- *Kuvaus:* `auxp` on SHA384-tiiviste käyttäjän valtuuttamien kernelin laajennusten luettelon (UAKL) käytännöstä. Tätä käytetään apukernelkokoelmaa luotaessa apuna varmistamaan, että apukernelkokoelmaan sisällytetään vain käyttäjän hyväksymiä kernelin laajennuksia. Tämän kentän asettaminen edellyttää `smb2`:n käyttöä. Käyttäjät muuttavat `auxp`-arvoa implisiittisesti muuttaessaan käyttäjän valtuuttamien kernelin laajennusten luetteloa (UAKL), kun he hyväksyvät kernelin laajennuksia Järjestelmäasetusten Suojaus ja yksityisyys -osiossa.

Apukernelkokoelman (AuxKC) Image4-vaatimustiedoston tiiviste (auxi)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* macOS
- *Kuvaus:* Kun järjestelmä on tarkistanut, että käyttäjän valtuuttamien kernelin laajennusten luettelon (UAKL) tiiviste vastaa LocalPolicyn `auxp`-kenttää, se pyytää LocalPolicyn allekirjoittamisesta vastaavaa Secure Enclave -prosessorin appia allekirjoittamaan apukernelkokoelman. Seuraavaksi apukernelkokoelman Image4-vaatimustiedoston allekirjoituksen SHA384-tiiviste sijoitetaan LocalPolicyyn, jotta käynnistettäessä vältetään mahdollinen sekoittuminen ja yhdistäminen aikaisemmin allekirjoitettuihin käyttöjärjestelmän apukernelkokoelmiin. Jos iBoot löytää LocalPolicysta `auxi`-kentän, se yrittää ladata tallennetun apukernelkokoelman ja varmistaa sen allekirjoituksen. Se tarkistaa myös, että apukernelkokoelmaan liitetyn Image4-vaatimustiedoston tiiviste vastaa `auxi`-kentästä löytyvää arvoa. Jos apukernelkokoelman lataaminen epäonnistuu mistä tahansa syystä, järjestelmä jatkaa käynnistystä ilman tätä käynnistyskohdetta, ja näin ollen mitään muiden valmistajien kernelin laajennuksia ei ladata. auxi-kentän asettaminen LocalPolicyssa edellyttää `auxp`-kenttää. Käyttäjät muuttavat `auxi`-arvoa implisiittisesti muuttaessaan käyttäjän valtuuttamien kernelin laajennusten luetteloa (UAKL), kun he hyväksyvät kernelin laajennuksia Järjestelmäasetusten Suojaus ja yksityisyys -osiossa.

Apukernelkokoelman (AuxKC) kuitin tiiviste (auxr)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* macOS
- *Kuvaus:* `auxr` on SHA384-tiiviste apukernelkokoelman kuitista, jossa kerrotaan apukernelkokoelmaan sisällytettyjen kernelin laajennusten tarkka joukko. Apukernelkokoelman kuitti voi olla käyttäjän valtuuttamien kernelin laajennusten luettelon (UAKL) alajoukko, koska kernelin laajennuksia voidaan jättää pois apukernelkokoelmasta, vaikka ne olisivat käyttäjän valtuuttamia, jos on tiedossa, että niitä käytetään hyökkäyksiin. Lisäksi jotkin kernelin laajennukset, joita on mahdollista käyttää käyttäjän ja kernelin rajan rikkomiseen, voivat johtaa joidenkin toimintojen menettämiseen esimerkiksi siten, että Apple Payta ei voi käyttää tai 4K- ja HDR-sisältöä ei voi toistaa. Käyttäjien, jotka haluavat pitää nämä ominaisuudet käytössä, tulee rajoittaa tiukemmin kernelin laajennusten sisällyttämistä apukernelkokoelmaan. `auxr`-kentän asettaminen LocalPolicyssa edellyttää `auxp`-kenttää. Käyttäjät muuttavat `auxr`-arvoa implisiittisesti rakentaessaan uuden apukernelkokoelman Järjestelmäasetusten Suojaus ja yksityisyys -osiossa.

CustomOS:n Image4-vaatimustiedoston tiiviste (coih)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* `coih` on CustomOS:n Image4-vaatimustiedoston SHA384-tiiviste. iBoot (eikä XNU-kernel) käyttää tämän vaatimustiedoston tietosisältöä hallinnan siirtämiseen. Käyttäjät muuttavat `coih`-arvoa implisiittisesti käyttäessään `kmutil configure-boot`-komentorivityökalua 1TR-ympäristössä.

APFS-taltioryhmän UUID (vuid)

- *Tyyppi:* OctetString (16)
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* `vuid` kertoo sen taltioryhmän, jota kernelin tulisi käyttää juurena. Tämä kenttä on ensisijassa tietoa, eikä sitä käytetä suojausrajoituksiin. Käyttäjä asettaa `vuid`:n implisiittisesti luodessaan uuden käyttöjärjestelmäasennuksen.

Avaimensalausavaimen (KEK) ryhmä-UUID (kuid)

- *Tyyppi:* OctetString (16)
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* `kuid` kertoo käynnistetyn taltion. Avaimensalausavainta on tyypillisesti käytetty tietojen suojaukseen. Sitä käytetään suojaamaan kunkin LocalPolicyn allekirjoitusavainta. Käyttäjä asettaa `kuid`:n implisiittisesti luodessaan uuden käyttöjärjestelmäasennuksen.

Parina olevan recoveryOS:n luotetun käynnistyksen käytännön mittaus (prot)

- *Tyyppi:* OctetString (48)
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* Parina olevan recoveryOS:n luotetun käynnistyksen käytännön mittaus (Trusted Boot Policy Measurement, TBPM) on erityinen toistuva SHA384-tiivistelaskenta LocalPolicyn Image4-vaatimustiedostosta ilman nonceja, jotta saadaan eri aikoina yhtenevä mittaus (koska noncet kuten `lpnh` päivittyvät usein). `prot`-kenttä, joka on ainoastaan kussakin macOS:n LocalPolicyssa, kertoo, mikä recoveryOS:n LocalPolicy on macOS:n LocalPolicya vastaava pari.

Secure Enclaven allekirjoittama recoveryOS:n LocalPolicy on olemassa (hrlp)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* `hrlp` kertoo, onko (edellä käsitelty) `prot`-arvo mittaus Secure Enclaven allekirjoittamasta recoveryOS:n LocalPolicysta vai ei. Jos se ei ole, recoveryOS:n LocalPolicyn allekirjoittaa Applen allekirjoituspalvelin verkossa, joka allekirjoittaa muun muassa macOS:n Image4-tiedostot.

Paikallinen käyttöjärjestelmäversio (love)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR, recoveryOS, macOS
- *Kuvaus:* `love` kertoo käyttöjärjestelmäversion, jolle LocalPolicy on luotu. Versio saadaan seuraavan vaiheen vaatimustiedostosta LocalPolicyn luomisen aikana ja sitä käytetään recoveryOS-parirajoitusten pakottamiseen.

Suojattu monikäynnistys (smb0)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR, recoveryOS
- *Kuvaus:* Jos `smb0` löytyy ja arvo on tosi, LLB sallii seuraavan vaiheen Image4-vaatimustiedoston yleisen allekirjoituksen sen sijaan että vaatisi yksilöllisen allekirjoituksen. Käyttäjät voivat muuttaa tätä kenttää laskemalla suojaustason alennettuun suojaukseen käyttäen Käynnistyksen suojaustyökalua tai `bputil`-työkalua.

Suojattu monikäynnistys (smb1)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* Jos `smb1` löytyy ja arvo on tosi, iBoot sallii Secure Enclaven allekirjoittaa sellaisia kohteita kuten muokattu kernelkokoelma samalla avaimella kuin LocalPolicyn. `smb1` edellyttää `smb0`:n käyttöä. Käyttäjät voivat muuttaa tätä kenttää laskemalla suojauksen tason sallivaan suojaukseen käyttäen komentorivityökaluja kuten `csrutil` tai `bputil`.

Suojattu monikäynnistys (smb2)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* Jos `smb2` löytyy ja arvo on tosi, iBoot sallii Secure Enclaven allekirjoittaa apukernelkokoelman (AuxKC) samalla avaimella kuin LocalPolicyn. `smb2` edellyttää `smb0`:n käyttöä. Käyttäjät voivat muuttaa tätä kenttää laskemalla suojaustason alennettuun suojaukseen ja sallimalla muiden valmistajien kernelin laajennukset käyttäen Käynnistyksen suojaustyökalua tai `bputil`-työkalua.

Suojattu monikäynnistys (smb3)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* Jos `smb3` löytyy ja arvo on tosi, joku laitteen käyttäjä on asettanut järjestelmänsä mobiililaitteiden hallintaan (MDM). Tämä kenttä saa LocalPolicya hallitsevan Secure Enclave -prosessorin apin hyväksymään MDM-todennuksen sen sijaan että se vaatisi paikallisen käyttäjän todennusta. Käyttäjät voivat muuttaa tätä kenttää ottaessaan Käynnistyksen suojaustyökalulla tai `bputil`-työkalulla käyttöön hallitun muiden valmistajien kernelin laajennusten ja ohjelmistopäivitysten hallinnan. (macOS 11.2:ssa tai uudemmissa MDM voi myös aloittaa päivityksen uusimpaan macOS-versioon, jos nykyinen suojauksen tila on Täysi suojaus.)

Suojattu monikäynnistys (smb4)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* macOS
- *Kuvaus:* Jos `smb4` löytyy ja arvo on tosi, laite on asetettu käyttöjärjestelmän MDM-hallintaan Apple School Managerilla, Apple Business Managerilla tai Apple Business Essentialsilla. Tämä kenttä saa LocalPolicya hallitsevan Secure Enclave -apin hyväksymään MDM-todennuksen sen sijaan että se vaatisi paikallisen käyttäjän todennusta. MDM-ratkaisu muuttaa tätä kenttää, kun se havaitsee, että laitteen sarjanumero on jossakin näistä kolmesta palvelusta.

Järjestelmän eheyden suojaus (sip0)

- *Tyyppi:* 64-bittinen allekirjoittamaton kokonaisluku
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* `sip0` sisältää olemassa olevan järjestelmän eheyden suojauksen (SIP) käytännön bitit, jotka aikaisemmin tallennettiin NVRAM:iin. Uudet järjestelmän eheyden suojauksen bitit lisätään tähän (sen sijaan että käytettäisiin LocalPolicyn kenttiä alla kuvatulla tavalla), jos niitä käytetään vain macOS:ssä eikä LLB:n toimesta. Käyttäjät voivat muuttaa tätä kenttää poistaessaan järjestelmän eheyden suojauksen käytöstä ja laskiessaan suojaustasoksi sallivan suojauksen. Muutos tehdään käyttämällä `csrutil`-työkalua 1TR:stä.

Järjestelmän eheyden suojaus (sip1)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* Jos `sip1` löytyy ja sen arvo on tosi, iBoot hyväksyy, että allekirjoitetun järjestelmätaltion juuritiivisteen tarkistus epäonnistuu. Käyttäjät voivat muuttaa tätä kenttää käyttämällä `csrutil`-työkalua tai `bputil`-työkalua 1TR:stä.

Järjestelmän eheyden suojaus (sip2)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* Jos sip2 löytyy ja sen arvo on tosi, iBoot ei lukitse laitetason *CTRR (Configurable Text Read-only Region)* -rekisteriä, joka merkitsee kernelin muistin ei-kirjoitettavaksi. Käyttäjät voivat muuttaa tätä kenttää käyttämällä `csrutil`-työkalua tai `bputil`-työkalua 1TR:stä.

Järjestelmän eheyden suojaus (sip3)

- *Tyyppi:* Totuusarvo
- *Muuttuvat ympäristöt:* 1TR
- *Kuvaus:* Jos `sip3` löytyy ja sen arvo on tosi, iBoot ei pakota sisäänrakennettua sallittujen luetteloaan boot-args-NVRAM-muuttujalle. Muussa tapauksessa tämä suodattaisi kernelille annettavat valinnat. Käyttäjät voivat muuttaa tätä kenttää käyttämällä `csrutil`-työkalua tai `bputil`-työkalua 1TR:stä.

Varmenteet ja RemotePolicy

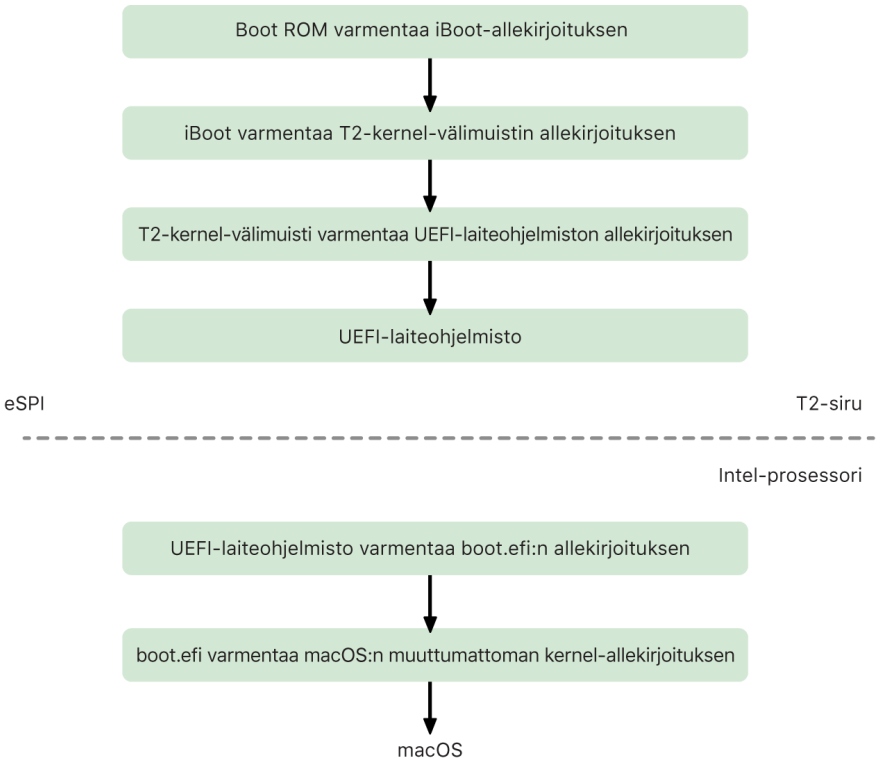
Kuten kohdassa LocalPolicyn allekirjoitusavaimen luominen ja hallinta kerrotaan, LocalPolicyn Image4 sisältää myös omistajaidentiteetin varmenteen (OIC) ja sisällytetyn RemotePolicyn.

Intel-pohjaiset Mac-tietokoneet

Intel-pohjaisen Macin käynnistysprosessi

Intel-pohjaiset Mac-tietokoneet, joissa on Apple T2 Security -siru

Kun Apple T2 Security -sirulla varustettu Intel-pohjainen Mac-tietokone käynnistetään, siru suorittaa suojatun käynnistyksen Boot ROMista samalla tavoin kuin iPhonessa, iPadissa ja Apple siliconilla varustetussa Macissa. Tämä tarkistaa iBoot-käynnistyslataajan ja on ensimmäinen vaihe luottamusketjussa. iBoot tarkistaa kernelin ja kernelin laajennusten koodin T2-sirulla, joka sitten tarkistaa Intelin UEFI-laiteohjelmiston. UEFI-laiteohjelmisto ja siihen liitetty allekirjoitus ovat saatavilla alun perin vain T2-siruun.



Tarkistuksen jälkeen UEFI-laiteohjelmistotiedosto sijoitetaan T2-sirun muistin osioon. Tämä muisti asetetaan Intel-prosessorin saataville eSPI:n (enhanced Serial Peripheral Interface) kautta. Kun Intel-prosessori käynnistyy ensimmäistä kertaa, se hakee UEFI-laiteohjelmiston eSPI:n kautta T2-sirun muistissa olevasta laiteohjelmiston kopiosta, jonka eheys on tarkistettu.

Luottamusketjun arviointi jatkuu Intel-prosessorissa, jossa UEFI-laiteohjelmisto arvioi boot.efin (joka on macOS:n käynnistyslataaja) allekirjoituksen. Intelissä olevat macOS:n suojatun käynnistyksen allekirjoitukset tallennetaan samaan Image4-muotoon, jota käytetään iOS:ssä, iPadOS:ssä ja T2-sirun suojatussa käynnistyksessä, ja Image4-tiedostoja jäsentävä koodi on sama koodi kuin on käytössä nykyisessä iOS:n ja iPadOS:n suojatussa käynnistyksessä. Boot.efi puolestaan tarkistaa uuden tiedoston nimeltä immutablekernel allekirjoituksen. Kun suojattu käynnistys on käytössä, immutablekernel-tiedosto vastaa kaikkia Applen kernelin laajennuksia, joita tarvitaan macOS:n käynnistykseen. Suojatun käynnistyksen käytäntö loppuu, kun hallinta siirretään immutablekernel-tiedostolle, ja sen jälkeen macOS:n suojauskäytännöt (kuten järjestelmän eheyden suojaus ja allekirjoitetut kernelin laajennukset) astuvat voimaan.

Jos tässä prosessissa ilmenee virheitä, Mac siirtyy palautustilaan, Apple T2 Security -sirun palautustilaan tai Apple T2 Security -sirun DFU-tilaan.

Microsoft Windows Intel-pohjaisessa Macissa, jossa on T2-siru

Suojattua käynnistystä tukeva Intel-pohjainen Mac luottaa oletusarvoisesti vain Applen allekirjoittamaan sisältöön. Boot Camp -asennusten suojauksen parantamiseksi Apple tarjoaa kuitenkin myös tukea Windowsin suojatulle käynnistämiselle. UEFi (Unified Extensible Firmware Interface) -laiteohjelmistossa on kopio Microsoft Windowsin Production CA 2011 -varmenteesta, jota käytetään Microsoft-käynnistyslataajien todentamiseen.

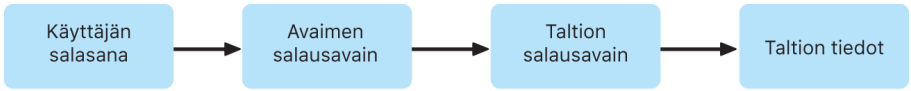
Huomaa: Tällä hetkellä Microsoft Corporation UEFI CA 2011 -varmenteelle ei ole luottamusta, joka sallisi Microsoftin kumppaneiden allekirjoittaman koodin tarkistamisen. Tätä UEFI CA -varmennetta käytetään yleensä muiden käyttöjärjestelmien, kuten Linux-versioiden, käynnistyslataajien aitouden varmistamiseen.

Windowsin suojatun käynnistyksen tuki ei ole kuitenkaan oletuksena käytössä. Se otetaan käyttöön Boot Camp -apurilla (BCA). Kun käyttäjä ajaa Boot Camp -apurin, macOS määritetään uudelleen luottamaan Microsoftin itse allekirjoittamaan koodiin käynnistyksen aikana. Kun Boot Camp -apuri on valmis ja jos macOS ei läpäise Applen omaa luottamuksen arviointia suojatussa käynnistyksessä, UEFI-laiteohjelmisto yrittää arvioida kohteen luottamuksen UEFI:n suojatun käynnistyksen alustuksen perusteella. Jos luottamuksen arviointi onnistuu, Mac etenee ja käynnistää Windowsin. Jos se ei onnistu, Mac siirtyy recoveryOS:ään ja ilmoittaa käyttäjälle luottamusarvioinnin virheestä.

Intel-pohjaiset Mac-tietokoneet, joissa ei ole T2-sirua

Intel-pohjainen Mac, jossa ei ole T2-sirua, ei tue suojattua käynnistystä. Siksi UEFi (Unified Extensible Firmware Interface) -laiteohjelmisto lataa macOS:n käynnistysohjelman (boot.efi) tiedostojärjestelmästä ilman varmennusta ja käynnistysohjelma lataa kernelin (prelinkedkernel) tiedostojärjestelmästä ilman varmennusta. Käynnistysketjun eheyden suojaamista varten käyttäjien pitäisi ottaa käyttöön kaikki seuraavat suojausmenetelmät:

- *Järjestelmän eheyden suojaus (SIP):* Tämä ominaisuus on oletuksena käytössä, ja se suojaa käynnistysohjelmaa haitalliselta kirjoitukselta macOS:n toiminnan aikana.
- *FileVault:* Tämän voi tehdä kahdella tavalla: joko käyttäjä tai mobiililaitteen hallinnan (MDM) ylläpitäjä voi ottaa sen käyttöön. Tämä estää hyökkääjää käyttämästä fyysisessä hyökkäyksessä kohdelevytilaa ja korvaamasta käynnistysohjelmaa.
- *Laiteohjelmiston salasana:* Tämä voidaan ottaa käyttöön kahdella tavalla: joko käyttäjän tai MDM-ylläpitäjän toimesta. Tämä auttaa estämään fyysistä hyökkääjää käyttämästä vaihtoehtoisia käynnistystiloja, kuten recoveryOS:ää, yhden käyttäjän tilaa tai kohdelevytilaa, joista käynnistysohjelma voidaan korvata. Tämä auttaa myös estämään käynnistämistä vaihtoehtoiselta tallennusvälineeltä, jolloin hyökkääjä voisi suorittaa koodin ja korvata käynnistysohjelman.



Käynnistystilat Intel-pohjaiselle Macille, jossa on Apple T2 Security -siru

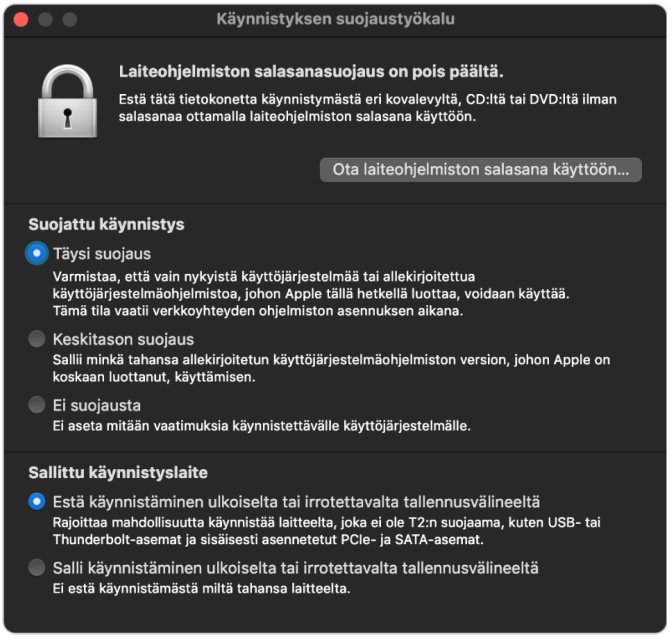
Intel-pohjaisessa Macissa, jossa on Apple T2 Security -siru, on eri käynnistystiloja, joihin voidaan siirtyä käynnistyksen aikana painamalla näppäinyhdistelmiä, jotka UEFI-laiteohjelmisto tai käynnistysohjelma tunnistavat. Jotkin käynnistystilat, kuten yhden käyttäjän tila, eivät toimi, jollei Käynnistyksen suojaustyökalussa ole suojauskäytännön asetukseksi muutettu Ei suojausta.

Tila	Näppäinyhdistelmä	Kuvaus
macOS:n käynnistys	ei mitään	UEFI-laiteohjelmisto siirtää hallinnan macOS-käynnistysohjelmalle (UEFI-appi), joka siirtää hallinnan macOS:n kernelille. Tavallisessa Macin käynnistyksessä, kun FileVault on käytössä, macOS:n käynnistysohjelma näyttää sisäänkirjautumisikkunan, jossa annettavalla salasanalla tallennustilan salaus puretaan.
Käynnistyksenhallinta	Optio (⌥)	UEFI-laiteohjelmisto käynnistää sisäisen UEFI-apin, joka näyttää käyttäjälle käynnistyslaitteen valinnan käyttöliittymän.
Kohdelevytila (target disk mode, TDM)	T	UEFI-laiteohjelmisto käynnistää sisäisen UEFI-apin, joka tuo näkyviin sisäisen tallennuslaitteen lohkoperusteisena tallennuslaitteena FireWirellä, Thunderboltilla, USB:llä tai näiden kolmen yhdistelmällä (riippuen Macin mallista).
Yhden käyttäjän tila	Komento (⌘)-S	macOS:n kernel siirtää –s-lipun launchd-argumenttivektoriin, ja sitten launchd luo yhden käyttäjän komentotulkin Konsoli-apin TTY:hyn. *Huomaa:* Jos käyttäjä poistuu komentotulkista, macOS jatkaa käynnistystä sisäänkirjautumisikkunaan.
recoveryOS	Komento (⌘)-R	UEFI-laiteohjelmisto lataa minimaalisen macOS:n sisäisellä tallennuslaitteella olevasta allekirjoitetusta levytiedostosta (.dmg).
Internet-recoveryOS	Optio (⌥)–komento (⌘)-R	Allekirjoitettu levytiedosto ladataan internetistä käyttäen HTTP:tä.
Vianmääritys	D	UEFI-laiteohjelmisto lataa minimaalisen UEFI-vianmääritysympäristön sisäisellä tallennuslaitteella olevasta allekirjoitetusta levytiedostosta.
Internet-vianmääritys	Optio (⌥)-D	Allekirjoitettu levytiedosto ladataan internetistä käyttäen HTTP:tä.
Windows-käynnistys	ei mitään	Jos Windows on asennettu Boot Campilla, UEFI-laiteohjelmisto siirtää hallinnan Windowsin käynnistysohjelmalle, joka siirtää hallinnan Windows-kernelille.

Käynnistyksen suojaustyökalu Macissa, jossa on Apple T2 Security -siru

Yleiskatsaus

Intel-pohjaisessa Macissa, jossa on Apple T2 Security -siru, Käynnistyksen suojaustyökalu käsittelee useita suojauskäytännön asetuksia. Työkaluun pääsee käynnistämällä recoveryOS:ään ja valitsemalla Lisäapit-valikosta Käynnistyksen suojaustyökalun, ja se suojaa tuettuja suojausasetuksia, jottei hyökkääjä pääsisi helposti muuttamaan niitä.



Kriittiset käytäntömuutokset vaativat todentamisen, myös palautustilassa. Kun Käynnistyksen suojaustyökalu avataan ensimmäisen kerran, se pyytää käyttäjää syöttämään ylläpitäjän salasanan ensisijaisesta macOS-asennuksesta, joka on liitetty nykyiseen käynnistettävään recoveryOS:ään. Jos ylläpitäjää ei ole, sellainen täytyy luoda ennen kuin käytäntöä voidaan muuttaa. T2-siru vaatii, että Mac-tietokone on käynnistetty recoveryOS:ään ja että Secure Enclave -pohjaisilla tunnistetiedoilla todentaminen on tapahtunut, ennen kuin tällainen käytännön muutos voidaan tehdä. Suojauskäytännön muutoksilla on kaksi implisiittistä vaatimusta. recoceryOS täytyy olla:

- käynnistetty tallennuslaitteelta, joka on suoraan yhdistettynä T2-siruun, koska muiden laitteiden osioissa ei ole Secure Enclaven tukemia tunnistetietoja, jotka on sidottu sisäiseen tallennuslaitteeseen.
- APFS-pohjaisessa taltiossa, koska vain levyn esikäynnistys-APFS-taltion Secure Enclave -alueelle lähetettyjen todentamistietojen säilyttämistä tuetaan. HFS plus -alustetut taltiot eivät voi käyttää suojattua käynnistystä.

Tämä käytäntö on näkyvissä vain T2-sirulla varustettujen Intel-pohjaisten Mac-tietokoneiden Käynnistyksen suojaustyökalussa. Vaikka useimmissa käyttötapauksissa suojatun käynnistyksen käytäntöön ei pitäisi tarvita muutoksia, käyttäjät lopulta kuitenkin hallitsevat laitteen asetuksia ja voivat valita suojatun käynnistystoiminnon ottamisen pois käytöstä tai heikentämisen Macissa omista tarpeistaan riippuen.

Suojatun käynnistyksen käytännön muutokset, jotka tehdään tästä apista, koskevat vain Intel-prosessorissa tehtävää luottamusketjun arvioinnin vahvistamista. T2-sirun suojattu käynnistys -valinta on aina käytössä.

Suojatun käynnistyksen käytäntö voidaan määrittää johonkin näistä kolmesta asetuksesta: Täysi suojaus, Keskitason suojaus ja Ei suojausta. Ei suojausta -asetus ottaa Intel-prosessorin suojatun käynnistyksen arvioinnin kokonaan pois käytöstä ja sallii käyttäjän käynnistää, mitä hän haluaa.

Täysi suojaus -käynnistyskäytäntö

Täysi suojaus on oletuksena käytettävä käynnistyskäytäntö, ja se käyttäytyy paljolti samoin kuin iOS ja iPadOS tai Apple siliconilla varustetun Macin Täysi suojaus. Kun ohjelmisto ladataan ja sen asennusta valmistellaan, sille hankitaan yksilöllinen allekirjoitus, jonka allekirjoituspyynnössä on ECID-tunniste (Exclusive Chip Identification), joka on tässä tapauksessa T2-sirun yksilöllinen tunnus. Allekirjoituspalvelimen takaisin antama allekirjoitus on siten yksilöllinen ja käytettävissä vain kyseisessä T2-sirussa. UEFi (Unified Extensible Firmware Interface) -laiteohjelmisto on suunniteltu varmistamaan, että kun Täysi suojaus -käytäntö on käytössä, annettu allekirjoitus on Applen allekirjoittama ja lisäksi allekirjoitettu tälle tietylle Macille, mikä sitoo macOS:n version tähän Maciin. Tämä auttaa estämään heikennyshyökkäyksiä, joista kerrotaan Apple siliconilla varustetun Macin täyttä suojausta käsittelevässä osiossa.

Keskitason suojaus -käynnistyskäytäntö

Keskitason suojaus -käynnistyskäytäntö on melko samanlainen kuin perinteinen UEFI:n suojattu käynnistys, jossa toimittaja (tässä tapauksessa Apple) luo digitaalisen allekirjoituksen koodiin varmistaakseen, että se on peräisin toimittajalta. Tällä tavalla hyökkääjiä estetään syöttämästä allekirjoittamatonta koodia. Kutsumme tätä allekirjoitusta ”yleiseksi” allekirjoitukseksi, koska sitä voidaan käyttää kuinka kauan tahansa missä tahansa sellaisessa Macissa, jossa on sillä hetkellä asetettuna Keskitason suojaus -käytäntö. iOS, iPadOS ja itse T2-siru eivät tue yleisiä allekirjoituksia. Tämä asetus ei yritä estää heikennyshyökkäyksiä.

Tallennusvälineen käynnistyskäytäntö

Tallennusvälineen käynnistyskäytäntö on olemassa vain Intel-pohjaisessa T2-sirulla varustetussa Macissa, ja se on riippumaton suojatun käynnistyksen käytännöstä. Niinpä vaikka käyttäjä ottaisi suojatun käynnistyksen pois käytöstä, tämä ei muuta sitä, että oletuksena Macin käynnistys miltä tahansa muulta tallennusvälineeltä kuin suoraan T2-siruun yhteydessä olevalta tallennusvälineeltä estetään. (Tallennusvälineen käynnistyskäytäntöä ei tarvita Apple siliconilla varustetussa Macissa. Jos haluat lisätietoja, katso Käynnistyslevyn suojauskäytäntöhallinta.)

Laiteohjelmiston salasanasuojaus Intel-pohjaisessa Macissa

Intel-pohjaisissa Mac-tietokoneissa, joissa on Apple T2 Security -siru, macOS tukee laiteohjelmiston salasanaa, joka auttaa estämään laiteohjelmiston asetusten tahatonta muokkaamista tietyssä Macissa. Laiteohjelmiston salasana on suunniteltu estämään vaihtoehtoisten käynnistystilojen valitseminen, kuten käynnistäminen recoveryOS:ään tai yhden käyttäjän tilaan, järjestelmän käynnistäminen valtuuttamattomalta taltiolta tai kohdelevytilaan käynnistäminen.

Huomaa: Laiteohjelmiston salasanaa ei tarvita Apple siliconilla varustetussa Macissa, koska sen rajoittama kriittinen laiteohjelmistotoiminnallisuus on siirretty recoveryOS:ään ja (kun FileVault on käytössä) recoveryOS vaatii käyttäjän todennuksen ennen kriittiseen toiminnallisuuteen pääsyä.

Laiteohjelmistosalasanan perustilaan päästään recoveryOS:n Laiteohjelmiston salasanatyökalusta Intel-pohjaisessa Macissa, jossa *ei ole* T2-sirua, ja Käynnistyksen suojaustyökalusta Intel-pohjaisessa Macissa, jossa *on* T2-siru. Lisävalinnat (kuten mahdollisuus kysyä salasanaa jokaisen käynnistyksen yhteydessä) ovat saatavilla `firmwarepasswd`-komentorivityökalulla macOS:ssä.

Laiteohjelmiston salasanan asettaminen on erityisen tärkeää fyysisen hyökkäysriskin pienentämiseksi Intel-pohjaisissa Mac-tietokoneissa, joissa ei ole T2-sirua. Laiteohjelmiston salasana voi auttaa estämään hyökkääjää käynnistämästä recoveryOS:ään, josta hän muuten voisi ottaa järjestelmän eheyden suojauksen (SIP) pois käytöstä. Koska käynnistämistä vaihtoehtoiselta tallennusvälineeltä rajoitetaan, hyökkääjä ei voi suorittaa etuoikeutettua koodia toisesta käyttöjärjestelmästä ja hyökätä oheislaitteiden laiteohjelmistoihin.

Laiteohjelmistosalasanan nollausmekanismi auttaa käyttäjiä, jotka unohtavat salasanansa. Käyttäjät painavat näppäinyhdistelmää käynnistyksen yhteydessä, jolloin näkyviin tulee mallikohtainen merkkijono, joka annetaan AppleCarelle. AppleCare allekirjoittaa digitaalisesti resurssin, jonka allekirjoituksen tarkistaa URI-tunniste (Uniform Resource Identifier). Jos allekirjoitus kelpaa ja sisältö sopii kyseiseen Maciin, UEFI-laiteohjelmisto poistaa laiteohjelmiston salasanan.

macOS 10.15:ssä lisättiin `–disable–reset–capability`-valinta `firmwarepasswd`-komentorivityökaluun, jotta käyttäjät voivat halutessaan valita, että vain he itse voivat poistaa laiteohjelmiston salasanan ohjelmiston avulla. Ennen tämän asetuksen määrittämistä käyttäjien täytyy hyväksyä, että jos salasana unohtuu ja se täytyy poistaa, käyttäjä vastaa siihen tarvittavan emolevyn vaihdon kustannuksista. Organisaatioiden, jotka haluavat suojata Mac-tietokoneitaan ulkoisilta hyökkääjiltä ja työntekijöiltä, täytyy asettaa laiteohjelmiston salasana organisaation omistamille järjestelmille. Tämä voidaan tehdä laitteelle seuraavilla tavoilla:

- provisiointivaiheessa käsin käyttämällä `firmwarepasswd`-komentorivityökalua
- muun valmistajan hallintatyökaluilla, jotka käyttävät `firmwarepasswd`-komentorivityökalua
- mobiililaitteiden hallinnan (MDM) avulla

recoveryOS ja vianmääritysympäristöt Intel-pohjaiselle Macille

recoveryOS

RecoveryOS on täysin erillinen pää-macOS:stä, ja kaikki sen sisältö on tallennettu levytiedostoon nimeltä BaseSystem.dmg. Siellä on myös siihen liittyvä BaseSystem.chunklist-tiedosto, jota käytetään BaseSystem.dmg-tiedoston eheyden tarkistamiseen. Chunklist-tiedosto on sarja tiivisteitä BaseSystem.dmg-tiedoston 10 Mt:n paloille. UEFi (Unified Extensible Firmware Interface) -laiteohjelmisto arvioi chunklist-tiedoston allekirjoituksen ja arvioi sitten jokaisen osion tiiviste kerrallaan BaseSystem.dmg-tiedostosta. Tämä auttaa varmistamaan, että se vastaa chunklist-tiedostossa olevaa allekirjoitettua sisältöä. Jos jokin näistä tiivisteistä ei täsmää, käynnistäminen paikallisesta recoveryOS:stä keskeytetään ja UEFI-laiteohjelmisto yrittää käynnistää sen sijaan internet-recoveryOS:stä.

Jos tarkistus onnistuu, UEFI-laiteohjelmisto tuo BaseSystem.dmg-tiedoston näkyviin RAM-levynä ja käynnistää siinä olevan boot.efi-tiedoston. UEFI-laiteohjelmiston ei tarvitse tehdä erityistä tarkastusta boot.efi-tiedostolle eikä boot.efi-tiedoston tarvitse tarkastaa kerneliä, koska käyttöjärjestelmän valmiiden sisältöjen (joista nämä elementit ovat vain osa) eheys on jo tarkistettu.

Applen vianmääritys

Paikallisen vianmääritysympäristön käynnistys toimii lähes samalla tavalla kuin recoveryOS. Erillisiä AppleDiagnostics.dmg- ja AppleDiagnostics.chunklist-tiedostoja käytetään, mutta ne tarkistetaan samalla tavalla kuin BaseSystem-tiedostot. UEFI-laiteohjelmisto ei käynnistä boot.efi-tiedostoa, vaan levytiedoston (dmg-tiedosto) sisällä olevan diags.efi-tiedoston, joka puolestaan käynnistää useat muut UEFI-ajurit, jotka voivat kytkeytyä laitteistoon ja tarkistaa sen virheet.

Internet-recoveryOS ja vianmääritysympäristö

Jos paikallisten palautus- tai vianmääritysympäristöjen käynnistyksessä ilmenee virhe, UEFI-laiteohjelmisto yrittää ladata levytiedostot internetistä. (Käyttäjä voi myös erityisesti pyytää levytiedostojen hakua internetistä käyttämällä tiettyjä näppäinyhdistelmiä käynnistyksen yhteydessä.) OS-palautuspalvelimelta ladattujen levytiedostojen ja chunklist-tiedostojen eheyden tarkistus tehdään samalla tavalla kuin tallennuslaitteelta haettujen levytiedostojen.

Vaikka yhteys OS-palautuspalvelimelle muodostetaan HTTP:llä, kaiken ladatun sisällön eheys tarkistetaan silti edellä kuvatulla tavalla, mikä suojaa sisältöä verkkoa hallitsevan hyökkääjän manipuloinnilta. Jos yksittäisen osion eheyden tarkistus epäonnistuu, se pyydetään uudelleen OS-palautuspalvelimelta 11 kertaa ennen luovuttamista ja virheen näyttämistä.

Kun internet-palautus- ja vianmääritystilat lisättiin Mac-tietokoneisiin vuonna 2011, päätettiin, että on parempi käyttää yksinkertaisempaa HTTP-siirtoa ja käsitellä sisällön todentaminen chunklist-mekanismia käyttäen sen sijaan, että käytettäisiin monimutkaisempaa HTTPS:ää UEFI-laitteistossa ja näin kasvatettaisiin laiteohjelmiston hyökkäyspintaa.

Allekirjoitetun järjestelmätaltion suojaus iOS:ssä, iPadOS:ssä ja macOS:ssä

Apple esitteli macOS 10.15:ssä vain luku -muotoisen järjestelmätaltion, joka on omaan tarkoitukseensa varattu eristetty taltio järjestelmäsisällölle. macOS 11:ssä tai uudemmissa järjestelmäsisällön suojaksi on lisätty vahva salausteknologiaan perustuva suojaus käyttämällä *allekirjoitettua järjestelmätaltiota (Signed System Volume - SSV)*. Allekirjoitetussa järjestelmätaltiossa on kernelmekanismi, joka tarkistaa järjestelmäsisällön eheyden ajon aikana ja hylkää kaiken sellaisen datan – oli se sitten koodia tai ei – joka ei ole kelvollisesti Applen salausavaimella allekirjoittamaa. iOS 15:stä ja iPadOS 15:stä alkaen myös iOS- ja iPadOS-laitteen järjestelmätaltio saa allekirjoitetun järjestelmätaltion salausteknologiaan perustuvan suojauksen.

Sen lisäksi että allekirjoitettu järjestelmätaltio auttaa estämään minkään käyttöjärjestelmän osana olevan Apple-ohjelmiston peukaloimista, se myös tekee macOS-ohjelmiston päivittämisen luotettavammaksi ja paljon turvallisemmaksi. Jos päivitystä ei voida tehdä, järjestelmän vanha versio voidaan palauttaa ilman uudelleenasennusta, koska allekirjoitettu järjestelmätaltio käyttää APFS:n (Apple File System) tilannevedoksia.

Siitä lähtien kun APFS otettiin käyttöön, se on taannut tiedostojärjestelmän metadatan eheyden käyttämällä ei-kryptografisia tarkistussummia sisäiselle tallennuslaitteelle. Allekirjoitettu järjestelmätaltio vahvistaa eheysmekanismia lisäämällä salausavaimella lasketut tiivisteet laajentaen sen näin kattamaan tiedostojen jokaisen tavun. Sisäisen tallennuslaitteen data (mukaan lukien tiedostojärjestelmän metadata) tiivistetään salausavaimella lukupolussa ja tiivistettä verrataan odotettuun arvoon tiedostojärjestelmän metadatassa. Mikäli ne eivät täsmää, järjestelmä olettaa, että dataa on peukaloitu, eikä anna tätä dataa sitä pyytävälle ohjelmistolle.

Kukin allekirjoitetun järjestelmätaltion SHA256-tiiviste tallennetaan päätiedostojärjestelmän metadatapuuhun, joka tiivistetään. Puun kukin solmu varmistaa rekursiivisesti alisolmujensa tiivisteiden eheyden samoin kuin binäärisessä tiivistepuussa (Merkle-puu). Juurisolmun tiivisteen arvo, jota kutsutaan *sinetiksi*, perustuu siis allekirjoitetun järjestelmätaltion jokaiseen datatavuun, mikä puolestaan tarkoittaa, että näin saatava kryptografinen allekirjoitus kertoo koko järjestelmätaltion eheydestä.

macOS:n asennuksen ja päivityksen aikana tiedostojärjestelmästä lasketaan uusi sinetti laitteella. Tätä mittausta verrataan Applen allekirjoittamaan mittaukseen. Apple siliconilla varustetussa Macissa käynnistyslataaja tarkistaa sinetin ennen hallinnan siirtämistä kernelille. Intel-pohjaisessa Macissa, jossa on Apple T2 Security -siru, käynnistyslataaja välittää mittauksen ja allekirjoituksen kernelille, joka sitten tarkistaa sinetin suoraan ennen kuin tuo juuritiedostojärjestelmän näkyviin. Kummassakin tapauksessa, jos tarkistus epäonnistuu, käynnistysprosessi pysähtyy ja käyttäjää kehotetaan asentamaan macOS uudelleen. Tämä menettely toistetaan jokaisella käynnistyskerralla, ellei käyttäjä ole valinnut alemman suojauksen tilaa ja erikseen valinnut allekirjoitetun järjestelmätaltion ottamista pois käytöstä.

iOS- ja iPadOS-ohjelmistopäivitysten aikana järjestelmätaltio valmistellaan ja lasketaan uudelleen samalla tavalla. iOS:n ja iPadOS:n käynnistyslataajat tarkistavat, että sinetti on vahingoittumaton ja että se vastaa Applen allekirjoittamaa arvoa, ennen kuin ne sallivat laitteen käynnistää kernelin. Vastaamattomuudesta käynnistyksen aikana seuraa kehotus käyttäjälle päivittää laitteen järjestelmäohjelmisto. Käyttäjien ei sallita poistaa käytöstä allekirjoitetun järjestelmätaltion suojausta iOS:ssä ja iPadOS:ssä.

Allekirjoitettu järjestelmätaltio ja koodin allekirjoitus

Koodin allekirjoitus on edelleen käytössä ja kernelin pakottama. Allekirjoitettu järjestelmätaltio tarjoaa suojaa aina kun mitään dataa luetaan sisäisestä tallennuslaitteesta. Koodin allekirjoitus puolestaan tarjoaa suojaa, kun Mach-O-tiedostoja peilataan muistiin suoritustiedostona. Sekä allekirjoitettu järjestelmätaltio että koodin allekirjoitus suojaavat suoritettavaa koodia kaikissa luku- ja suorituspoluissa.

Allekirjoitettu järjestelmätaltio ja FileVault

macOS 11:ssä ei järjestelmätaltiota tarvitse enää salata, sillä allekirjoitettu järjestelmätaltio hoitaa vastaavan suojauksen järjestelmän sisällölle. Tiedostojärjestelmä havaitsee kaikki siihen levon aikana tehdyt muutokset dataa luettaessa. Jos käyttäjä on ottanut FileVaultin käyttöön, käyttäjän sisältö datataltiolla salataan edelleen käyttäjältä saatua salaisuutta käyttäen.

Jos käyttäjä poistaa allekirjoitetun järjestelmätaltion käytöstä, levossa olevasta järjestelmästä tulee haavoittuva peukaloinnille, ja tällaisen peukaloinnin avulla hyökkääjä voisi mahdollisesti saada selvitettyä salattuja käyttäjän tietoja, kun järjestelmä seuraavan kerran käynnistyy. Siksi järjestelmä ei salli käyttäjän ottaa allekirjoitettua järjestelmätaltiota pois käytöstä, jos FileVault on käytössä. Tietojen suojaus levossa täytyy olla käytössä tai pois käytöstä molemmille taltioille samalla tavoin.

macOS 10.15:ssä ja aiemmissa FileVault suojaa käyttöjärjestelmäohjelmistoa levossa salaamalla käyttäjän sisällön ja järjestelmäsisällön avaimella, jota suojaa käyttäjältä saatu salaisuus. Tämän ansiosta laitteen fyysisesti käyttöönsä saanut hyökkääjä ei pääse järjestelmäohjelmiston sisältävään tiedostojärjestelmään tai voi muokata sitä.

Allekirjoitettu järjestelmätaltio ja Mac, jossa on Apple T2 Security -siru

Macissa, jossa on Apple T2 Security -siru, allekirjoitettu järjestelmätaltio suojaa vain itse macOS:n. Suojattu käynnistys suojaa ohjelmistoa, joka toimii T2-sirulla ja tarkistaa macOS:n.

Turvalliset ohjelmistopäivitykset

Tietoturva on jatkuva prosessi. Ei riitä, että tehtaalla asennettu käyttöjärjestelmäversio käynnistetään luotettavasti, vaan tarvitaan myös nopea ja turvallinen keino saada uusimmat suojauspäivitykset. Apple julkaisee säännöllisesti ohjelmistopäivityksiä, joilla vastataan uusiin tietoturvauhkiin. iOS- ja iPadOS-laitteiden käyttäjät saavat päivitysilmoitukset laitteeseen. Mac-käyttäjät löytävät saatavilla olevat päivitykset Järjestelmäasetuksista. Päivitykset jaetaan langattomasti, jotta uusimmat suojausominaisuudet saadaan nopeasti käyttöön.

Päivitysprosessi

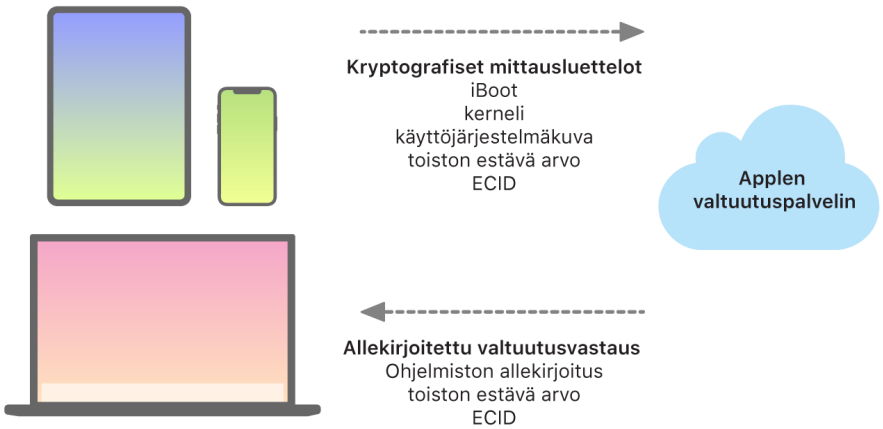
Päivitysprosessi käyttää samaa laitteistopohjaista luottamuksen perustaa (RoT), jota suojattu käynnistys käyttää, ja joka on suunniteltu asentamaan ainoastaan Applen allekirjoittamaa koodia. Lisäksi päivitysprosessi käyttää järjestelmäohjelmiston valtuutusta iOS- ja iPadOS-laitteissa sekä sellaisissa Mac-tietokoneissa, joissa Käynnistyksen suojaustyökalussa on asetettu suojatun käynnistyksen käytännöksi Täysi suojaus. Järjestelmäohjelmiston valtuutuksessa ohjelmiston allekirjoitus tarkistetaan, ja vain Applen aktiivisesti allekirjoittama käyttöjärjestelmäversio asennetaan. Näiden suojausprosessien ansiosta, Apple voi lopettaa vanhojen, tunnettuja haavoittuvuuksia sisältävien käyttöjärjestelmäversioiden allekirjoittamisen. Tämä auttaa estämään hyökkäykset, jossa pyritään asentamaan vanha haavoittuva käyttöjärjestelmäversio nykyisen tilalle.

Ohjelmistopäivityksen turvallisuuden parantamiseksi niissä tapauksissa, kun päivitettävä laite on fyysisesti liitettynä Maciin, ladataan ja asennetaan iOS:n tai iPadOS:n täysi kopio. Langattomasti ladatut ohjelmistopäivitykset sen sijaan eivät lataa koko käyttöjärjestelmää, vaan *vain päivitykseen tarvittavat komponentit*. Tämä parantaa verkon tehokkuutta. Ohjelmistopäivityksiin voidaan myös hyödyntää Sisältövälimuisti-ominaisuutta Macissa, jossa on macOS 10.13 tai uudempi. Kun iOS- ja iPadOS-laitteet saavat päivityksen Macin sisältövälimuistista, sitä ei tarvitse ladata jokaiselle laitteelle erikseen internetistä. (Niiden täytyy silti muodostaa yhteys Applen palvelimille, jotta päivitysprosessi voidaan suorittaa loppuun.)

Yksilölliseksi tehty päivitysprosessi

Päivityksessä muodostetaan yhteys Applen asennuksen valtuutuspalvelimeen, joka sisältää luettelon kryptografisista mittauksista asennusnipun jokaiselle asennettavalle osalle (esimerkiksi iBoot, kernel ja käyttöjärjestelmälevytiedosto), satunnaisen toiston estävän arvon (nonce) ja laitteen yksilöllisen ECID-tunnuksen.

Valtuutuspalvelin vertaa esitettyä mittausluetteloa versioihin, joiden asennus on sallittu, ja löytäessään osuman lisää ECID:n mittaukseen ja allekirjoittaa tuloksen. Palvelin antaa koko allekirjoitetun paketin laitteelle osana päivitysprosessia. ECID:n lisääminen ”personoi” valtuutuksen pyytävään laitteeseen. Valtuuttamalla ja allekirjoittamalla vain tunnetut mittaukset palvelin auttaa varmistamaan, että päivitys tapahtuu täsmälleen Applen määrittämällä tavalla.



Käynnistyksen luottamusketjun varmennus varmistaa, että allekirjoitus tulee Applelta ja että tallennuslaitteelta ladatun kohteen arvot, yhdessä laitteen ECID:n kanssa, vastaa allekirjoitettua. Nämä vaiheet on suunniteltu varmistamaan, että yksilöintiä tukevissa laitteissa valtuutus on tiettyyn laitteeseen ja että vanhempaa käyttöjärjestelmää tai laiteohjelmistoa yhdestä laitteesta ei voida kopioida toiseen laitteeseen. Nonce auttaa estämään hyökkääjää tallentamasta palvelimen vastausta ja käyttämästä sitä laitteen peukaloimiseen tai järjestelmäohjelmiston muuttamiseen muulla tavoin.

Yksilöintiprosessi on syy siihen, miksi verkkoyhteys Appleen on välttämätön aina päivitettäessä laitetta, jossa on Applen suunnittelema siru, mukaan lukien Intel-pohjainen Mac, jossa on Apple T2 Security -siru.

Lisäksi käyttäjän datataltiota ei koskaan liitetä käyttöön ohjelmistopäivityksen aikana. Se estää tietojen lukemisen tai kirjoittamisen kyseisiltä taltioilta päivitysten aikana.

Jos laitteessa on Secure Enclave, tämä laitteisto tarkistaa myös ohjelmistonsa eheyden käyttämällä järjestelmäohjelmiston valtuutusta ja sen on suunniteltu estämään vanhempien versioiden asentaminen.

Käyttöjärjestelmän eheys

Tietoturva on Applen käyttöjärjestelmäohjelmistojen suunnittelun keskiössä. Suunnitteluun kuuluvat laitetason luottamuksen perusta (RoT, Root of Trust), jota käytetään mahdollistamaan suojattu käynnistys, sekä nopea ja turvallinen suojattu ohjelmistopäivitysprosessi. Applen käyttöjärjestelmät käyttävät myös siruun pohjautuvia laitteisto-ominaisuuksiaan, jotka on erityisesti tehty auttamaan estämään hyväksikäyttöä, kun käyttöjärjestelmä on toiminnassa. Nämä ajonaikaiset ominaisuudet suojaavat luotetun koodin eheyttä, kun sitä suoritetaan. Lyhyesti sanottuna Applen käyttöjärjestelmäohjelmisto auttaa torjumaan hyökkäys- ja hyväksikäyttötekniikoita riippumatta siitä, tulevatko ne haitallisesta apista, verkosta tai mistä tahansa muusta kanavasta. Tässä luetellut suojaukset ovat saatavilla tuetulla Applen suunnittelemalla järjestelmäpiirillä varustetuissa laitteissa iOS:ssä, iPadOS:ssä, tvOS:ssä, watchOS:ssä sekä uusimpana macOS:ssä Apple siliconilla varustetussa Macissa.

Ominaisuus	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	M1-perhe
Kernelin eheyden suojaus	✓	✓	✓	✓	✓	✓
Nopeat luparajoitukset		✓	✓	✓	✓	✓
Järjestelmän lisäprosessorin eheyden suojaus			✓	✓	✓	✓
PAC-koodit			✓	✓	✓	✓
Page Protection Layer (PPL)		✓	✓	✓	✓	Katso huomautus alla.

Huomaa: Page Protection Layer (PPL) vaatii, että alusta suorittaa *ainoastaan* allekirjoitettua ja luotettua koodia. Tämä suojausmalli ei sovellu macOS:lle.

Kernelin eheyden suojaus

Kun käyttöjärjestelmän kernel saa valmistelun tehtyä, otetaan käyttöön kernelin eheyden suojaus (KIP), jonka tehtävä on auttaa estämään kernelin ja ajurien koodin muutoksia. Muistiohjain tarjoaa suojatun fyysisen muistitilan, jota iBoot käyttää kernelin ja kernelin laajennusten lataamiseen. Kun käynnistys on valmis, muistiohjain kieltää kirjoittamisen suojatulle fyysiselle muistialueelle. Appeja suorittavan prosessorin muistinhallintayksikkö (MMU) on määritetty auttamaan estämään etuoikeutetun koodin peilaus suojatun muistialueen ulkopuolella olevasta fyysisestä muistista ja auttamaan estämään fyysisen muistin kirjoitettavat peilaukset kernelin muistialueelle.

Uudelleenmäärityksen estämiseksi kernelin eheyden suojauksen käyttöönottanut laitteisto lukitaan käynnistysprosessin valmistumisen jälkeen.

Nopeat luparajoitukset

Apple A11 Bionic- ja S3-järjestelmäpiireistä lähtien, piireihin on lisätty uusi laitteiston primitiivi nimeltään nopeat luparajoitukset. Nämä rajoitukset sisältävät prosessorirekisterin, jolla voidaan rajoittaa lupia nopeasti ja säiekohtaisesti. Nopeiden luparajoitusten (joita kutsutaan myös APRR-rekistereiksi) ansiosta tuetut käyttöjärjestelmät voivat nopeasti rajoittaa muistin lupia ilman järjestelmäkutsun mukanaan tuomaa lisäkuormaa ja sivutaulukon läpikäyntiä tai tyhjennystä. Nämä rekisterit vähentävät vielä yhdellä tasolla verkosta tulevien hyökkäysten vaaraa erityisesti ajonaikaisesti käännettävän (JIT-käännettävän) koodin tapauksessa, koska muistia ei voida suorittaa tehokkaasti samaan aikaan kuin sitä luetaan tai siihen kirjoitetaan.

Järjestelmän lisäprosessorin eheyden suojaus

Lisäprosessorin laiteohjelmisto käsittelee monia tärkeitä järjestelmätehtäviä, kuten Secure Enclavea, kuvasensoriprosessoria ja liikeapuprosessoria. Siksi sen suojaus on tärkeä osa järjestelmän tietoturvaa. Lisäprosessorin laiteohjelmiston muutosten estämiseksi Apple käyttää mekanismia nimeltä *järjestelmän lisäprosessorin eheyden suojaus (System Coprocessor Integrity Protection, SCIP)*.

SCIP toimii pitkälti kuten kernelin eheyden suojaus (KIP): Käynnistyksessä iBoot lataa jokaisen lisäprosessorin laiteohjelmiston suojatulle muistialueelle, joka on tarkoitukseen varattu ja erotettu kernelin eheyden suojausalueesta. iBoot määrittää jokaisen lisäprosessorin muistiyksiköt auttaakseen estämään seuraavia:

- suoritettavat peilaukset (mapping) sen suojatun muistialueen ulkopuolella
- kirjoitettavat peilaukset sen suojatun muistialueen sisäpuolella

Myös Secure Enclaven käyttöjärjestelmää käytetään Secure Enclaven SCIPin määritystä varten käynnistyksen aikana. Kun käynnistymisprosessi on valmis, järjestelmän lisäprosessorin eheyden suojauksen käyttöönottoon käytetty laitteisto lukitaan. Tämä on suunniteltu estämään uudelleenmääritystä.

PAC-koodit

PAC (Pointer Authentication Codes) -koodeja käytetään suojaamaan muistin korruptoitumisvirheiden hyödyntämiseltä. Järjestelmäohjelmisto ja sisäiset apit käyttävät PAC-koodia apuna estämään funktio-osoittimien ja paluuosoitteiden (koodiosoittimien) muokkausta. PAC käyttää viittä salaista 128-bittistä arvoa kernelin käskyjen ja datan allekirjoittamiseen, ja jokaisella käyttäjätilaprosessilla on omat B-avaimet. Kohteet on suolattu ja allekirjoitettu alla kuvatulla tavalla:

Kohde	Avain	Suola
Funktion paluuosoite	IB	Tallennustilan osoite
Funktio-osoittimet	IA	0
Lohkon kutsufunktio	IA	Tallennustilan osoite
Objective-C-menetelmän välimuisti	IB	Tallennustilan osoite + luokka + valitsin
C++ V-tauluarvot	IA	Tallennustilan osoite + tiiviste (sekoitettu menetelmän nimi)
Laskettu Goto-etiketti	IA	Tiiviste (funktion nimi)
Kernel-säikeen tila	GA	•
Käyttäjäsäikeen tilarekisterit	IA	Tallennustilan osoite
C++ V-taulu-osoittimet	DA	0

Allekirjoitusarvo säilytetään 64-bittisen osoittimen yläosan käyttämättömissä täytebiteissä. Allekirjoitus varmennetaan ennen käyttöä, ja täyte palautetaan, mikä auttaa varmistamaan osoittimen osoitteen toimivuuden. Tulosten tarkistuksen epäonnistuminen johtaa keskeytymiseen. Tämä vahvistus lisää monien hyökkäysten vaikeutta, kuten ROP-hyökkäysten (return-oriented programming), jotka yrittävät huijata laitteen suorittamaan olemassa olevaa haitallista koodia manipuloimalla toiminnon paluuosoitetta, joka on tallennettu pinoon.

Page Protection Layer (PPL)

iOS:n, iPadOS:n ja watchOS:n Page Protection Layer -ominaisuus (PPL) on suunniteltu estämään käyttäjätilan koodin muokkaukset sen jälkeen, kun koodin allekirjoituksen tarkistus on valmis. PPL perustuu kernelin eheyden suojaukseen ja nopeisiin luparajoituksiin, ja se hallitsee sivutaulukkojen oikeuksien ohituksia. Näin varmistetaan, että vain PPL voi muokata suojattuja sivuja, jotka sisältävät käyttäjän koodia ja sivutaulukkoja. PPL pienentää hyökkäysmahdollisuuksia merkittävästi tukemalla järjestelmänlaajuista koodin eheyden vahvistusta silloinkin, kun kernel on vaarantunut. Tätä suojausta ei ole tarjolla macOS:ssä, koska PPL on käytettävissä ainoastaan järjestelmissä, joissa vaaditaan kaiken suoritettavan koodin olevan allekirjoitettua.

Muut macOS:n järjestelmän suojauksen ominaisuudet

Muut macOS:n järjestelmän suojauksen ominaisuudet

macOS toimii laajemmassa joukossa laitteistoja (esimerkiksi Intel-prosessorit, Intel-prosessorit yhdistettynä Apple T2 Security -siruun sekä Apple silicon -pohjaiset järjestelmäpiirit), ja se tukee monia tietokoneen yleisiä käyttötapoja. Siinä missä jotkut käyttäjät käyttävät vain mukana tulevia tai App Storesta saatavia perusappeja, toiset puolestaan ovat kernel-kehittäjiä, joiden tarvitsee poistaa käytöstä jokseenkin kaikki alustan suojaukset voidakseen ajaa ja testata koodiaan korkeimmilla luottamustasoilla suoritettuna. Useimmat käyttäjät ovat jossakin näiden ääripäiden välillä, ja monilla heistä on oheislaitteita ja ohjelmistoja, jotka vaativat eritasoisia pääsyoikeuksia. Apple suunnitteli macOS-alustan laitteiston, ohjelmistot ja palvelut integroidulla lähestymistavalla. Se on alusta, joka tarjoaa sisäänrakennetun tietoturvan ja helpottaa määrittelyjen tekoa, käyttöönottoa ja hallintaa, mutta tarjoaa myös sellaiset muuntelumahdollisuudet, joita käyttäjät odottavat. macOS sisältää myös keskeiset tietoturvateknologiat, joita IT-ammattilaiset tarvitsevat avuksi yrityksen tietojen suojauksen ja macOS:n integrointiin suuryritysten suojatuissa verkkoympäristöissä.

Seuraavat ominaisuudet tukevat macOS:n käyttäjien erilaisia tarpeita ja auttavat suojaamaan tarvittavat ratkaisut. Niihin sisältyvät:

- Allekirjoitetun järjestelmätaltion suojaus
- Järjestelmän eheyden suojaus
- Luottamusvälimuistit
- Oheislaitteiden suojaus
- Rosetta 2:n (automaattinen kääntäminen) tuki ja suojaus Apple siliconilla varustetulla Macilla
- DMA:n tuki ja suojaus
- Kernelin laajennusten (kext) tuki ja suojaus
- Optio-ROMin tuki ja suojaus
- UEFI-laiteohjelmiston suojaus Intel-pohjaisilla Mac-tietokoneilla

Järjestelmän eheyden suojaus

macOS hyödyntää kernelin oikeuksia rajoittaakseen kriittisten järjestelmätiedostojen kirjoittamista. Tätä rajoittamista kutsutaan *järjestelmän eheyden suojaukseksi (System Integrity Protection - SIP)*. Tämä ominaisuus on erillinen laitteistopohjaisesta kernelin eheyden suojauksesta (Kernel Integrity Protection - KIP), joka on käytettävissä Apple siliconilla varustetussa Macissa ja suojaa kernelin muokkaamiselta muistissa. Järjestelmän eheyden suojausta käytetään kernelin eheyden suojauksen lisäksi. Tähän ja useisiin muihin kernel-tason suojauksiin, kuten eristykseen (sandboxing) ja tietosäiliöön, hyödynnetään pakollista pääsynhallintaa.

Pakollinen pääsynhallinta

macOS käyttää pakollista pääsynhallintaa, eli kehittäjän luomia tietoturvarajoitteita määrittäviä käytäntöjä, joita ei voida ohittaa. Tämä lähestymistapa eroaa harkinnanvaraisesta pääsynhallinnasta, jossa käyttäjät voivat ohittaa tietoturvakäytäntöjä mieltymystensä mukaan.

Pakollinen pääsynhallinta ei näy käyttäjille, mutta se on perusteknologiaa, joka auttaa mahdollistamaan useita tärkeitä ominaisuuksia. Niitä ovat esimerkiksi eristys, käyttörajoitukset, hallitut asetukset, laajennukset ja järjestelmän eheyden suojaus.

Järjestelmän eheyden suojaus

Järjestelmän eheyden suojaus rajoittaa erityisissä tärkeissä tiedostojärjestelmäsijainneissa olevat komponentit vain luettaviksi. Tämä auttaa estämää haitallista koodia muokkaamasta niitä. Järjestelmän eheyden suojaus on tietokonekohtainen asetus, joka on oletuksena päällä, kun käyttäjä päivittää OS X 10.11:een tai uudempaan. Intel-pohjaisessa Macissa asetuksen laittaminen pois päältä poistaa suojauksen kaikilta osioilta fyysisessä tallennuslaitteessa. macOS käyttää tätä suojauskäytäntöä jokaiseen järjestelmässä toimivaan prosessiin riippumatta siitä, toimiiko se eristettynä vai ylläpitäjän oikeuksilla.

Luottamusvälimuistit

Yksi suojatun käynnistysketjun kohteista on staattinen luottamusvälimuisti. Se on luotettu tietue kaikista allekirjoitetun järjestelmätaltion Mach-O-binääritiedostoista. Kutakin Mach-O-tiedostoa edustaa koodihakemiston tiiviste. Tehokasta hakua varten nämä tiivisteet lajitellaan ennen niiden lisäämistä luottamusvälimuistiin. Koodihakemisto on tulos `codesign(1)`:n suorittamasta allekirjoitusoperaatiosta. Luottamusvälimuistin käytön pakottaminen edellyttää, että järjestelmän eheyden suojaus pidetään käytössä. Jotta luottamusvälimuistin pakottaminen voidaan poistaa käytöstä Apple siliconilla varustetussa Macissa, suojatun käynnistyksen tilaksi täytyy määrittää Salliva suojaus.

Kun binääritiedosto suoritetaan (joko osana uutta aliprosessia tai kuvattaessa suoritettavaa koodia olemassa olevaan prosessiin), sen koodihakemisto otetaan tiivistettäväksi. Jos näin saatava tiiviste löytyy luottamusvälimuistista, binääritiedostolle luodut suoritettavat kuvaukset saavat alustan oikeudet – eli niillä voi olla mikä tahansa oikeus ja ne voidaan suorittaa ilman allekirjoituksen aitouden enempää tarkistamista. Tämä eroaa Intel-pohjaisesta Macista, jossa käyttöjärjestelmäsisältö saa alustan oikeudet binääritiedostot allekirjoittavalta Applen varmenteelta. (Tämä varmenne ei rajoita sitä, mitä oikeuksia binääritiedostolla voi olla.)

Alustaan kuulumattomilla binääritiedostoilla (esimerkiksi oikeaksi todistettu muun valmistajan koodi) täytyy olla kelvolliset varmenneketjut, jotta niitä suoritetaan, ja niiden mahdollisia oikeuksia rajoittaa allekirjoitusprofiili, jonka kehittäjä on saanut Apple Developer Program -ohjelmasta.

Kaikki macOS:n mukana toimitettavat binääritiedostot allekirjoitetaan käyttäen *alustatunnistetta*. Apple siliconilla varustetussa Macissa tätä tunnistetta käytetään kertomaan, että vaikka binääritiedosto on Applen allekirjoittama, sen saa suorittaa vain, jos sen koodihakemiston tiiviste löytyy luottamusvälimuistista. Intel-pohjaisessa Macissa alustatunnistetta käytetään vanhempien macOS-versioiden binääritiedostojen oikeuksien kohdennettuun kumoamiseen. Tämä kohdennettu kumoaminen auttaa estämään kyseisten binääritiedostojen suorittamista uudemmissa versioissa.

Staattinen luottamusvälimuisti lukitsee binääritiedostojen joukon täysin tiettyyn macOS-versioon. Tämä toimintatapa auttaa estämään Applen vanhempia käyttöjärjestelmiä varten aikanaan kelvollisesti allekirjoittamien binääritiedostojen käyttämisen uudempien käyttöjärjestelmien kanssa, jotta hyökkääjä voisi hyötyä niistä.

Käyttöjärjestelmän ulkopuolella toimitettava alustakoodi

Apple toimittaa joitakin binääritiedostoja, joita ei allekirjoiteta alustatunnisteella. Näitä on esimerkiksi Xcodessa ja kehittäjätyökalujen kokoelmassa. Niiden suorittaminen sallitaan kuitenkin alustan oikeuksilla Apple siliconilla ja T2-sirulla varustetussa Macissa. Koska tällainen alustaohjelmisto toimitetaan erillisenä macOS:stä, staattisen luottamusvälimuistin kumoamistoiminta ei koske sitä.

Ladattavat luottamusvälimuistit

Apple toimittaa tiettyjen ohjelmistopakettien mukana *ladattavia luottamusvälimuisteja*. Näissä välimuisteissa on sama tietorakenne kuin staattisessa luottamusvälimuistissa. Vaikka järjestelmässä on vain yksi staattinen luottamusvälimuisti ja sen sisältö on aina varmasti lukittu kirjoitussuojatuille alueille, kun kernelin aikaisen vaiheen valmistelu on suoritettu, ladattavat luottamusvälimuistit lisätään järjestelmään ajon aikana.

Nämä luottamusvälimuistit todennetaan joko käyttäen samaa mekanismia, joka todentaa käynnistyksen laiteohjelmiston (yksilöidään käyttäen Applen luotettua allekirjoituspalvelua) tai yleisellä allekirjoituksella todennettuina kohteina (joiden allekirjoitus ei sido niitä tiettyyn laitteeseen).

Yksilöllisesti allekirjoitettu luottamusvälimuisti toimitetaan esimerkiksi Apple siliconilla varustetun Macin kentällä tehtävään vianmääritykseen käytettävän levytiedoston mukana. Tämä luottamusvälimuisti allekirjoitetaan yksilöllisesti levytiedoston kanssa ja ladataan kohteena olevan Macin kerneliin, kun se käynnistetään vianmääritystilaan. Tämän luottamusvälimuistin ansiosta levytiedostossa oleva ohjelmisto voi toimia alustan oikeuksin.

Yleisellä allekirjoituksella todennettu luottamusvälimuisti toimitetaan esimerkiksi macOS-ohjelmistopäivitysten mukana. Tämän luottamusvälimuistin ansiosta ohjelmistopäivityksen sisältämä koodiosio (*päivityksen aivot*) voi toimia alustan oikeuksin. Päivityksen aivokoodi tekee ohjelmistopäivityksessä sellaisen työn, jota isäntäjärjestelmä ei voi tehdä johdonmukaisesti järjestelmästä toiseen.

Oheislaiteprosessorien suojaus Mac-tietokoneilla

Kaikissa nykyaikaisissa tietokonejärjestelmissä on monia sisäisiä oheislaiteprosessoreita, jotka on tarkoitettu esimerkiksi virranhallintaan ja verkon ja näytönohjaimen hallintaan. Usein nämä oheislaiteprosessorit on suunniteltu yhteen tarkoitukseen ja ne ovat vähemmän tehokkaita kuin ensisijainen prosessori. Jos sisäisissä oheislaitteissa ei ole riittävästi suojausta, niistä tulee kohde helpompia kohteita etsiville hyökkääjille, jotka voivat niiden kautta tartuttaa käyttöjärjestelmän pysyvästi. Oheislaiteprosessorin laiteohjelmiston tartuttamisen jälkeen hyökkääjä voisi hyökätä ensisijaisessa prosessorissa olevaan ohjelmistoon tai kaapata suoraan arkaluontoisia tietoja. (Esimerkiksi Ethernet-laite voi nähdä salaamattomien pakettien sisällöt.)

Apple tekee työtä vähentääkseen tarvittavien oheislaiteprosessoreiden määrää ja välttääkseen malleja, jotka vaativat laiteohjelmiston. Kun erillisiä prosessoreja ja niiden omaa laiteohjelmistoa kuitenkin tarvitaan, tehdään toimenpiteitä, jotka auttavat varmistamaan, ettei hyökkääjä voisi jäädä kyseiseen prosessoriin. Tähän voidaan käyttää jompaakumpaa kahdesta prosessorin tarkistustavasta:

- Suorittamalla prosessoria siten, että se lataa tarkistetun laiteohjelmiston ensisijaisesta prosessorista käynnistyksen yhteydessä
- Käyttämällä oheislaiteprosessorille omaa suojattua käynnistysketjua, jossa oheislaiteprosessori tarkistaa oman laiteohjelmistonsa aina Macin käynnistyessä

Apple tekee yhteistyötä oheislaiteprosessorien toimittajien kanssa ja valvoo niiden toteutuksia sekä parantaa niiden suunnittelua, jotta ne sisältäisivät halutut ominaisuudet, kuten:

- Minimisalaustasot
- Huonoksi tunnetun ohjelmiston vahvan kumoamisen
- Vianmäärityskäyttöliittymien käytöstäpoiston
- Laiteohjelmiston allekirjoittaminen kryptografisilla avaimilla, jotka on tallennettu Applen hallitsemiin laitteiston suojausmoduuleihin (HSM)

Apple on tehnyt viime vuosina yhteistyötä muutamien yritysten kanssa, jotta nekin ottaisivat käyttöön samat Image4-tietorakenteet, vahvistuskoodin ja allekirjoitusinfrastruktuurin, joita Apple itse käyttää Apple siliconissa.

Kun tallennustilaton toiminta tai tallennustilan ja suojatun käynnistyksen yhdistelmä ei ole vaihtoehtona, malli vaatii, että laiteohjelmistopäivitykset on allekirjoitettu ja varmistettu kryptografisesti ennen kuin pysyvää tallennustilaa voidaan päivittää.

Rosetta 2 Apple siliconilla varustetussa Macissa

Apple siliconilla varustettu Mac voi suorittaa x86_64-käskykannalle käännettyä koodia käyttäen *Rosetta 2* -käännösmekanismia. Käännöstyyppejä on kaksi: ajonaikainen JIT (just-in-time) ja ennenaikainen AOT (ahead-of-time).

JIT-kääntäminen

JIT-kääntämistä käytettäessä x86_64-muotoinen Mach-O tunnistetaan aikaisessa kohdassa levytiedoston suorituspolussa. Kun tällaisia levytiedostoja tulee vastaan, kernel siirtää hallinnan erityiselle Rosetta-käännösosalle dynaamisten linkkien editorin (`dyld(1)`) sijaan. Käännösosa kääntää sitten x86_64-sivut levytiedoston suorittamisen aikana. Tämä kääntäminen tapahtuu kokonaan prosessissa. Kernel vertaa edelleen kunkin x86_64-sivun kooditiivisteitä koodin allekirjoitukseen, joka on liitetty binääritiedostoon, kun sivu tuodaan sisään. Mikäli tiivisteet eivät täsmää, kernel pakottaa kyseiselle prosessille sopivan korjauskäytännön.

AOT-kääntäminen

Käytettäessä ennenaikaista (AOT) kääntämispolkua x86_64-binääritiedostot luetaan tallennustilasta aikoina, jotka järjestelmä määrittää optimaalisiksi koodin reaktionopeuden kannalta. Käännetyt artefaktit kirjoitetaan tallennustilaan erityistyyppisenä Mach-O-tiedostona. Tämä tiedosto on samankaltainen kuin suoritettava levytiedosto, mutta varustettu merkinnällä, joka kertoo sen olevan käännetty toisesta levytiedostosta.

Tässä mallissa AOT-käännetty artefakti saa kaikki identiteettitietonsa alkuperäiseltä suoritettavalta x86_64-levytiedostolta. Tämän sidoksen pakottamiseksi etuoikeutettu käyttäjätilan entiteetti allekirjoittaa käännösartefaktin käyttäen Secure Enclaven hallitsemaa laitekohtaista avainta. Avain vapautetaan vain etuoikeutetulle käyttäjätilan entiteetille, joka tunnistetaan sellaiseksi rajoitetulla oikeudella. Käännösartefaktia varten luotu koodihakemisto sisältää suoritettavan alkuperäisen x86_64-levytiedoston koodihakemiston tiivisteen. Itse käännösartefaktin allekirjoitusta kutsutaan *lisäallekirjoitukseksi*.

AOT-käännösputki alkaa samoin kuin JIT-käännösputki, eli kernel siirtää hallinnan ajonaikaiselle Rosettalle dynaamisten linkkien editorin (`dyld(1)`) sijaan. Ajonaikainen Rosetta kuitenkin lähettää Rosetta-järjestelmäpalvelulle prosessien välisen kommunikaation (IPC) kyselyn, joka kysyy, onko senkertaiselle suoritettavalle levytiedostolle saatavilla AOT-käännös. Jos se löytyy, Rosetta-palvelu antaa viittauksen kyseiseen käännökseen ja se kuvataan prosessiin ja suoritetaan. Suorittamisen aikana kernel vaatii käännösartefaktin koodihakemistotiivisteet, jotka on todennettu allekirjoituksella, jonka juuri on laitekohtaisessa allekirjoitusavaimessa. Alkuperäisen x86_64-levytiedoston koodihakemiston tiivisteet eivät ole mukana tässä prosessissa.

Käännetyt artefaktit tallennetaan tietosäiliöön, johon pääsee ajon aikana ainoastaan Rosetta-palvelu. Rosetta-palvelu hallitsee pääsyä välimuistiinsa jakamalla yksittäisille käännösartefakteille kirjoitussuojattuja tiedostokuvaajia. Tämä rajoittaa pääsyä AOT-artefaktien välimuistiin. Palvelun prosessien välinen kommunikaatio ja riippuvuusjalanjälki pidetään tarkoituksellisesti hyvin suppeina sen hyökkäyspinnan rajoittamiseksi.

Jos alkuperäisen x86_64-levytiedoston koodihakemiston tiiviste ei vastaa AOT-käännösartefaktin allekirjoitukseen koodattua, tätä tulosta kohdellaan kuin epäkelpoa koodin allekirjoitusta ja toimitaan sen mukaisesti.

Jos etäprosessi kyselee kerneliltä AOT-käännetyn suoritettavan tiedoston oikeuksia tai muita koodin identiteettiominaisuuksia, sille palautetaan alkuperäisen x86_64-levytiedoston identiteettiominaisuudet.

Staattisen luottamusvälimuistin sisältö

macOS 11:ssä tai uudemmassa on moniarkkitehtuuriset Mach-binäärit, joissa on osat x86_64- ja arm64-tietokonekoodeista. Apple siliconilla varustetun Macin käyttäjä voi päättää suorittaa x86_64-järjestelmäbinääriä Rosetta-putken kautta esimerkiksi ladatakseen liitännäisen, josta ei ole natiivi-arm64-versiota. Tämän lähestymistavan tukemiseksi macOS:n mukana tuleva staattinen luottamusvälimuisti sisältää yleensä kolme koodihakemiston tiivistettä jokaiselle Mach-O-tiedostolle:

- Koodihakemiston tiiviste arm64:lle
- Koodihakemiston tiiviste x86_64:lle
- Koodihakemiston tiiviste x86_64-puolen AOT-käännökselle

Rosettan AOT-kääntäminen on determinististä sikäli, että samasta syötteestä tulee aina samanlainen tuotos riippumatta kääntämisen ajankohdasta tai siihen käytetystä laitteesta.

macOS:n koonnin aikana jokaiselle Mach-O-tiedostolle tehdään Rosettan AOT-käännös kyseisen macOS-version käännösputkessa, ja saatava koodihakemiston tiiviste tallennetaan luottamusvälimuistiin. Tehokkuussyistä varsinaisia käännettyjä tuotteita ei toimiteta käyttöjärjestelmän mukana. Ne muodostetaan uudelleen käyttäjän pyytäessä niitä.

Kun x86_64-levytiedosto suoritetaan Apple siliconilla varustetussa Macissa, mikäli kyseisen levytiedoston koodihakemiston tiiviste on staattisessa luottamusvälimuistissa, tulokseksi saatavan AOT-artefaktin koodihakemiston tiivisteen odotetaan *myös* olevan staattisessa luottamusvälimuistissa. Tällaisia tuotteita ei allekirjoiteta laitekohtaisella avaimella, koska allekirjoitusauktoriteetti perustuu Applen suojattuun käynnistysketjuun.

Allekirjoittamaton x86_64-koodi

Apple siliconilla varustettu Mac ei salli natiivin arm64-koodin suorittamista ilman siihen liitettyä kelvollista allekirjoitusta. Tämä allekirjoitus voi yksinkertaisimmillaan olla ad hoc -allekirjoitus (vrt. `codesign(1)`), jossa ei ole mitään oikeaa identiteettitietoa epäsymmetrisen avainparin salaisesta puolesta (se on yksinkertaisesti binääritiedoston todentamaton mittaus).

Binäärien yhteensopivuuden vuoksi käännetyn x86_64-koodin suorittaminen Rosettan kautta sallitaan ilman mitään allekirjoitustietoa. Tälle koodille ei välitetä määrättyä identiteettiä laitekohtaisessa Secure Enclave -allekirjoituksessa, ja se suoritetaan täsmälleen samoilla rajoituksilla kuin natiivi allekirjoittamaton koodi suoritetaan Intel-pohjaisessa Macissa.

DMA-suojaukset Mac-tietokoneilla

Jotta nopeiden liitäntöjen, kuten PCIe:n, FireWiren, Thunderboltin ja USB:n, suoritusteho saataisiin suureksi, tietokoneiden täytyy tukea suoraa muistin hakua eli DMA:ta oheislaitteille. Se tarkoittaa, että niiden täytyy voida lukea RAM-muistia ja kirjoittaa siihen ilman prosessorin jatkuvaa osallistumista. Vuodesta 2012 alkaen Mac-tietokoneissa on ollut useita eri teknologioita, jotka suojaavat DMA:ta. Näin lopputuloksena on kaikkien PC-tietokoneiden paras ja kattavin DMA-suojausten valikoima.

DMA-suojaukset Apple siliconilla varustetulle Macille

Applen järjestelmäpiirit sisältävät I/O-muistinhallintayksikön (IOMMU) jokaiselle järjestelmän DMA-agentille, mukaan lukien PCIe- ja Thunderbolt-portit. Koska jokaisella IOMMU-yksiköllä on omat osoitteenmuunnostaulukkonsa DMA-pyyntöjä varten, PCIe:llä tai Thunderboltilla yhdistetyt oheislaitteet pääsevät vain siihen muistiin, joka on nimenomaan määritetty niiden käyttöön. Oheislaitteet eivät pääse muille järjestelmän osille – kuten kernelille tai laiteohjelmistolle – kuuluvaan muistiin tai muille oheislaitteille määritettyyn muistiin. Jos IOMMU havaitsee, että oheislaite yrittää päästä muistiin, joka ei ole määritetty sen käyttöön, se laukaisee kernel panic -virheen.

DMA-suojaukset Intel-pohjaiselle Macille

Intel-pohjaiset Mac-tietokoneet, joissa on Intel Virtualization Technology for Directed I/O (VT-d) -teknologia, valmistelevat IOMMU:n ottaen käyttöön DMA:n uudelleenmäärityksen ja uudelleenmäärityksen keskeytystilanteessa hyvin aikaisessa vaiheessa käynnistysprosessin aikana, mikä vähentää useita erilaisia suojauksen haavoittuvuuksia. Applen IOMMU-laitteisto aloittaa toiminnan käytäntönään oletusarvoinen kieltäminen, joten siitä hetkestä alkaen kun järjestelmään laitetaan virta päälle, se alkaa automaattisesti estää oheislaitteiden DMA-pyyntöjä. Kun ohjelmisto on valmistellut IOMMU:t, ne alkavat sallia oheislaitteiden DMA-pyyntöjä muistialueille, jotka on nimenomaisesti määritetty niiden käytettäviksi.

Huomaa: PCIe:iden uudelleenmääritys keskeytystilanteessa ei ole tarpeellinen Apple siliconilla varustetun Macin kanssa, koska kukin IOMMU käsittelee omien oheislaitteidensa MSI:t.

macOS 11:stä alkaen kaikissa Apple T2 Security -sirulla varustetuissa Mac-tietokoneissa käytetään UEFI-ajureita, jotka helpottavat DMA:ta rajoitetussa tason 3 ympäristössä, kun nämä ajurit toimivat ulkoisten laitteiden pareina. Tämä ominaisuus auttaa vähentämään suojauksen haavoittuvuuksia, joita voi ilmetä, kun haitallinen laite on odottamattomalla tavalla vuorovaikutuksessa UEFI-ajurin kanssa käynnistyksen aikaan. Erityisesti se vähentää DMA-puskureita käsittelevien ajurien haavoittuvuuksien vaikutusta.

Kernelin laajennukset macOS:ssä

macOS 11:stä alkaen, jos muiden valmistajien kernelin laajennuksia otetaan käyttöön, niitä ei voi ladata kerneliin milloin tahansa. Sen sijaan ne yhdistetään *apukernelkokoelmaan (AuxKC)*, joka ladataan käynnistysprosessin aikana. Apple siliconilla varustetussa Macissa apukernelkokoelman mittaus kirjataan LocalPolicyyn (aikaisemmissa laitteistoissa apukernelkokoelma sijaitsi datataltiolla). Apukernelkokoelman uudelleenkokoaminen vaatii käyttäjän antaman hyväksynnän ja macOS:n uudelleenkäynnistyksen. Muutokset ladataan kerneliin, kun järjestelmä käynnistetään uudelleen, edellyttäen että suojatun käynnistyksen tasoksi on määritetty alennettu suojaus.

Tärkeää: Kernelin laajennuksia ei enää suositella macOS:lle. Kernelin laajennukset vaarantavat käyttöjärjestelmän eheyden ja luotettavuuden, ja Apple suosittelee käyttäjiä valitsemaan ratkaisuja, jotka eivät vaadi kernelin laajennuksia.

Kernelin laajennukset Apple siliconilla varustetussa Macissa

Kernelin laajennukset täytyy erikseen ottaa käyttöön Apple siliconilla varustetulle Macille pitämällä virtapainiketta painettuna käynnistyksen aikana, jolloin siirrytään One True Recovery (1TR) -tilaan, laskemalla suojaustasoksi Alennettu suojaus ja valitsemalla valintaneliö, jolla kernelin laajennukset otetaan käyttöön. Tämä edellyttää myös ylläpitäjän salasanan antamista suojaustason alentamista varten. 1TR ja salasanan vaatiminen vaikeuttavat yhdessä macOS:stä käsin aloittavien puhtaasti ohjelmistopohjaisten hyökkääjien aikomuksia viedä kernelin laajennuksia macOS:ään saadakseen käyttöönsä kernelin oikeudet.

Kun käyttäjä on valtuuttanut kernelin laajennusten latauksen, edellä kuvattua käyttäjän hyväksymän kernelin laajennusten latauksen kulkua käytetään kernelin laajennusten asennuksen valtuuttamiseen. Edellä käsiteltyä latauksessa käytettävää valtuutusta käytetään myös käyttäjän valtuuttamien kernelin laajennusten luettelon (UAKL) SHA384-tiivisteen tallentamisessa LocalPolicyyn. Kernelinhallintadaemon (`kmd`) vastaa ainoastaan käyttäjän valtuuttamien kernelin laajennusten luettelosta löytyvien kernelin laajennusten kelpuuttamisesta apukernelkokoelmaan sisällyttämiseksi.

- Jos järjestelmän eheyden suojaus on käytössä, kunkin kernelin laajennuksen allekirjoitus tarkistetaan ennen sen sisällyttämistä apukernelkokoelmaan.
- Jos järjestelmän eheyden suojaus ei ole käytössä, kernelin laajennuksen allekirjoitusta ei vaadita.

Tämä lähestymistapa mahdollistaa sallivan suojauksen työnkulut, joissa kehittäjät tai käyttäjät, jotka eivät osallistu Apple Developer Program -ohjelmaan, testaavat kernelin laajennuksia ennen niiden allekirjoittamista.

Kun apukernelkokoelma luodaan, sen mittaus lähetetään Secure Enclavelle allekirjoitettavaksi ja sisällytettäväksi Image4-tietorakenteeseen, jonka iBoot voi arvioida käynnistyksen yhteydessä. Osana apukernelkokoelman rakentamista luodaan myös kernelin laajennusten kuitti. Tämä kuitti sisältää luettelon kernelin laajennuksista, jotka sisällytettiin apukernelkokoelmaan, koska tämä voi olla alijoukko käyttäjän hyväksymien kernelin laajennusten luettelosta, mikäli joukosta löydettiin kiellettyjä kernelin laajennuksia. Apukernelkokoelman Image4-tietorakenteen SHA384-tiiviste ja kernelin laajennusten kuitti sisällytetään LocalPolicyyn. Apukernelkokoelman Image4-tiivistettä käytetään iBootin käynnistyksen yhteydessä suoritettavaan lisätarkistukseen, joka auttaa varmistamaan, ettei uudemman LocalPolicyn kanssa ole mahdollista käynnistää vanhempaa Secure Enclaven allekirjoittamaa apukernelkokoelman Image4-tiedostoa. Alijärjestelmät kuten Apple Pay käyttävät kernelin laajennusten kuittia selvittääkseen, onko ladattujen kernelin laajennusten joukossa sellaisia, jotka voisivat vaikuttaa macOS:n luotettavuuteen. Jos näin on, Apple Pay -ominaisuudet saatetaan poistaa käytöstä.

Vaihtoehdot kernelin laajennuksille (macOS 10.15 tai uudempi)

macOS 10.15:ssä kehittäjät voivat laajentaa macOS:n käyttömahdollisuuksia asentamalla ja hallitsemalla järjestelmälaajennuksia, jotka toimivat käyttäjätilassa eivätkä kernel-tasolla. Koska järjestelmälaajennukset toimivat käyttäjätilassa, ne lisäävät macOS:n vakautta ja turvallisuutta. Kernelin laajennuksilla on täysi pääsyoikeus koko käyttöjärjestelmään, mutta käyttäjätilassa toimivilla laajennuksilla on vain niiden oman toiminnon suorittamiseen tarvittavat oikeudet.

Sovelluskehysten, kuten DriverKit, EndpointSecurity ja NetworkExtension, avulla kehittäjät voivat kirjoittaa USB- ja HID-ajureita, päätelaitteiden suojaustyökaluja (kuten tietojen menettämisen estämisen agentit tai muut päätelaiteagentit) sekä VPN- ja verkkotyökaluja – täysin ilman kernelin laajennusten kirjoittamista. Kolmansien osapuolien suojausagentteja tulisi käyttää vain, jos ne hyödyntävät näitä API-rajapintoja tai jos niillä on vakaa suunnitelma siirtyä käyttämään niitä ja lopettaa kernelin laajennuksien käyttö.

Käyttäjän hyväksymä kernelin laajennusten lataus

Suojauksen parantamiseksi kernelin laajennuksien lataamiseen tarvitaan käyttäjän hyväksyntä, kun macOS 10.13 asennetaan tai kun macOS 10.13 on asennettu. Tätä prosessia kutsutaan *käyttäjän hyväksymäksi kernelin laajennusten latauksekseksi*. Kernelin laajennuksen hyväksyntään tarvitaan ylläpitäjän valtuutus. Kernelin laajennukset eivät tarvitse valtuutusta seuraavissa tapauksissa:

- Ne on asennettu Maciin, kun siinä on ollut macOS 10.12 tai vanhempi.
- Laajennukset korvaavat aikaisemmin hyväksyttyjä laajennuksia.
- Niiden latautuminen on sallittu ilman käyttäjän suostumusta käytettäessä `spctl`-komentorivityökalua, joka on saatavilla käynnistettäessä Mac recoveryOS:stä.
- Niiden lataaminen sallitaan mobiililaitteen hallintamäärityksellä (MDM).

  macOS 10.13.2:sta alkaen käyttäjät voivat määrittää MDM:llä luettelon kernelin laajennuksista, jotka latautuvat ilman käyttäjän hyväksyntää. Tämä valinta edellyttää Macia, jossa on macOS 10.13.2 ja joka on rekisteröity MDM:ään Apple School Managerilla, Apple Business Managerilla tai käyttäjän tekemällä MDM-rekisteröinnillä.

Optio-ROMin suojaus macOS:ssä

Huomaa: Apple siliconilla varustettu Mac ei tällä hetkellä tue optio-ROMeja.

Optio-ROMin suojaus Apple T2 Security -sirulla varustetussa Macissa

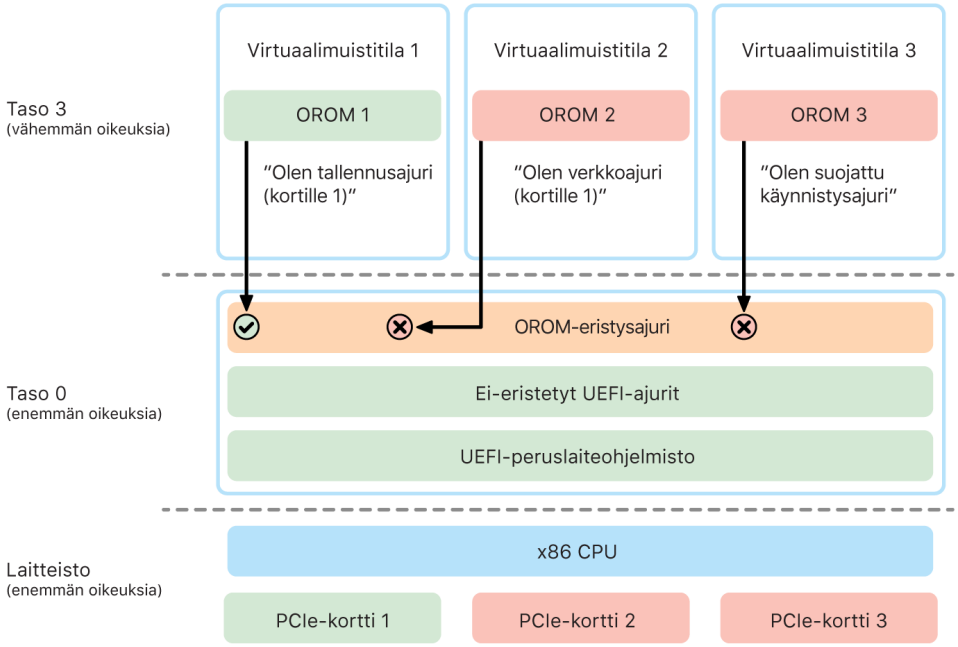
Thunderbolt- ja PCIe-laitteissa voi olla ”optio-ROM (OROM)” fyysisesti liitettynä laitteeseen. (Tämä ei yleensä ole oikea ROM, vaan se on uudelleenkirjoitettava siru, johon on tallennettu laiteohjelmisto.) UEFI-pohjaisissa järjestelmissä laiteohjelmisto on yleensä UEFI-ajuri, jonka UEFI-laiteohjelmisto lukee ja suorittaa. Suoritetun koodin pitäisi valmistella ja määrittää laitteisto, josta se on haettu, jotta laitteisto voidaan antaa muun laiteohjelmiston käyttöön. Tätä ominaisuutta tarvitaan, jotta erikoistuneet muun valmistajan laitteistot voivat ladata ja toimia käynnistyksen aikaisimmissa vaiheissa (esimerkiksi käynnistyä ulkoisista RAID-pakoista).

OROMit ovat kuitenkin yleensä uudelleenkirjoitettavia, joten jos hyökkääjä korvaa hyväksytyn oheislaitteen OROMin, hyökkääjän koodi suoritetaan käynnistysprosessin aikaisessa vaiheessa, jolloin hyökkääjä voi peukaloida suoritusympäristöä ja vahingoittaa myöhemmin ladattavan ohjelmiston eheyttä. Samoin jos hyökkääjä ottaa oman haittalaitteensa käyttöön järjestelmässä, hän voi suorittaa haitallista koodia.

macOS 10.12.3:ssa vuoden 2011 jälkeen myytyjen Mac-tietokoneiden toimintaa muutettiin siten, että OROMeja ei suoriteta oletuksena Macin käynnistyksessä, jollei tiettyä näppäinyhdistelmää paineta. Tämä näppäinyhdistelmä suojasi haitallisten OROMien tahattomalta käyttöönotolta macOS:n käynnistysvaiheessa. Myös laiteohjelmiston salasanatyökalun oletustoimintaa muutettiin siten, että kun käyttäjä on asettanut laiteohjelmiston salasanan, OROMeja ei voida suorittaa, vaikka näppäinyhdistelmää painettaisiin. Tämä esti fyysistä hyökkääjää ottamasta tarkoituksella käyttöön haitallista OROMia. Käyttäjät, joiden täytyy edelleen käyttää OROMeja, kun laiteohjelmiston salasana on asetettuna, voivat määrittää ei-oletusarvoisen vaihtoehdon `firmwarepasswd`-komentorivityökalulla macOS:ssä.

OROM-eristys suojauskeinona

macOS 10.15:ssä UEFI-laiteohjelmistoon päivitettiin OROMien eristys ja niiden oikeuksien poisto. UEFI-laiteohjelmisto suorittaa yleensä kaiken koodin, mukaan lukien OROMit, prosessorin maksimioikeustasolla 0 ja käyttää yhtä jaettua virtuaalimuistitilaa kaikille koodeille ja tiedoille. Taso 0 on oikeustaso, jolla macOS-kernel toimii, kun taas apit toimivat matalammalla oikeustasolla, tasolla 3. OROM-eristys poistaa OROMien oikeudet hyödyntämällä virtuaalista muistinerotusta samalla tavalla kuin kernel ja sitten laittamalla OROMit toimimaan tasolla 3.



Eristys lisäksi rajoittaa merkittävästi liittymiä, joita OROMit voivat kutsua (mikä muistuttaa kerneleiden järjestelmäkutsujen rajoittamista) ja laitetyyppiä, joksi OROM voi rekisteröityä (mikä muistuttaa appien hyväksyntää). Tämän mallin etuna on, että haitalliset OROMit eivät voi enää kirjoittaa suoraan minne tahansa tason 0 muistissa. Sen sijaan ne on rajoitettu erittäin kapeaan ja tarkasti määritettyyn eristykseen. Tämä rajoitettu käyttöliittymä pienentää merkittävästi hyökkäysmahdollisuuksia ja pakottaa hyökkääjät ensin pääsemään pois eristyksestä ja laajentamaan oikeuksiaan.

UEFI-laiteohjelmiston suojaus Intel-pohjaisessa Macissa

Apple T2 Security -sirulla varustetussa Intel-pohjaisessa Macissa on suojaus, jossa käytetään UEFI-laiteohjelmistoa (Intel).

Yleiskatsaus

Vuodesta 2006 alkaen Mac-tietokoneet, joissa on Intel-pohjainen prosessori, ovat käyttäneet Intel-laiteohjelmistoa, joka perustuu EFI-käyttöliittymän (Extensible Firmware Interface) EDK-kehityspaketin versioon 1 tai 2. EDK2-pohjainen koodi noudattaa UEFI (Unified Extensible Firmware Interface) -määrityksiä. Tässä osiossa Intel-laiteohjelmistoa kutsutaan *UEFI-laiteohjelmistoksi*. UEFI-laiteohjelmisto oli ensimmäinen Intel-sirulla suoritettava koodi.

Intel-pohjaisessa Macissa, jossa ei ole Apple T2 Security -sirua, UEFI-laiteohjelmiston luottamuksen perusta on siru, jonne laiteohjelmisto on tallennettu. Apple allekirjoittaa UEFI-laiteohjelmistopäivitykset digitaalisesti ja laiteohjelmisto tarkistaa tämän allekirjoituksen ennen päivitystä. Heikennyshyökkäyksiä auttaa estämään se, että päivityksissä täytyy aina olla uudempi versio kuin nykyinen versio. Hyökkääjä, jolla on fyysinen pääsy Maciin, voisi kuitenkin mahdollisesti päästä laitteiston avulla käsiksi laiteohjelmiston muistisiruun ja päivittää siruun haitallista sisältöä. Samalla tavoin jos haavoittuvuuksia löydetään UEFI-laiteohjelmiston käynnistyksen alkuvaiheesta (ennen kuin se estää kirjoittamisen muistisirulle), tämä voisi johtaa UEFI-laiteohjelmiston pysyvään tartuntaan. Tämä on laitteiston arkkitehtoninen rajoitus, joka on yhteinen useimmille Intel-pohjaisille PC-tietokoneille. Se on olemassa myös kaikissa Intel-pohjaisissa Mac-tietokoneissa, joissa ei ole T2-sirua.

UEFI-laiteohjelmistoa muuttavien fyysisten hyökkäysten estämiseksi Mac-tietokoneiden arkkitehtuuri uudistettiin siten, että UEFI-laiteohjelmiston luottamuksen perusta on T2-sirussa. Näissä Mac-tietokoneissa UEFI-laiteohjelmiston luottamuksen perusta (RoT) on T2-laiteohjelmisto, kuten osiossa Intel-pohjaisen Macin käynnistysprosessi kerrotaan.

Intel Management Engine (ME) -alikomponentti

Yksi UEFI-laiteohjelmistoon tallennettu alikomponentti on *Intel ME (Management Engine)* -laiteohjelmisto. ME:tä (erillistä prosessoria ja alijärjestelmää Intel-siruilla) käytetään etupäässä ääni- ja videosisällön tekijänoikeussuojaukseen Macissa, jossa on vain Intel-pohjainen näytönohjain. Tämän alikomponentin hyökkäysmahdollisuuksien vähentämiseksi Intel-pohjaisessa Macissa on muokattu ME-laiteohjelmisto, josta useimmat komponentit on poistettu. Koska tuloksena oleva Macin ME-laiteohjelmisto on pienempi kuin oletusarvoinen minimikoonnos, jonka Intel tarjoaa, siinä ei enää ole monia tietoturvatutkijoiden aiemmin julkisesti arvostelemia komponentteja.

Järjestelmänhallintatila (SMM)

Intel-prosessoreissa on normaalista toiminnasta eroava erityinen suoritustila. Tämä *järjestelmänhallintatila (SMM)* tehtiin alun perin sellaisten toimintojen käsittelyyn, joissa aika on merkittävä tekijä, kuten virranhallinnan käsittelyyn. Mac-tietokoneet ovat aiemmin käyttäneet kyseisten tehtävien suorittamiseen erillistä mikro-ohjainta nimeltä *järjestelmänhallintayksikkö (SMC)*. Järjestelmänhallintayksikkö ei ole enää erillinen mikro-ohjain, vaan se on integroitu T2-siruun.

watchOS-järjestelmän suojaus

Apple Watch käyttää monia samoja laitteistoon pohjautuvia alustan suojausominaisuuksia, joita iOS ja iPadOS käyttävät. Apple Watch esimerkiksi:

- suorittaa suojatun käynnistyksen ja suojatut ohjelmistopäivitykset
- ylläpitää käyttöjärjestelmän eheyttä
- auttaa suojaamaan tiedot sekä laitteessa että viestiessään pariksi asetetun iPhonen kanssa tai internetin kautta

Siinä ovat tuettuja Järjestelmän suojaus -osiossa luetellut teknologiat (kuten kernelin eheyden suojaus, sinetöity avaimen suojaus ja SCIP) sekä tietojen suojaus, avainnippu ja verkkoteknologiat.

watchOS:n päivittäminen

watchOS voidaan määrittää päivittymään yön aikana. Jos haluat lisätietoja siitä, kuinka Apple Watchin pääsykoodi tallennetaan ja sitä käytetään päivityksen aikana, katso Avainvarastot.

Ranteentunnistus

Jos ranteentunnistus on käytössä, laite lukittuu automaattisesti pian sen jälkeen, kun käyttäjä ottaa sen pois ranteestaan. Jos ranteentunnistus on pois käytöstä, Apple Watch voidaan lukita Ohjauskeskuksesta. Kun Apple Watch on lukittu, Apple Payta voidaan käyttää ainoastaan syöttämällä pääsykoodi Apple Watchissa. Ranteentunnistus laitetaan pois päältä iPhonen Apple Watch -apilla. Tämä asetus voidaan määrittää myös mobiililaitteen hallintaratkaisulla (MDM).

Aktivointilukitus

Kun Missä on…? -toiminto on laitettu päälle iPhonessa, sen pariksi asetettu Apple Watch voi käyttää aktivointilukitusta. Aktivointilukitus vaikeuttaa kadonneen tai varastetun Apple Watchin käyttämistä tai myymistä. Aktivointilukitus vaatii käyttäjän Apple ID:n ja salasanan Apple Watchin laiteparin poistamiseen, tyhjentämiseen tai uudelleenaktivointiin.

Suojattu parinmuodostus iPhonen kanssa

Apple Watch voi olla kerralla vain yhden iPhonen parina. Kun Apple Watch -pari puretaan, iPhone antaa ohjeet kaiken sisällön ja kaikkien tietojen poistamiseen.

Apple Watchin ja iPhonen välinen parinmuodostus suojataan käyttämällä kaistan ulkopuolista prosessia julkisten avainten vaihtoon, jota seuraa Bluetooth Low Energy (BLE) -linkin jaettu salaisuus. Apple Watchissa näkyy animoitu kuvio, jonka iPhonen kamera lukee. Kuvio sisältää koodatun salaisuuden, jota käytetään kaistan ulkopuoliseen parinmuodostukseen BLE 4.1:n kautta. Tavallista BLE-pääsyavaimen syöttöä käytetään tarvittaessa parinmuodostuksen varamenetelmänä.

Kun BLE-istunto on muodostettu ja salattu Bluetooth Core Specification -määritysten korkeimmalla suojausprotokollalla, iPhone ja Apple Watch vaihtavat avaimia jommallakummalla seuraavista tavoista:

- Applen IDS-palvelusta (Apple Identity Service) mukautetulla prosessilla. Applen IDS-palvelu on kuvattu osiossa iMessagen suojauksen yleiskatsaus.
- IKEv2/IPSeciä käyttävällä avainten vaihdolla. Avainten vaihto alussa todennetaan käyttäen joko Bluetooth-istunnon avainta (kun muodostetaan laitepari) tai IDS-avaimia (kun käyttöjärjestelmä päivitetään). Kumpikin laite muodostaa satunnaisen julkisen ja yksityisen 256-bittisen Ed25519-avaimen parin, ja laitteet vaihtavat aluksi julkiset avaimet keskenään avaintenvaihtoprosessissa.

Huomaa: Avaintenvaihtoon ja salaukseen käytettävä mekanismi vaihtelee riippuen iPhonen ja Apple Watchin käyttöjärjestelmäversioista. iPhone-laitteet, joissa on iOS 13 tai uudempi, ja joiden pariksi asetetaan Apple Watch, jossa on watchOS 6 tai uudempi, käyttävät avaintenvaihtoon ja salauksen ainoastaan IKEv2/IPseciä.

Kun avaimet on vaihdettu:

- Bluetooth-istunnon avain hylätään ja kaikki tietoliikenne iPhonen ja Apple Watchin välillä salataan käyttäen toista edellä kerrotuista tavoista. Lisäksi salatut Bluetooth, Wi-Fi ja mobiililinkit tarjoavat toisen salaustason.
- (Vain IKEv2/IPsec) Avaimet tallennetaan Järjestelmä-avainnippuun ja niitä käytetään tulevien laitteiden välisten IKEv2/IPsec-istuntojen todentamiseen. Tästä eteenpäin tietoliikenne näiden laitteiden välillä salataan ja sen eheys suojataan käyttäen AES-256-GCM:ää tai ChaCha20-Poly1305:tä (256-bittiset avaimet) iPhone-laitteissa, joissa on iOS 15 tai uudempi ja joiden parina on Apple Watch Series 4 tai uudempi, jossa on watchOS 8 tai uudempi.

BLE-laiteosoitetta vaihdellaan 15 minuutin välein, jotta pienennetään riskiä, että laitetta seurattaisiin paikallisesti, jos joku lähettäisi pysyvää tunnistetta.

Suoratoistodataa tarvitsevien appien tukemiseksi tarjotaan salausta menetelmillä, jotka on kuvattu kohdassa FaceTimen suojaus. Menetelmissä käytetään joko pariksi liitetyn iPhonen tarjoamaa Applen IDS-palvelua tai suoraa internet-yhteyttä.

Apple Watch käyttää laitteiston salaamaa tallennustilaa sekä tiedostojen ja avainnipun kohteiden luokkaperusteista suojausta. Avainnipun kohteille käytetään myös avainvarastoja, joiden käyttöä hallitaan. Apple Watchin ja iPhonen väliseen tietoliikenteeseen käytetyt avaimet varmistetaan myös luokkaperusteisella suojauksella. Jos haluat lisätietoja, katso Tietojen suojauksen avainvarastot.

Automaattinen lukituksen avaaminen ja Apple Watch

Useamman Apple-laitteen käytön helpottamiseksi jotkin laitteet voivat automaattisesti avata toisten laitteiden lukituksen tietyissä tilanteissa. Automaattista lukituksen avaamista voidaan käyttää kolmella tavalla:

- iPhone voi avata Apple Watchin lukituksen.
- Apple Watch voi avata Macin lukituksen.
- Apple Watch voi avata iPhonen lukituksen, kun se tunnistaa käyttäjän, jonka nenä ja suu on peitetty.

Kaikki kolme käyttötapausta rakentuvat samalle perustalle: niissä käytetään molemmin puolin todennettavaa STS-protokollaa (Station-to-Station), ominaisuuden käyttöönoton yhteydessä vaihdetaan pitkäaikaiset avaimet ja jokaiselle pyynnölle sovitaan yksilölliset väliaikaiset istuntoavaimet. Pohjalla olevasta tiedonsiirtokanavasta riippumatta STS-tunneli sovitaan suoraan kummankin laitteen Secure Enclaven välillä ja kaikki kryptografinen materiaali pidetään tällä suojatulla alueella (lukuun ottamatta Mac-tietokoneita, joissa ei ole Secure Enclavea; niiden STS-tunneli päättyy kerneliin).

Lukituksen avaaminen

Lukituksen avaamisen kokonaisuus voidaan jakaa kahteen vaiheeseen. Ensin avattava laite (”kohde”) muodostaa avaamista varten kryptografisen salaisuuden ja lähettää sen lukituksen avaavalle laitteelle (”aloittaja”). Myöhemmin aloittaja avaa lukituksen aikaisemmin luotua salaisuutta käyttäen.

Laitteet yhdistyvät toisiinsa BLE-yhteydellä valmistellakseen lukituksen avaamiseen tarvittavat tiedot. Kohdelaitteen satunnaisesti luoma 32-tavuinen avaussalaisuus lähetetään aloittajalle STS-tunnelissa. Kun lukitus seuraavan kerran avataan biometrisella tunnisteella tai pääsykoodilla, kohdelaite salaa pääsykoodijohdetun avaimensa (PDK) avaussalaisuudella ja hävittää avaussalaisuuden muististaan.

Kun laitteet suorittavat lukituksen avaamisen, ne aloittavat uuden BLE-yhteyden ja käyttävät sitten vertais-Wi-Fiä arvioidakseen turvallisesti etäisyyden toisiinsa. Jos laitteet ovat vaaditun etäisyyden sisällä toisistaan ja tietoturvakäytäntöjen vaatimukset täyttyvät, aloittaja lähettää avaussalaisuutensa kohteelle STS-tunnelissa. Sen jälkeen kohde muodostaa uuden 32-tavuisen avaussalaisuuden ja lähettää sen aloittajalle. Jos aloittajan lähettämä nykyinen avaussalaisuus purkaa onnistuneesti lukituksenavaustietueen salauksen, kohdelaitteen lukitus avataan ja PDK-avain salataan uudelleen uudella avaussalaisuudella. Lopuksi uusi avaussalaisuus ja PDK-avain hävitetään kohteen muistista.

Apple Watchin automaattisen lukituksen avaamisen tietoturvakäytännöt

Jotta käyttö olisi vaivattomampaa, iPhone voi avata Apple Watchin suoraan alkukäynnistyksen jälkeen ilman että käyttäjän tarvitsee ensin syöttää pääsykoodia itse Apple Watchissa. Kun lukitus avataan ensimmäisen kerran tämän ominaisuuden käyttöönottamisen jälkeen, muodostetaan satunnainen avaussalaisuus, jota käyttäen luodaan pitkäaikainen vara-avaintietue, joka tallennetaan Apple Watchin avainvarastoon. Vara-avaintietueen salaisuus tallennetaan iPhonen avainnippuun ja sitä käytetään uuden istunnon aloittamiseen aina Apple Watchin uudelleenkäynnistyksen jälkeen.

iPhonen automaattisen lukituksen avaamisen tietoturvakäytännöt

iPhonen lukituksen automaattiseen avaamiseen Apple Watchilla sovelletaan tavallisten lisäksi ylimääräisiä tietoturvakäytäntöjä. Apple Watchia ei voida käyttää Face ID:n sijasta iPhonen muille toiminnoille, kuten Apple Paylle tai appien valtuuttamiselle. Kun Apple Watch on onnistuneesti avannut pariksi asetetun iPhonen lukituksen, kellossa näkyy ilmoitus ja se antaa avauksesta kertovan tuntopalautteen. Jos käyttäjä napauttaa ilmoituksessa Lukitse iPhone -painiketta, kello lähettää iPhonelle lukituskomennon BLE-yhteydellä. Kun iPhone vastaanottaa lukituskomennon, se lukittuu ja poistaa käytöstä sekä Face ID:n että lukituksen avaamisen Apple Watchilla. Seuraavaan iPhonen lukituksen avaamiseen tarvitaan iPhonen pääsykoodi.

Pariksi asetetun iPhonen lukituksen avaaminen Apple Watchilla (kun toiminto on otettu käyttöön) edellyttää seuraavien vaatimusten täyttymistä:

- iPhonen lukitus on pitänyt avata toisella tavalla ainakin kerran sen jälkeen, kun siihen liitetty Apple Watch on kiinnitetty ranteeseen ja sen lukitus on avattu.
- Tunnistinten on pystyttävä havaitsemaan, että käyttäjän nenä ja suu on peitetty.
- Mitattu etäisyys saa olla enintään 2–3 metriä.
- Apple Watch ei saa olla unitilassa.
- Apple Watchin tai iPhonen lukitus on pitänyt avata äskettäin tai Apple Watchin on pitänyt havaita fyysistä liikettä, joka kertoo käyttäjän olevan aktiivinen (eikä esimerkiksi nukkumassa).
- iPhonen lukitus on pitänyt avata vähintään kerran viimeisten 6,5 tunnin aikana.
- iPhonen on oltava sellaisessa tilassa, jossa lukituksen avaaminen Face ID:llä on sallittu. (Jos haluat lisätietoja tästä, katso Face ID, Touch ID, pääsykoodit ja salasanat.)

Hyväksynnän antaminen macOS:ssä Apple Watchilla

Kun automaattinen lukituksen avaaminen Apple Watchilla on käytössä, Apple Watchia voidaan käyttää Touch ID:n sijasta tai sen kanssa seuraavien valtuutus- ja todentamispyyntöjen hyväksymiseen:

- macOS ja Applen apit, jotka pyytävät valtuutusta
- muiden valmistajien apit, jotka pyytävät todentamista
- tallennetut Safari-salasanat
- Suojatut muistiinpanot

Suojattu Wi-Fin, mobiiliyhteyden, iCloudin ja Gmailin käyttö

Kun Apple Watch ei ole Bluetoothin kantaman alueella, Wi-Fiä tai mobiilidataa voidaan käyttää sen sijaan. Apple Watch liittyy automaattisesti Wi-Fi-verkkoihin, joihin on liitytty pariksi liitetyllä iPhonella ja joiden tunnistetiedot on synkronoitu Apple Watchiin, kun molemmat laitteet ovat olleet kantaman alueella. Automaattinen liittymistoiminto voidaan määrittää verkkokohtaiseksi Apple Watchin Asetukset-apin Wi-Fi-osiossa. Wi-Fi-verkkoihin, joihin ei ole liitytty koskaan aiemmin kummallakaan laitteella, voidaan liittyä käsin Apple Watchin Asetukset-apin Wi-Fi-osiossa.

Kun Apple Watch ja iPhone ovat kantaman ulkopuolella, Apple Watch hakee sähköpostit yhdistämällä suoraan iCloudin ja Gmailin palvelimille, eikä synkronoi sähköpostitietoja pariksi liitetyllä iPhonella internetin kautta. Gmail-tileissä käyttäjän täytyy todentautua Googlelle iPhonen Apple Watch -apin Mail-osiossa. Googlelta saatu OAuth-tunniste lähetetään Apple Watchiin salattuna Applen IDS-palvelulla, jotta sitä voidaan käyttää sähköpostin hakemiseen. Tätä OAuth-tunnistetta ei koskaan käytetä yhteyden muodostamiseen Gmail-palvelimen kanssa pariksi liitetystä iPhonesta.

Satunnaislukujen generointi

Kryptografiset näennäissatunnaislukugeneraattorit (cryptographic pseudo-random number generator, CPRNG) ovat tärkeä osa turvallista ohjelmistoa. Tätä varten Apple tarjoaa ohjelmiston kryptografisen näennäissatunnaislukugeneraattorin, joka toimii iOS-, iPadOS-, macOS-, tvOS- ja watchOS-kerneleissä. Se kerää entropiaa järjestelmästä ja tarjoaa turvalliset satunnaisluvut kuluttajille kernelissä ja käyttäjätilassa.

Entropialähteet

Kernelin kryptografinen näennäissatunnaislukugeneraattori siemennetään useista entropialähteistä käynnistyksen ja laitteen käyttöiän aikana. Näitä ovat (riippuen saatavuudesta):

- Secure Enclaven laitteisto-TRNG
- Käynnistyksen aikana kerätty ajoitusperusteinen värinä
- Laitekeskeytyksistä kerätty entropia
- Siementiedosto, jota käytetään entropian säilyttämiseen käynnistyksien välillä
- Intelin satunnaiskäskyt, esimerkiksi RDSEED ja RDRAND (vain Intel-pohjainen Mac)

Kernelin kryptografinen näennäissatunnaislukugeneraattori

Kernelin kryptografinen näennäissatunnaislukugeneraattori on Fortunasta johdettu malli, joka tähtää 256-bittiselle suojaustasolle. Se tarjoaa laadukkaita satunnaislukuja käyttäjätilan kuluttajille seuraavien API:en kautta:

- `getentropy`(2)-järjestelmäkutsu
- Näennäissatunnaislukulaite (/dev/random)

Kernelin kryptografinen näennäissatunnaislukugeneraattori hyväksyy käyttäjän toimittamaa entropiaa näennäissatunnaislukulaitteeseen kirjoituksen kautta.

Applen tietoturvatutkimuslaite

Applen tietoturvatutkimuslaite on erityisen suojauselementin sisältävä iPhone, jossa tietoturvatutkijat voivat tutkia iOS-järjestelmää ilman, että heidän tarvitsee murtaa tai poistaa käytöstä iPhone-alustan suojausominaisuuksia. Tutkijat voivat itse ladata tällaiseen laitteeseen sisältöä, joka toimii alustan kaltaisin oikeuksin. Tällä tavoin he voivat tehdä tutkimusta alustalla, joka vastaa paremmin tavallisessa tuotannossa olevia laitteita.

Tietoturvatutkimuslaitteiden suorituskäytännön muutokset toteutetaan iBootin muunnelmalla ja käynnistyskernelkokoelmassa. Tämä auttaa varmistamaan, että tietoturvatutkimuslaitteiden suorituskäytäntö ei vaikuta käyttäjälaitteisiin. Muunnelmat eivät käynnisty käyttäjälaitteistossa. Tutkimuskäyttöön tarkoitettu iBoot tarkistaa, että laitteessa on uusi suojauselementin tila, ja menee paniikkisilmukkaan, jos sitä suoritetaan laitteistossa, joka ei ole tarkoitettu tutkimuskäyttöön.

Cryptex-alijärjestelmä mahdollistaa tutkijalle yksilöllisen luottamusvälimuistin ja vastaavan sisällön sisältävän levytiedoston lataamisen. Käytössä on useita kerrostetun suojauksen keinoja, jotka on suunniteltu varmistamaan, että tämä alijärjestelmä ei salli suorittamista käyttäjien laitteissa:

- `launchd` ei lataa `cryptexd`:n launchd-ominaisuusluetteloa, jos se havaitsee tavallisen asiakaslaitteen.
- `cryptexd` keskeyttää toiminnan, jos se havaitsee tavallisen asiakaslaitteen.
- `AppleImage4` ei kaupittele tutkimus-cryptexin tarkistamiseen käytettävää noncea tavallisessa asiakaslaitteessa.
- Allekirjoituspalvelin kieltäytyy antamasta yksilöllistä allekirjoitusta cryptex-levytiedostolle laitteeseen, joka ei ole nimenomaisesti sallittujen luettelossa.

Tietoturvatutkijan yksityisyyden turvaamiseksi Applelle lähetetään yksilöinnin aikana ainoastaan suoritustiedostojen tai kernelvälimuistin mittaukset (esimerkiksi tiivisteet) ja tietoturvatutkimuslaitteen tunnisteet. Apple ei saa laitteeseen ladattavan krypteksin sisältöä.

Sen estämiseksi, että pahantahtoinen taho yrittäisi naamioida tutkimuslaitteen käyttäjälaitteeksi huijatakseen kohteen käyttämään sitä tavanomaisessa käytössä, tietoturvatutkimuslaite eroaa käyttäjälaitteesta seuraavilla tavoilla:

- Tietoturvatutkimuslaitteet käynnistyvät vain, kun niihin ladataan virtaa. Tähän voidaan käyttää Lightning-kaapelia tai Qi-yhteensopivaa laturia. Jos laitteeseen ei ladata virtaa käynnistyksen aikana, se menee palautustilaan. Jos käyttäjä aloittaa virran latauksen ja käynnistää laitteen uudelleen, se käynnistyy normaalisti. Kun XNU käynnistyy, laitteen ei tarvitse enää latautua, jotta sen toiminta jatkuu.
- iBoot-käynnistyksen aikana Apple-logon alla näkyy teksti *Tietoturvan tutkimuslaite*.
- XNU-kernel käynnistyy yksityiskohtaiset tiedot näyttävässä tilassa.
- Laitteen sivuun on kaiverrettu viesti: "Property of Apple. Confidential and Proprietary. Call +1 877 595 1125."

Käynnistyksen jälkeen näkyviin tulevassa ohjelmistossa käytetään lisäksi seuraavia keinoja:

- Laitteen käyttöönoton aikana näkyy teksti *Tietoturvantutkimuslaite*.
- Lukitulla näytöllä ja Asetukset-apissa näkyy teksti *Tietoturvantutkimuslaite*.

Tietoturvatutkimuslaitteissa tutkijat voivat tehdä seuraavia asioita, joita käyttäjälaitteissa ei voi tehdä. Tutkijat voivat

- ladata itse laitteeseen suoritettavaa koodia vapaasti määritettävillä oikeuksilla käyttäen samaa oikeustasoa kuin Applen käyttöjärjestelmäkomponentit
- käynnistää palveluita käynnistyksen yhteydessä
- saada sisällön pysymään läpi uudelleenkäynnistysten
- käyttää `research.com.apple.license-to-operate`-oikeutta salliakseen prosessin tehdä vianmääritystä mille tahansa muulle prosessille järjestelmässä, mukaan lukien järjestelmäprosessit.

  Ainoastaan RESEARCH-variantti kernelin laajennuksesta AppleMobileFileIntegrity kunnioittaa nimiavaruutta `research.`; asiakaslaitteessa mikä tahansa prosessi, jolla on tämä oikeutus, lopetetaan allekirjoituksen tarkistuksen aikana.
- yksilöidä ja palauttaa muokatun kernelvälimuistin.

Salaus ja tietojen suojaus

Salauksen ja tietojen suojauksen yleiskatsaus

Suojatun käynnistysketjun, järjestelmän suojauksen ja appien suojauksen ominaisuudet auttavat tarkistamaan, että laitteessa suoritetaan vain luotettua koodia ja appeja. Applen laitteissa on lisäsalausominaisuuksia, jotka suojaavat käyttäjän tietoja silloinkin, kun muut suojausinfrastruktuurin osat ovat vaarantuneet (esimerkiksi jos laite katoaa tai jos siinä suoritetaan ei-luotettua koodia). Nämä ominaisuudet hyödyttävät sekä käyttäjiä että IT-ylläpitäjiä, sillä henkilökohtaiset ja yrityksen tiedot ovat suojattuina, ja jos laite varastetaan tai se katoaa, saatavilla on menetelmiä, joilla se voidaan tyhjentää välittömästi kokonaan etänä.

iOS- ja iPadOS-laitteet käyttävät tiedostonsalausmenetelmää nimeltä *tietojen suojaus*, kun taas Intel-pohjaisen Macin tiedot on suojattu taltionsalausteknologialla nimeltä *FileVault*. Apple siliconilla varustettu Mac käyttää hybridimallia, joka tukee tietojen suojausta. Siinä on kuitenkin kaksi huomioitavaa ominaisuutta: Matalinta suojaustasoa (luokka D) ei tueta, ja oletustaso (luokka C) käyttää taltioavainta ja toimii aivan kuin FileVault Intel-pohjaisessa Macissa. Kaikissa tapauksissa avaintenhallintahierarkioiden juurihakemisto on Secure Enclaven erillisessä sirussa, ja erillinen AES-komponentti tukee linjanopeudella toimivaa salausta ja auttaa varmistamaan, että pitkäaikaisia salausavaimia ei tarjota kernelin käyttöjärjestelmälle tai prosessorille (jossa ne voisivat vaarantua). (Intel-pohjainen Mac, jossa on T1 tai jossa ei ole Secure Enclavea, ei käytä erillistä sirua FileVaultin salausavaimiensa suojaamiseen.)

Sen lisäksi, että tietojen suojaus ja FileVault auttavat torjumaan luvatonta tietojen käyttöä, Apple käyttää *käyttöjärjestelmän kerneleitä* huolehtimaan osaltaan suojauksesta ja tietoturvasta. Kernel käyttää pääsynhallintaa appien eristykseen (millä rajoitetaan sitä, mihin tietoihin appi pääsee) sekä mekanismia nimeltä *tietosäiliö* (sen sijaan, että rajoitettaisiin, mitä kutsuja jokin appi voi tehdä, tämä mekanismi rajoittaa kaikkien muiden pyytävien appien pääsyä apin tietoihin).

Pääsykoodit ja salasanat

Apple käyttää pääsykoodeja iOS:ssä ja iPadOS:ssä ja salasanoja macOS:ssä suojaamaan käyttäjän tietoja pahantahtoiselta hyökkäykseltä. Mitä pidempi pääsykoodi tai salasana on, sitä vahvempi se on ja sitä helpommin sillä voidaan estää väsytyshyökkäykset. Apple hankaloittaa hyökkäyksiä vielä lisää pakotetuilla viiveillä (iOS:lle ja iPadOS:lle) ja rajoittamalla salasanayritysten määrää (Macille).

Kun käyttäjä ottaa laitteen pääsykoodin tai salasanan käyttöön iOS:ssä tai iPadOS:ssä, hän samalla ottaa automaattisesti käyttöön tietojen suojauksen. Tietojen suojausta käytetään myös muissa laitteissa, joissa on Applen järjestelmäpiiri (SoC). Näitä ovat Apple siliconilla varustettu Mac, Apple TV ja Apple Watch. macOS:ssä Apple käyttää ohjelmistoon sisältyvää taltionsalausohjelmaa nimeltä *FileVault*.

Miten vahvat salasanat ja pääsykoodit parantavat suojausta

iOS ja iPadOS tukevat kuusinumeroisia, nelinumeroisia ja halutun pituisia aakkosnumeerisia pääsykoodeja. Pääsykoodi tai salasana avaa laitteen, mutta toimii myös eräiden salausavainten entropiana. Tämän ansiosta hyökkääjä, jolla on laite hallussaan, ei saa tietyissä suojausluokissa olevia tietoja ilman pääsykoodia.

Pääsykoodi tai salasana on sidottu laitteen UID:hen, joten väsytyshyökkäykset on tehtävä kohteena olevalla laitteella. Suurilla toistomäärillä näistä yrityksistä tehdään hitaampia. Toistomäärä kalibroidaan niin, että yksi yritys kestää noin 80 millisekuntia. Kaikkien mahdollisten pieniä kirjaimia ja numeroita sisältävien kuusimerkkisten pääsykoodien kokeileminen kestäisi peräti yli 5,5 vuotta.

Mitä vahvempi käyttäjän pääsykoodi on, sitä vahvemmaksi salausavain tulee. Käyttäessään Face ID:tä ja Touch ID:tä käyttäjä voi luoda paljon vahvemman pääsykoodin kuin mikä muuten olisi käytännöllistä. Vahvempi pääsykoodi lisää entropian todellista määrää, mikä suojaa tietojen suojaukseen käytettäviä salausavaimia haittaamatta laitteen useita kertoja päivässä tehtävän avauksen käyttökokemusta.

Jos syötetään pitkä salasana, joka sisältää vain numeroita, lukitulla näytöllä näytetään vain numeronäppäimistö eikä täyttä näppäimistöä. Pidempi numeerinen pääsykoodi voi olla helpompaa syöttää kuin lyhyempi aakkosnumeerinen pääsykoodi, mutta se tarjoaa vastaavan suojaustason.

Käyttäjät voivat määrittää pidemmän aakkosnumeerisen pääsykoodin valitsemalla Pääsykoodivalinnat-kohdassa Asetukset > ”Touch ID ja pääsykoodi” tai ”Face ID ja pääsykoodi” ja valitsemalla sitten Aakkosnumeerinen koodi.

Miten pitenevä viive hankaloittaa väsytyshyökkäyksiä (iOS, iPadOS)

iOS:ssä ja iPadOS:ssä pääsykoodin väsytyshyökkäysten hankaloittamiseksi väärän pääsykoodin syöttämisestä lukitulla näytöllä seuraa pitenevä aikaviive alla olevan taulukon mukaisesti.

Yritykset	Toteutettu viive
1–4	ei mitään
5	1 minuutti
6	5 minuuttia
7–8	15 minuuttia
9	1 tunti

Jos Poista data -valinta on käytössä (valitaan kohdassa Asetukset > Touch ID ja pääsykoodi), kymmenen peräkkäisen virheellisen pääsykoodin syöttöyrityksen jälkeen kaikki tallennettu sisältö ja asetukset poistetaan. Saman väärän pääsykoodin peräkkäisiä syöttöyrityksiä ei lasketa. Tämä asetus on saatavilla myös ylläpitokäytäntönä käyttäen tätä ominaisuutta tukevaa mobiililaitteiden hallintaratkaisua (MDM) tai käyttäen Microsoft Exchange ActiveSyncia. Asetuksen raja voidaan määrittää myös pienemmäksi.

Laitteissa, joissa on Secure Enclave, viiveet toteuttaa Secure Enclave. Jos laite käynnistetään uudelleen ajoitetun viiveen aikana, viive on silti käytössä ja ajastin aloittaa kuluvan jakson alusta.

Miten pitenevä viive hankaloittaa väsytyshyökkäyksiä (macOS)

Väsytyshyökkäyksiä auttaa estämään se, että Macin käynnistyksessä sallitaan enintään 10 salasanayritystä sisäänkirjautumisikkunassa tai käytettäessä kohdelevytilaa. Riittävä määrä vääriä yrityksiä aiheuttaa pitenevät aikaviiveet. Viiveet toteuttaa Secure Enclave. Jos Mac käynnistetään uudelleen ajoitetun viiveen aikana, viive on silti käytössä ja ajastin aloittaa kuluvan jakson alusta.

Alla olevassa taulukossa näkyvät salasanayritysten väliset viiveet Apple siliconilla tai T2-sirulla varustetussa Macissa.

Yritykset	Toteutettu viive
5	1 minuutti
6	5 minuuttia
7	15 minuuttia
8	15 minuuttia
9	1 tunti
10	Pois käytöstä

Jotta haittaohjelmiston olisi vaikeampi aiheuttaa pysyvää tietojen menetystä yrittämällä hyökätä käyttäjän salasanaan, nämä rajoitukset eivät ole käytössä sen jälkeen, kun käyttäjä kirjautuu onnistuneesti sisään Maciin, mutta ne palautetaan taas uudelleenkäynnistyksen jälkeen. Jos 10 yritystä on käytetty, käytettävissä on 10 lisäyritystä, kun laite on käynnistetty recoveryOS:ään. Jos myös nämä yritykset on käytetty, käytettävissä on 10 lisäyritystä jokaista FileVault-palautusmekanismia kohden (iCloud-palautus, FileVault-palautusavain ja organisaation avain), jolloin lisäyrityksiä on enimmillään 30. Sen jälkeen kun nämä lisäyritykset on käytetty, Secure Enclave ei enää käsittele pyyntöjä purkaa taltion salaus tai vahvistaa salasana, ja levyn tietoja ei voida palauttaa.

Auttaakseen pitämään tiedot suojattuina yritysympäristössä IT-osaston tulisi määrittää FileVault-asetuskäytännöt käyttäen MDM-ratkaisua. Organisaatiot voivat hallita salattuja taltioita useilla eri tavoilla, kuten organisaation palautusavaimilla, henkilökohtaisilla palautusavaimilla (jotka voidaan valinnaisesti tallentaa MDM:llä) tai niiden yhdistelmällä. Avaimen kierrättäminen voidaan myös asettaa käytännöksi MDM:llä.

Apple T2 Security -sirulla varustetussa Macissa salasanalla on samanlainen tehtävä, mutta muodostettua avainta käytetään tietojen suojaus -teknologian sijaan FileVault-salaukselle. macOS tarjoaa myös enemmän salasanan palautusvaihtoehtoja:

- iCloud-palautus
- FileVault-palautus
- organisaation FileVault-avain

Tietojen suojaus

Tietojen suojauksen yleiskatsaus

Apple käyttää teknologiaa nimeltä tietojen suojaus, jolla suojataan flash-muistiin tallennettuja tietoja Applen järjestelmäpiirin sisältävissä laitteissa, kuten iPhonessa, iPadissa, Apple Watchissa, Apple TV:ssä ja Apple siliconilla varustetussa Macissa. Tietojen suojauksen ansiosta laite voi reagoida yleisiin tapahtumiin, kuten saapuviin puheluihin, mutta samalla käyttäjätiedot voidaan salata korkeatasoisesti. Tietyt järjestelmäapit (kuten Viestit, Mail, Kalenteri, Yhteystiedot ja Kuvat) sekä Terveys-apin data-arvot käyttävät oletuksena Tietojen suojausta. Muiden valmistajien apit saavat tämän suojauksen automaattisesti.

Toteutus

Tietojen suojaus toteutetaan luomalla ja hallitsemalla avainhierarkiaa. Se perustuu laitteiston salausteknologioihin, jotka on sisäänrakennettu Applen laitteisiin. Tietojen suojausta hallitaan tiedostokohtaisesti määrittämällä jokaiselle tiedostolle luokka. Saatavuus määritetään sillä perusteella, onko luokka-avaimet avattu. APFS:n (Apple File System) ansiosta tiedostojärjestelmä voi jakaa avaimet alakategorioihin tilakohtaisesti (tiedoston osioilla voi olla eri avaimet).

Aina, kun datataltioon luodaan tiedosto, tietojen suojaus luo uuden 256-bittisen avaimen (*tiedostokohtainen avain*) ja antaa sen laitteiston AES-komponentille, joka salaa tiedoston tällä avaimella, kun se kirjoitetaan flash-muistiin. A14- ja A15-laitteissa ja M1-perheen laitteissa salaus käyttää AES-256:ta XTS-tilassa. Siinä 256-bittiseen tiedostokohtaiseen avaimeen käytetään avaimen derivointifunktiota (NIST Special Publication 800-108), jotta saadaan 256-bittinen tweak-avain ja 256-bittinen salausavain. Laitteistosukupolvet A9:stä A13:een sekä S5, S6 ja S7 käyttävät AES-128:aa XTS-tilassa. Siinä 256-bittinen tiedostokohtainen avain jaetaan, jotta saadaan 128-bittinen tweak-avain ja 128-bittinen salausavain.

Apple siliconilla varustetussa Macissa tietojen suojauksen oletusluokka on C (katso Tietojen suojausluokat), mutta se käyttää tilakohtaisen tai tiedostokohtaisen avaimen sijaan taltioavainta. Tämä luo käyttäjätiedoille käytännössä FileVaultin suojausmallin. Käyttäjien täytyy silti edelleen valita FileVault käyttöön, jotta he saavat täyden suojauksen, jossa salausavainhierarkia sidotaan heidän salasanaansa. Kehittäjät voivat myös valita korkeamman suojausluokan, joka käyttää tiedosto- tai tilakohtaista avainta.

Tietojen suojaus Apple-laitteissa

Tietojen suojausta käyttävissä Apple-laitteissa kutakin tiedostoa suojaa yksilöllinen tiedostokohtainen (tai tilakohtainen) avain. NIST AED -avaimensalausalgoritmia käyttäen salattu avain salataan edelleen yhdellä useista luokka-avaimista riippuen siitä, miten tiedostoon on tarkoitus päästä. Salattu tiedostokohtainen avain tallennetaan tiedoston metadataan.

Laitteet, joissa on APFS, voivat tukea tiedostojen kloonausta (nollakopiot CoW (copy-on-write) -teknologialla). Jos tiedosto on kloonattu, molemmat kloonin osat saavat uuden avaimen tiedostoon kirjoittamisen hyväksymiseen, jotta uudet tiedot kirjoitetaan tallennuslaitteeseen uudella avaimella. Ajan myötä tiedosto voi koostua eri tiloista (tai osista), jotka kuuluvat eri avaimiin. Kaikkia laajennoksia, joista tiedosto koostuu, suojataan kuitenkin samalla luokka-avaimella.

Kun tiedosto avataan, sen metadatan salaus puretaan tiedostojärjestelmän avaimella, ja näin saadaan salattu tiedostokohtainen avain ja merkintä siitä, mikä luokka sitä suojaa. Tiedostokohtaisen (tai tilakohtaisen) avaimen salaus poistetaan luokan avaimella ja se toimitetaan laitteiston AES-komponentille, joka purkaa tiedoston salauksen, kun se luetaan flash-muistista. Kaikki salattujen tiedostoavainten käsittely tapahtuu Secure Enclavessa. Tiedostoavainta ei koskaan paljasteta suoraan appeja suorittavalle prosessorille. Käynnistyksen aikana Secure Enclave sopii väliaikaisen avaimen AES-komponentin kanssa. Kun Secure Enclave purkaa tiedoston avaimien salauksen, ne salataan uudelleen lyhytaikaisella avaimella ja lähetetään takaisin appeja suorittavalle prosessorille.

Kaikkien datataltion tiedostojärjestelmässä olevien tiedostojen metatiedot salataan satunnaisella taltioavaimella, joka luodaan, kun käyttöjärjestelmä asennetaan ensimmäisen kerran tai kun käyttäjä tyhjentää laitteen. Tämä avain salataan ja paketoidaan pitkäaikaista säilytystä varten avaimen salaavalla avaimella, jonka tietää vain Secure Enclave. Avaimen salaava avain vaihtuu joka kerran, kun käyttäjä tyhjentää laitteen. Secure Enclave on A9-järjestelmäpiireissä (ja uudemmissa) riippuvainen entropiasta, jota tukevat uudelleentoiston estävät järjestelmät, pyyhittävyyden mahdollistamiseksi ja sen avaimen salaavan avaimen sekä muiden resurssien suojaamiseksi. Jos haluat lisätietoja, katso Suojattu pysyvä tallennustila.

Tiedostokohtaisten tai tilakohtaisten avainten tapaan myöskään datataltion metatietojen avainta ei koskaan paljasteta suoraan appeja suorittavalle prosessorille, vaan Secure Enclave tarjoaa sen sijaan väliaikaisen, käynnistyskohtaisen avaimen. Kun salatun tiedostojärjestelmän avain tallennetaan, se salataan lisäksi ”pyyhittävällä avaimella”, joka tallennetaan pyyhittävään tallennustilaan, tai tallennuslaiteavaimen salausavaimella, jota suojaa Secure Enclaven uudelleentoiston estomekanismi. Tämä avain ei tarjoa tiedoille lisäsuojausta. Sen sijaan se on suunniteltu nopeasti poistettavaksi pyydettäessä (jos käyttäjä pyytää sitä valitsemalla Poista kaikki sisältö ja asetukset -vaihtoehdon tai jos käyttäjä tai ylläpitäjä tekee etätyhjennyskomennon mobiililaitteiden hallintaratkaisun (MDM), Microsoft Exchange ActiveSyncin tai iCloudin kautta). Avaimen poistaminen tällä tavalla tekee kaikista tiedostoista kryptografisesti sellaisia, ettei niihin pääse käsiksi.

Tiedoston sisältö voidaan salata yhdellä tai useammalla tiedostokohtaisella (tai tilakohtaisella) avaimella, joka on pakattu luokka-avaimella ja tallennettu tiedoston metatietoihin, jotka puolestaan on salattu tiedostojärjestelmän avaimella. Luokka-avainta suojaa laitteiston UID ja joissain luokissa käyttäjän pääsykoodi. Tämä hierarkia tarjoaa joustavuutta ja tehokkuutta. Esimerkiksi tiedoston luokan vaihtamiseksi tarvitsee vain pakata sen tiedostokohtainen avain uudelleen, ja pääsykoodin muuttaminen vain uudelleensalaa luokka-avaimen.

Tietojen suojausluokat

Kun Tietojen suojausta tukevassa laitteessa luodaan uusi tiedosto, tiedoston luonut appi määrittää sille luokan. Jokainen luokka määrittää erilaisilla käytännöillä, milloin tietoja voidaan käyttää. Seuraavissa osioissa kuvaillaan perusluokat ja -käytännöt. Apple silicon -pohjaiset Mac-tietokoneet eivät tue luokkaa D: Ei suojausta, ja suojaus muodostetaan sisään- ja uloskirjautumisen yhteydessä (ei lukittaessa tai lukitusta avattaessa kuten iPhonessa, iPadissa ja iPod touchissa).

Luokka	Suojaustyyppi
Luokka A: Täysi suojaus	NSFileProtectionComplete
Luokka B: Suojattu ellei avoimena	NSFileProtectionCompleteUnlessOpen
Luokka C: Suojattu ensimmäiseen käyttäjän todentamiseen saakka *Huomaa:* macOS luo taltioavaimen avulla FileVault-suojauksen ominaisuudet.	NSFileProtectionCompleteUntilFirstUserAuthentication
Luokka D: Ei suojausta *Huomaa:* Ei tuettu macOS:ssä.	NSFileProtectionNone

Täysi suojaus

NSFileProtectionComplete: Luokka-avain on suojattu avaimella, joka on johdettu käyttäjän pääsykoodista tai salasanasta ja laitteen UID:stä. Pian sen jälkeen, kun käyttäjä lukitsee laitteen (10 sekunnin kuluessa, jos Vaadi salasana -asetukseksi on asetettu Välittömästi), purettu luokka-avain poistetaan, jolloin mitään kyseisen luokan tietoja ei voida käyttää, ennen kuin käyttäjä syöttää pääsykoodinsa uudelleen tai avaa laitteen (kirjautuu siihen sisään) Face ID:llä tai Touch ID:llä.

Pian sen jälkeen, kun viimeinen käyttäjä on kirjautunut macOS:ssä ulos laitteelta, purettu luokka-avain poistetaan, jolloin mitään kyseisen luokan tietoja ei voida käyttää, ennen kuin joku käyttäjä taas syöttää pääsykoodinsa tai kirjautuu laitteeseen Touch ID:llä.

Suojattu ellei avoimena

NSFileProtectionCompleteUnlessOpen: Joitakin tiedostoja täytyy ehkä kirjoittaa, kun laite on lukittuna tai käyttäjä on kirjautunut ulos. Hyvä esimerkki tästä on sähköpostiliitteiden lataaminen taustalla. Tämä toiminta saadaan aikaan käyttämällä epäsymmetristä elliptisen käyrän salausta (ECDH over Curve25519). Tavallista tiedostokohtaista avainta suojataan avaimella, joka on johdettu käyttämällä yksivaiheista Diffie-Hellman-avaimen sopimista NIST SP 800-56A:ssa kuvatulla tavalla.

Sopimuksen lyhytaikainen julkinen avain tallennetaan yhdessä pakatun tiedostokohtaisen avaimen kanssa. Käytetty avaimen derivointifunktio (KDF) on ketjuavaimen derivointifunktio (Concatenation Key Derivation Function) (hyväksytty vaihtoehto 1), kuten on kuvattu osiossa 5.8.1 NIST SP 800-56A:ssa. AlgorithmID jää pois. PartyUInfo ja PartyVInfo ovat lyhytaikaisia ja staattisia julkisia avaimia. SHA256:ta käytetään hajautusfunktioon. Kun tiedosto suljetaan, tiedostokohtainen avain poistetaan muistista. Kun tiedosto avataan uudelleen, jaettu salaisuus luodaan uudelleen Suojattu ellei avoimena -luokan yksityisellä avaimella ja tiedoston lyhytaikaisella julkisella avaimella, joita käytetään purkamaan tiedostokohtainen avain, jota käytetään sitten tiedoston salauksen purkamiseen.

macOS:ssä NSFileProtectionCompleteUnlessOpen-avaimen yksityinen osa on käytettävissä niin kauan kun joku järjestelmän käyttäjistä on kirjautunut sisään tai todennettu.

Suojattu ensimmäiseen käyttäjän todentamiseen saakka

NSFileProtectionCompleteUntilFirstUserAuthentication: Tämä luokka toimii samalla tavalla kuin Täysi suojaus, paitsi että purettua luokka-avainta ei poisteta muistista, kun laite lukitaan tai käyttäjä kirjautuu ulos. Tämän luokan suojauksessa on samanlaisia ominaisuuksia kuin pöytätietokoneen koko taltion salauksessa, ja se suojaa tietoja hyökkäyksiltä, joihin liittyy uudelleenkäynnistys. Tämä on oletusluokka kaikille muiden valmistajien appitiedoille, joille ei ole määritetty tietojen suojausluokkaa.

macOS:ssä tämä luokka käyttää taltioavainta, joka on käytettävissä niin kauan kuin taltio on näkyvissä, ja se toimii aivan kuten FileVault.

Ei suojausta

NSFileProtectionNone: Tätä luokka-avainta suojaa vain UID, ja sitä säilytetään pyyhittävässä tallennustilassa. Koska kaikki avaimet, joita tarvitaan tämän luokan tiedostojen salauksen purkamiseen, on tallennettu laitteeseen, salauksesta on hyötyä vain nopeassa etätyhjennyksessä. Jos tiedostolle ei ole määritetty tietojen suojausluokkaa, se säilytetään silti salattuna (kuten kaikki tiedot iOS- ja iPadOS-laitteessa).

Tätä ei tueta macOS:ssä.

Huomaa: macOS:n taltioissa, jotka eivät vastaa käynnistettyä käyttöjärjestelmää, kaikkiin tietojen suojausluokkiin pääsee niin kauan kuin taltio on näkyvissä. Tietojen oletussuojausluokka on NSFileProtectionCompleteUntilFirstUserAuthentication. Tilakohtainen avaintoiminta on käytettävissä sekä Rosetta 2- että natiiviapeille.

Tietojen suojauksen avainvarastot

Sekä tiedostojen että avainnipun Tietojen suojauksen luokkien avaimet kootaan avainvarastoihin niissä hallittaviksi iOS:ssä, iPadOS:ssä, watchOS:ssä ja tvOS:ssä. Nämä käyttöjärjestelmät käyttävät seuraavia avainvarastoja: käyttäjä, laite, varmuuskopio, vara-avain ja iCloud-varmuuskopio.

Käyttäjän avainvarasto

Käyttäjän avainvarastoon on tallennettu laitteen normaalikäytössä tarvittavat salatut luokka-avaimet. Esimerkiksi kun pääsykoodi syötetään, *NSFileProtectionComplete* ladataan käyttäjän avainvarastosta, ja sen salaus puretaan. Se on binäärinen ominaisuusluettelo (.plist) -tiedosto, joka on tallennettu Ei suojausta -luokkaan.

Laitteissa, joissa on A9-järjestelmäpiiriä vanhemmat järjestelmäpiirit, .plist-tiedoston sisältö on salattu avaimella, jota säilytetään pyyhittävässä tallennustilassa. Jotta suojausta voidaan välittää eteenpäin avainvarastoille, tämä avain poistetaan ja luodaan uudelleen joka kerta, kun käyttäjä muuttaa pääsykoodinsa.

Laitteissa, joissa on A9 tai uudempi järjestelmäpiiri, .plist-tiedosto sisältää avaimen, joka ilmoittaa, että avainvarasto on tallennettu lokeroon, jota suojaa Secure Enclaven hallitsema toiston estävä nonce.

Secure Enclave hallitsee käyttäjän avainvarastoa, ja siltä voidaan kysellä laitteen lukitustilaa. Se raportoi laitteen olevan lukitsematon vain, jos kaikki käyttäjän avainvaraston luokka-avaimet ovat käytettävissä ja ne on avattu onnistuneesti.

Laitteen avainvarasto

Laitteen avainvarastoon tallennetaan salatut luokka-avaimet, joita käytetään laitekohtaisiin tietoihin liittyviin toimintoihin. Jaettuun käyttöön määritetyt iPadOS-laitteet tarvitsevat joskus pääsyä tunnistetietoihin, ennen kuin kukaan käyttäjä on kirjautunut sisään. Siksi vaaditaan avainvarasto, jota ei ole suojattu käyttäjän pääsykoodilla.

iOS ja iPadOS eivät tue käyttäjäkohtaisen tiedostojärjestelmäsisällön kryptografista erottelua, minkä vuoksi järjestelmä salaa laitteen avainvaraston luokka-avaimien avulla tiedostokohtaiset avaimet. Avainnippu kuitenkin käyttää luokka-avaimia käyttäjän avainvarastosta käyttäjän avainnipun kohteiden suojaamiseksi. Yhden käyttäjän käytettäviksi määritetyissä iOS- ja iPadOS-laitteissa (oletusmääritys) laitteen avainvarasto ja käyttäjän avainvarasto ovat sama varasto, ja niitä suojataan käyttäjän pääsykoodilla.

Varmuuskopion avainvarasto

Varmuuskopion avainvarasto luodaan, kun Finder (macOS 10.15:ssä tai uudemmassa) tai iTunes (macOS 10.14:ssä tai aiemmassa) tekee salatun varmuuskopion, ja se tallennetaan tietokoneelle, jolle laite varmuuskopioidaan. Luodaan uusi avainvarasto, jossa on uudet avaimet, ja sen jälkeen varmuuskopioidut tiedot salataan uudelleen näihin uusiin avaimiin. Kuten aiemmin kerrottiin, ei-siirrettävät avainnipun kohteet pysyvät salattuina UID:stä muodostetulla avaimella, jolloin ne voidaan palauttaa laitteeseen, josta ne alun perin varmuuskopioitiin, mutta jolloin niitä ei voida käyttää muissa laitteissa.

Avainvarastoa suojataan asetetulla salasanalla, ja se suoritetaan PBKDF2:n 10 miljoonalla toistolla. Suuresta toistomäärästä huolimatta sitä ei ole sidottu tiettyyn laitteeseen, ja siten useisiin tietokoneisiin samaan aikaan kohdistettua väsytyshyökkäystä voitaisiin teoreettisesti käyttää varmuuskopion avainvarastoon käsiin pääsemiseksi. Tätä uhkaa voidaan lieventää tarpeeksi vahvalla salasanalla.

Jos käyttäjä päättää olla salaamatta varmuuskopiota, varmuuskopiotiedostoja ei salata riippumatta niiden tietojen suojausluokasta, mutta avainnippu pysyy suojattuna UID:stä muodostetulla avaimella. Tämän vuoksi avainnipun kohteet siirtyvät uuteen laitteeseen vain, jos varmuuskopiolle on asetettu salasana.

Avainvarastotallenne

Avainvarastotallennetta käytetään synkronointiin Finderin kanssa (macOS 10.15 tai uudemmat) tai iTunesin kanssa (macOS 10.14 tai vanhemmat) USB:n kautta ja mobiililaitteiden hallintaan (MDM). Tämän avainvaraston avulla Finder tai iTunes voi varmuuskopioida ja synkronoida edellyttämättä, että käyttäjä syöttää pääsykoodin, ja sen ansiosta MDM-ratkaisu voi tyhjentää etänä käyttäjän pääsykoodin. Se on tallennettu tietokoneeseen, jota käytetään Finder- tai iTunes-synkronointiin, tai MDM-ratkaisuun, joka hallitsee laitetta etänä.

Avainvarastotallenne parantaa käyttökokemusta laitteen synkronoinnissa, jolloin mahdollisesti tarvitaan pääsy kaikkiin tietoluokkiin. Kun pääsykoodilla lukittu laite yhdistetään ensimmäistä kertaa Finderiin tai iTunesiin, käyttäjää kehotetaan syöttämään pääsykoodi. Laite luo sitten avainvarastotallenteen, jossa on samat luokka-avaimet, joita käytetään laitteessa ja jota suojataan äsken luodulla avaimella. Avainvarastotallenne ja sitä suojaava avain on jaettu laitteen ja isännän tai palvelimen välille siten, että tiedot on tallennettu laitteeseen Suojattu ensimmäiseen käyttäjän todentamiseen saakka -luokkaan. Tämän vuoksi laitteen pääsykoodi täytyy syöttää, ennen kuin käyttäjä varmuuskopioi Finderilla tai iTunesilla ensimmäistä kertaa uudelleenkäynnistyksen jälkeen.

Jos ohjelmistopäivitys ladataan langattomasti, käyttäjältä pyydetään pääsykoodia, kun päivitys aloitetaan. Tätä käytetään luomaan turvallisesti kertakäyttöinen avaustunniste, joka avaa käyttäjän avainvaraston päivityksen jälkeen. Tunnistetta ei voida luoda syöttämättä käyttäjän pääsykoodia, ja aiemmin luotu tunniste mitätöidään, jos käyttäjän pääsykoodi muuttuu.

Kertakäyttöiset avaustunnisteet on tarkoitettu joko ohjelmistopäivityksen valvottuun tai itsenäiseen asennukseen. Ne salataan avaimella, joka muodostetaan Secure Enclavessa olevan monotonisen laskurin nykyisestä arvosta, avainvaraston UUID:stä ja Secure Enclaven UID:stä.

A9-järjestelmäpiireissä (ja uudemmissa) kertakäyttöinen avaustunniste ei enää käytä laskureita tai pyyhittävää tallennustilaa. Sen sijaan sitä suojaa Secure Enclave, jota ohjaa toiston estävä arvo.

Valvottuihin ohjelmistopäivityksiin tarkoitettu kertakäyttöinen avaustunniste vanhenee 20 minuutissa. iOS 13:ssa ja iPadOS 13.1:ssä ja uudemmissa tunniste tallennetaan nyt Secure Enclaven suojaamaan lokeroon. Ennen iOS 13:a tämä tunniste vietiin Secure Enclavesta ja kirjoitettiin pyyhittävään tallennustilaan tai suojattiin Secure Enclaven uudelleentoiston estomekanismilla. Käytäntöajastin lisäsi laskurin lukemaa, jos laitetta ei uudelleenkäynnistetty 20 minuutin kuluessa.

Valvomattomia ohjelmistopäivityksiä tehdään, kun järjestelmä havaitsee, että päivitys on saatavilla, ja jokin seuraavista toteutuu:

- Automaattiset päivitykset on määritetty käyttöön iOS 12:ssa (tai uudemmassa).
- Käyttäjä valitsee Asenna myöhemmin, kun käyttäjälle ilmoitetaan päivityksestä.

Kun käyttäjä on syöttänyt pääsykoodinsa, luodaan kertakäyttöinen avaustunniste. Se voi pysyä voimassa Secure Enclavessa enintään 8 tuntia. Jos päivitystä ei ole vielä tehty, tämä kertakäyttöinen avaustunniste tuhotaan jokaisen lukituksen yhteydessä ja luodaan uudelleen aina seuraavan avauksen yhteydessä. Jokainen avaaminen aloittaa 8 tunnin aikaikkunan. Kahdeksan tunnin kuluttua käytäntöajastin mitätöi kertakäyttöisen avaustunnisteen.

iCloud-varmuuskopion avainvarasto

iCloud-varmuuskopion avainvarasto on samanlainen kuin varmuuskopion avainvarasto. Kaikki tämän avainvaraston luokka-avaimet ovat epäsymmetrisiä (käyttäen Curve25519:ää, kuten Suojattu ellei avoimena -tiedonsuojausluokka). Epäsymmetristä avainvarastoa käytetään myös varmuuskopiointiin iCloud-avainnipun avainnipun palautusaspektissa.

Avainten suojaaminen vaihtoehtoisissa käynnistystiloissa

Tietojen suojaus on suunniteltu tarjoamaan pääsy käyttäjän tietoihin vasta onnistuneen tunnistautumisen jälkeen ja vain valtuutetulle käyttäjälle. Tietojen suojausluokat on suunniteltu tukemaan erilaisia käyttötarkoituksia, kuten mahdollisuutta lukea ja kirjoittaa joitakin tietoja silloinkin, kun laite on lukittuna (mutta kun sen lukitus on kerran avattu). Vaihtoehtoisissa käynnistystiloissa käyttäjätietoihin pääsylle tehdään lisäsuojauksia, kuten sellaisia, joita käytetään DFU-tilassa, palautustilassa, Apple-vianmäärityksessä tai jopa ohjelmistopäivityksen aikana. Nämä ominaisuudet perustuvat yhdistelmään laitteiston ja ohjelmiston ominaisuuksia, ja niitä on laajennettu Applen suunnitteleman sirun kehittymisen myötä.

Ominaisuus	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1-perhe
Palautus: Kaikki tietojen suojausluokat suojataan	✓	✓	✓	✓	✓
Vaihtoehtoiset DFU-tilan käynnistykset, Palautus ja ohjelmistopäivitykset: Luokan A, B ja C tietojen suojaus		✓	✓	✓	✓

Secure Enclaven AES-komponentissa on lukittavia ohjelmiston siemenbittejä. Kun avaimia luodaan UID:stä, nämä siemenbitit sisällytetään avaimen johtamisfunktioon avainten lisähierarkioiden luomiseksi. Siemenbitin käyttötapa vaihtelee järjestelmäpiiristä riippuen:

- Applen A10- ja S3-järjestelmäpiireistä alkaen siemenbitti on tarkoitettu käyttäjän pääsykoodilla suojattujen avainten erottamiseen. Siemenbitti asetetaan avaimille, jotka vaativat käyttäjän pääsykoodin (mukaan lukien tietojen suojausluokkien A, B ja C avaimet), ja poistetaan avaimilta, jotka eivät vaadi käyttäjän pääsykoodia (mukaan lukien tiedostojärjestelmän metatietojen avain ja luokan D avaimet).
- iOS 13:ssa ja uudemmissa ja iPadOS 13.1:ssä tai uudemmissa, joiden laitteissa on A10 tai uudempi, pääsy käyttäjän tietoihin estetään kryptografisesti, kun laitteet käynnistetään vianmääritystilaan. Tämä saavutetaan lisäämällä siemenbitti, jonka asetus hallitsee mahdollisuutta käyttää tallennuslaiteavainta, jota itsessään tarvitaan kaikkien tietojen suojauksella salatun taltion metatietojen (ja sen vuoksi kaiken tiedostojen sisällön) käyttämiseen. Tämä suojaus sisältää kaikissa luokissa (A, B, C ja D) suojatut tiedostot, eikä vain ne, jotka vaativat käyttäjän salasanan.
- A12-järjestelmäpiireissä Secure Enclaven Boot ROM lukitsee pääsykoodin siemenbitin, jos appeja suorittava prosessori on siirtynyt DFU-tilaan (Device Firmware Upgrade) tai Palautustilaan. Kun pääsykoodin siemenbitti on lukittu, mitään toimintoja sen muuttamiseksi ei sallita. Tämä on suunniteltu estämään käyttäjän pääsykoodilla suojattujen tietojen käyttöä.

Laitteen palauttaminen sen jälkeen, kun se on siirtynyt DFU-tilaan, palauttaa sen hyväksi tunnettuun tilaan, jolloin voidaan olla varmoja, että siinä on vain muokkaamatonta Applen allekirjoittamaa koodia. DFU-tilaan voidaan siirtyä käsin.

Lue seuraava Applen tukiartikkeli siitä, kuinka laite asetetaan DFU-tilaan:

Laite	Artikkeli
iPhone, iPad, iPod touch	Jos unohdit iPhonen pääsykoodin
Apple TV	Jos näet varoitussymbolin Apple TV:ssä
Apple siliconilla varustettu Mac	Apple siliconilla varustetun Macin elvyttäminen tai palauttaminen

Käyttäjän tietojen suojaaminen hyökkäyksen yhteydessä

Käyttäjätietoja tavoittelevat hyökkääjät koettavat yleensä erilaisia menetelmiä: salattujen tietojen vieminen toiselle tallennuslaitteelle väsytyshyökkäystä varten, käyttöjärjestelmäversion muokkaaminen tai laitteen suojauskäytännön muu muokkaaminen tai heikentäminen hyökkäyksen helpottamiseksi. Laitteella oleviin tietoihin hyökkääminen edellyttää usein kommunikaatiota laitteen kanssa fyysisen liitännän kautta, kuten Lightningin tai USB:n kautta. Apple-laitteet sisältävät ominaisuuksia, jotka auttavat torjumaan kyseisiä hyökkäyksiä.

Apple-laitteet tukevat teknologiaa, jonka nimi on *sinetöity avaimen suojaus (Sealed Key Protection, SKP)*, joka on suunniteltu varmistamaan, että kryptografinen materiaali ei ole käyttökelpoista laitteen ulkopuolella, tai jota käytetään, jos käyttöjärjestelmäversioon tai suojausasetuksiin tehdään muutoksia ilman tarvittavaa käyttäjän valtuutusta. Tätä ominaisuutta *ei* tarjoa Secure Enclave, vaan sitä tukevat alemmassa kerroksessa olevat laitteistorekisterit. Ne antavat lisäsuojaa käyttäjätietojen salauksen purkamisessa tarvittaville avaimille riippumatta Secure Enclavesta.

Huomaa: SKP on saatavilla vain laitteissa, joissa on Applen suunnittelema järjestelmäpiiri.

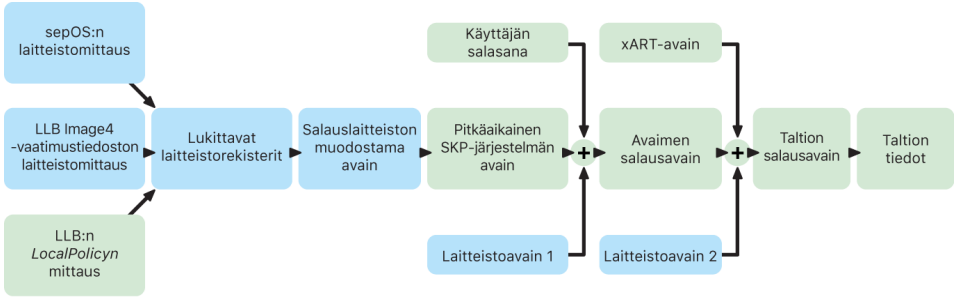
Ominaisuus	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, M1-perhe
Sinetöity avaimen suojaus	✓	✓	✓	✓	✓

iPhone ja iPad voidaan myös määrittää aktivoimaan tietoliikenneyhteydet vain silloin, kun laite on todennäköisemmin sen valtuuttaman omistajan hallussa fyysisesti.

Sinetöity avaimen suojaus (Sealed Key Protection, SKP)

Tietojen suojausta tukevissa Apple-laitteissa avaimensalausavainta (KEK) suojataan (eli se sinetöidään) järjestelmäohjelmiston mittauksilla, ja se on myös sidottu UID:hen, joka on saatavilla vain Secure Enclavesta. Apple siliconilla varustetussa Macissa KEK-avaimen suojausta vahvistetaan lisäämällä tietoja järjestelmän suojauskäytännöstä, sillä macOS tukee kriittisiä suojauskäytäntömuutoksia (kuten suojatun käynnistyksen tai järjestelmän eheyden suojauksen poistaminen käytöstä), joita ei tueta muilla alustoilla. Apple siliconilla varustetussa Macissa tämä suojaus kattaa FileVault-avaimet, koska FileVault toteutetaan Tietojen suojauksella (luokka C).

Avainta, joka muodostetaan sitomalla käyttäjän salasana pitkäaikaiseen SKP-avaimeen ja laitteistoavain 1:een (UID Secure Enclavesta) nimitetään *salasanajohdetuksi avaimeksi*. Tätä avainta käytetään suojaamaan käyttäjän avainvarastoa (kaikilla tuetuilla alustoilla) ja KEK-avainta (vain macOS) ja sitten mahdollistamaan biometrinen lukituksen avaaminen tai automaattinen lukituksen avaaminen muilla laitteilla, kuten Apple Watchilla.



Kun Secure Enclaven käyttöjärjestelmä ladataan, Secure Enclaven käynnistyksen valvonta tallentaa sen mittauksen. Kun appeja suorittavan prosessorin Boot ROM mittaa LLB:hen liitetyn Image4-vaatimustiedoston, tämä vaatimustiedosto sisältää mittauksen kaikesta muusta ladattavasta järjestelmän parina olevasta laiteohjelmistosta. LocalPolicy sisältää ladattavan macOS:n keskeisimmät suojausmääritykset. LocalPolicyssa on myös `nsih`-kenttä, joka on tiiviste macOS:n Image4-vaatimustiedostosta. macOS:n Image4-vaatimustiedosto sisältää mittaukset kaikesta macOS:n parina olevasta laiteohjelmistosta ja keskeisistä macOS:n käynnistyskohteista kuten käynnistyskernelkokoelmasta tai allekirjoitetun järjestelmätaltion (SSV) hajautus.

Jos hyökkääjä odottamatta onnistuisi muuttamaan jotakin yllämainituista mitatuista laiteohjelmistoista, ohjelmistoista tai suojausmääritysten osista, tämä muuttaa laitteistorekistereihin tallennettuja mittauksia. Mittausten muuttumisesta seuraa, että salauslaitteiston muodostama *järjestelmän mittauksen juuriavain (System Measurement Root Key, SMRK)* saa eri arvon, mikä rikkoo avainhierarkian sinetin. Tämän seurauksena *SMDK-avain (System Measurement Device Key)* ei ole käytettävissä, mistä puolestaan seuraa, että KEK-avain ja siten myöskään tiedot eivät ole käytettävissä.

Kun järjestelmään ei kohdistu hyökkäystä, sen on kuitenkin hyväksyttävä oikeat ohjelmistopäivitykset, jotka muuttavat laiteohjelmiston mittauksia ja LocalPolicyn `nsih`-kenttää uuden macOS:n mittausten mukaisiksi. Muissa järjestelmissä, jotka yrittävät yhdistää laiteohjelmiston mittaukset, mutta joissa ei ole luotettavaksi tiedettyä totuuden lähdettä, käyttäjän täytyy poistaa suojaus käytöstä, päivittää laiteohjelmisto ja sen jälkeen ottaa suojaus jälleen käyttöön, jotta saadaan uusi mittausten vertailutaso. Tämä lisää merkittävästi riskiä, että hyökkääjä voisi peukaloida laiteohjelmistoa päivityksen aikana. Järjestelmää auttaa se, että Image4-vaatimustiedosto sisältää kaikki tarvittavat mittaukset. Laitteisto, joka purkaa SMDK:n salauksen SMRK:lla, kun mittaukset täsmäävät normaalin käynnistyksen aikana, pystyy myös salaamaan SMDK:n esitetylle tulevalle SMRK:lle. Kun määritetään ohjelmistopäivityksen jälkeen odotetut mittaukset, laitteisto voi salata SMDK:n, jota voi käyttää nykyisessä käyttöjärjestelmässä, siten että sitä voi edelleen käyttää tulevassa käyttöjärjestelmässä. Samaten, kun asiakas muuttaa hyväksyttävällä tavalla suojausasetuksiaan LocalPolicyssa, SMDK on salattava tulevalle SMRK:lle sen LocalPolicyn mittauksen pohjalta, jonka LLB laskee seuraavassa uudelleenkäynnistyksessä.

Tietoliikenneyhteyksien aktivointi turvallisesti iOS:ssä ja iPadOS:ssä

Jos iOS- tai iPadOS-laitteessa ei ole muodostettu tietoliikenneyhteyttä äskettäin, käyttäjien täytyy aktivoida Face ID:llä, Touch ID:llä tai pääsykoodilla tietoliikenneyhteydet Lightning-, USB- tai Smart Connector -liitännän kautta. Tämä rajoittaa merkittävästi fyysisesti liitettyjen laitteiden, kuten haitallisten laturien, hyökkäysmahdollisuuksia, mutta mahdollistaa samalla muiden lisälaitteiden käyttämisen kohtuullisilla aikarajoilla. Jos iOS- tai iPadOS-laitteen lukittumisesta tai lisälaitteen tietoliikenneyhteyden päättämisestä on kulunut yli tunti, laite ei salli uusien tietoliikenneyhteyksien muodostamista, ennen kuin laitteen lukitus on avattu. Tämän tunnin ajanjakson aikana sallitaan vain avattuun laitteeseen aiemmin liitettyjen lisälaitteiden tietoliikenneyhteyksien muodostaminen. Nämä lisälaitteet muistetaan 30 päivän ajan sen jälkeen, kun ne viimeksi yhdistettiin. Jos tuntematon lisälaite yrittää muodostaa tietoliikenneyhteyden tänä aikana, kaikkien lisälaitteiden tietoliikenneyhteydet Lightningin, USB:n ja Smart Connectorin kautta poistetaan käytöstä, kunnes laite taas avataan. Tämä tunnin ajanjakso:

- auttaa varmistamaan, että laitteensa Maciin tai PC:hen, lisälaitteisiin tai kaapelin kautta CarPlayhin usein yhdistävien käyttäjien ei tarvitse syöttää pääsykoodia joka kerta liittäessään laitteensa
- on välttämätön, sillä lisälaite-ekosysteemi ei tarjoa kryptografisesti luotettavaa tapaa tunnistaa lisälaitteita ennen tietoliikenneyhteyden muodostamista.

Lisäksi jos tietoliikenneyhteyden muodostamisesta lisälaitteen kanssa on yli kolme päivää, laite estää uudet tietoliikenneyhteydet heti, kun se lukittuu. Tämä lisää suojausta sellaisille käyttäjille, jotka eivät yleensä käytä tällaisia lisälaitteita. Myös tietoliikenneyhteydet Lightningin, USB:n ja Smart Connectorin kautta poistetaan käytöstä, kun laite on tilassa, jossa se vaatii pääsykoodin biometrisen tunnistuksen uudelleenkäyttöönottoon.

Käyttäjät voivat ottaa uudelleen käyttöön aina päällä olevat tietoliikenneyhteydet asetuksissa (joidenkin avustavien laitteiden käyttöönotto tekee tämän automaattisesti).

Apple File Systemin rooli

Apple File System (APFS) on Applen oma tiedostojärjestelmä, joka on suunniteltu salaus huomioon ottaen. APFS toimii kaikilla Applen alustoilla – niin iPhonessa, iPadissa, iPod touchissa, Macissa, Apple TV:ssä kuin myös Apple Watchissa. Tämä flash-/SSD-muistille optimoitu tiedostojärjestelmä tukee vahvaa salausta, CoW-metadataa (copy-on-write), tilan jakamista, tiedostojen ja hakemistojen kloonausta sekä tilannevedoksia. Lisäksi se tukee nopeaa hakemiston koon uudelleenmääritystä, atomisesti turvallisia tallennusprimitiivejä ja parannettuja tiedostojärjestelmän perustoimintoja. Sen ainutlaatuinen CoW-design käyttää I/O-yhdistämistä maksimisuorituskyvyn tarjoamiseen varmistaen samalla tietojen luotettavuuden.

Tilan jakaminen

APFS varaa tallennustilaa tarpeen mukaan. Kun yhdessä APFS-säiliössä on useita taltioita, säiliön vapaa tila jaetaan ja se voidaan varata mille tahansa yksittäiselle taltiolle tarpeen mukaan. Kukin taltio käyttää vain osan säiliöstä, joten käytettävissä oleva on säiliön kokonaismäärä pois lukien kaikissa säiliön taltioissa käytössä oleva tila.

Useita taltioita

macOS 10.15:ssä tai uudemmassa APFS-säiliön, jota käytetään Macin käynnistämiseen, täytyy sisältää vähintään viisi taltiota, joista kolme ensimmäistä on kätketty käyttäjältä:

- *Esikäynnistystaltio:* Tämä taltio on salaamaton, ja se sisältää tiedot, jotka tarvitaan kunkin säiliössä olevan järjestelmätaltion käynnistämiseen.
- *VM-taltio:* Tämä taltio on salaamaton, ja macOS käyttää sitä salattujen swap-tiedostojen tallentamiseen.
- *Palautustaltio:* Tämä taltio on salaamaton, ja sen on oltava käytettävissä ilman järjestelmätaltion lukituksen avaamista, jotta laite voidaan käynnistää recoveryOS:ään.
- *Järjestelmätaltio:* Sisältää seuraavat:
  - kaikki Macin käynnistämiseen tarvittavat tiedostot
  - kaikki macOS:n natiivisti asentamat apit (apit, jotka olivat aiemmin /Apit-kansiossa ja ovat nyt /Järjestelmä/Apit-kansiossa)

Huomaa: Oletuksena mikään prosessi ei voi kirjoittaa järjestelmätaltioon, eivät edes Applen järjestelmäprosessit.

- *Datataltio:* Sisältää tietoja, jotka voivat muuttua, kuten:
  - käyttäjän kansiossa olevat tiedot, mukaan lukien kuvat, musiikki, videot ja dokumentit
  - käyttäjän asentamat apit, mukaan lukien AppleScript- ja Automator-apit
  - käyttäjän, organisaation tai muiden valmistajien appien asentamat muokatut sovelluskehykset ja daemonit
  - muut sijainnit, jotka käyttäjä omistaa ja joihin käyttäjä voi kirjoittaa, kuten /Apit, /Kirjasto, /Käyttäjät, /Taltiot, /usr/local, /private, /var ja /tmp

Datataltio luodaan jokaiselle uudelle järjestelmätaltiolle. Esikäynnistys-, VM- ja palautustaltiot ovat kaikki jaettuja eikä niitä ei ole monistettu.

macOS 11:ssä tai uudemmissa järjestelmätaltiosta tallennetaan tilannevedos. Käyttöjärjestelmä käynnistyy järjestelmätaltion tilannevedoksesta eikä pelkästään kirjoitussuojatusta järjestelmätaltiosta.

iOS:ssä ja iPadOS:ssä tallennustila on jaettu vähintään kahteen APFS-taltioon:

- Järjestelmätaltio
- Datataltio

Avainnipun tietojen suojaus

Monien appien täytyy käsitellä salasanoja ja muita lyhyitä mutta luottamuksellisia tietoja, kuten avaimia ja sisäänkirjautumistunnuksia. Avainnippu tarjoaa turvallisen tavan näiden kohteiden tallentamiseen. Applen eri käyttöjärjestelmät käyttävät eri menetelmiä avainnipun eri suojausluokkiin liittyvien vaatimusten täyttämiseen. macOS:ssä (mukaan lukien Apple siliconilla varustettu Mac) Tietojen suojausta ei käytetä suoraan näiden vaatimusten täyttämiseen.

Yleiskatsaus

Avainnipun kohteet salataan kahdella eri AES-256-GCM-avaimella: taulukkoavaimella (metatiedot) ja rivikohtaisella avaimella (salaisuusavain). Avainnipun metatiedot (kaikki attribuutit paitsi kSecValue) salataan haun nopeuttamiseksi metatietoavaimella, ja salaisuusarvo (kSecValueData) salataan salaisuusavaimella. Metatietoavainta suojaa Secure Enclave, mutta se on tallennettu appeja suorittavan prosessorin välimuistiin, jotta avainnipulle voi tehdä nopeita kyselyjä. Salaisuusavain edellyttää aina Secure Enclaven käyttöä.

Avainnippu toteutetaan tiedostojärjestelmään tallennettuna SQLite-tietokantana. Tietokantoja on vain yksi, ja `securityd`-daemon määrittää, mihin avainnipun kohteisiin kukin prosessi tai appi pääsee. Avainnipun käytön API:t tekevät daemonille kutsuja, joissa kysellään apin ”avainnipun käyttöryhmien”, ”appitunnisteen” ja ”appiryhmän” oikeuksia. Sen sijaan, että pääsyä rajoitettaisiin yhteen prosessiin, käyttöoikeusryhmien ansiosta avainnipun kohteita voidaan jakaa appien kesken.

Avainnipun kohteet voidaan jakaa vain saman kehittäjän appien välillä. Avainnipun kohteiden jakaminen edellyttää, että muiden valmistajien apit käyttävät appiryhmien kautta käyttöoikeusryhmiä, joissa on Apple Developer Program -ohjelman kautta saatu etuliite. Etuliitteen vaatimus ja appiryhmien yksilöllisyys toteutetaan koodin allekirjoituksella, provisiointiprofiileilla ja Apple Developer Program -ohjelmalla.

Avainnipun tiedot suojataan luokkarakenteella, joka on samantapainen kuin tietojen suojauksessa käytetty rakenne. Näiden luokkien käyttäytyminen vastaa tietojen suojausluokkia, mutta ne käyttävät erillisiä avaimia ja toimintoja.

Saatavuus	Tiedostojen tietojen suojaus	Avainnipun tietojen suojaus
Kun laite ei ole lukittu	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Kun laite on lukittu	NSFileProtectionCompleteUnlessOpen	–
Ensimmäisen avaamisen jälkeen	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Aina	NSFileProtectionNone	kSecAttrAccessibleAlways
Pääsykoodi käytössä	–	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

Taustalla tehtäviä päivityspalveluja käyttävät apit voivat käyttää *kSecAttrAccessibleAfterFirstUnlock*-luokkaa avainnipun kohteille, joita täytyy käyttää taustalla tehtävien päivitysten aikana.

kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly-luokka toimii samalla tavalla kuin *kSecAttrAccessibleWhenUnlocked*, mutta se on käytettävissä vain, kun laitteeseen on määritetty pääsykoodi. Tämä luokka on vain järjestelmän avainvarastossa. Niitä:

- Ei synkronoida iCloud-avainnippuun
- Ei varmuuskopioida
- Ei sisällytetä avainvarastotallenteeseen

Jos pääsykoodi poistetaan tai nollataan, kohteista tehdään käyttökelvottomia poistamalla luokka-avaimet.

Muissa avainnipun luokissa on Vain tämä laite -vastinpari, joka on aina suojattu UID:llä, kun se kopioidaan laitteesta varmuuskopioinnin aikana. Tämä tekee siitä hyödyttömän, jos se palautetaan eri laitteeseen. Apple on ottanut huomioon sekä turvallisuuden että käytettävyyden valitsemalla avainnipun luokat, jotka riippuvat suojattavan tiedon luokasta ja siitä, milloin sitä tarvitaan iOS:ssä ja iPadOS:ssä. Esimerkiksi VPN-varmenteen täytyy aina olla saatavilla, jotta laitteen yhteys on jatkuva, mutta se on luokiteltu ”ei-siirrettäväksi”, jotta sitä ei voi siirtää toiseen laitteeseen.

Avainnipun tietoluokkien suojaus

Avainnipun kohteisiin käytetään alla lueteltuja luokkasuojauksia.

Kohde	Käytettävissä
Wi-Fi-salasanat	Ensimmäisen avaamisen jälkeen
Sähköpostitilit	Ensimmäisen avaamisen jälkeen
Microsoft Exchange ActiveSync -tilit	Ensimmäisen avaamisen jälkeen
VPN-salasanat	Ensimmäisen avaamisen jälkeen
LDAP, CalDAV, CardDAV	Ensimmäisen avaamisen jälkeen
Sosiaalisen verkon tilin tunnukset	Ensimmäisen avaamisen jälkeen
Handoff-mainostuksen salausavaimet	Ensimmäisen avaamisen jälkeen
iCloud-tunnus	Ensimmäisen avaamisen jälkeen
iMessage-avaimet	Ensimmäisen avaamisen jälkeen
Kotijaon salasana	Kun laite ei ole lukittu
Safari-salasanat	Kun laite ei ole lukittu
Safari-kirjanmerkit	Kun laite ei ole lukittu
Finder/iTunes-varmuuskopio	Kun laite ei ole lukittu, ei-siirrettävä
Asetusprofiilin asentamat yksityiset avaimet	Kun laite ei ole lukittu, ei-siirrettävä
VPN-varmenteet	Aina, ei-siirrettävä
Bluetooth®-avaimet	Aina, ei-siirrettävä
Applen push-ilmoituspalvelun (APNs) tunnus	Aina, ei-siirrettävä
iCloud-varmenteet ja yksityinen avain	Aina, ei-siirrettävä
SIM PIN	Aina, ei-siirrettävä
Asetusprofiilin asentamat varmenteet	Aina
Missä on…? -tunnus	Aina
Puheposti	Aina

Avainnipun käytön hallinta

Avainniput voivat asettaa käytönvalvontaluetteloiden (ACL) avulla käytäntöjä pääsy- ja todennusvaatimuksille. Kohteet voivat muodostaa käyttäjän läsnäoloa vaativia ehtoja määrittämällä, ettei niitä voi käyttää ilman todennusta Face ID:llä, Touch ID:llä tai syöttämällä laitteen pääsykoodi tai salasana. Kohteisiin pääsyä voidaan myös rajoittaa määrittämällä, että Face ID- tai Touch ID -rekisteröinti ei ole saanut muuttua kohteen lisäämisen jälkeen. Tämä rajoitus auttaa estämään sen, että hyökkääjä lisäisi oman sormenjälkensä voidakseen käyttää avainnipun kohdetta. Käytönvalvontaluettelot arvioidaan Secure Enclaven sisällä ja vapautetaan kerneliin vain, jos niiden määritetyt rajoitukset täyttyvät.

Avainnippuarkkitehtuuri macOS:ssä

macOS tarjoaa myös pääsyn avainnippuun, joka tallentaa kätevästi ja turvallisesti käyttäjätunnukset ja salasanat, digitaaliset identiteetit, salausavaimet ja suojatut muistiinpanot. Sitä voidaan käyttää avaamalla Avainnipun käyttö -appi kansiossa /Apit/Lisäapit/. Avainnippua käyttämällä poistetaan vaatimus syöttää (tai jopa muistaa) jokaisen resurssin tunnistetiedot. Jokaiselle Mac-käyttäjälle luodaan oletusavainnippu, mutta käyttäjät voivat luoda muita avainnippuja erityisiin tarkoituksiin.

Käyttäjän avainnippujen lisäksi macOS luottaa joihinkin järjestelmäavainnippuihin, jotka sisältävät ei-käyttäjäkohtaisia todentamisresursseja, kuten verkon tunnistetiedot ja julkisen avaimen infrastruktuurin (public key infrastructure, PKI) identiteetit. Esimerkiksi Järjestelmäjuuret-avainnippu on muuttumaton ja tallentaa internetin PKI-juurivarmentajan (CA) varmenteet, jotka mahdollistavat yleiset palvelut kuten verkkopankit ja verkkokaupat. Käyttäjä voi edesauttaa sisäisten sivustojen ja palveluiden varmentamista ottamalla käyttöön sisäisesti jaettuja varmenteita hallituilla Mac-tietokoneilla.

FileVault

Taltion salaaminen FileVaultilla macOS:ssä

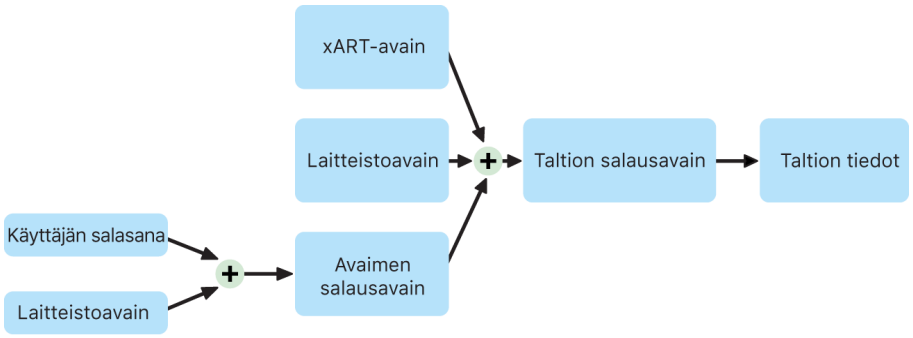
Mac-tietokoneissa on FileVault, joka on sisäänrakennettu salausratkaisu kaiken levossa olevan datan suojaamiseen. FileVault suojaa AES-XTS-tietojensalausalgoritmilla taltiot kokonaan sisäisillä ja ulkoisilla tallennuslaitteilla.

Apple siliconilla varustetun Macin FileVault toteutetaan käyttämällä tietojen suojausluokkaa C taltioavaimella. Apple T2 Security -sirulla tai Apple siliconilla varustetussa Macissa suoraan Secure Enclaveen yhteydessä olevat salatut sisäiset tallennuslaitteet käyttävät sen laitteiston ja AES-komponentin suojausominaisuuksia. Kun käyttäjä on laittanut FileVaultin päälle Macissa, käyttäjän kirjautumistietoja tarvitaan käynnistysprosessissa.

Sisäinen tallennustila FileVaultin ollessa päällä

Ilman sisäänkirjautumistietoja tai kryptografista palautusavainta sisäiset APFS-taltiot on salattu ja suojattu luvattomalta käytöltä, vaikka fyysinen tallennuslaite irrotettaisiin ja kiinnitettäisiin toiseen tietokoneeseen. macOS 10.15:ssä tämä pätee sekä järjestelmä- että datataltioon. macOS 11:stä alkaen järjestelmätaltio suojataan käyttämällä allekirjoitettua järjestelmätaltiota (Signed System Volume - SSV), mutta datataltio suojataan edelleen salaamalla. Sisäisen taltion salaus Apple siliconilla tai T2-sirulla varustetussa Macissa toteutetaan luomalla ja hallitsemalla avainhierarkiaa. Se perustuu laitteiston salausteknologioihin, jotka on sisäänrakennettu siruun. Tämä avainhierarkia on suunniteltu saavuttamaan samanaikaisesti neljä tavoitetta:

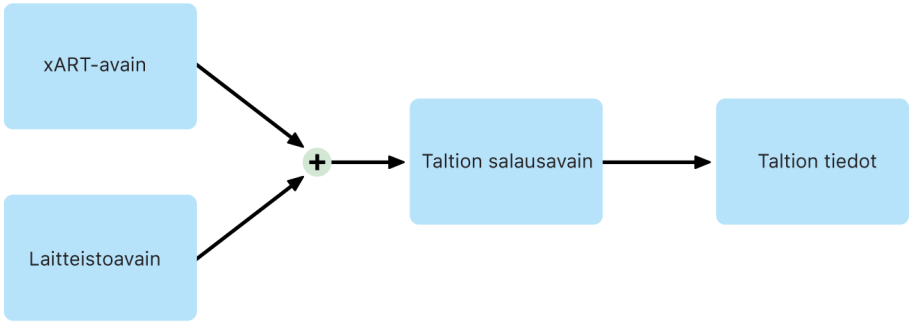
- käyttäjän salasanan vaatiminen salauksen purkamista varten
- järjestelmän suojaaminen suoraan Macista irrotettuun tallennuslaitteeseen kohdistuvalta väsytyshyökkäykseltä
- sujuvan ja turvallisen menetelmän tarjoaminen sisällön tyhjentämiseen poistamalla tarvittavat kryptografiset materiaalit
- käyttäjien salasanan vaihtomahdollisuus (ja sen kautta myös tiedostojen suojaamiseen käytettyjen salausavaimien) edellyttämättä koko taltion salaamista uudelleen



Apple siliconilla varustetussa Macissa sekä Macissa, jossa on T2-siru, kaikki FileVault-avainten käsittely tehdään Secure Enclavessa. Salausavaimia ei koskaan paljasteta suoraan Intel-prosessorille. Kaikkiin APFS-taltioihin luodaan oletuksena taltion salausavain. Taltion ja metatietojen sisältö salataan tällä taltion salausavaimella, joka on salattu luokka-avaimella. Luokka-avainta suojataan käyttäjän salasanan ja laitteiston UID:n yhdistelmällä, kun FileVault on päällä.

Sisäinen tallennustila FileVaultin ollessa pois päältä

Jos FileVaultia ei laiteta päälle Apple siliconilla tai T2-sirulla varustetussa Macissa ensimmäisen käyttöönottoapuriprosessin aikana, taltio salataan silti, mutta taltion salausavainta suojaa vain laitteiston UID Secure Enclavessa.



Jos FileVault laitetaan päälle myöhemmin (välitön prosessi, sillä tiedot on jo salattu), toiston estävä mekanismi auttaa estämään vanhan avaimen (joka perustuu vain laitteiston UID:hen) käytön taltion salauksen purkamiseen. Taltiota suojataan sen jälkeen käyttäjän salasanan ja laitteiston UID:n yhdistelmällä aiemmin kuvatulla tavalla.

FileVault-taltioiden poistaminen

Kun taltio poistetaan, Secure Enclave poistaa turvallisesti taltion salausavaimen. Tämä auttaa estämään avaimen käyttöä jatkossa, myös Secure Enclavelta. Lisäksi kaikki taltion salausavaimet salataan tallennuslaiteavaimella. Tallennuslaiteavain ei tarjoa tiedoille lisäsuojausta, vaan sen sijaan se mahdollistaa tietojen sujuvan ja turvallisen poistamisen, sillä ilman sitä salauksen purkaminen on mahdotonta.

Apple siliconilla tai T2-sirulla varustetussa Macissa tallennuslaiteavain poistetaan varmasti Secure Enclaven tukemalla teknologialla, kuten MDM-etäkomennoilla. Tallennuslaiteavaimen poistaminen tällä tavalla tekee taltiosta kryptografisesti mahdottoman käyttää.

Irrotettavat tallennuslaitteet

Ulkoisen tallennuslaitteen salaus ei käytä Secure Enclaven suojausominaisuuksia, ja sen salaus tehdään samalla tavalla kuin Intel-pohjaisessa Macissa, jossa ei ole T2-sirua.

FileVaultin hallinta macOS:ssä

Organisaatiot voivat hallita FileVaultia macOS:ssä käyttämällä SecureTokenia tai Bootstrap Tokenia.

Secure Tokenin käyttö

macOS 10.13:ssa tai uudemmissa oleva Apple File System (APFS) -järjestelmä muuttaa sen, kuinka FileVault-salausavaimia generoidaan. macOS:n aikaisemmissa versioissa CoreStorage-taltioilla FileVault-salausprosessissa käytettävät avaimet luotiin, kun käyttäjä tai organisaatio laittoi FileVaultin päälle Macissa. macOS:n APFS-taltioilla avaimet luodaan joko käyttäjän luomisen aikana, asetettaessa ensimmäisen käyttäjän salasana tai kun käyttäjä kirjautuu ensimmäisen kerran Maciin. Tämä salausavaimien toteutus, luomisaika ja tallennustapa ovat kaikki osa ominaisuutta nimeltä *Secure Token*. Secure Token -avain on salattu versio avaimensalausavaimesta (key encryption key, KEK), joka suojataan käyttäjän salasanalla.

Kun FileVault otetaan käyttöön APFS:llä, käyttäjä voi edelleen tehdä seuraavia:

- käyttää olemassa olevia työkaluja ja prosesseja, kuten henkilökohtaista palautusavainta (personal recovery key, PRK), joka voidaan tallentaa vara-avaimeksi mobiililaitteiden hallintaratkaisua (MDM) käyttäen.
- luoda ja käyttää organisaation palautusavainta (institutional recovery key, IRK).
- viivyttää FileVaultin käyttöönottoa, kunnes käyttäjä kirjautuu Maciin tai Macista pois.

macOS 11:ssä ensimmäisen salasanan asettamisesta Macin kaikkein ensimmäiselle käyttäjälle seuraa, että tämä käyttäjä saa Secure Token -avaimen. Joissakin työnkuluissa tätä ei ehkä haluta, koska aikaisemmin ensimmäisen Secure Token -avaimen antaminen on edellyttänyt kyseisen käyttäjätilin sisäänkirjautumista. Tämä voidaan estää lisäämällä `;DisabledTags;SecureToken` ohjelmallisesti luodun käyttäjän `AuthenticationAuthority`-attribuuttiin ennen käyttäjän salasanan asettamista, kuten alla on havainnollistettu:

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

Bootstrap Tokenin käyttö

macOS 10.15:ssä esiteltiin uusi ominaisuus nimeltä *Bootstrap Token*, joka auttaa antamaan Secure Token -avaimen liikkuville tileille ja valinnaiselle laiterekisteröinnillä luodulle ylläpitäjän tilille (”hallittu ylläpitäjä”). macOS 11:ssä Bootstrap Token voi antaa Secure Token -avaimen kenelle tahansa Mac-tietokoneeseen kirjautuvalle käyttäjälle, paikalliset käyttäjätilit mukaan lukien. macOS 10.15:n tai uudemman Bootstrap Token -ominaisuuden käyttäminen edellyttää seuraavia:

- Macin rekisteröinti MDM:ään käyttäen Apple School Manageria tai Apple Business Manageria, jolloin Macista tulee valvottu
- MDM-toimittajan tuki

macOS 10.15.4:ssä tai uudemmissa Bootstrap Token luodaan ja tallennetaan MDM-ratkaisuun, kun ensimmäinen Secure Tokenin saava käyttäjä kirjautuu tietokoneelle. Edellytyksenä on, että MDM-ratkaisu tukee tätä ominaisuutta. Bootstrap Token voidaan myös tarvittaessa luoda ja tallentaa MDM-ratkaisuun käyttäen `profiles`-komentorivityökalua.

macOS 11:ssä Bootstrap Tokenia voidaan käyttää muuhunkin kuin Secure Token -avaimen antamiseen käyttäjätileille. Jos Bootstrap Token on saatavilla Apple siliconilla varustetussa Macissa, sitä voidaan käyttää sekä kernelin laajennusten että ohjelmistopäivitysten asennusten valtuuttamiseen MDM-hallinnassa.

Miten Apple suojaa käyttäjien henkilökohtaiset tiedot

Appien pääsyoikeuden estäminen käyttäjätietoihin

Sen lisäksi, että Applen laitteet salaavat levossa olevat tiedot, ne auttavat estämään appeja käyttämästä käyttäjän henkilökohtaisia tietoja ilman lupaa hyödyntäen useita teknologioita, mm. tietosäiliötä. iOS:n ja iPadOS:n Asetuksissa sekä macOS:n Järjestelmäasetuksissa käyttäjät voivat katsoa, mille apeille he ovat sallineet pääsyn tiettyihin tietoihin, ja sallia tai poistaa pääsyn jatkossa. Pääsyä voidaan rajoittaa seuraavissa:

- *iOS, iPadOS ja macOS:* Kalenterit, Kamera, Yhteystiedot, Mikrofoni, Kuvat, Muistutukset, puheentunnistus
- *iOS ja iPadOS:* Bluetooth, Koti, Media, media-apit ja Apple Music, liikunta sekä kuntoilu
- *iOS ja watchOS:* Terveys
- *macOS:* Syötön tarkkailu (esimerkiksi näppäimistön käyttö), kehotteet, näyttötallennus (esimerkiksi still-kuvat ja video), Järjestelmäasetukset

iOS 13.4:ssä tai uudemmissa ja iPadOS 13.4:ssä tai uudemmissa kaikkien muiden valmistajien appien tiedot suojataan automaattisesti tietosäiliöön. Tietosäiliö auttaa suojaamaan tietoja luvattomalta käytöltä jopa siinäkin tapauksessa, että niitä käyttämään pyrkivät prosessit eivät itsessään ole eristettyjä. Lisäominaisuuksia iOS 15:ssä tai uudemmissa ovat Lähiverkko, Lähitoiminnot, Tutkimuksen tunnistin- ja käyttötiedot sekä Keskity.

Jos käyttäjä kirjautuu iCloudiin, iOS- ja iPadOS-apeille sallitaan oletuksena pääsy iCloud Driveen. Käyttäjät voivat hallita kunkin apin oikeuksia Asetusten iCloud-osiossa. iOS ja iPadOS tarjoavat lisäksi rajoituksia, jotka on suunniteltu estämään tietoja liikkumasta mobiililaitteiden hallintaratkaisulla (MDM) asennettujen appien ja tilien sekä käyttäjän asentamien appien ja tilien välillä.

Käyttäjän terveystietojen käytön estäminen

HealthKit tarjoaa keskitetyn tallennuspaikan terveys- ja kuntoilutiedoille iPhonessa ja Apple Watchissa. HealthKit toimii myös suoraan terveys- ja kuntoilulaitteiden kanssa. Näitä ovat esimerkiksi yhteensopivat Bluetooth Low Energy (BLE) -sykemittarit ja moniin iOS-laitteisiin sisältyvä liikeapuprosessori. Kaikki HealthKitin vuorovaikutus terveys- ja kuntoiluappien, terveydenhuoltolaitosten sekä terveys- ja kuntoilulaitteiden kanssa edellyttää käyttäjän hyväksyntää. Nämä tiedot tallennetaan käyttäen tietojen suojausluokkaa Suojattu ellei avoimena. Pääsystä tietoihin luovutaan 10 minuuttia sen jälkeen, kun laite on lukittunut, ja tietoihin pääsee taas, kun käyttäjä seuraavan kerran avaa lukituksen pääsykoodilla, Face ID:llä tai Touch ID:llä.

Terveys- ja kuntoilutietojen kerääminen ja tallentaminen

HealthKit myös kerää ja tallentaa hallintatietoja, kuten appien pääsyoikeuksia, HealthKitiin yhdistettyjen laitteiden nimiä ja aikataulutustietoja, joita käytetään appien käynnistämiseen, kun uutta tietoa on saatavilla. Näiden tietojen tallennuksessa käytetään tietojen suojausluokkaa Suojattu ensimmäiseen käyttäjän todentamiseen saakka. Terveystiedot, jotka tuotetaan laitteen ollessa lukittuna esimerkiksi, kun käyttäjä harrastaa liikuntaa, tallennetaan väliaikaisiin lokitiedostoihin. Ne tallennetaan käyttäen tietojen suojausluokkaa Suojattu ellei avoimena. Kun laitteen lukitus avataan, väliaikaiset lokitiedostot tuodaan ensisijaisiin terveystietokantoihin ja poistetaan, kun tietojen yhdistäminen on saatu valmiiksi.

Terveystietoja voidaan tallentaa iCloudiin. Terveystietojen päästä päähän -salaus edellyttää iOS 12:ta tai uudempaa ja kaksiosaista todennusta. Muussa tapauksessa käyttäjän tiedot salataan kyllä tallennustilassa ja siirrettäessä, mutta niitä ei salata päästä päähän. Kun käyttäjä laittaa kaksiosaisen todennuksen päälle ja päivittää iOS 12:een tai uudempaan, käyttäjän terveystiedot siirretään päästä päähän -salaukseen.

Jos käyttäjä varmuuskopioi laitteensa käyttäen Finderia (macOS 10.15:ssä tai uudemmissa) tai iTunesia (macOS 10.14:ssä tai vanhemmissa), terveystiedot tallennetaan vain, mikäli varmuuskopio on salattu.

Potilaskertomukset

Käyttäjät voivat kirjautua Terveys-apissa tuettuihin terveysjärjestelmiin saadakseen kopion potilaskertomuksistaan. Kun käyttäjä yhdistetään terveysjärjestelmään, käyttäjä todentaa henkilöllisyytensä käyttäen OAuth 2 -asiakkaan tunnistetietoja. Yhdistämisen jälkeen potilaskertomustiedot ladataan suoraan terveydenhuoltolaitokselta käyttäen suojattua TLS 1.3 -yhteyttä. Ladatut potilaskertomustiedot tallennetaan suojatusti muiden terveystietojen kanssa.

Terveystietojen eheys

Tietokantaan tallennettuihin tietoihin sisältyy metadataa kunkin tietueen alkuperän seuraamista varten. Tähän metadataan sisältyy appitunniste, josta ilmenee, mikä appi on tallentanut tietueen. Lisäksi valinnaiseen metadatakohteeseen voidaan sisällyttää digitaalisesti allekirjoitettu kopio tietueesta. Tämä on tarkoitettu luotetun laitteen tuottamien tietueiden tietojen eheyden varmistamiseen. Digitaalisen allekirjoituksen muotona on Cryptographic Message Syntax (CMS), joka on määritelty RFC 5652:ssa.

Muiden valmistajien appien pääsy terveystietoihin

HealthKit API:n käyttöä hallitaan oikeuksilla, ja appien on noudatettava tietojen käyttörajoituksia. Apit eivät esimerkiksi saa hyödyntää terveystietoja mainonnassa. Appeja vaaditaan myös kertomaan käyttäjälle tietosuojakäytäntö, jossa on käsitelty tarkasti, miten appi käyttää terveystietoja.

Appien oikeutta käyttää terveystietoja hallitaan käyttäjän Tietosuoja-asetuksissa. Kun apit pyytävät pääsyä terveystietoihin, käyttäjää pyydetään sallimaan käyttö samoin kuten Yhteystietojen, Kuvien ja muiden iOS:n tietolähteiden kanssa. Terveystietojen osalta kuitenkin apeille sallitaan erikseen tietojen lukeminen ja kirjoittaminen ja pääsy kuhunkin terveystietotyyppiin. Käyttäjät voivat katsoa ja perua antamiaan terveystietojen käyttöoikeuksia valitsemalla Asetukset > Terveys > Tietojen käyttö ja laitteet.

Jos apit saavat oikeuden kirjoittaa tietoja, ne saavat myös lukea kirjoittamansa tiedot. Jos apit saavat oikeuden lukea tietoja, ne voivat lukea kaikkien lähteiden kirjoittamia tietoja. Apit eivät kuitenkaan voi määrittää muille apeille sallittua pääsyä. Lisäksi apit eivät voi tietää varmasti, onko niille annettu lukuoikeus terveystietoihin. Kun apilla ei ole lukuoikeutta, kaikkien kyselyiden vastaus on ”ei tietoja”. Se on sama kuin tyhjästä tietokannasta saatava vastaus. Tämä on suunniteltu estämään appeja päättelemästä käyttäjän terveydentilaa selvittämällä, minkä tyyppisiä tietoja käyttäjä seuraa.

Käyttäjien SOS-tiedot

Terveys-appi tarjoaa käyttäjille mahdollisuuden täyttää SOS-tietolomakkeeseen tiedot, jotka voivat olla tärkeitä terveydellisessä hätätilanteessa. Tiedot syötetään ja päivitetään käsin, eikä niitä synkronoida terveystietokannoissa olevien tietojen kanssa.

SOS-tiedot näytetään napauttamalla Hätätilanne-painiketta lukitulla näytöllä. Tiedot tallennetaan laitteeseen käyttäen tietojen suojausluokkaa Ei suojausta, jotta niihin pääsee ilman laitteen pääsykoodin syöttämistä. SOS-tiedot ovat valinnainen ominaisuus, jota käyttäessään käyttäjät voivat valita, miten he painottavat yhtäältä turvallisuuttaan ja toisaalta yksityisyyttä. Nämä tiedot varmuuskopioidaan iCloud-varmuuskopioon iOS 13:ssa tai aiemmissa. iOS 14:ssä SOS-tiedot synkronoidaan laitteiden välillä CloudKitiä käyttäen ja salataan samalla tavoin kuin muutkin terveystiedot.

Terveystietojen jako

iOS 15:ssä Terveys-appi tarjoaa käyttäjille mahdollisuuden jakaa terveystietojaan muiden käyttäjien kanssa. Terveystiedot jaetaan kahden käyttäjän välillä käyttäen iCloudin päästä päähän -salausta, eikä Apple pääse tietoihin, jotka lähetetään Terveys-apin kautta. Tämän ominaisuuden käyttämistä varten sekä lähettävällä että vastaanottavalla käyttäjällä tulee olla iOS 15 tai uudempi ja molemmilla tulee olla käytössä kaksiosainen todennus.

Käyttäjät voivat myös jakaa terveystietonsa terveydenhuollon palveluntarjoajien kanssa käyttämällä Terveys-apin Jaa toimittajan kanssa -ominaisuutta. Tätä ominaisuutta käyttäen jaetut tiedot ovat ainoastaan käyttäjän valitsemien terveydenhuollon palveluntarjoajien saatavilla käyttäen päästä päähän -salausta. Apple ei ylläpidä salausavaimia, joilla voidaan purkaa salaus, katsoa tai muulla tavoin päästä käyttämään Jaa toimittajan kanssa -ominaisuuden kautta jaettuja terveystietoja eikä Applella ole pääsyä näihin avaimiin. Lisätietoja siitä, miten tämä palvelu on suunniteltu suojaamaan käyttäjän terveystietoja, löytyy ohjeen Apple Registration Guide for Healthcare Organizations osiosta Security and Privacy.

Digitaalinen allekirjoittaminen ja salaus

Käytönvalvontaluettelot

Avainnipun data jaetaan osiin ja suojataan käytönvalvontaluetteloilla (access control list, ACL). Sen seurauksena muiden valmistajien apit eivät voi käyttää toisten appien tunnistetietoja, ellei käyttäjä hyväksy sitä. Tämä suojaus tarjoaa mekanismin organisaation kaikkien appien ja palveluiden todentamistietojen suojaamiseen Applen laitteissa.

Mail

Mail-apissa käyttäjät voivat lähettää viestejä, jotka ovat digitaalisesti allekirjoitettuja ja salattuja. Mail etsii automaattisesti isot ja pienet kirjaimet erottelevan RFC 5322 -sähköpostiosoitteen aiheen tai aiheen vaihtoehtoiset nimet digitaalisista allekirjoitus- ja salausvarmenteista mukaan liitetyistä PIV (Personal Identification Verification) -tunnisteista yhteensopivissa älykorteissa. Jos määritetty sähköpostitili vastaa liitetyssä PIV-tunnisteessa olevan digitaalisen allekirjoitus- tai salausvarmenteen sähköpostiosoitetta, Mail näyttää automaattisesti allekirjoituspainikkeen uuden viestin ikkunan työkalupalkissa. Jos Maililla on vastaanottajan sähköpostisalauksen varmenne tai se havaitsee sen Microsoft Exchangen yleisessä osoiteluettelossa (global address list, GAL), uuden viestin ikkunan työkalupalkkiin tulee näkyviin kuvake, jossa lukon lukitus on avattuna. Lukittua lukkoa kuvaava kuvake osoittaa, että viesti lähetetään salattuna vastaanottajan julkisella avaimella.

Viestikohtainen S/MIME

iOS, iPadOS ja macOS tukevat viestikohtaista S/MIME:ä. Tämä tarkoittaa, että S/MIME-käyttäjät voivat allekirjoittaa ja salata kaikki viestit oletusarvoisesti tai vain yksittäisiä viestejä.

S/MIME-identiteettejä voidaan toimittaa Applen laitteisiin käyttämällä asetusprofiilia, mobiililaitteiden hallintaratkaisua (MDM), SCEP:tä tai Microsoftin Active Directoryn varmenteen myöntäjää.

Älykortit

macOS 10.12 ja uudemmat sisältävät PIV-korttien natiivituen. Kaupalliset ja julkisen sektorin organisaatiot käyttävät näitä kortteja laaja-alaisesti kaksiosaiseen todennukseen, digitaaliseen allekirjoittamiseen ja salaukseen.

Älykorteissa on yksi tai useampi digitaalinen identiteetti, jolla on julkisen avaimen ja yksityisen avaimen muodostama pari ja siihen liittyvä varmenne. Älykortin lukituksen avaaminen PIN-koodilla sallii pääsyn todennus-, salaus- ja allekirjoitustoiminnoissa käytettäviin yksityisavaimiin. Varmenne määrittää sen, mihin avainta voidaan käyttää, mitä attribuutteja siihen liittyy ja onko se varmentajan (CA) varmenteella vahvistettu (allekirjoitettu).

Älykortteja voidaan käyttää kaksiosaiseen todennukseen. Kortin avaamiseen tarvittavat kaksi osaa ovat ”jotakin, joka käyttäjällä on” (kortti) ja ”jotakin, jonka käyttäjä tietää” (PIN-koodi). macOS 10.12:ssa tai uudemmassa on myös natiivituki älykortin kirjautumisikkunan todentamiseen ja asiakkaan varmenteen todentamiseen Safarin avulla verkkosivustoissa. Lisäksi se tukee Kerberos-todentamista avainpareilla (PKINIT), mikä mahdollistaa kertakirjautumisen Kerberosta tukeviin palveluihin. Jos haluat lisätietoja älykorteista ja macOS:stä, katso Älykorttien integroinnin johdanto *Apple-alustojen käyttöönotossa*.

Salatut levytiedostot

macOS:ssä salatut levytiedostot palvelevat suojattuina säiliöinä, joihin käyttäjät voivat tallentaa tai siirtää luottamuksellisia dokumentteja ja muita tiedostoja. Salatut levytiedostot luodaan Levytyökalulla, joka löytyy sijainnista /Apit/Lisäapit. Levytiedostot salataan 128- tai 256-bittisellä AES-salauksella. Mac käsittelee näkyviin tuotua levytiedostoa kuten paikallista Maciin liitettyä taltiota, joten käyttäjät voivat kopioida, siirtää ja avata sillä olevia tiedostoja ja kansioita. Kuten FileVaultinkin kanssa, levytiedoston sisältö salataan ja puretaan reaaliajassa. Salattujen levytiedostojen avulla käyttäjät voivat vaihtaa dokumentteja, tiedostoja ja kansioita turvallisesti tallentamalla salatun levytiedoston irrotettavalle medialle, lähettämällä sen sähköpostin liitteenä tai tallentamalla sen etäpalvelimelle. Jos haluat lisätietoja salatuista levytiedostoista, katso Levytyökalun käyttöopas.

Appien suojaus

Appien suojauksen yleiskatsaus

Apit ovat tänä päivänä suojausarkkitehtuurin kriittisimpiä elementtejä. Apit tarjoavat käyttäjille merkittäviä tuottavuusetuja, mutta saattavat vaikuttaa myös negatiivisesti järjestelmän suojaukseen, vakauteen ja käyttäjätietoihin, jos niitä ei käsitellä oikein.

Tämän vuoksi Apple tarjoaa useita tasoja suojaa auttaakseen varmistamaan, ettei apeissa ole tunnettuja haittaohjelmistoja eikä niitä ole peukaloitu. Lisäsuojaukset pitävät huolen, että appien pääsyä käyttäjien tietoihin rajoitetaan tarkasti. Nämä suojausrajoitteet tarjoavat vakaan ja turvallisen alustan apeille sekä mahdollistavat sen, että tuhannet kehittäjät voivat tarjota satojatuhansia appeja iOS:lle, iPadOS:lle ja macOS:lle vaikuttamatta järjestelmän eheyteen. Käyttäjät voivat käyttää näitä appeja Apple-laitteissaan ilman, että heidän tarvitsee pelätä viruksia, haittaohjelmistoja tai luvattomia hyökkäyksiä.

iPhonessa, iPadissa ja iPod touchissa kaikki apit hankitaan App Storesta ja ne kaikki eristetään mahdollisimman tiukan suojauksen aikaansaamiseksi.

Macissa monet apit saadaan App Storesta, mutta Mac-käyttäjät voivat myös ladata ja käyttää appeja internetistä. macOS tarjoaa internet-latausta varten lisähallintaa suojaukseen. Oletuksena macOS 10.15:ssä ja uudemmissa kaikkien Mac-appien täytyy olla Applen oikeiksi todistamia, jotta ne käynnistyvät. Tämä vaatimus auttaa varmistamaan, että näissä apeissa ei ole tunnettuja haittaohjelmistoja, mutta ei kuitenkaan edellytä, että apit olisi hankittu App Storen kautta. Lisäksi macOS:ssä on huippuluokan virustorjunta, jolla estetään ja tarvittaessa poistetaan haittaohjelmistoja.

Sandbox-eristys toimii lisäsuojana alustoilla ja auttaa suojaamaan käyttäjätietoja siltä, että apit käyttäisivät niitä ilman lupaa. macOS:ssä kriittisten alueiden tiedot on suojattu, mikä auttaa varmistamaan, että käyttäjät hallitsevat kaikkien appien pääsyä Työpöytä-, Dokumentit- ja Lataukset-kansioiden tiedostoihin sekä muihin alueisiin riippumatta siitä, onko pääsyä yrittävät apit eristetty vai ei.

Natiiviominaisuus	**Muun valmistajan vastaava**
Ei-hyväksyttyjen liitännäisten luettelo, ei-hyväksyttyjen Safari-laajennusten luettelo	Virus-/haittaohjelmistomääritelmät
Tiedostokaranteeni	Virus-/haittaohjelmistomääritelmät
XProtect-/YARA-allekirjoitukset	Virus-/haittaohjelmistomääritelmät; päätelaitteiden suojaus

Natiiviominaisuus	Muun valmistajan vastaava
Gatekeeper	Päätelaitteiden suojaus; pakottaa apeille koodin allekirjoituksen auttaakseen varmistamaan, että vain luotettu ohjelmisto suoritetaan.
eficheck (Välttämätön Macille, jossa ei ole Apple T2 Security -sirua)	Päätelaitteiden suojaus; piilohallintaohjelmien tunnistus
Appipalomuuri	Päätelaitteiden suojaus; palomuuri
Pakettisuodatin (pf)	Palomuuriratkaisut
Järjestelmän eheyden suojaus	Sisältyy macOS:ään
Pakollinen pääsynhallinta	Sisältyy macOS:ään
Kernelin laajennusten ohituslista	Sisältyy macOS:ään
Pakollinen apin koodin allekirjoitus	Sisältyy macOS:ään
Appien oikeaksi todistaminen	Sisältyy macOS:ään

Appien suojaus iOS:ssä ja iPadOS:ssä

Johdanto appien suojaukseen iOS:ssä ja iPadOS:ssä

Toisin kuin muut mobiilialustat, iOS ja iPadOS eivät anna käyttäjien asentaa mahdollisesti haitallisia allekirjoittamattomia appeja verkkosivustoilta tai suorittaa ei-luotettuja appeja. Ajon aikana koodin allekirjoituksella tarkistetaan, että kaikki suoritettavat muistisivut on tehty sellaisiksi kuin ne ladataan, mikä auttaa varmistamaan, että appia ei ole muokattu asennuksen tai viime päivityksen jälkeen.

Kun appi on varmennettu hyväksytystä lähteestä peräisin olevaksi, iOS ja iPadOS ottavat käyttöön suojausominaisuudet, joiden ansiosta muut apit tai järjestelmän osat eivät vaarannu.

Appikoodin allekirjoitusprosessi iOS:ssä ja iPadOS:ssä

iOS:ssä ja iPadOS:ssä Apple suojaa appien käyttöä muun muassa sellaisilla ratkaisuilla kuin pakollinen koodin allekirjoitus ja ehdoton kehittäjien sisäänkirjaus.

Pakollinen koodin allekirjoitus

Kun iOS- tai iPadOS-kernel on käynnistynyt, se hallitsee, mitä käyttäjäprosesseja ja appeja voidaan suorittaa. iOS ja iPadOS auttavat varmistamaan, että kaikki apit tulevat tunnetusta ja hyväksytystä lähteestä eikä niitä ole peukaloitu, edellyttämällä, että kaikki suoritettava koodi on allekirjoitettu Applen myöntämällä varmenteella. Laitteen omat apit, kuten Mail ja Safari, ovat Applen allekirjoittamia. Muiden valmistajien apit täytyy myös varmistaa ja allekirjoittaa Applen myöntämällä varmenteella. Pakollinen koodin allekirjoitus laajentaa luottamusketjua käyttöjärjestelmästä appeihin ja auttaa estämään muiden valmistajien appeja lataamasta allekirjoittamattomia koodiresursseja tai käyttämästä itsestään muuttuvaa koodia.

Kuinka kehittäjät allekirjoittavat apit

Kehittäjät voivat allekirjoittaa appinsa läpäistyään varmenteen tarkistuksen (Apple Developer Program -ohjelman kautta). He voivat myös upottaa appiensa sisään sovelluskehyksiä ja saada niiden koodin varmistettua Applen myöntämällä varmenteella (tiimitunnistemerkkijonoa käyttäen).

- *Varmenteen tarkistus:* Jotta kehittäjät voivat kehittää ja asentaa appeja iOS- tai iPadOS-laitteisiin, heidän on rekisteröidyttävä Apple Developer Program -ohjelmaan. Apple tarkistaa jokaisen kehittäjän (henkilön tai yrityksen) todellisen identiteetin ennen varmenteen myöntämistä heille. Varmenteella kehittäjät voivat allekirjoittaa appeja ja lähettää niitä App Storeen jaeltaviksi. Tämän ansiosta kaikki App Store -apit ovat yhdistettävissä henkilöön tai organisaatioon, mikä toimii esteenä haittaohjelmistojen luomiselle. Apple on myös tarkistanut ne auttaakseen varmistamaan, että ne toimivat yleisesti kuvatulla tavalla ja ettei niissä ole ilmiselviä virheitä tai muita merkille pantavia ongelmia. Aiemmin kuvaillun teknologian lisäksi tämä tarkistusprosessi auttaa käyttäjiä luottamaan heidän ostamiensa appien laatuun.
- *Koodin allekirjoituksen varmistus:* iOS:ssä ja iPadOS:ssä kehittäjät voivat upottaa sovelluskehyksiä appiensa sisälle. Niitä voivat käyttää itse appi tai appiin upotetut laajennukset. Jotta järjestelmä- ja muita appeja suojataan lataamasta muiden valmistajien koodia niiden osoiteavaruudessa, järjestelmä varmistaa allekirjoituksen kaikilta dynaamisilta kirjastoilta, joihin prosessi linkittyy käynnistyksen aikana. Tämän vahvistuksen tekee joukkueen tunniste (Team Identifier), joka saadaan Applen myöntämästä varmenteesta. Joukkueen tunniste on 10-merkkinen aakkosnumeerinen merkkijono, kuten 1A2B3C4D5F. Ohjelma voi linkittyä mihin tahansa alustakirjastoon, joka tulee järjestelmän mukana, tai mihin tahansa kirjastoon, jonka koodin allekirjoituksessa on sama joukkueen tunniste kuin pääsuoritustiedostossa. Koska järjestelmän mukana tulevissa suoritustiedostoissa ei ole joukkueen tunnistetta, ne voidaan linkittää vain kirjastoihin, jotka tulevat järjestelmän mukana.

Yrityksen omien sisäisten appien tarkistaminen

Ehdot täyttävät yritykset voivat myös kirjoittaa omia yrityksen sisäisiä appeja, jotta niitä voidaan käyttää organisaatiossa ja jakaa työntekijöille. Yritykset ja organisaatiot voivat hakea Apple Developer Enterprise Program (ADEP) -ohjelmaan. Saat lisätietoja ja voit tarkistaa kelpoisuusvaatimukset Apple Developer Enterprise Program -verkkosivustolta. Kun organisaatiosta on tullut ADEP-ohjelman jäsen, se voi rekisteröityä, jotta se saa provisiointiprofiilin, jolla sallitaan yrityksen omien sisäisten appien toimia sen valtuuttamissa laitteissa.

Käyttäjillä on oltava provisiointiprofiili asennettuna, jotta nämä apit voivat toimia. Tämä auttaa varmistamaan, että vain organisaation tarkoittamat käyttäjät voivat ladata apit iOS- ja iPadOS-laitteilleen. Mobiililaitteen hallinnan (MDM) avulla asennettuihin appeihin luotetaan ehdottomasti, koska organisaation ja laitteen välinen suhde on jo muodostettu. Muussa tapauksessa käyttäjien täytyy hyväksyä apin provisiointiprofiili Asetuksissa. Organisaatiot voivat myös estää käyttäjiä hyväksymästä appeja tuntemattomilta kehittäjiltä. Kun yrityksen oma sisäinen appi käynnistetään ensimmäistä kertaa, laitteen täytyy saada positiivinen vahvistus Applelta, jotta apin suorittaminen sallitaan.

Ajonaikaisen prosessin suojaus iOS:ssä ja iPadOS:ssä

iOS ja iPadOS auttavat varmistamaan ajonaikaisen suojauksen käyttämällä eristystä, oikeuksia ja ASLR-tekniikkaa (Address Space Layout Randomization).

Eristys

Kaikki muiden valmistajien apit eristetään (sandbox), jotta ne eivät pääse käsiksi muiden appien tallentamiin tiedostoihin tai tekemään muutoksia laitteeseen. Eristys on suunniteltu estämään appeja keräämästä tai muokkaamasta muiden appien tallentamia tietoja. Jokaisella apilla on tiedostoillensa oma kotihakemisto, joka määritetään sattumanvaraisesti, kun appi asennetaan. Jos muun valmistajan apin täytyy käyttää muiden tietoja, se tekee sen vain palveluilla, jotka iOS ja iPadOS varta vasten tarjoavat.

Järjestelmätiedostot ja resurssit on myös erotettu käyttäjän apeista. Suurin osa iOS:n ja iPadOS:n järjestelmätiedostoista ja resursseista suoritetaan oikeudettomana käyttäjänä ”mobile”, kuten myös kaikki muiden valmistajien apit. Koko käyttöjärjestelmäosio tuodaan näkyviin kirjoitussuojattuna. Tarpeettomia työkaluja, kuten etäkirjautumispalveluja, ei ole sisällytetty järjestelmäohjelmistoon, ja rajapinnat eivät salli appien laajentaa niiden omia oikeuksia, jotta ne voisivat muokata muita appeja tai iOS:ää ja iPadOS:ää.

Oikeuksien käyttö

Muiden valmistajien appien pääsyä käyttäjän tietoihin ja ominaisuuksiin (kuten iCloud ja laajennettavuus) hallitaan oikeuksilla. Oikeudet ovat appiin allekirjoitettuja avain-arvo-pareja, jotka mahdollistavat ajonaikaisia tekijöitä, kuten UNIXin käyttäjätunnusta, pidemmälle menevän todentamisen. Koska oikeudet on digitaalisesti allekirjoitettu, niitä ei voida muuttaa. Järjestelmäapit ja prosessit suorittavat oikeuksilla toimintoja, jotka muuten vaatisivat prosessin suorittamisen pääkäyttäjänä (root). Tämä vähentää järjestelmäappien tai prosessien vaarantumisesta aiheutuvaa oikeuksien eskalaatiota.

Lisäksi apit voivat suorittaa taustaprosessointia vain järjestelmän tarjoamien API:en kautta. Tämän ansiosta apit voivat jatkaa toimintaa heikentämättä suorituskykyä tai vaikuttamatta merkittävästi akunkestoon.

ASLR (Address Space Layout Randomization)

ASLR (Address Space Layout Randomization) auttaa suojaamaan muistin korruptoitumisvirheiden hyödyntämiseltä. Vakioapit käyttävät ASLR:ää apuna satunnaistamaan kaikki muistialueet käynnistyksessä. Sen lisäksi, että ASLR toimii käynnistyksen yhteydessä, se myös satunnaistaa suoritettavan koodin, järjestelmäkirjastojen ja muiden ohjelmointielementtien muistiosoitteet, mikä pienentää edelleen monien hyökkäysten todennäköisyyttä. Esimerkiksi "return-to-libc"-hyökkäys yrittää huijata laitteen suorittamaan haittakoodia manipuloimalla pinon ja järjestelmäkirjastojen muistiosoitteita. Näiden sijoittelun satunnaistaminen tekee hyökkäyksen toteuttamisesta vaikeampaa erityisesti useissa laitteissa. Xcode ja iOS:n ja iPadOS:n kehitysympäristöt kääntävät muiden valmistajien apit automaattisesti ASLR-tuki päällä.

Execute Never -ominaisuus

iOS ja iPadOS tarjoavat lisäsuojaa ARMin Execute Never (XN) -ominaisuudella, joka merkitsee muistisivuja ei-suoritettaviksi. Apit voivat käyttää sekä kirjoitettavia että suoritettavia muistisivuja vain tiukasti kontrolloiduissa tilanteissa: Kernel tarkistaa dynaamisen koodinallekirjoitusoikeuden, joka on vain Applella. Silloinkin vain yksi `mmap`-kutsu voi pyytää suoritettavaa ja kirjoitettavaa sivua, jolle annetaan satunnaistettu osoite. Safari käyttää tätä ominaisuutta JavaScript-JIT-kääntäjässään.

Tukilaajennukset iOS:ssä, iPadOS:ssä ja macOS:ssä

iOS, iPadOS ja macOS sallivat appien tarjota toimintoja toisille apeille laajennusten avulla. Laajennukset ovat tiettyyn tarkoitukseen suunniteltuja allekirjoitettuja suoritettavia binääritiedostoja, jotka on pakattu appiin. Järjestelmä tunnistaa laajennukset automaattisesti asennuksen aikana ja tarjoaa ne muiden appien saataville täsmäysjärjestelmän avulla.

Laajennuspisteet

Laajennuksia tukevaa järjestelmäaluetta kutsutaan *laajennuspisteeksi*. Jokainen laajennuspiste tarjoaa API-rajapintoja ja valvoo käytäntöjä kyseiselle alueelle. Järjestelmä määrittää, mitkä laajennukset ovat käytettävissä, laajennuspistekohtaisten täsmäyssääntöjen avulla. Järjestelmä käynnistää automaattisesti laajennusprosesseja tarpeen mukaan ja hallitsee niiden kokonaiskestoa. Oikeuksilla voidaan rajoittaa laajennusten käytettävyyttä tietyille järjestelmäapeille. Esimerkiksi Tänään-näkymän widgetti näkyy vain Ilmoituskeskuksessa, ja jakolaajennus on käytettävissä vain Jako-osiossa. Laajennuspisteitä ovat esimerkiksi Tänään-widgetit, jakaminen, toiminnot, kuvan muokkaus, tiedostontarjoaja ja muokattu näppäimistö.

Laajennusten kommunikaatio

Laajennukset toimivat niiden omassa osoiteavaruudessa. Laajennuksen ja apin, josta se aktivoitiin, välinen kommunikaatio käyttää prosessien välistä kommunikaatiota, jonka välittää järjestelmän sovelluskehys. Niillä ei ole pääsyä toistensa tiedostoihin tai muistiavaruuksiin. Laajennukset on suunniteltu olemaan eristyksissä toisistaan, niitä säilyttävistä apeista ja niitä käyttävistä apeista. Ne eristetään kuten muutkin muiden valmistajien apit, ja niillä on säiliö erillään sisältävän apin säiliöstä. Niissä on kuitenkin samat tietosuojaohjaimien käyttöoikeudet kuin säiliöapissa. Jos käyttäjä antaa Yhteystiedoille pääsyn appiin, pääsy annetaan appiin sisällytetyille laajennuksille, mutta ei apin aktivoimille laajennuksille.

Muokattujen näppäimistöjen käyttö

Muokatut näppäimistöt ovat erityistyyppinen laajennus, sillä käyttäjä ottaa sen käyttöön koko järjestelmään. Kun se on otettu käyttöön, näppäimistön laajennusta käytetään kaikille tekstikentille paitsi pääsykoodin syötölle ja suojattuun tekstinäkymään. Käyttäjän tietojen siirron rajoittamiseksi muokatut näppäimistöt toimivat oletuksena erittäin rajatussa eristyksessä, joka estää pääsyn verkkoon ja palveluihin, jotka suorittavat verkkotoimintoja prosessin puolesta, ja API-rajapintoihin, jotka sallisivat laajennuksen kaapata kirjoitustietoja. Muokattujen näppäimistöjen kehittäjät voivat pyytää laajennukselleen avointa pääsyoikeutta, jolla järjestelmä suorittaa laajennuksen oletuseristyksessä, kun se on saanut hyväksynnän käyttäjältä.

MDM ja laajennukset

Laitteissa, jotka on rekisteröity mobiililaitteen hallintaratkaisuun (MDM), dokumentti- ja näppäimistölaajennukset noudattavat hallitun avaamisen sääntöjä. Esimerkiksi MDM-ratkaisu voi auttaa estämään käyttäjiä viemästä dokumenttia hallitusta apista hallitsemattomaan dokumentintarjoajaan tai auttaa estämään heitä käyttämästä hallitsematonta näppäimistöä hallitun apin kanssa. Lisäksi appien kehittäjät voivat estää muiden valmistajien näppäimistölaajennusten käytön apeissaan.

Appien suojaus ja appiryhmät iOS:ssä ja iPadOS:ssä

Organisaatiot voivat suojata apit iOS:ssä ja iPadOS:ssä luotettavasti käyttämällä IOS SDK:ta ja liittymällä appiryhmään Apple Developer -portaalissa.

Tietojen suojaaminen apeissa

iOS Software Development Kit (SDK) iOS:lle ja iPadOS:lle tarjoaa kattavan joukon API-rajapintoja, joilla muiden valmistajien ja yrityksen sisäisten kehittäjien on helppoa käyttää tietojen suojausta ja varmistaa paras mahdollinen suojaus apeissaan. Tietojen suojaus on saatavilla tiedosto- ja tietokantarajapinnoille, mukaan lukien NSFileManager, CoreData, NSData ja SQLite.

Mail-apin tietokanta (mukaan lukien liitteet), hallitut kirjat, Safari-kirjanmerkit, appien käynnistystiedostot ja sijaintitiedot tallennetaan myös salaamalla, ja käyttäjän pääsykoodilla suojatut avaimet ovat laitteessa. Kalenteri (paitsi liitteet), Yhteystiedot, Muistutukset, Muistiinpanot, Viestit ja Kuvat käyttävät tietojen suojausoikeutta Suojattu ensimmäiseen käyttäjän todentamiseen saakka.

Käyttäjän asentamille apeille, joille ei ole asetettu tiettyä tietojen suojausluokkaa, määritetään oletusarvoisesti luokka Suojattu ensimmäiseen käyttäjän todentamiseen saakka.

Appiryhmään liittyminen

Tietyn kehittäjätilin omistamat apit ja laajennukset voivat jakaa sisältöä, kun ne on määritetty osaksi appiryhmää. Kehittäjän vastuulla on luoda sopivat ryhmät Apple Developer -portaalissa ja sisällyttää niihin halutut apit ja laajennukset. Kun apit on määritetty osaksi appiryhmää, niillä on pääsy seuraaviin:

- jaettu taltiolla oleva tallennussäiliö, joka pysyy laitteessa niin kauan, kunnes vähintään yksi ryhmän appi on asennettu
- jaetut asetukset
- jaetut avainnipun kohteet

Apple Developer -portaali auttaa varmistamaan, että appien ryhmätunnukset (GID) ovat ainutlaatuisia appien ekosysteemissä.

Lisälaitteiden varmistaminen iOS:ssä ja iPadOS:ssä

Made for iPhone, iPad ja iPod touch (MFi) -lisenssiohjelma tarjoaa varmistetuille lisälaitevalmistajille pääsyn iPod Accessories Protocol (iAP) -protokollaan ja tarvittaviin laitteiston apukomponentteihin.

Kun MFi-lisälaite kommunikoi iOS- tai iPadOS-laitteen kanssa käyttäen Lightning- tai USB-C-liitintä tai Bluetoothia, laite pyytää lisälaitetta vahvistamaan, että Apple on valtuuttanut sen, vastaamalla Applen antamalla varmenteella, jonka laite tarkistaa. Laite lähettää haasteen, johon lisälaitteen täytyy vastata allekirjoitetulla vastauksella. Koko tästä prosessista huolehtii muokattu integroitu piiri (IC), jonka Apple tarjoaa hyväksytyille lisälaitevalmistajille ja joka on läpinäkyvä itse lisälaitteelle.

Lisälaitteet voivat pyytää pääsyä eri siirtotapoihin ja toimintoihin, kuten pääsyä digitaaliseen äänentoistoon Lightning- tai USB-C-kaapelin kautta tai Bluetoothin kautta saatuihin sijaintitietoihin. Todentamis-IC on suunniteltu varmistamaan, että vain hyväksytyt lisälaitteet saavat täyden pääsyn laitteeseen. Jos lisälaite ei tue todentamista, sen pääsyoikeus rajoitetaan analogiseen ääneen ja pieneen joukkoon sarjaäänentoistosäätimiä (UART).

AirPlay varmistaa todentamis-IC:n avulla, että Apple on hyväksynyt vastaanottimet. AirPlay-äänentoisto ja CarPlay-videontoisto käyttävät MFi-SAP (Secure Association Protocol) -protokollaa, joka salaa lisälaitteen ja laitteen välisen kommunikaation AES128:lla laskuritilassa (CTR). Lyhytaikaiset avaimet vaihdetaan ECDH-avaimenvaihdolla (Curve25519) ja allekirjoitetaan todentamis-IC:n 1024-bittisellä RSA-avaimella osana Station-to-Station (STS) -protokollaa.

Appien suojaus macOS:ssä

Johdanto appien suojaukseen macOS:ssä

Appien suojaus macOS:ssä koostuu useista päällekkäisistä kerroksista. Ensimmäinen niistä on mahdollisuus suorittaa vain allekirjoitettuja ja luotettuja appeja App Storesta. Lisäksi macOS:ssä on suojauksia, jotka auttavat varmistamaan, että internetistä ladatuissa apeissa ei ole tunnettuja haittaohjelmistoja. macOS sisältää teknologioita, jotka havaitsevat ja poistavat haittaohjelmistoja, sekä lisäsuojauksia, jotka on suunniteltu estämään ei-luotettuja appeja pääsemästä käyttäjätietoihin. Applen palvelut, kuten oikeaksi todistaminen ja XProtectin päivitykset, on suunniteltu estämään haittaohjelmistojen asentamista. Tarvittaessa nämä palvelut löytävät haittaohjelmiston, joka on saattanut aluksi jäädä tunnistamatta, ja poistavat sen nopeasti ja tehokkaasti. macOS-käyttäjät voivat kuitenkin käyttää suojausmallia, joka sopii heille itselleen parhaiten – eli myös suorittaa täysin allekirjoittamatonta ja ei-luotettua koodia.

Appikoodin allekirjoitusprosessi macOS:ssä

Kaikki App Storesta hankitut apit ovat Applen allekirjoittamia. Tämä allekirjoittaminen on suunniteltu varmistamaan, ettei niitä ole peukaloitu tai muutettu. Apple allekirjoittaa kaikki Apple-laitteiden tarjoamat apit.

macOS 10.15:ssä kaikkien muualla kuin App Storessa jaettavien appien täytyy olla kehittäjän Applen myöntämällä kehittäjävarmenteella allekirjoittamia (yhdessä yksityisen avaimen kanssa) ja Applen oikeaksi todistamia, jotta ne toimivat Gatekeeperin oletusasetuksilla. Talon sisälläkin kehitetyt apit tulisi allekirjoittaa Applen myöntämällä kehittäjävarmenteella, jotta käyttäjät voivat varmistaa niiden eheyden.

macOS:ssä koodin allekirjoitus ja oikeaksi todistaminen toimivat itsenäisesti, ja eri toimijat voivat tehdä niitä eri tavoitteita varten. Koodin allekirjoituksen tekee kehittäjä omalla kehittäjän tunnuksen varmenteellaan (jonka Apple on myöntänyt). Tämän allekirjoituksen varmistaminen takaa käyttäjälle, että kehittäjän ohjelmistoa ei ole peukaloitu sen jälkeen, kun kehittäjä on luonut ja allekirjoittanut sen. Oikeaksi todistamisen voi tehdä kuka tahansa ohjelmiston jakeluketjussa, ja se takaa, että Applelle on tarjottu koodista kopio, joka on tarkistettu haittaohjelmistojen varalta, eikä siitä ole löytynyt tunnettua haittaohjelmistoa. Oikeaksi todistamisen tuloksena on tiketti, joka tallennetaan Applen palvelimille, ja se voidaan valinnaisesti pinota appiin (kuka tahansa voi tehdä sen) mitätöimättä kehittäjän allekirjoitusta.

Pakollinen pääsynhallinta (Mandatory Access Controls, MACs) edellyttää koodin allekirjoittamista järjestelmän suojaamien oikeuksien sallimista varten. Esimerkiksi palomuurin läpäisyä vaativien appien koodi täytyy allekirjoittaa sopivalla MAC-oikeudella.

Gatekeeper ja ajonaikainen suojaus macOS:ssä

macOS tarjoaa Gatekeeper-teknologian ja ajonaikaisen suojauksen, jotka auttavat varmistamaan, että käyttäjän Macissa toimii vain luotettu ohjelmisto.

Gatekeeper

macOS sisältää suojausteknologian nimeltä *Gatekeeper*, joka on suunniteltu auttamaan varmistamaan, että vain luotettu ohjelmisto toimii käyttäjän Macissa. Kun käyttäjä lataa ja avaa apin, liitännäisen tai asennuspaketin muualta kuin App Storesta, Gatekeeper tarkistaa, että ohjelmisto on tunnetulta kehittäjältä ja että Apple on todistanut, ettei siinä ole tunnettua haitallista sisältöä eikä sitä ole muokattu. Gatekeeper myös pyytää käyttäjän hyväksyntää ennen ladatun ohjelmiston ensimmäistä avaamista, jottei käyttäjää varmasti ole huijattu suorittamaan koodia, jonka käyttäjä uskoi olevan vain datatiedosto.

Oletuksena Gatekeeper auttaa varmistamaan, että kaikki ladattu ohjelmisto on App Storen allekirjoittamaa tai rekisteröidyn kehittäjän allekirjoittamaa ja Applen oikeaksi todistamaa. App Storen tarkistusprosessi ja oikeaksi todistaminen on suunniteltu varmistamaan, että apit eivät sisällä tunnettua haittaohjelmistoa. Siksi oletusarvoisesti *kaikki macOS:ssä oleva ohjelmisto tarkistetaan tunnettujen haittaohjelmistojen varalta, kun se avataan ensimmäisen kerran, riippumatta siitä, kuinka se on tullut Maciin*.

Käyttäjillä ja organisaatioilla on mahdollisuus sallia vain App Storesta asennettu ohjelmisto. Vaihtoehtoisesti käyttäjät voivat ohittaa Gatekeeperin käytännöt ja avata minkä tahansa ohjelmiston, jollei sitä ole rajoitettu mobiililaitteiden hallintaratkaisulla (MDM). Organisaatiot voivat määrittää MDM:llä Gatekeeperin asetukset, mukaan lukien sellaisen ohjelmiston salliminen, joka on allekirjoitettu eri identiteeteillä. Gatekeeper voidaan myös ottaa tarvittaessa kokonaan pois käytöstä.

Gatekeeper suojaa myös haitallisten liitännäisten jakelulta harmittomien appien mukana. Sellaisessa jakelutavassa apin käyttäminen käynnistää haitallisen liitännäisen lataamisen käyttäjän tietämättä. Tarvittaessa Gatekeeper avaa apit satunnaisesta kirjoitussuojatusta sijainnista. Tämä on suunniteltu estämään apin mukana tulevien liitännäisten automaattista lataamista.

Ajonaikainen suojaus

Järjestelmätiedostot, resurssit ja kernel on suojattu käyttäjän appitilalta. Kaikkien App Store -appien pääsyä muiden appien tietoihin on rajoitettu eristyksellä. Jos App Storesta hankittu appi tarvitsee toisen apin tietoja, se voi käyttää niitä vain macOS:n tarjoamilla rajapinnoilla ja palveluilla.

Suojaaminen haittaohjelmistoilta macOS:ssä

Apple tunnistaa ja estää haittaohjelmistoja käyttäen uhkatietojen analysointiprosessia.

Kolme suojauskerrosta

Haittaohjelmistosuojaukset on jaettu kolmeen kerrokseen:

1. *Haittaohjelmiston käynnistämisen tai suorittamisen estäminen:* App Store tai Gatekeeper yhdessä oikeaksi todistamisen kanssa

2. *Haittaohjelmiston suorittamisen estäminen asiakasjärjestelmissä:* Gatekeeper, oikeaksi todistaminen ja XProtect

3. *Suoritetun haittaohjelmiston korjaaminen:* XProtect

Ensimmäinen suojauskerros on suunniteltu ehkäisemään haittaohjelmistojen jakelua ja estämään niitä käynnistymästä kertaakaan. Tämä on sekä App Storen että Gatekeeperin ja oikeaksi todistamisen tavoite.

Seuraava suojauskerros auttaa varmistamaan, että jos haittaohjelmisto pääsee Maciin, se tunnistetaan ja estetään nopeasti. Tämän tavoitteena on estää leviäminen ja korjata Mac-järjestelmät, jos haittaohjelmisto on jo saanut siellä jalansijaa. XProtect täydentää tätä suojausta yhdessä Gatekeeperin ja oikeaksi todistamisen kanssa.

Lopuksi XProtect toimii korjatakseen haittaohjelmiston, joka on onnistunut käynnistymään.

Yhdessä nämä suojaukset, joista kerrotaan tarkemmin jäljempänä, tukevat parhaiden käytäntöjen mukaista suojausta viruksilta ja haittaohjelmistoilta. Erityisesti Apple siliconilla varustetussa Macissa on lisäsuojauksia, joilla rajoitetaan mahdollisia haittaohjelmiston aiheuttamia vahinkoja, jos se on onnistunut käynnistymään. Katso ohjeesta Appien pääsyoikeuden estäminen käyttäjätietoihin tapoja, joilla macOS voi auttaa suojaamaan käyttäjän tietoja haittaohjelmistoilta, ja ohjeesta Käyttöjärjestelmän eheys tapoja, joilla macOS voi rajoittaa toimintoja, joita haittaohjelmisto voi suorittaa järjestelmässä.

Notarisointi

Notarisointi on Applen tarjoama haittaohjelmistojen tunnistuspalvelu. Kehittäjät, jotka haluavat jaella macOS-appeja App Storen ulkopuolella, lähettävät appinsa tarkistettaviksi osana jakeluprosessia. Apple tarkistaa ohjelmiston tunnettujen haittaohjelmistojen varalta, ja jos niitä ei löydetä, se luo oikeaksi todistamisen tiketin. Yleensä kehittäjät liittävät tämän tiketin appiinsa, jotta Gatekeeper voi tarkistaa ja käynnistää apin myös offline-tilassa.

Apple voi myös luoda kumoamistiketin apeille, jotka ovat tunnetusti haitallisia, vaikka ne olisi todistettu aiemmin oikeiksi. macOS tarkistaa säännöllisesti uudet kumoamistiketit, jotta Gatekeeperillä on uusimmat tiedot ja jotta se voi estää sellaisten tiedostojen käynnistyksen. Tämä prosessi voi estää haittaohjelmia erittäin nopeasti, sillä taustalla tehtäviä päivityksiä tehdään paljon useammin kuin uusia XProtect-allekirjoituksia lähettäviä taustalla tehtäviä päivityksiä. Lisäksi tätä suojausta voidaan käyttää sekä appeihin, jotka on aiemmin todistettu oikeiksi, että appeihin, joita ei ole aiemmin todistettu oikeiksi.

XProtect

macOS:ssä on sisäänrakennettuna virustorjuntateknologia nimeltä *XProtect* tunnistepohjaista haittaohjelmistojen tunnistusta ja poistamista varten. Järjestelmä käyttää YARA-tunnisteita. Ne ovat työkalu haittaohjelmistojen tunnistamiseen tunnisteen perusteella, ja Apple päivittää allekirjoituksia säännöllisesti. Apple tarkkailee uusien haittaohjelmistojen tartuntoja ja leviämistä ja päivittää tunnisteita automaattisesti riippumatta järjestelmän päivityksistä auttaakseen suojelemaan Macia haittaohjelmistoilta. XProtect tunnistaa ja estää automaattisesti tunnetun haittaohjelmiston suorittamisen. macOS 10.15:ssä ja uudemmissa XProtect tarkistaa tunnetun haittasisällön varalta aina, kun:

- Appi käynnistetään ensimmäistä kertaa
- Appi on muuttunut (tiedostojärjestelmässä)
- Xprotect-tunnisteita päivitetään

Kun XProtect havaitsee tunnetun haittaohjelmiston, ohjelmisto estetään, käyttäjälle ilmoitetaan ja hänelle annetaan mahdollisuus siirtää ohjelmisto roskakoriin.

Huomaa: Notarisointi toimii tunnetuille tiedostoille (tai tiedostotiivisteille), ja sitä voidaan käyttää apeissa, jotka on jo aiemmin käynnistetty. XProtectin tunnistepohjaiset säännöt ovat yleisluontoisempia kuin tietty tiedostotiiviste, joten se voi löytää versioita, joita Apple ei ole huomannut. XProtect tarkistaa vain apit, jotka ovat muuttuneet tai jotka käynnistetään ensimmäistä kertaa.

XProtect sisältää myös haitat korjaavaa teknologiaa siltä varalta, että haittaohjelma pääsisi Maciin saakka. Se esimerkiksi korjaa haittaohjelmistotartuntoja Applen automaattisesti toimittamien päivitysten perusteella (toimitetaan osana automaattisia järjestelmän datatiedostojen päivityksiä ja suojauspäivityksiä). Se myös poistaa haittaohjelmiston saadessaan päivitettyä tietoa ja tekee määräajoin tarkistuksia tartuntojen varalta. XProtect ei käynnistä Macia automaattisesti uudelleen.

XProtectin automaattiset suojauspäivitykset

Apple julkistaa päivitykset XProtectille automaattisesti uusimpien uhkatietojen perusteella. Oletuksena macOS tarkistaa nämä päivitykset päivittäin. Oikeaksi todistamisen päivitykset, jotka toimitetaan CloudKit-synkronoinnilla, tapahtuvat paljon useammin.

Miten Apple toimii, kun uusi haittaohjelmisto havaitaan

Kun haittaohjelmisto havaitaan, voidaan tehdä useita toimenpiteitä:

- Siihen liittyvät kehittäjävarmenteet perutaan.
- Oikeaksi todistamisen kumoustiketit luodaan kaikille tiedostoille (apeille ja siihen liittyville tiedostoille).
- Xprotect-tunnisteita kehitetään ja julkaistaan.

  Näitä tunnisteita käytetään myös takautuvasti aiemmin oikeiksi todistettuihin ohjelmistoihin. Jos tehdään uusia havaintoja, voidaan tehdä yksi tai useampi edellä kerrotuista toiminnoista.

Haittaohjelmiston havaitseminen laukaisee toimenpidesarjan seuraavien sekuntien, tuntien ja päivien aikana, jotta Mac-käyttäjillä on käytössään paras mahdollinen suojaus.

Appien tiedostojen käytön hallinta macOS:ssä

Applen mielestä käyttäjillä täytyy olla oikeus täyteen läpinäkyvyyteen, suostumuksen antamiseen ja sen hallintaan, mitä apit tekevät käyttäjien tiedoilla. macOS 10.15:ssä järjestelmä vaatii tätä toimintamallia, joka auttaa varmistamaan, että kaikkien appien täytyy saada käyttäjän hyväksyntä, ennen kuin ne voivat käyttää Dokumentit-, Lataukset- tai Työpöytä-kansiossa, iCloud Drivessa tai verkkotaltioilla olevia tiedostoja. macOS 10.13:ssa ja uudemmissa tallennuslaitteen täyttä käyttöoikeutta vaativat apit täytyy lisätä varta vasten Järjestelmäasetuksissa. Lisäksi käyttöapu- ja automaatio-ominaisuudet vaativat käyttäjän luvan. Tämä auttaa varmistamaan, etteivät ne kierrä muita suojauksia. Pääsykäytännöstä riippuen käyttäjiä voidaan pyytää muuttamaan tai heidän voi olla tarpeen muuttaa asetusta kohdassa Järjestelmäasetukset > Suojaus ja yksityisyys > Yksityisyys:

Kohde	**Appi pyytää käyttäjältä**	**Käyttäjän täytyy muuttaa tietosuoja-asetuksia**
Käyttöapu		✓
Sisäisen tallennustilan täysi käyttöoikeus		✓
Tiedostot ja kansiot *Huomaa:* Sisältää Työpöydän, Dokumentit, Lataukset, verkkotaltiot ja siirrettävät taltiot	✓	
Automaatio (Applen tapahtumat)	✓	

Käyttäjän Roskakorissa olevat kohteet on suojattu kaikilta apeilta, joilla on levyn täysi käyttöoikeus. Käyttäjältä ei pyydetä apin käyttöoikeutta. Jos käyttäjä haluaa, että apit voivat käyttää tiedostoja, ne täytyy siirtää Roskakorista muuhun sijaintiin.

Kun käyttäjä laittaa FileVaultin päälle Macissa, käyttäjältä pyydetään voimassa olevat tunnistetiedot ennen käynnistysprosessin jatkamista ja pääsyn saamista erityisiin käynnistystiloihin. Ilman sisäänkirjautumistietoja tai palautusavainta koko taltio on salattu ja suojattu luvattomalta käytöltä, vaikka tallennuslaite irrotettaisiin ja kiinnitettäisiin toiseen tietokoneeseen.

Jotta tiedot pysyvät suojattuina yritysympäristössä, IT-osaston täytyy määrittää FileVault-asetuskäytännöt käyttäen mobiililaitteiden hallintaa (MDM). Organisaatiot voivat hallita salattuja taltioita useilla eri tavoilla, kuten organisaation palautusavaimilla, henkilökohtaisilla palautusavaimilla (jotka voidaan valinnaisesti tallentaa MDM:llä) tai niiden yhdistelmällä. Avaimen kierrättäminen voidaan myös asettaa käytännöksi MDM:llä.

Suojausominaisuudet Muistiinpanot-apissa

Muistiinpanot-apissa iPhonessa, iPadissa, Macissa ja iCloud-verkkosivustolla on Suojatut muistiinpanot -ominaisuus, jolla käyttäjät voivat suojata tiettyjen muistiinpanojen sisällön. Käyttäjät voivat myös jakaa muistiinpanoja suojatusti muiden kanssa.

Suojatut muistiinpanot

Suojatut muistiinpanot on salattu päästä päähän käyttäjän antamalla salauslauseella, joka vaaditaan muistiinpanojen katsomiseen iOS-, iPadOS- ja macOS-laitteissa ja iCloud-verkkosivustolla. Jokaisella iCloud-tilillä (mukaan lukien Omassa laitteessa -laitetilit) voi olla erillinen salauslause.

Kun käyttäjä suojaa muistiinpanon, 16-tavuinen avain johdetaan käyttäjän salauslauseesta PBKDF2:lla ja SHA256:lla. Muistiinpano ja kaikki sen liitteet salataan AES-GCM:llä (Galois/Counter Mode). Core Dataan ja CloudKitiin luodaan uudet tietueet, joihin tallennetaan salattu muistiinpano, liitteet, tunniste ja valmisteluvektori. Kun uudet tietueet on luotu, alkuperäiset salaamattomat tiedot poistetaan. Salausta tukevia liitteitä ovat kuvat, piirrokset, taulukot, kartat ja verkkosivut. Muuntyyppisiä liitteitä sisältäviä muistiinpanoja ei voida salata. Ei-tuettuja liitteitä ei voida myöskään lisätä suojattuihin muistiinpanoihin.

Jos käyttäjä haluaa katsoa suojattua muistiinpanoa, hänen täytyy syöttää oma salauslauseensa tai suorittaa todennus Face ID:llä tai Touch ID:llä. Kun käyttäjän todentaminen suojatun muistiinpanon katselua tai luomista varten on onnistunut, Muistiinpanot avaa suojatun istunnon. Kun suojattu istunto on avoinna, käyttäjä voi katsoa tai suojata muita muistiinpanoja ilman lisätodentamista. Suojattu istunto koskee kuitenkin vain muistiinpanoja, jotka on suojattu annetulla salauslauseella. Käyttäjän täytyy silti todentautua eri salauslauseella suojattuja muistiinpanoja varten. Suojattu istunto suljetaan, kun:

- käyttäjä napauttaa Muistiinpanoissa Lukitse nyt -painiketta
- Muistiinpanot vaihdetaan taustalle yli kolmeksi minuutiksi (8 minuutiksi macOS:ssä)
- iOS- tai iPadOS-laite lukittuu.

Jos käyttäjä haluaa muuttaa suojatun muistiinpanon salauslausetta, käyttäjän täytyy syöttää nykyinen salauslause, koska Face ID:tä ja Touch ID:tä ei voi käyttää salauslauseen muuttamiseen. Kun uusi salauslause on valittu, Muistiinpanot-appi salaa uudelleen kaikkien samalla tilillä olevien edellisellä salauslauseella salattujen muistiinpanojen avaimet.

Jos käyttäjä kirjoittaa salauslauseen väärin kolme kertaa peräkkäin, Muistiinpanot-appi näyttää käyttäjän antaman vihjeen, jos käyttäjä antoi vihjeen käyttöönoton yhteydessä. Jos käyttäjä ei edelleenkään muista salauslausetta, hän voi nollata sen Muistiinpanojen asetuksissa. Tällä ominaisuudella käyttäjät voivat luoda uusia suojattuja muistiinpanoja, joissa on uusi salauslause, mutta he eivät pääse näkemään aiemmin suojattuja muistiinpanoja. Aiemmin suojattuja muistiinpanoja voidaan edelleen katsoa, jos vanha salauslause muistetaan. Salauslauseen nollaaminen edellyttää käyttäjän iCloud-tilin salauslausetta.

Jaetut muistiinpanot

Muistiinpanot, joita ei ole salattu päästä päähän salauslauseella, voidaan jakaa muiden kanssa. Jaetut muistiinpanot käyttävät edelleen CloudKit-salattua datatyyppiä teksteille ja liitteille, joita käyttäjä laittaa muistiinpanoon. Tiedot salataan aina avaimella, joka on salattu CKRecord-tietueessa. Metatietoja, kuten luomis- ja muokkauspäivämääriä, ei salata. CloudKit hallitsee prosessia, jolla osallistujat voivat salata toistensa tietoja ja poistaa niiden salauksen.

Suojausominaisuudet Pikakomennot-apissa

Pikakomennot-apin pikakomennot voidaan valinnaisesti synkronoida Apple-laitteiden välillä iCloudin avulla. Pikakomennot voidaan myös jakaa muille käyttäjille iCloudin kautta. Pikakomennot tallennetaan paikallisesti salatussa muodossa.

Muokatut pikakomennot ovat monikäyttöisiä – ne ovat samankaltaisia kuin skriptit tai ohjelmat. Kun käyttäjä lataa pikakomentoja internetistä, käyttäjää varoitetaan, että Apple ei ole tarkistanut pikakomentoa, ja käyttäjälle annetaan mahdollisuus tarkistaa pikakomento. Laitteen suojaamiseksi haitallisilta pikakomennoilta järjestelmä lataa päivitetyt haittaohjelmistojen määritelmät. Tämän ansiosta haitalliset pikakomennot voidaan havaita ajonaikaisesti.

Muokatut pikakomennot voivat myös suorittaa käyttäjän määrittämän JavaScriptin Safarin verkkosivustoilla, kun ne avataan jakosivulta. Jotta laitetta suojattaisiin haitalliselta JavaScriptiltä, joka esimerkiksi huijaa käyttäjän suorittamaan skriptin käyttäjien tietoja keräävän sosiaalisen median verkkosivulla, JavaScript varmistetaan edellä mainittujen haittaohjelmistomääritelmien avulla. Kun käyttäjä suorittaa JavaScriptin ensimmäistä kertaa domainissa, käyttäjää kehotetaan sallimaan JavaScriptin sisältämien pikakomentojen suorittaminen kyseisen domainin nykyisellä verkkosivulla.

Palveluiden suojaus

Palveluiden suojauksen yleiskatsaus

Applella on laaja valikoima palveluita, joiden avulla käyttäjät saavat enemmän irti laitteistaan. Nämä palvelut tarjoavat tehokkaita ominaisuuksia pilvitallennukseen, synkronointiin, salasanan säilytykseen, todentamiseen, maksuun, viestintään ja muuhun suojaten samalla käyttäjien yksityisyyttä ja tietoja.

Tässä luvussa käsitellään suojausteknologioita, joita käytetään iCloudissa, Kirjaudu sisään Applella -palvelussa, Apple Payssa, iMessagessa, Apple Messages for Business -palvelussa, FaceTimessa, Missä on…? -palvelussa ja Jatkuvuus-palvelussa.

Huomaa: Kaikki Applen palvelut ja sisältö eivät ole käytettävissä kaikissa maissa tai kaikilla alueilla.

Apple ID ja hallittu Apple ID

Apple ID:n suojauksen yleiskatsaus

Apple ID on tili, jolla kirjaudutaan Applen palveluihin. Käyttäjien on tärkeää huolehtia Apple ID:nsä suojaamisesta estääkseen siltä osin tiliensä luvatonta käyttöä. Tämän edesauttamiseksi Apple ID:ille vaaditaan vahvat salasanat, jotka:

- ovat vähintään kahdeksan merkin pituisia
- sisältävät sekä kirjaimia että numeroita
- eivät saa sisältää kolmea tai useampaa samanlaista merkkiä peräkkäin
- eivät saa olla yleisesti käytettyjä salasanoja.

Käyttäjiä suositellaan luomaan vielä näitä sääntöjä vahvempia salasanoja lisäämällä salasanaan ylimääräisiä merkkejä ja välimerkkejä.

Apple lähettää lisäksi käyttäjille sähköpostiviestejä tai push-ilmoituksia tai molempia, kun tiliin tehdään tärkeitä muutoksia. Tällaisia muutoksia ovat esimerkiksi salasanan tai laskutustietojen muutokset tai Apple ID:n käyttäminen kirjautumiseen uudella laitteella. Jos käyttäjä huomaa mitään epäilyttävää, käyttäjiä ohjeistetaan vaihtamaan Apple ID:n salasana välittömästi.

Lisäksi Apple noudattaa useita käyttäjätilien suojaamiseksi laadittuja käytäntöjä ja menettelyitä. Näitä ovat sisäänkirjautumisen ja salasanan nollaamisen yrityskertojen määrän rajoittaminen, aktiivinen petosten valvonta, jolla pyritään tunnistamaan identiteettihyökkäykset niiden tapahtuessa, sekä käytäntöjen säännölliset arvioinnit, joiden myötä Apple pystyy sovittamaan toimintansa uuteen käyttäjien suojauksen kannalta merkitykselliseen tietoon.

Huomaa: Apple School Managerin tai Apple Business Managerin ylläpitäjä määrittää hallitun Apple ID:n salasanakäytännön.

Kaksiosainen todennus

Auttaakseen käyttäjiä suojaamaan tilinsä vieläkin paremmin Apple käyttää oletuksena *kaksiosaista todennusta* Apple ID:n lisäturvana. Se on suunniteltu varmistamaan, että vain tilin haltija pääsee tilille, vaikka joku muu tietäisikin salasanan. Kaksiosaista todennusta käytettäessä käyttäjän tilille pääsee vain luotetuista laitteista, kuten käyttäjän iPhonesta, iPadista, iPod touchista tai Macista, tai muista laitteista sitten, kun vahvistus on ensin suoritettu käyttäen joko luotettua laitetta tai luotettua puhelinnumeroa. Kirjauduttaessa ensimmäistä kertaa sisään uudella laitteella tarvitaan kaksi tunnistustietoa: Apple ID:n salasana ja kuusinumeroinen vahvistuskoodi, joka näkyy käyttäjän luotetuissa laitteissa tai lähetetään luotettuun puhelinnumeroon. Syöttämällä koodin käyttäjä vahvistaa, että hän luottaa uuteen laitteeseen ja että sisäänkirjautuminen on turvallista. Koska pelkkä salasana ei riitä tilille pääsemiseen, kaksiosainen todennus parantaa käyttäjän Apple ID:n ja kaikkien hänen Applelle tallentamiensa henkilötietojen suojausta. Se on integroitu suoraan iOS:ään, iPadOS:ään, macOS:ään, tvOS:ään, watchOS:ään ja Applen verkkosivustoilla käytettäviin todentamisjärjestelmiin.

Kun käyttäjä kirjautuu Applen verkkosivustolle käyttäen verkkoselainta, todennuksen toisena osana kaikkiin käyttäjän iCloud-tiliin liitettyihin luotettuihin laitteisiin lähetetään pyyntö hyväksyä selainistunto. Jos käyttäjä kirjautuu Applen verkkosivustolle luotetun laitteen selaimesta, vahvistuskoodi näkyy hänen käyttämässään laitteessa. Kun käyttäjä syöttää koodin laitteeseen, selainistunto hyväksytään.

Salasanan nollaaminen ja tilin palauttaminen

Jos Apple ID -tilin salasana unohtuu, käyttäjä voi nollata sen luotetulla laitteella. Jos luotettua laitetta ei ole käytettävissä ja salasana on tiedossa, käyttäjä voi suorittaa tekstiviestitodennuksen luotetun puhelinnumeron kautta. Lisäksi Apple ID voidaan palauttaa välittömästi käyttämällä aikaisemmin käytettyä pääsykoodia yhdessä tekstiviestin kanssa nollaamiseen. Jos näitä vaihtoehtoja ei voida käyttää, on noudatettava tilin palauttamisen prosessia. Jos haluat lisätietoja, katso Applen tukiartikkeli Tilin palautuksen käyttäminen, kun et voi nollata Apple ID:si salasanaa.

Hallitun Apple ID:n suojaus

Hallitut Apple ID:t toimivat kuten Apple ID, mutta ne omistaa ja niitä hallitsee yritys tai koulutusalan organisaatio. Nämä organisaatiot voivat nollata salasanoja, rajoittaa ostamista ja viestintää kuten FaceTimea ja Viestit-appia sekä määrittää rooleihin perustuvia oikeuksia työntekijöille, henkilöstölle, opettajille ja opiskelijoille.

Joitakin palveluita (kuten Apple Pay, iCloud-avainnippu, HomeKit ja Missä on...?) ei voi käyttää hallituilla Apple ID:illä.

Hallittujen Apple ID:iden tarkastaminen

Hallitut Apple ID:t myös tukevat *tarkastamista*, minkä ansiosta organisaatiot pystyvät täyttämään lain ja tietosuojan vaatimukset. Apple School Manager -ylläpitäjä, vastuuhenkilö tai opettaja voi tarkastaa tiettyjä hallittuja Apple ID -tilejä.

Tarkastajat voivat valvoa ainoastaan organisaation hierarkiassa omansa alapuolella olevia tilejä. Esimerkiksi opettajat voivat valvoa opiskelijoita, vastuuhenkilöt voivat tarkastaa opettajien ja opiskelijoiden tilejä ja ylläpitäjät voivat tarkastaa vastuuhenkilöiden, opettajien ja opiskelijoiden tilejä.

Kun Apple School Managerissa pyydetään tarkastustoiminnon kirjautumistietoja, luodaan erityinen tili, jolla on pääsy ainoastaan siihen hallittuun Apple ID:hen, jolle tarkastustoimintoa pyydettiin. Tarkastaja voi lukea ja muokata käyttäjän sisältöä, joka on tallennettu iCloudiin tai CloudKitiä käyttäviin appeihin. Jokainen tarkastuspääsyoikeuspyyntö kirjataan lokiin Apple School Managerissa. Lokeista näkyy, kuka tarkastaja oli, hallittu Apple ID, johon tarkastaja pyysi pääsyä, pyynnön ajankohta sekä suoritettiinko tarkastusta.

Hallitut Apple ID:t ja henkilökohtaiset laitteet

Hallittuja Apple ID:itä voidaan käyttää myös henkilökohtaisessa omistuksessa olevissa iOS- ja iPadOS-laitteissa ja Mac-tietokoneissa. Opiskelijat kirjautuvat sisään iCloudiin käyttäen oppilaitoksensa antamaa hallittua Apple ID:tä sekä lisäksi kotikäytön salasanaa, joka toimii toisena osana Apple ID:n kaksiosaisessa todennusprosessissa. Kun opiskelijat käyttävät henkilökohtaisessa laitteessa hallittua Apple ID:tä, iCloud-avainnippu ei ole käytettävissä, ja oppilaitos saattaa rajoittaa muita ominaisuuksia, kuten FaceTimea ja Viestit-appia. Kaikkia iCloud-dokumentteja, jotka opiskelijat luovat ollessaan sisäänkirjautuneina, voidaan tarkastaa edellä tässä osiossa kuvatulla tavalla.

iCloud

iCloudin suojauksen yleiskatsaus

iCloud tallentaa muun muassa käyttäjän yhteystiedot, kalenterit, kuvat ja dokumentit ja pitää tiedot ajan tasalla kaikissa käyttäjän laitteissa automaattisesti. Myös muiden valmistajien apit voivat käyttää iCloudia dokumenttien sekä appidatan avainarvojen tallentamiseen ja synkronoimiseen kehittäjän määrittämällä tavalla. Käyttäjät ottavat iCloudin käyttöön kirjautumalla sisään Apple ID:llä ja valitsemalla, mitä palveluita he haluavat käyttää. IT-ylläpitäjät voivat ottaa tietyt iCloudin ominaisuudet, kuten iCloud Driven ja iCloud-varmuuskopion, pois käytöstä mobiililaitteiden hallinnan (MDM) asetusprofiileilla.

iCloud käyttää vahvoja suojauksia ja noudattaa tiukkoja käytäntöjä käyttäjien tietojen suojaamiseksi. Suurin osa iCloudin tiedoista salataan ensin käyttäjän laitteessa käyttäen laitteen muodostamia iCloud-avaimia, ennen kuin ne ladataan iCloud-palvelimille. Niitä tietoja varten, jotka eivät ole päästä päähän salattuja, käyttäjän laite lähettää suojatusti nämä iCloud-avaimet iCloudin laitteiston suojausmoduuleihin (HSM) Applen datakeskuksissa. Näin Apple voi auttaa käyttäjää tietojen palauttamisessa ja purkaa tarvittaessa tietojen salauksen käyttäjän puolesta (esimerkiksi kun käyttäjä kirjautuu sisään uudella laitteella, palauttaa tiedot varmuuskopiosta tai käyttää iCloud-tietojaan verkkoselaimella). Käyttäjän laitteiden ja iCloud-palvelimien välillä liikkuvat tiedot salataan siirrettäessä erikseen TLS:llä, ja iCloud-palvelimet lisäävät vielä yhden salauskerroksen levossa olevien käyttäjän tietojen suojaksi.

Kun salausavaimet ovat Applen saatavilla, ne on suojattu Applen datakeskuksissa. Kolmannen osapuolen datakeskukseen tallennettuja tietoja prosessoitaessa näitä salausavaimia käyttää vain Applen ohjelmisto, joka toimii suojatuilla palvelimilla, ja vain välttämättömän prosessoinnin aikana. Tietosuojan ja tietoturvan lisäämiseksi monet Applen palvelut käyttävät päästä päähän -salausta, mikä tarkoittaa, että ainoastaan käyttäjät itse pääsevät iCloud-tietoihinsa ja on ainoastaan luotetuilta laitteilta, joihin he ovat kirjautuneet Apple ID:llään.

Apple tarjoaa käyttäjille kaksi vaihtoehtoa iCloudiin tallennettujen tietojensa salaamiseen ja suojaamiseen:

- **Vakiomuotoinen tietosuojaus (oletusasetus):** Käyttäjän iCloud-tiedot salataan, salausavaimet suojataan Applen datakeskuksissa ja Apple voi auttaa tietojen ja tilin palauttamisessa. Vain tietyt iCloud-tiedot salataan päästä päähän. Näitä päästä päähän salattuja tietokategorioita on 14, ja niitä ovat esimerkiksi Terveys-apin tiedot ja iCloud-avainnipun salasanat.
- **iCloudin edistyksellinen tietosuojaus:** Tämä valinnainen asetus tarjoaa Applen korkeimman tason suojauksen pilvidatalle. Jos käyttäjä valitsee edistyksellisen tietosuojauksen, ainoastaan hänen luotetut laitteensa voivat käyttää salausavaimia valtaosalle hänen iCloud-tiedoistaan, jotka on näin suojattu päästä päähän -salauksella. Kun edistyksellinen tietosuojaus laitetaan päälle, päästä päähän salattujen tietokategorioiden määrä kasvaa 23:een sisältäen muun muassa iCloud-varmuuskopion, Kuvat ja Muistiinpanot.

Päästä päähän -salauksella suojattujen iCloud-tietojen kategoriat on lueteltu Applen tukiartikkelissa iCloudin suojauksen yleiskatsaus.

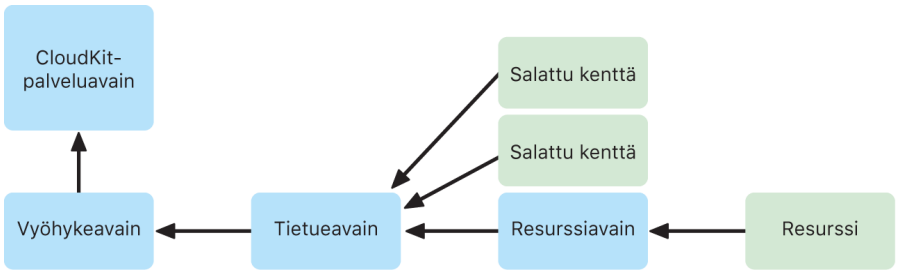
iCloudin salaus

Tietojen salaus iCloudissa on tiiviisti sidoksissa tietojen tallennusmalliin. Se alkaa CloudKit-sovelluskehyksistä ja rajapinnoista, jotka mahdollistavat apeille ja järjestelmäohjelmistoille tietojen tallentamisen iCloudiin käyttäjän puolesta ja pitävät kaiken ajan tasalla eri laitteissa ja verkossa.

CloudKitin salaus

CloudKit on sovelluskehys, joka mahdollistaa appikehittäjille avainarvodatan, rakenteisen datan ja resurssien (suuren datan, joka tallennetaan erillään tietokannasta, kuten kuvat ja videot) tallentamisen iCloudiin. CloudKit tukee sekä julkisia että yksityisiä tietokantoja säiliöihin ryhmiteltyinä. Julkiset tietokannat ovat yleisesti jaettuja ja niitä käytetään tyypillisesti yleisluontoisille resursseille eikä niitä salata. Yksityisiin tietokantoihin tallennetaan kunkin käyttäjän iCloud-tiedot.

CloudKit käyttää avainhierarkiaa, joka vastaa tietojen rakennetta. Kunkin säiliön yksityinen tietokanta on suojattu avainhierarkialla, jonka juuri on epäsymmetrinen avain nimeltä *CloudKit-palveluavain*. Nämä avaimet ovat erilaiset jokaiselle iCloud-käyttäjälle, ja ne muodostetaan käyttäjän luotetussa laitteessa. Kun tietoja kirjoitetaan CloudKitiin, kaikki tietueavaimet muodostetaan käyttäjän luotetussa laitteessa ja salataan asiaankuuluvalla avainhierarkialla ennen minkään tietojen lataamista palvelimelle.



Monissa Applen palveluissa, jotka on lueteltu Applen tukiartikkelissa iCloudin suojauksen yleiskatsaus, käytetään päästä päähän -salausta ja iCloud-avainnipun synkronoinnilla suojattua CloudKit-palveluavainta. Näiden CloudKit-säiliöiden palveluavaimet on tallennettu käyttäjän iCloud-avainnippuun, ja niiden suojausominaisuudet ovat samat kuin iCloud-avainnipulla, eli avaimet ovat käytettävissä vain käyttäjän luotetuissa laitteissa, eivätkä Apple tai kolmannet osapuolet pääse niihin. Mikäli laite katoaa, käyttäjä voi palauttaa iCloud-avainnippunsa tiedot käyttämällä iCloud-avainnipun suojattua palautusta, tilin palautuksen yhteyshenkilöitä tai tilin palautusavainta.

Salausavainten hallinta

CloudKitin salattujen tietojen suojaus perustuu vastaavien salausavainten suojaukseen. CloudKit-palveluavaimet jaetaan kahteen kategoriaan: päästä päähän salattuihin ja todennuksen jälkeen saatavilla oleviin.

- **Päästä päähän salatut palveluavaimet:** Päästä päähän salattuihin iCloud-palveluihin tarvittavat CloudKit-palvelun yksityiset avaimet eivät koskaan ole Applen palvelinten saatavilla. Palveluavainparit, jotka sisältävät yksityiset avaimet, luodaan paikallisesti käyttäjän luotetussa laitteessa ja siirretään käyttäjän muihin laitteisiin käyttäen iCloud-avainnipun suojausta. Vaikka Applen palvelimet toimivat välittäjinä iCloud-avainnipun palautuksessa ja synkronoinnissa, pääsy käyttäjän avainnipputietoihin on estetty näiltä palvelimilta salauksen avulla. Siinä pahimmassa tapauksessa, että käyttäjä menettää keinonsa käyttää iCloud-avainnippua ja kaikkia sen palautusmekanismeja, myös päästä päähän salatut tiedot CloudKitissä menetetään. Apple ei voi auttaa palauttamaan näitä tietoja.
- **Todennuksen jälkeen saatavilla olevat palveluavaimet:** Muiden palveluiden, kuten Kuvien ja iCloud Driven, palveluavaimet tallennetaan iCloudin laitteiston suojausmoduuleihin Applen datakeskuksissa, ja jotkin Applen palvelut voivat käyttää niitä. Kun käyttäjä kirjautuu iCloudiin uudella laitteella ja suorittaa todennuksen Apple ID:llään, Applen palvelimet voivat käyttää näitä avaimia ilman, että käyttäjältä tarvitaan enää muita toimia. Esimerkiksi kun käyttäjä on kirjautunut iCloud.comiin, hän voi saman tien katsella kuviaan verkossa. Tällaiset palveluavaimet ovat *todennuksen jälkeen saatavilla olevia* avaimia.

iCloudin edistyksellinen tietosuojaus

iCloudin edistyksellinen tietosuojaus on valinnainen asetus, joka tarjoaa Applen korkeimman tason suojauksen pilvidatalle. Kun käyttäjä laittaa edistyksellisen tietosuojauksen päälle, ainoastaan hänen luotetut laitteensa voivat käyttää salausavaimia valtaosalle käyttäjän iCloud-tiedoista, jotka on näin suojattu *päästä päähän -salauksella*. Jos käyttäjä laittaa edistyksellisen tietosuojauksen päälle, päästä päähän salattujen tietokategorioiden määrä kasvaa 14:stä 23:een sisältäen muun muassa iCloud-varmuuskopion, Kuvat ja Muistiinpanot.

iCloudin edistyksellinen tietosuojaus on saatavilla käyttäjille Yhdysvalloissa vuoden 2022 loppuun mennessä, ja sen tuominen muille markkinoille aloitetaan alkuvuodesta 2023.

Edistyksellisen tietosuojauksen ajatus on yksinkertainen: Kaikki CloudKit-palveluavaimet, jotka laite on muodostanut ja jotka on sen jälkeen lähetetty *todennuksen jälkeen saatavilla oleviin* iCloudin laitteiston suojausmoduuleihin (HSM) Applen datakeskuksissa, poistetaan näistä laitteiston suojausmoduuleista ja säilytetään sen sijaan ainoastaan tilin iCloud-avainnipun suojausalueella. Niitä käsitellään kuten aikaisempiakin *päästä päähän salattuja* palveluavaimia, mikä tarkoittaa, ettei Apple voi enää lukea tai käyttää näitä avaimia.

Edistyksellinen tietosuojaus suojaa automaattisesti myös sellaiset CloudKitin kentät, jotka muiden valmistajien kehittäjät päättävät merkitä salatuiksi, ja kaikki CloudKitin resurssit.

Edistyksellisen tietosuojauksen ottaminen käyttöön

Kun käyttäjä laittaa edistyksellisen tietosuojauksen päälle, hänen luotettu laitteensa tekee kaksi asiaa: Ensiksikin se kertoo käyttäjän muille päästä päähän -salauksen osallistuville laitteille, että käyttäjän on tarkoitus laittaa päälle edistyksellinen tietosuojaus. Tämä tapahtuu siten, että laite kirjoittaa uuden, laitteen paikallisilla avaimilla allekirjoitetun arvon iCloud-avainnipun laitemetatietoihin. Applen palvelimet eivät voi poistaa tai muokata tätä todistusta, kun se synkronoituu käyttäjän muihin laitteisiin.

Toiseksi laite käynnistää *todennuksen jälkeen saatavilla olevien* palveluavainten poiston Applen datakeskuksista. Koska nämä avaimet ovat iCloudin laitteiston suojausmoduulien suojaamia, poisto on välitön, pysyvä ja peruuttamaton. Kun avaimet on poistettu, Apple ei enää voi käyttää *mitään* käyttäjän palveluavaimilla suojattuja tietoja. Tässä vaiheessa laite aloittaa epäsymmetristen avainten kierrätyksen, jossa luodaan uusi palveluavain kullekin palvelulle, jonka avain oli aikaisemmin Applen palvelinten saatavilla. Jos avainten kierrätys epäonnistuu verkkoyhteyden katkeamisen tai jonkin muun virheen vuoksi, laite yrittää avainten kierrätystä uudelleen, kunnes se onnistuu.

Kun palveluavainten kierrätys on tehty onnistuneesti, uusien palveluun kirjoitettujen tietojen salausta ei voida purkaa vanhalla palveluavaimella. Ne on suojattu uudella avaimella, jota hallitsevat ainoastaan käyttäjän luotetut laitteet ja joka ei koskaan ole ollut Applen saatavilla.

Edistyksellinen tietosuojaus ja iCloud.com-verkkokäyttö

Kun käyttäjä laittaa ensimmäisen kerran päälle edistyksellisen tietosuojauksen, hänen tietojensa iCloud.com-verkkokäyttö laitetaan automaattisesti pois päältä. Tämä tapahtuu siksi, että iCloudin WWW-palvelimet eivät enää voi käyttää avaimia, jotka tarvitaan käyttäjän tietojen salauksen purkamiseen ja niiden näyttämiseen. Käyttäjä voi halutessaan laittaa verkkokäytön takaisin päälle ja käyttää salattuja iCloud-tietojaan verkkoselaimessa luotetun laitteensa avulla.

Kun verkkokäyttö on laitettu päälle, käyttäjän on valtuutettava sisäänkirjautuminen jollakin luotetuista laitteistaan joka kerta, kun hän vierailee iCloud.comissa. Tämä valtuutus tekee verkkokäytön laitteella mahdolliseksi. Seuraavan tunnin ajan kyseinen laite hyväksyy tietyiltä Applen palvelimilta tulevia pyyntöjä lähettää yksittäisiä palveluavaimia, mutta ainoastaan sellaisia, jotka vastaavat iCloud.comissa normaalisti käytettävien sallittujen palveluiden luetteloa. Toisin sanoen, vaikka käyttäjä valtuuttaa sisäänkirjautumisen verkkoselaimessa, palvelimen pyynnöllä ei voida saada käyttäjän laitetta lähettämään palveluavaimia sellaisille tiedoille, joita ei ole tarkoitettu näytettäviksi iCloud.comissa (kuten Terveys-apin tiedot tai iCloud-avainnipun salasanat). Applen palvelimet pyytävät ainoastaan palveluavaimia, joita ne tarvitsevat purkaakseen salauksen juuri niiltä tiedoilta, joita käyttäjä pyytää käyttää verkkoselaimessa. Aina kun palveluavain lähetetään, se salataan käyttäjän valtuuttamaan selainistuntoon sidotulla lyhytaikaisella avaimella, ja käyttäjän laitteessa näytetään ilmoitus, jossa kerrotaan, minkä iCloud-palvelun tiedot ovat tilapäisesti Applen palvelinten käytettävissä.

Käyttäjän valintojen säilyttäminen

Ainoastaan käyttäjä voi muokata edistyksellisen tietosuojauksen ja iCloud.com-verkkokäytön asetuksia. Nämä arvot tallennetaan käyttäjän iCloud-avainnipun laitemetatietoihin, ja niitä voidaan muuttaa ainoastaan jollakin käyttäjän luotetuista laitteista. Applen palvelimet eivät voi muokata näitä asetuksia käyttäjän sijasta eivätkä palauttaa aikaisempia asetuksia.

Suojaus käytettäessä jakamista ja yhteistyötä

Useimmissa tapauksissa kun käyttäjät jakavat sisältöä yhteistyötä varten (esimerkiksi jaettuja muistiinpanoja, jaettuja muistutuksia, jaettuja kansioita iCloud Drivessa tai jaetun iCloud-kuvakirjaston) ja kaikilla käyttäjillä on käytössä edistyksellinen tietosuojaus, Applen palvelimia käytetään ainoastaan jaon muodostamiseen, mutta ne eivät voi käyttää jaettujen tietojen salausavaimia. Sisältö pysyy salattuna päästä päähän, ja sitä voidaan käyttää ainoastaan osallistujien luotetuilla laitteilla. Apple voi tallentaa jokaisen jako-operaation nimen ja sitä edustavan miniatyyrin vakiomuotoisella tietosuojauksella näyttääkseen vastaanottaville käyttäjille esikatselun.

Jos käyttöoikeudeksi valitaan yhteistyöhön ryhdyttäessä ”kaikki, joilla on linkki”, sisältö tulee Applen palvelinten saataville käyttäen vakiomuotoista tietosuojausta, koska palvelinten on voitava tarjota sisältö käyttöön kenelle tahansa, joka avaa verkko-osoitteen.

Yhteistyö iWorkissa ja Kuvat-apin jaettujen albumien ominaisuus eivät tue edistyksellistä tietosuojausta. Kun käyttäjät tekevät yhteistyötä iWork-dokumentissa tai avaavat iWork-dokumentin jaetusta kansiosta iCloud Drivessa, dokumentin salausavaimet lähetetään suojatusti iWork-palvelimille Applen datakeskuksissa. Tämä johtuu siitä, että reaaliaikainen yhteistyö iWorkissa vaatii osallistujien dokumenttiin tekemien muutosten yhteensovittamista palvelinpuolella. Jaettuihin albumeihin lisätyt kuvat tallennetaan vakiomuotoisella tietosuojauksella, koska ominaisuus mahdollistaa albumien julkisen jakamisen verkossa.

Edistyksellisen tietosuojauksen poistaminen käytöstä

Käyttäjä voi milloin tahansa laittaa edistyksellisen tietosuojauksen pois päältä. Jos hän päättää tehdä niin:

1. Käyttäjän laite kirjaa ensin uuden valinnan iCloud-avainnipun osallistumismetatietoihin, ja tämä asetus synkronoidaan suojatusti kaikkiin käyttäjän laitteisiin.

2. Käyttäjän laite lähettää suojatusti palveluavaimet kaikkia *todennuksen jälkeen saatavilla olevia* palveluita varten iCloudin laitteiston suojausmoduuleihin Applen datakeskuksissa. Tähän ei koskaan sisälly avaimia sellaisille palveluille, jotka ovat päästä päähän salattuja vakiomuotoista tietosuojausta käytettäessä, kuten iCloud-avainnipulle tai Terveys-apille.

Laite lähettää sekä alkuperäiset palveluavaimet, jotka luotiin ennen edistyksellisen tietosuojauksen laittamista päälle, että uudet palveluavaimet, jotka on luotu sen jälkeen, kun käyttäjä laittoi ominaisuuden päälle. Tällä tavoin kaikki näiden palveluiden tiedot ovat käytettävissä todennuksen jälkeen ja tili palaa vakiomuotoiseen tietosuojaukseen, jossa Apple voi taas auttaa käyttäjää palauttamaan suurimman osan tiedoistaan, jos hän ei pääse käyttämään tiliään.

Edistyksellisen tietosuojauksen ulkopuolelle jäävät iCloud-tiedot

Koska iCloudin Mailin, Yhteystietojen ja Kalenterin on toimittava yhdessä yleisten sähköposti-, yhteystieto- ja kalenterijärjestelmien kanssa, ne eivät ole päästä päähän salattuja.

iCloud tallentaa joitakin tietoja ilman käyttäjäkohtaisilla CloudKit-palveluavaimilla suojaamista, vaikka edistyksellinen tietosuojaus olisi päällä. CloudKit-tietuekentät on nimenomaisesti määriteltävä salatuiksi säiliön mallissa, jotta ne suojataan, ja salattujen kenttien lukeminen ja kirjoittaminen vaatii siihen tarkoitettujen rajapintojen käyttämistä. Tiedoston tai objektin muokkauspäivää ja -aikaa käytetään käyttäjän tietojen järjestämiseen, ja Apple käyttää tiedosto- ja kuvadatan tarkistussummia apuna deduplikoinnissa eli kaksoiskappaleiden karsimisessa ja käyttäjän iCloudissa ja laitteessa olevan tallennustilan optimoimisessa. Kaikki tämä tapahtuu ilman pääsyä itse tiedostoihin tai kuviin. Salauksen käytöstä tietyille tietokategorioille kerrotaan yksityiskohtaisesti Applen tukiartikkelissa iCloudin suojauksen yleiskatsaus.

Päätökset sellaisista ratkaisuista, kuten tarkistussummien käyttämisestä tietojen deduplikointiin (tunnettu tekniikka, josta käytetään nimeä *konvergoituva salaus*), sisältyivät iCloud-palveluiden alkuperäiseen suunnitteluun silloin, kun ne julkaistiin. Nämä metatiedot ovat aina salattuja, mutta Apple tallentaa salausavaimet käyttäen vakiomuotoista tietosuojausta. Apple haluaa edelleen vahvistaa suojausta kaikille käyttäjille ja aikoo siksi varmistaa, että suurempi osa tiedoista, mukaan lukien tällaiset metatiedot, salataan päästä päähän, kun edistyksellinen tietosuojaus on käytössä.

Edistyksellisen tietosuojauksen vaatimukset

iCloudin edistyksellisen tietosuojauksen laittaminen päälle vaatii seuraavia asioita:

- Käyttäjän tilin on tuettava päästä päähän -salausta. Päästä päähän -salaus vaatii kaksiosaisen todennuksen käyttäjän Apple ID:lle ja sen, että luotettuihin laitteisiin on asetettu pääsykoodi tai salasana. Jos haluat lisätietoja, katso Applen tuliartikkeli Apple ID:n kaksiosainen todennus.
- Laitteisiin, joissa käyttäjä on kirjautunut Apple ID:llään, täytyy olla päivitetty iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 ja uusin iCloudin Windows-versio. Tämä vaatimus estää sen, että aikaisemmat iOS-, iPadOS-, macOS-, tvOS- tai watchOS-versiot käsittelisivät väärin uusia palveluavaimia ja lähettäisivät ne uudelleen *todennuksen jälkeen saatavilla oleviin* laitteiston suojausmoduuleihin yrittäessään virheellisesti korjata tilin tilan.
- Käyttäjän on otettava käyttöön ainakin yksi vaihtoehtoinen palautuskeino (yksi tai useampi palautuksen yhteyshenkilö tai palautusavain), jota hän voi käyttää iCloud-tietojensa palauttamiseen, jos ei pääse käyttämään tiliään.

Jos palautuskeinot eivät toimi, esimerkiksi koska palautuksen yhteyshenkilön tiedot ovat vanhentuneet, tai jos käyttäjä unohtaa ne, Apple ei voi auttaa palauttamaan käyttäjän päästä päähän salattuja iCloud-tietoja.

iCloudin edistyksellinen tietosuojaus voidaan laittaa päälle ainoastaan tavallisille Apple ID:ille. Hallittuja Apple ID:itä ja lasten tilejä (vaihtelee maittain ja alueittain) ei tueta.

iCloud-varmuuskopioinnin suojaus

iCloud varmuuskopioi tiedot päivittäin Wi-Fi-verkon kautta, kuten laitteiden asetukset, appidatan, kuvat ja videot kameran rullasta ja keskustelut Viestit-apista. iCloud-varmuuskopiointi tapahtuu ainoastaan, kun laite on lukittu, yhdistetty virtalähteeseen ja yhteydessä internetiin Wi-Fi-verkon kautta. iOS:ssä ja iPadOS:ssä tallennukseen käytettävän salauksen huomioiva iCloud-varmuuskopiointi on suunniteltu sekä pitämään tiedot suojattuina että mahdollistamaan itsenäisesti tapahtuva inkrementaalinen varmistus ja palautus. Oletuksena iCloud-varmuuskopion palveluavain varmuuskopioidaan suojatusti iCloudin laitteiston suojausmoduuleihin Applen datakeskuksissa ja se on osa todennuksen jälkeen saatavilla olevien tietojen kategoriaa. Jos käyttäjä laittaa päälle iCloudin edistyksellisen tietosuojauksen, iCloud-varmuuskopion palveluavain suojataan päästä päähän -salauksella ja se on ainoastaan käyttäjän saatavilla hänen luotetuilla laitteillaan.

Kun luodaan tiedostoja käyttäen tietojen suojausluokkia, joihin ei pääse laitteen ollessa lukittuna, niiden tiedostokohtaiset avaimet salataan käyttäen luokka-avaimia iCloud-varmuuskopion avainvarastosta ja tiedostot varmuuskopioidaan iCloudiin alkuperäisessä salatussa tilassaan. Kaikki tiedostot salataan siirron aikana, ja tallennettaessa ne salataan käyttäen tileihin perustuvia avaimia kohdassa CloudKitin salaus kerrotulla tavalla.

iCloud-varmuuskopion avainvarasto sisältää epäsymmetriset (Curve25519) avaimet tietojen suojausluokille, jotka eivät ole käytettävissä, kun laite on lukittu. Käyttäjän tiedostojen kopioista ja iCloud-varmuuskopion avainvarastosta muodostuva varmuuskopiokokonaisuus tallennetaan käyttäjän iCloud-tilille. iCloud-varmuuskopion avainvarasto suojataan satunnaisella avaimella, joka myös tallennetaan varmuuskopiokokonaisuuteen. Käyttäjän iCloud-salasanaa ei käytetä salauksessa, jolloin iCloud-salasanan vaihtaminen ei tee olemassa olevia varmuuskopioita käyttökelvottomiksi.

Palautuksessa varmuuskopioidut tiedostot, iCloud-varmuuskopion avainvarasto ja avainvaraston avain noudetaan käyttäjän iCloud-tililtä. iCloud-varmuuskopion avainvaraston salaus puretaan käyttäen sen avainta, minkä jälkeen avainvaraston tiedostokohtaisia avaimia käytetään varmuuskopiokokonaisuuden tiedostojen salauksen purkamiseen. Tiedostot kirjoitetaan tiedostojärjestelmään uusina tiedostoina, jolloin ne salataan uudelleen tietojen suojausluokkansa mukaisesti.

iCloud-varmuuskopioon sisällytetään seuraava sisältö:

- Tietueet ostetuista musiikista, elokuvista, TV-ohjelmista, apeista ja kirjoista. Käyttäjän iCloud-varmuuskopio sisältää tiedot ostetusta sisällöstä käyttäjän laitteella, mutta ei itse ostettua sisältöä. Kun käyttäjä tekee palautuksen iCloud-varmuuskopiosta, hänen ostamansa sisältö ladataan automaattisesti iTunes Storesta, App Storesta, Apple TV -apista tai Apple Booksista. Joitakin sisältötyyppejä ei ladata automaattisesti kaikissa maissa tai kaikilla alueilla, eivätkä aikaisemmat ostot ole ehkä saatavilla, jos ne on hyvitetty tai ne eivät ole enää saatavilla kyseisessä kaupassa. Koko ostohistoria on liitetty käyttäjän Apple ID:hen.
- Kuvat ja videot käyttäjän laitteilla. Huomaa, että jos käyttäjä laittaa iCloud-kuvat päälle iOS 8.1:ssä, iPadOS 13.1:ssä tai OS X 10.10.3:ssa tai uudemmissa, kuvat ja videot tallennetaan jo iCloudiin, joten niitä ei sisällytetä käyttäjän iCloud-varmuuskopioon.
- Yhteystiedot, kalenteritapahtumat, muistutukset ja muistiinpanot
- Laitteen asetukset
- Appidata
- Koti-valikko ja appien järjestys

- HomeKitin määritykset
- SOS-tiedot
- Sanelimen salasana (vaatii tarvittaessa varmuuskopioinnin aikana käytetyn fyysisen SIM-kortin)
- Viestit-, Apple Messages for Business-, teksti- (SMS) ja multimediaviestit (MMS) (vaatii tarvittaessa varmuuskopioinnin aikana käytetyn fyysisen SIM-kortin)

iCloud-varmuuskopiota käytetään myös laitteen paikallisen avainnipun varmuuskopioimiseen. Se on salattu avaimella, joka muodostetaan laitteen Secure Enclaven UID:n juurisalausavaimesta. Tämä avain on yksilöllinen kullekin laitteelle, eikä se ole Applen tiedossa. Näin tietokanta voidaan palauttaa ainoastaan samalle laitteelle, josta se on peräisin, eikä kukaan muu, ei edes Apple, voi lukea sitä. Jos haluat lisätietoja, katso Secure Enclave -alue.

iCloud-viestit

iCloud-viestit pitävät käyttäjän koko viestihistorian päivitettynä ja saatavilla kaikissa laitteissa.

Käytettäessä vakiomuotoista tietosuojausta iCloud-viestit salataan päästä päähän, kun iCloud-varmuuskopio ei ole käytössä. Kun iCloud-varmuuskopio on käytössä, varmuuskopio sisältää kopion iCloud-viestien salausavaimesta, jotta Apple voi auttaa käyttäjää palauttamaan viestinsä, vaikka hän ei pääsisi käyttämään iCloud-avainnippua eikä luotettuja laitteitaan. Jos käyttäjä poistaa iCloud-varmuuskopion käytöstä, hänen laitteessaan muodostetaan uusi avain suojaamaan tulevia iCloud-viestejä. Uusi avain tallennetaan ainoastaan iCloud-avainnippuun, joka on ainoastaan käyttäjän käytettävissä hänen luotetuilla laitteillaan, eikä säiliöön kirjoitettavien uusien tietojen salausta voida purkaa säiliön vanhalla avaimella.

Kun käytetään edistyksellistä tietosuojausta, iCloud-viestit salataan aina päästä päähän. Kun iCloud-varmuuskopio laitetaan päälle, kaikki sen sisällä salataan päästä päähän, mukaan lukien iCloud-viestien salausavain. Sekä iCloud-varmuuskopion palveluavain että iCloud-viestien säiliön avain korvataan, kun käyttäjä laittaa päälle edistyksellisen tietosuojauksen. Jos haluat lisätietoja, katso Applen tukiartikkeli iCloudin suojauksen yleiskatsaus.

Tilin palautuksen yhteyshenkilön suojaus

Käyttäjät voivat lisätä jopa viisi luottamaansa henkilöä tilin palautuksen yhteyshenkilöiksi, jotka voivat auttaa käyttäjiä palauttamaan iCloud-tilinsä ja -tietonsa, mukaan lukien kaikki päästä päähän salatut tiedot, riippumatta siitä, onko edistyksellinen tietosuojaus käytössä. Sen enempää Applella kuin palautuksen yhteyshenkilölläkään ei yksinään ole tarvittavia tietoja käyttäjän päästä päähän salattujen iCloud-tietojen palauttamiseen.

Palautuksen yhteyshenkilö on suunniteltu käyttäjän yksityisyyttä ajatellen. Käyttäjän valitsemat palautuksen yhteyshenkilöt eivät ole Applen tiedossa. Applen palvelimet saavat tietoa palautuksen yhteyshenkilöstä vasta palautusyrityksen myöhäisessä vaiheessa, kun käyttäjä pyytää yhteyshenkilöltä apua ja yhteyshenkilö aloittaa varsinaisen palautuksessa avustamisen. Tätä tietoa ei säilytetä, kun palautus on valmis.

Palautuksen yhteyshenkilön suojausprosessi

Kun käyttäjä ottaa käyttöön tilin palautuksen yhteyshenkilön, avain, jolla pääsee käyttäjän iCloud-tietoihin (mukaan lukien päästä päähän salatut iCloudKit-tiedot), salataan vahvalla satunnaisella avaimella. Tämä satunnainen avain jaetaan palautuksen yhteyshenkilölle ja Applelle annettaviin osiin. Palautusta tehtäessä alkuperäinen avain saadaan käyttöön ja käyttäjän iCloud-tietoihin päästään ainoastaan, kun nämä kahtia jaetun avaimen osat liitetään takaisin yhteen.

Kun tilin palautuksen yhteyshenkilö otetaan käyttöön, käyttäjän laite viestii Applen palvelimien kanssa lähettääkseen niille Applen haltuun tulevan avaintieto-osan. Sen jälkeen se luo päästä päähän salatun CloudKit-säiliön palautuksen yhteyshenkilön kanssa tämän tarvitseman osan jakamista varten. Sekä Apple että palautuksen yhteyshenkilö saavat lisäksi käyttäjältä saman valtuutussalaisuuden, jota tarvitaan myöhemmin palautukseen. Palautuksen yhteyshenkilöiden kutsumisen ja hyväksymisen tietoliikenne tapahtuu käyttäen molemmin puolin todennettua IDS-kanavaa. Palautuksen yhteyshenkilön vastaanottamat tiedot tallennetaan automaattisesti hänen iCloud-avainnippuunsa. Apple ei pääse CloudKit-säiliön sisältöön eikä myöskään tämän tiedon tallentavaan iCloud-avainnippuun. Kun jakaminen suoritetaan, Applen palvelimet näkevät vain palautuksen yhteyshenkilön anonyymin tunnuksen.

Kun käyttäjän myöhemmin tarvitsee palauttaa tilinsä ja iCloud-tietonsa, hän voi pyytää apua palautuksen yhteyshenkilöltään. Silloin palautuksen yhteyshenkilön laite muodostaa palautuskoodin, jonka palautuksen yhteyshenkilö antaa käyttäjälle ulkoista reittiä pitkin (esimerkiksi kasvokkain tai puhelinsoitolla). Käyttäjä syöttää tämän palautuskoodin laitteeseensa muodostaakseen SPAKE2+-protokollaa käyttäen laitteiden välille suojatun yhteyden, jonka sisältö ei ole Applen käytettävissä. Applen palvelimet koordinoivat tätä vuorovaikutusta, mutta Apple ei voi panna palautusprosessia alulle.

Kun suojattu yhteys on muodostettu ja kaikki vaadittavat turvatarkistukset on tehty, palautuksen yhteyshenkilön laite palauttaa takaisin palautusta pyytävälle käyttäjälle osansa avaintiedosta sekä aikaisemmin luodun valtuutussalaisuuden. Käyttäjä esittää tämän valtuutussalaisuuden Applen palvelimelle, ja se antaa käyttöön Applen säilyttämän avaintiedon. Valtuutussalaisuuden esittämisellä saadaan myös valtuutus tilin salasanan nollaamiseen, jotta pääsy tilille saadaan palautettua.

Lopuksi käyttäjän laite liittää Applelta ja tilin palautuksen yhteyshenkilöltä saadun avaintiedon takaisin yhteen ja käyttää sitten sitä käyttäjän iCloud-tietojen salauksen purkamiseen ja palauttamiseen.

Käytössä on suojauskeinoja, joiden on tarkoitus estää palautuksen yhteyshenkilöä aloittamasta palautusta ilman käyttäjän suostumusta. Yksi keino on käyttäjän tilin toiminnan aktiivisuuden tarkistaminen. Jos tili on aktiivisessa käytössä, palautukseen palautuksen yhteyshenkilön avulla vaaditaan myös laitteen viimeaikaisen pääsykoodin tai iCloud-suojakoodin tietämistä.

Tilin perijän suojaus

Jos käyttäjä haluaa, että nimetyt perijät pääsevät hänen iCloud-tietoihinsa hänen kuolemansa jälkeen, hän voi ottaa tililleen käyttöön tilin perijät. Tilin perijä pääsee kaikkiin edesmenneen käyttäjän iCloud-tietoihin, mukaan lukien lähes kaikki päästä päähän salatut tiedot mutta ei kuitenkaan iCloud-avainnipun tietoja, kuten tilien salasanoja. Tilin perijän taustalla oleva teknologia on samankaltainen kuin palautuksen yhteyshenkilön toimintatapa: vahva satunnainen avain jaetaan osiin Applen ja tilin perijän kesken siten, ettei kumpikaan pysty yksinään purkamaan minkään tietojen salausta. Perijä saa samat tietoluokat riippumatta siitä, käyttikö käyttäjä edistyksellistä tietosuojausta.

Perijän saamasta avaintiedosta käytetään käyttäjädokumentaatiossa nimitystä pääsyavain, ja se tallennetaan automaattisesti tuettuihin laitteisiin, mutta se voidaan myös tulostaa ja tallentaa käyttöä varten ei-sähköisessä muodossa. Jos haluat lisätietoja, katso Applen tuliartikkeli Apple ID:n tilin perijän lisääminen.

Käyttäjän kuoleman jälkeen tilin perijät kirjautuvat sisään Applen pyyntösivustolle käyttöoikeuden saamista varten. Siihen vaaditaan kuolintodistus ja se valtuutetaan osittain edellisessä osiossa mainitulla valtuutusavaimella. Kun kaikki turvatarkistukset on suoritettu, Apple antaa käyttäjätunnuksen ja salasanan uudelle tilille ja vapauttaa tarvittavan avaintiedon tilin perijälle.

Jotta pääsyavain olisi helpompi syöttää, kun sitä tarvitaan, se esitetään aakkosnumeerisena koodina, johon on liitetty QR-koodi. Kun se on syötetty, pääsy edesmenneen käyttäjän iCloud-tietoihin palautetaan. Tämä voidaan suorittaa laitteella tai pääsy voidaan hankkia verkossa. Jos haluat lisätietoja, katso Applen tukiartikkeli Apple-tilin käyttöoikeuden pyytäminen tilin perijänä.

Suojatun iCloud-lähetyksen suojaus

Suojattu iCloud-lähetys auttaa suojaamaan käyttäjiä ensisijaisesti silloin, kun he selaavat verkkoa Safarilla, mutta se sisältää myös kaikki DNS-nimenselvityspyynnöt. Tämä auttaa varmistamaan, ettei mikään yksittäinen taho, ei edes Apple, pysty yhdistämään käyttäjän IP-osoitetta hänen selaustoimintaansa. Tämä toteutetaan käyttämällä eri välipalvelimia: Applen hallitsemaa sisääntulovälipalvelinta ja sisällöntarjoajan hallitsemaa ulosmenovälipalvelinta. Jotta käyttäjä voi käyttää suojattua iCloud-lähetystä, hänellä täytyy olla käytössä iOS 15, iPadOS 15 tai macOS 12.0.1 tai uudempi ja hänen täytyy olla kirjautunut Apple ID:llään iCloud+-tilille. Silloin suojattu iCloud-lähetys voidaan laittaa päälle kohdassa Asetukset > iCloud tai Järjestelmäasetukset > iCloud.

Jos haluat lisätietoja, katso iCloud Private Relay Overview.

Pääsykoodien ja salasanojen hallinta

Pääsykoodisuojauksen yleiskatsaus

iOS, iPadOS ja macOS mahdollistavat käyttäjille helpon todennuksen muiden valmistajien appeihin ja verkkosivustoille, joissa käytetään salasanoja. Paras ratkaisu salasanojen hallintaan on, ettei salasanaa tarvitse käyttää. Kirjaudu sisään Applella -toiminnolla käyttäjät voivat kirjautua muiden valmistajien appeihin ja verkkosivustoille ilman, että heidän tarvitsee luoda ja hallita uutta tiliä tai salasanaa, ja sisäänkirjautuminen on suojattu Apple ID:n kaksiosaisella todennuksella. Jos sivusto ei tue Kirjaudu sisään Applella -toimintoa, Automaattinen vahva salasana -ominaisuus mahdollistaa käyttäjän laitteelle yksilöllisten vahvojen salasanojen automaattisen luomisen, synkronoimisen ja syöttämisen sivustoja ja appeja varten. iOS:ssä ja iPadOS:ssä salasanat tallennetaan erityiseen salasanan automaattisen täytön avainnippuun, jota käyttäjä voi hallita valitsemalla Asetukset > Salasanat.

macOS:ssä voi hallita tallennettuja salasanoja Safarin Salasanat-asetuksissa. Tätä synkronointijärjestelmää voidaan myös käyttää käyttäjän manuaalisesti luomien salasanojen synkronoimiseen.

Kirjaudu sisään Applella -toiminnon suojaus

Kirjaudu sisään Applella -toiminto on tietosuojaa kunnioittava vaihtoehto muille kertakirjautumisjärjestelmille. Sisäänkirjautuminen tapahtuu nopeasti ja tehokkaasti yhdellä napautuksella, ja samalla käyttäjälle tarjotaan enemmän läpinäkyvyyttä ja hallintaa henkilötietojensa käyttöön.

Kirjaudu sisään Applella -toiminnolla käyttäjät voivat luoda tilin ja kirjautua sisään appeihin ja verkkosivustoille käyttäen heillä jo olevaa Apple ID:tä, ja he voivat hallita paremmin henkilötietojaan. Apit voivat pyytää vain käyttäjän nimeä ja sähköpostiosoitetta tiliä luotaessa, ja käyttäjä voi aina valita: hän voi jakaa henkilökohtaisen sähköpostisoitteensa apille tai päättää pitää henkilökohtaisen sähköpostisoitteensa yksityisenä ja käyttää sen sijaan uutta Applen yksityistä sähköpostin välityspalvelua. Tämä sähköpostin välityspalvelu jakaa yksilöllisen anonyymin sähköpostiosoitteen, josta viestit välitetään käyttäjän henkilökohtaiseen osoitteeseen. Näin käyttäjä voi edelleen saada hyödylliset viestit kehittäjältä ja samalla suojata ja hallita paremmin henkilötietojaan.

Kirjaudu sisään Applella -toiminto on tehty turvallisuutta ajatellen. Kaikilta Kirjaudu sisään Applella -toiminnon käyttäjiltä vaaditaan kaksiosaista todennusta Apple ID:lle. Kaksiosainen todennus auttaa suojaamaan paitsi käyttäjän Apple ID:tä myös appeihin luotavia tilejä. Lisäksi Apple on kehittänyt ja integroinut Kirjaudu sisään Applella -palveluun tietosuojaa kunnioittavan petostentorjuntasignaalin. Sen ansiosta kehittäjät voivat luottaa siihen, että heidän saamansa uudet käyttäjät ovat todellisia ihmisiä eivätkä botteja tai skriptattuja tilejä.

Automaattiset vahvat salasanat

Kun iCloud-avainnippu on käytössä, iOS, iPadOS ja macOS luovat käyttäjille yksilöllisiä satunnaisista merkeistä koostuvia vahvoja salasanoja, kun käyttäjät luovat tilin verkkosivustolle tai vaihtavat salasanaa Safarissa. iOS:ssä ja iPadOS:ssä automaattisten vahvojen salasanojen luominen on myös saatavilla apeissa. Jos käyttäjä ei halua käyttää vahvoja salasanoja, hänen on tietoisesti valittava olla käyttämättä niitä. Luodut salasanat tallennetaan avainnippuun ja pidetään ajan tasalla kaikissa käyttäjän iCloud-avainnippua käyttävissä laitteissa.

Oletuksena iOS:n ja iPadOS:n luomat salasanat ovat 20 merkin pituisia. Niissä on yksi numero, yksi iso kirjain, kaksi yhdysviivaa ja 16 pientä kirjainta. Näin luotujen vahvojen salasanojen entropia on 71 bittiä.

Salasanojen luominen perustuu heuristiikkoihin, jotka määrittävät, että salasanakentän käyttäjäkokemus on tarkoitettu salasanan luomista varten. Jos heuristiikka ei tunnista kontekstisidonnaisen salasanan käyttöä salasanan luomisessa, appikehittäjät voivat kertoa sen asettamalla tekstikenttään tyypin `UITextContentType.newPassword` ja verkkosivukehittäjät voivat asettaa <input>-elementeillensä attribuutin `autocomplete="new-password"`.

Apit ja verkkosivustot voivat tarjota salasananluontisääntöjä, jotka auttavat varmistamaan, että luodut salasanat ovat yhteensopivia asianmukaisten palveluiden kanssa. Kehittäjät voivat antaa näitä sääntöjä käyttämällä luokkaa `UITextInputPasswordRules` tai `passwordrules`-attribuuttia input-elementeille. Laitteet luovat sitten vahvimman mahdollisen näiden sääntöjen mukaisen salasanan.

Salasanan automaattisen täytön suojaus

Salasanan automaattinen täyttö täyttää automaattisesti avainnippuun tallennetut tunnistetiedot. iCloud-avainnipun salasanojen hallinta ja salasanan automaattinen täyttö tarjoavat seuraavat ominaisuudet:

- Tunnistetietojen täyttäminen apeissa ja verkkosivustoilla
- Vahvojen salasanojen luominen
- Salasanojen tallentaminen sekä apeissa että verkkosivustoilla Safarissa
- Salasanojen suojattu jakaminen käyttäjän yhteystiedoissa oleville tahoille
- Salasanojen antaminen lähellä olevalle tunnistetietoja pyytävälle Apple TV:lle

Salasanojen luominen ja tallentaminen apeissa sekä salasanojen antaminen Apple TV:lle ovat käytettävissä vain iOS:ssä ja iPadOS:ssä.

Salasanan automaattinen täyttö apeissa

iOS:ssä ja iPadOS:ssä käyttäjät voivat syöttää tallennettuja käyttäjätunnuksia ja salasanoja tunnistetietokenttiin apeissa samalla tavoin kuin salasanan automaattinen täyttö toimii Safarissa. iOS:ssä ja iPadOS:ssä käyttäjät napauttavat avainta näytön näppäimistön QuickType-palkissa. Mac Catalystia käyttäen tehdyissä macOS-apeissa tunnistetietokenttien vieressä näkyy Salasanat-pudotusvalikko.

Kun apilaa on vahva liitos verkkosivustoon, joka käyttää apple-app-site-association-tiedoston avulla toimivaa liittämismekanismia ja samaa apin ja verkkosivuston liittämismekanismia, iOS:n ja iPadOS:n QuickType-palkki ja macOS:n pudotusvalikko ehdottavat suoraan tunnistetietoja apille, jos ne on tallennettu salasanojen automaattisen täytön avainnippuun. Näin käyttäjät voivat halutessaan paljastaa Safarin tallentamat tunnistetiedot apille samoilla suojausominaisuuksilla ilman, että apin tarvitsee käyttää ohjelmointirajapintaa.

Salasanan automaattinen täyttö ei paljasta tunnistetietoja apille, ennen kuin käyttäjä suostuu tunnistetiedon antamiseen apille. Tunnistetietoluettelot hankitaan tai esitetään apin prosessin ulkopuolella.

Kun apin ja verkkosivuston välillä on luotettu suhde ja käyttäjä antaa tunnistetiedot apissa, iOS ja iPadOS voivat kehottaa käyttäjää tallentamaan tunnistetiedot salasanan automaattisen täytön avainnippuun myöhempää käyttöä varten.

Appien pääsy tallennettuihin salasanoihin

iOS-, iPadOS- ja macOS-apit voivat pyytää apua salasanan automaattisen täytön avainnipulta kirjatessaan käyttäjää sisään käyttäen `ASAuthorizationPasswordProvider`-mekanismia ja `SecAddSharedWebCredential`-APIa. Salasanan tarjoajaa ja sen pyyntöä voidaan käyttää yhdessä Kirjaudu sisään Applella -toiminnon kanssa, joten samaa APIa kutsutaan auttamaan käyttäjiä kirjautumaan sisään appiin riippumatta siitä, onko käyttäjän tili salasanapohjainen vai luotu käyttäen Kirjaudu sisään Applella -toimintoa.

Apeille sallitaan pääsy tallennettuihin salasanoihin ainoastaan, jos apin kehittäjä ja verkkosivuston ylläpitäjä ovat hyväksyneet sen ja käyttäjä on antanut suostumuksensa. Appikehittäjät ilmaisevat, että apin on tarkoitus päästä Safarin tallentamiin salasanoihin, sisällyttämällä oikeutuksen appiinsa. Oikeutuksessa on lueteltu liitettyjen verkkosivustojen täydelliset domain-nimet, ja verkkosivustoilla täytyy olla palvelimellaan tiedosto, jossa luetellaan Applen hyväksymien appien yksilölliset apin tunnisteet.

Kun appi, jolla on com.apple.developer.associated-domains-oikeutus, asennetaan, iOS ja iPadOS tekevät TLS-pyynnön kullekin luettelossa olevalle verkkosivustolle pyytäen yhtä seuraavista tiedostoista:

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

Jos asennettavan apin tunniste on tiedoston luettelossa, iOS ja iPadOS merkitsevät verkkosivuston ja apin välisen suhteen luotetuksi. Kutsuista näille kahdelle API:lle seuraa kehotus käyttäjälle ainoastaan silloin, kun kyseessä on luotettu suhde. Tällöin käyttäjän on annettava suostumuksensa, ennen kuin salasanoja paljastetaan apille, päivitetään tai poistetaan.

Salasanojen turvallisuutta koskevat suositukset

Salasanan automaattista täyttöä varten tallennettujen salasanojen luettelo iOS:ssä, iPadOS:ssä ja macOS:ssä näyttää varoituksen, jos käyttäjän salasanaa on *käytetty uudelleen* muilla verkkosivustoilla, sitä pidetään *heikkona* tai se on nähty *tietovuodossa*.

Yleiskatsaus

Saman salasanan käyttäminen useammalle kuin yhdelle palvelulle voi altistaa kyseiset tilit hyökkäyksille, joissa käytetään toisesta järjestelmästä haltuun saatuja käyttäjätunnuksia ja salasanoja (stuffing). Jos johonkin palveluun murtaudutaan ja sen salasanat vuotavat, hyökkääjät voivat kokeilla samoja käyttäjätunnuksia ja salasanoja muissa palveluissa päästäkseen muille tileille.

- Salasanat merkitään *uudelleenkäytetyiksi*, jos samaa salasanaa havaitaan käytettävän tallennettuna salasanana eri domaineille.
- Salasanat merkitään *heikoiksi*, jos hyökkääjä voi helposti arvata ne. iOS, iPadOS ja macOS tunnistavat helposti muistettavien salasanojen luomisessa yleisesti käytettyjä kaavoja, kuten sanakirjasta löytyvien sanojen käyttäminen, tavalliset merkkien korvaukset (esimerkiksi ″s4l4s4n4″ sanan ″salasana″ sijasta), näppäimistöstä löytyvät kaavat (esimerkiksi ″q12we34r″ QWERTY-näppäimistössä) tai toistuvat sarjat (esimerkiksi ″123123″). Näillä kaavoilla muodostetaan usein salasanoja, jotka täyttävät palvelun vähimmäisvaatimukset, mutta niitä käyttävät usein myös hyökkääjät, jotka yrittävät murtaa salasanan väsytyshyökkäysmenetelmällä.

  Koska monet palvelut nimenomaan vaativat 4 tai 6 numeroa sisältävää PIN-koodia, nämä lyhyet pääsykoodit arvioidaan eri säännöillä. PIN-koodia pidetään heikkona, jos se on jokin tavallisimmista PIN-koodeista, jos se on nouseva tai laskeva numerosarja kuten ″1234″ tai ″8765″ tai jos siinä on toistuva kaava kuten ″123123″ tai ″123321″.
- Salasanat merkitään *vuotaneiksi*, jos salasanojen valvontaominaisuus voi kertoa niiden olleen mukana tietovuodossa. Jos haluat lisätietoja, katso Salasanojen valvonta.

Heikot, uudelleenkäytetyt tai vuotaneet salasanat joko merkitään salasanaluettelossa (macOS) tai näytetään erityisessä Suojaussuositukset-liitännässä. Jos käyttäjä kirjautuu Safarissa sisään verkkosivustolle käyttäen aikaisemmin tallennettua salasanaa, joka on hyvin heikko tai joka on vaarantunut tietovuodossa, hänelle näytetään varoitus, jossa suositellaan painokkaasti päivittämistä automaattiseen vahvaan salasanaan.

Tilin todennuksen turvallisuuden päivittäminen iOS:ssä ja iPadOS:ssä

Apit, jotka käyttävät tilin todennuksen muokkauksen laajennusta (todentamispalveluiden sovelluskehyksessä), voivat tarjota salasanapohjaisille tileille mahdollisuuden päivittää turvallisuutensa helposti painiketta napauttamalla. Ne voivat siirtyä käyttämään Kirjaudu sisään Applella -palvelua tai automaattista vahvaa salasanaa. Tämä laajennuspiste on saatavilla iOS:lle ja iPadOS:lle.

Jos laajennuspiste on otettu käyttöön apissa ja se on asennettu laitteeseen, käyttäjät näkevät laajennuksen päivitysvaihtoehdot katsoessaan suojaussuosituksia kyseiseen appiin liittyville tunnistetiedoille Asetuksissa iCloud-avainnipun salasanojen hallinnassa. Päivityksiä tarjotaan myös, kun käyttäjä kirjautuu appiin riskialttiilla tunnistetiedolla. Apit voivat kieltää järjestelmää tarjoamasta käyttäjille päivitysvaihtoehtoja sisäänkirjautumisen yhteydessä. Uutta AuthenticationServices-API:a käyttäen apit voivat myös käyttää laajennusta ja hoitaa päivitykset itse, mieluiten joko apin tiliasetus- tai tilinhallintanäytöstä.

Apit voivat kehittäjän valinnan mukaan tukea päivitystä vahvoihin salasanoihin, Kirjaudu sisään Applella -toimintoon tai molempiin. Vahvaan salasanaan päivitettäessä järjestelmä luo käyttäjälle automaattisen vahvan salasanan. Tarvittaessa appi voi antaa muokatut salasanasäännöt, joita noudatetaan uutta salasanaa luotaessa. Kun käyttäjä vaihtaa tilin salasanaa käyttävästä Kirjaudu sisään Applella -toimintoa käyttäväksi, järjestelmä antaa laajennukselle uuden Kirjaudu sisään Applella -tunnistetiedon tiliin liitettäväksi. Käyttäjän Apple ID -sähköpostiosoitetta ei anneta osana tunnistetietoa. Kun päivittäminen Kirjaudu sisään Applella -toimintoon on tehty onnistuneesti, järjestelmä poistaa aikaisemmin käytetyn salasanatunnistetiedon käyttäjän avainnipusta, jos se on tallennettu sinne.

Tilin todennuksen muokkauksen laajennusten on mahdollista suorittaa käyttäjälle lisätodennus ennen päivitystä. Jos päivitys on aloitettu salasanojen hallinnassa tai sen jälkeen, kun appiin on kirjauduttu sisään, laajennus antaa päivitettävän tilin käyttäjätunnuksen ja salasanan. Apissa tehtävissä päivityksissä annetaan vain käyttäjätunnus. Jos laajennus vaatii käyttäjän lisätodennusta, se voi pyytää näyttämään muokatun käyttöliittymänäkymän ennen päivityksen etenemistä. Tämä käyttöliittymänäkymän näyttäminen on suunniteltu käyttötapauksille, joissa käyttäjä valtuuttaa päivityksen kaksiosaisen todennuksen toisella osalla.

Salasanojen valvonta

Salasanojen valvonta on ominaisuus, joka vertaa käyttäjän salasanan automaattisen täytön avainnippuun tallennettuja salasanoja jatkuvasti päivittyvään ja kerättävään luetteloon salasanoista, joiden tiedetään paljastuneen erilaisten verkossa toimivien organisaatioiden vuodoissa. Jos tämä ominaisuus on käytössä, valvova protokolla vertaa jatkuvasti käyttäjän salasanojen automaattisen täytön luetteloa kerättyyn luetteloon.

Valvonnan toiminta

Käyttäjän laite suorittaa jatkuvasti kiertäviä tarkistuksia käyttäjän salasanoille tehden kyselyitä aikavälein, jotka ovat riippumattomia käyttäjän salasanoista tai salasanojen hallinnan käytön kaavoista. Tämä auttaa varmistamaan, että tarkistustilat pysyvät ajan tasalla senhetkiseen vuodetuista salasanoista kerättyyn luetteloon nähden. Sen auttamiseksi, että tietoa käyttäjällä olevien erillisten salasanojen määrästä ei pääsisi vuotamaan, pyynnöt jaetaan eriin ja suoritetaan rinnakkain. Kussakin erässä tarkistetaan rinnakkain määrätty määrä salasanoja ja mikäli käyttäjällä on salasanoja tätä määrää vähemmän, luodaan kyselyihin lisättäviksi satunnaisia salasanoja, jotta määrä saadaan täyteen.

Miten salasanoja verrataan

Salasanoja verrataan kaksiosaisessa prosessissa. Yleisimmät vuotaneet salasanat ovat paikallisessa luettelossa käyttäjän laitteella. Jos käyttäjän salasana on tässä luettelossa, hän saa heti ilmoituksen ilman mitään kanssakäymistä laitteen ulkopuoleisten kohteiden kanssa. Tämä on suunniteltu varmistamaan, ettei mitään tietoa tietovuodon takia suuressa riskissä olevista käyttäjän salasanoista pääsisi vuotamaan.

Jos salasana ei ole yleisimpien luettelossa, sitä verrataan harvinaisempiin vuotaneisiin salasanoihin.

Käyttäjän salasanojen vertaaminen koottuun luetteloon

Applen palvelimet osallistuvat tarkistukseen, kun etsitään osumia salasanalle, joka ei esiinny paikallisessa luettelossa. Jotta oikeiden käyttäjien salasanoja ei päätyisi Applelle, käyttäjän salasanoja etsitään suuresta vuodettujen salasanojen joukosta käyttäen yksityisiä salattuja joukkoja siten, että osapuolille selviävät vain *yksityisten joukkojen leikkauksessa* olevat alkiot (Private Set Intersection eli PSI-protokolla). Tämä on suunniteltu varmistamaan, että pienemmässä murtoriskissä olevista salasanoista jaetaan Applelle hyvin vähän tietoa. Käyttäjän salasanan osalta tieto rajoittuu 15-bittiseen etuliitteeseen kryptografisesta tiivisteestä. Yleisimpien vuotaneiden salasanojen poistaminen tästä vuorovaikutteisesta prosessista ja paikallisen luettelon käyttäminen niille pienentää muutosta (delta) salasanojen suhteellisessa yleisyydessä verkkopalveluiden säilöissä, mikä estää käyttäjien salasanojen päättelemistä näistä hauista.

Taustalla toimiva protokolla jakaa kerättyjen salasanojen luettelon, johon sisältyi kirjoitusajankohtana noin 1,5 miljardia salasanaa, 2^{15} eri säilöön. Säilö, johon salasana kuuluu, määräytyy sen SHA256-tiivistearvon 15 ensimmäisen bitin perusteella. Lisäksi kukin vuotanut salasana pw on yhdistetty elliptisen käyrän pisteeseen NIST P256 -käyrällä: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, jossa α on vain Applen tiedossa oleva salainen satunnainen avain ja H_{SWU} on satunnaisoraakkelifunktio, joka liittää salasanat käyrän pisteisiin Shallue-van de Woestijne-Ulas -menetelmään pohjautuen. Tämä muunnos on suunniteltu piilottamaan salasanojen arvot laskennallisesti ja se auttaa estämään äskettäin vuotaneiden salasanojen paljastumista Salasanojen valvonnan kautta.

Yksityisten joukkojen leikkauksen laskemista varten käyttäjän laite määrittää säilön, johon käyttäjän salasana kuuluu, käyttäen λ:aa eli 15-bittistä etuliitettä SHA256(upw):stä, jossa upw on yksi käyttäjän salasanoista. Laite luo oman satunnaisen vakionsa β ja lähettää palvelimelle pisteen $P_c = \beta \cdot H_{SWU}(upw)$ sekä pyynnön λ:aa vastaavasta säilöstä. Tässä β kätkee tiedon käyttäjän salasanasta ja rajoittaa salasanasta Applelle paljastuvan tiedon λ:aan. Lopuksi palvelin ottaa käyttäjän laitteen lähettämän pisteen, laskee $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$ ja palauttaa laitteelle sen sekä oikean pisteiden säilön, joka on $B\lambda=\{ P_{pw} \mid$ SHA256(pw) alkaa etuliitteellä λ$\}$.

Palautettuja tietoja käyttäen laite pystyy laskemaan yhtälön $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$ ja vahvistamaan, että käyttäjän salasana on vuotanut, jos $\alpha P_c \in B'_\lambda$.

Salasanojen lähettäminen toisille käyttäjille tai Applen laitteille

Apple lähettää salasanat suojatusti muille käyttäjille tai Apple-laitteille AirDropilla sekä Apple TV:ssä.

Tunnistetietojen tallentaminen toiseen laitteeseen AirDropilla

Kun iCloud on käytössä, käyttäjät voivat lähettää tallennetut tunnistetiedot toiseen laitteeseen käyttäen AirDropia. Tunnistetiedot sisältävät käyttäjätunnuksen ja salasanan sekä verkkosivuston, jolle ne on tallennettu. Tunnistetietojen lähettäminen AirDropilla toimii aina Vain yhteystiedot -tilassa riippumatta käyttäjän asetuksista. Vastaanottavassa laitteessa tunnistetiedot tallennetaan käyttäjän suostumuksen jälkeen käyttäjän salasanan automaattisen täytön avainnippuun.

Tunnistetietojen täyttäminen apeissa Apple TV:ssä

Salasanan automaattisella täytöllä voidaan täyttää tunnistetietoja appeihin Apple TV:ssä. Kun käyttäjä kohdistaa käyttäjätunnus- tai salasanatekstikenttään tvOS:ssä, Apple TV lähettää salasanan automaattisen täytön pyynnön Bluetooth Low Energy (BLE) -yhteydellä.

Lähellä olevissa iPhoneissa, iPadeissa tai iPod toucheissa näkyy kehotus, joka kutsuu käyttäjää jakamaan tunnistetiedon Apple TV:n kanssa. Näin salausmenetelmä määritetään:

- Jos laitteessa ja Apple TV:ssä käytetään samaa iCloud-tiliä, laitteiden välinen salaus tapahtuu automaattisesti.
- Jos laite on kirjautunut toiselle iCloud-tilille kuin Apple TV, käyttäjää kehotetaan luomaan salattu yhteys PIN-koodin avulla. iPhonen täytyy olla lukitsematon ja lähellä Siri Remotea, joka on asetettu Apple TV:n pariksi, jotta se saa kehotuksen.

Kun salattu yhteys on muodostettu käyttäen BLE-yhteyden salausta, tunnistetieto lähetetään Apple TV:lle ja täytetään automaattisesti oikeisiin tekstikenttiin apissa.

Tunnistetietojen tarjoajan laajennukset

iOS:ssä, iPadOS:ssä ja macOS:ssä käyttäjät voivat nimetä tähän toimintoon osallistuvan muun valmistajan apin tunnistetietojen tarjoajaksi salasanan automaattiselle täytölle Salasanat-asetuksissa (iOS ja iPadOS) tai Järjestelmäasetusten Laajennukset-asetuksissa (macOS). Tämä mekanismi rakentuu appilaajennuksille. Tunnistetietojen tarjoajan laajennuksen tulee tarjota näkymä, jossa tunnistetiedot valitaan, ja laajennus voi valinnaisesti tarjota metadataa tallennetuista tunnistetiedoista, jotta tietoja voidaan tarjota suoraan QuickType-palkissa (iOS ja iPadOS) tai automaattisen täytön ehdotuksena (macOS). Metadata sisältää tunnistetiedon verkkosivuston ja siihen liittyvän käyttäjätunnuksen, mutta ei salasanaa. iOS, iPadOS ja macOS viestivät laajennuksen kanssa saadakseen salasanan, kun käyttäjä valitsee tunnistetiedon täytön appiin tai verkkosivustolle Safarissa. Tunnistetietojen metadata tallennetaan tunnistetietojen tarjoajan apin säiliöön ja poistetaan automaattisesti, kun apin asennus poistetaan.

iCloud-avainnippu

iCloud-avainnipun suojauksen yleiskatsaus

iCloud mahdollistaa salasanojen suojatun synkronoimisen käyttäjän iOS- ja iPadOS-laitteiden ja Mac-tietokoneiden välillä paljastamatta näitä tietoja Applelle. Vahvan tietosuojan ja suojauksen lisäksi iCloud-avainnipun suunnittelussa ja arkkitehtuurissa ovat olleet keskeisinä tavoitteina helppokäyttöisyys ja mahdollisuus avainnipun palauttamiseen. iCloud-avainnippu muodostuu kahdesta palvelusta: avainnipun synkronointi ja avainnipun palautus.

Apple on suunnitellut iCloud-avainnipun ja avainnipun palautuksen siten, että käyttäjän salasanat ovat suojattuina myös seuraavissa tilanteissa:

- Käyttäjän iCloud-tili on vaarantunut.
- iCloud on vaarantunut ulkoisen hyökkääjän tai työntekijän toimesta.
- Kolmas osapuoli pääsee käyttäjätileihin.

Salasanojen hallinnan integraatio iCloud-avainnippuun

iOS, iPadOS ja macOS voivat luoda automaattisesti salausteknisesti vahvoja satunnaisia merkkijonoja käytettäviksi tilien salasanoina Safarissa. iOS ja iPadOS voivat myös luoda vahvoja salasanoja apeille. Luodut salasanat tallennetaan avainnippuun ja synkronoidaan muihin laitteisiin. Avainnipun kohteet siirretään laitteesta laitteeseen Applen palvelimien kautta, mutta ne salataan siten, että Apple ja muut laitteet eivät voi lukea niiden sisältöä.

Suojattu salasanan synkronointi

Kun käyttäjä ottaa iCloud-avainnipun käyttöön ensimmäisen kerran, laite muodostaa luottamusverkoston ja luo itselleen synkronointi-identiteetin. Synkronointi-identiteetti koostuu yksityisestä avaimesta ja julkisesta avaimesta, ja se tallennetaan laitteen avainnippuun. Synkronointi-identiteetin julkinen avain pannaan luottamusverkostoon ja verkosto allekirjoitetaan kahteen kertaan: ensin synkronointi-identiteetin yksityisellä avaimella ja sitten uudelleen epäsymmetrisellä elliptisellä avaimella (käyttää P-256:ta), joka on muodostettu käyttäjän iCloud-tilin salasanasta. Verkostoon tallennetaan myös parametrit (satunnainen suolaus ja iteraatiot), joita käytetään käyttäjän iCloud-salasanaan perustuvan avaimen luomiseen.

Kaksiosaista todennusta käyttävillä tileillä luodaan lisäksi samanlainen synkronointiverkosto, joka tallennetaan CloudKitiin. Tässä järjestelmässä laitteiden identiteetit koostuvat kahdesta epäsymmetristen (P-384:ää käyttävien) elliptisten avainten parista, jotka myös tallennetaan avainnippuun. Kukin laite ylläpitää omaa luetteloaan luottamistaan identiteeteistä, ja allekirjoittaa tämän luettelon yhdellä identiteettiavaimistaan.

Synkronointiverkoston tallentaminen iCloudiin

Allekirjoitettu synkronointiverkosto tallennetaan käyttäjän iCloud-avainarvotallennustila-alueelle. Sitä ei voi lukea, jos käyttäjän iCloud-salasana ei ole tiedossa, eikä sitä voi muokata hyväksyttävästi ilman verkoston jäsenen synkronointi-identiteetin yksityistä avainta.

Kaksiosaista todennusta käyttävillä tileillä kunkin laitteen synkronointiluettelo tallennetaan CloudKitiin. Luetteloja ei voi lukea, jos käyttäjän iCloud-salasana ei ole tiedossa, eikä niitä voi muokata ilman omistavan laitteen yksityisiä avaimia.

Käyttäjän muiden laitteiden lisääminen synkronointiverkostoon

Kun uudet laitteet kirjautuvat iCloudiin, ne liittyvät iCloud-avainnipun synkronointiverkostoon jommallakummalla kahdesta tavasta: joko verkostossa jo olevan iCloud-avainnippulaitteen parina ja sen takaamana tai käyttämällä iCloud-avainnipun palautusta.

Pariin perustuvassa tavassa verkostoon pääsyä pyytävä laite luo uudet synkronointi-identiteetit sekä synkronointiverkostolle että synkronointiluetteloille (kaksiosaista todennusta käyttäville tileille) ja esittää ne takaajalaitteelle. Takaajalaite lisää uuden jäsenen julkisen avaimen synkronointiverkostoon ja allekirjoittaa sen uudelleen sekä synkronointi-identiteetillään että käyttäjän iCloud-salasanasta muodostetulla avaimella. Uusi synkronointiverkosto sijoitetaan iCloudiin, missä verkoston uusi jäsen allekirjoittaa sen samalla tavoin. Kaksiosaista todennusta käyttävillä tileillä takaajalaite myös antaa liittyvälle laitteelle *tositteen*, joka on allekirjoitettu sen identiteettiavaimilla ja joka kertoo, että pääsyä pyytävään laitteeseen tulisi luottaa. Sitten se päivittää yksilöllisen luotettujen synkronointi-identiteettien luettelonsa sisällyttäen pääsyä pyytävän laitteen siihen.

Nyt allekirjoitusverkostossa on kaksi jäsentä, joilla kummallakin on toisen julkinen avain. Nyt ne tilanteesta riippuen joko aloittavat yksittäisten avainnipun kohteiden vaihdon iCloud-avainarvotallennustilan kautta tai tallentavat ne CloudKitiin. Jos molemmilla verkoston jäsenillä on päivitykset samaan kohteeseen, valitaan jompikumpi, jolloin lopputulos on yhtenäinen. Kukin synkronoitava kohde salataan siten, että salauksen voi purkaa ainoastaan käyttäjän luottamusverkostossa oleva laite. Mikään muu laite tai Apple ei voi purkaa salausta.

Kun synkronointiverkostoon liittyy uusia laitteita, tämä ”liittymisprosessi” toistetaan. Esimerkiksi kun kolmas laite liittyy, se voidaan lisätä jommankumman verkostossa jo olevan laitteen parina. Kun uusia vertaislaitteita lisätään, kukin vertaislaite synkronoi uuden laitteen kanssa. Tämä on suunniteltu varmistamaan, että kaikilla jäsenillä on samat avainnipun kohteet.

Ainoastaan tietyt kohteet synkronoidaan

Jotkin avainnipun kohteet, kuten iMessage-avaimet, ovat laitekohtaisia, joten niiden kuuluu jäädä laitteeseen. Tämän vuoksi jokainen synkronoitava kohde on nimenomaisesti merkittävä `kSecAttrSynchronizable`-attribuutilla.

Apple asettaa tämän attribuutin Safarin käyttäjätiedoille (mukaan lukien käyttäjätunnukset, salasanat ja luottokorttien numerot) sekä Wi-Fi-salasanoille, HomeKitin salausavaimille ja muille avainnipun kohteille, jotka tukevat iCloudin päästä päähän -salausta.

Oletuksena muiden valmistajien appien lisäämiä avainnipun kohteita ei synkronoida. Kehittäjien on asetettava `kSecAttrSynchronizable`-attribuutti lisätessään kohteita avainnippuun.

iCloud-avainnipun suojattu palautus

iCloud-avainnippu turvatallentaa käyttäjien avainnipun tiedot Applelle *ilman*, että Applen sallitaan lukea salasanoja tai muita avainnipun sisältämiä tietoja. Avainnipun palautus toimii turvaverkkona, joka estää tietojen menettämisen, vaikka käyttäjällä olisi vain yksi laite. Tämä on erityisen tärkeää käytettäessä Safaria sattumanvaraisten, vahvojen salasanojen luomiseen verkkotileille, koska kyseiset salasanat on tallennettu ainoastaan avainnippuun.

Avainnipun palautuksen kulmakivenä on toinen todentaminen ja suojattu vara-avainpalvelu, jonka Apple on luonut nimenomaan tämän ominaisuuden tueksi. Käyttäjän avainnippu salataan käyttäen vahvaa pääsykoodia, ja vara-avainpalvelu tallentaa avainnipun kopion vain, jos tiukat ehdot täyttyvät.

Toisen todentamisen käyttäminen

Vahvan pääsykoodin luomiseen on olemassa useita tapoja:

- Jos kaksiosainen todennus on käytössä käyttäjän tilillä, laitteen pääsykoodia käytetään vara-avainnipun palauttamiseen.
- Jos kaksiosaista todennusta ei ole otettu käyttöön, käyttäjää pyydetään luomaan iCloud-suojakoodi antamalla kuusinumeroinen pääsykoodi. Jos kaksiosaista todennusta ei käytetä, käyttäjä voi myös vaihtoehtoisesti määrittää oman pidemmän koodin tai antaa laitteiden luoda kryptografisesti satunnaisen koodin, jonka käyttäjä voi ottaa talteen ja säilyttää itse.

Avainnipun turvatallennusprosessi

Kun pääsykoodi on luotu, avainnippu tallennetaan Applelle. iOS-, iPadOS- tai macOS-laite vie ensin kopion käyttäjän avainnipusta, salaa sen sitten avaimilla epäsymmetrisessä avainvarastossa ja sijoittaa sen käyttäjän iCloud-avainarvotallennustila-alueelle. Avainvarasto salataan käyttäjän iCloud-suojakoodilla ja tietuetallenteen tallentavan laitteiston suojausmoduulin (HSM) klusterin julkisella avaimella. Tästä tulee käyttäjän *iCloud-vara-avaintietue*. Kaksiosaista todennusta käyttävien tilien avainnippu myös tallennetaan CloudKitiin ja salataan väliavaimilla, jotka saa palautettua vain iCloud-vara-avaintietueen sisällöllä, mikä tarjoaa siten samantasoisen suojauksen.

Vara-avaintietueen sisällön avulla palautuksen saava laite voi myös liittyä uudelleen iCloud-avainnippuun. Se todistaa olemassa oleville laitteille, että palautuksen saanut laite on suorittanut vara-avainprosessin onnistuneesti ja on siis tilin omistajan valtuuttama.

Huomaa: Jos käyttäjä päättää valita kryptografisesti satunnaisen suojakoodin sen sijaan, että määrittäisi oman koodin tai käyttäisi nelinumeroista arvoa, vara-avaintietuetta ei tarvita. Sen sijaan satunnainen avain salataan suoraan iCloud-suojakoodilla.

Suojakoodin luomisen lisäksi käyttäjien täytyy rekisteröidä puhelinnumero. Se tarjoaa lisätodennuksen avainnipun palautuksessa. Käyttäjä saa tekstiviestin, johon täytyy vastata, jotta palautusta voidaan jatkaa.

iCloud-avainnipun vara-avainten suojaus

iCloud tarjoaa avainnipun vara-avaimille suojatun infrastruktuurin, joka auttaa varmistamaan, että ainoastaan valtuutetut käyttäjät ja laitteet voivat suorittaa palautuksen. Vara-avaintietueita vartioivat laitteiston suojausmoduuliklusterit ovat topografisesti iCloudin takana. Kukin valvoo avainta, jota käytetään vara-avaintietueiden salaamiseen edelläkuvatulla tavalla.

Avainnipun palauttamiseksi käyttäjän on todennettava henkilöllisyytensä iCloud-tilillä ja salasanalla ja vastattava rekisteröityyn puhelinnumeroonsa lähetettyyn tekstiviestiin. Kun se on tehty, käyttäjän on syötettävä iCloud-suojakoodinsa. Laitteiston suojausmoduuliklusteri varmistaa, että käyttäjä tietää iCloud-suojakoodinsa, käyttämällä SRP (Secure Remote Password) -protokollaa; itse koodia ei lähetetä Applelle. Kukin klusterin jäsen varmistaa itsenäisesti, ettei käyttäjä ole ylittänyt tietueen noutamisen sallittujen yrityskertojen enimmäismäärää. Tästä kerrotaan jäljempänä. Jos enemmistö päätyy hyväksyvään tulokseen, klusteri purkaa vara-avaintietuetta suojaavan salauksen ja lähettää sen käyttäjän laitteelle.

Seuraavaksi laite purkaa iCloud-suojakoodia käyttäen käyttäjän avainnipun salaamiseen käytettyjä satunnaisia avaimia suojaavan salauksen. Tällä avaimella puretaan salaus avainnipulta, joka on noudettu iCloudin avainarvotallennustilasta ja CloudKitistä, ja avainnippu palautetaan laitteeseen. Todentamista ja vara-avaintietueen palautusta voi yrittää iOS:llä, iPadOS:llä ja macOS:llä vain kymmenen kertaa. Usean epäonnistuneen yrityksen jälkeen tietue lukitaan ja käyttäjän on soitettava Applen tukeen saadakseen lisää yrityskertoja. Kymmenennen epäonnistuneen yrityksen jälkeen laitteiston suojausmoduuliklusteri tuhoaa vara-avaintietueen ja avainnippu menetetään lopullisesti. Tämä suojaa hyökkäyksiltä, joissa yritetään hankkia tietue väsytysmenetelmällä. Seurauksena on avainnipun tietojen menetys.

Nämä käytännöt on koodattu laitteiston suojausmoduulin laiteohjelmistoon. Ylläpitäjän pääsykortit, joilla laiteohjelmistoa voi muuttaa, on tuhottu. Kaikki yritykset muuttaa laiteohjelmistoa tai päästä käsiksi yksityiseen avaimeen saavat laitteiston suojausmoduuliklusterin poistamaan yksityisen avaimen. Jos näin kävisi, kunkin klusterin suojaaman avainnipun omistaja saa viestin, jossa kerrotaan, että vara-avaintietue on menetetty. He voivat sen jälkeen halutessaan rekisteröityä uudelleen.

Apple Pay

Apple Payn suojauksen yleiskatsaus

Apple Payn kanssa käyttäjät voivat maksaa tuetuilla iPhone-, iPad, Mac- ja Apple Watch -laitteilla helposti, turvallisesti ja yksityisesti myymälöissä, apeissa ja verkkosivustoilla Safarissa. Käyttäjät voivat myös lisätä Apple Payta tukevia matkakortteja, opiskelijakortteja ja kulkukortteja Applen Lompakkoon. Sen käyttö on yksinkertaista ja siihen on integroitu sekä laitteisto- että ohjelmistosuojaus.

Apple Pay on myös suunniteltu suojaamaan käyttäjän henkilötietoja. Apple Pay ei kerää mitään sellaisia maksutapahtumatietoja, jotka voidaan yhdistää takaisin käyttäjään. Maksutapahtumat ovat käyttäjän, myyjän ja kortinmyöntäjän välisiä.

Apple Payn osien suojaus

Apple Pay käyttää useita laitteiston ja ohjelmiston ominaisuuksia suojattujen ja luotettavien ostojen tarjoamiseen.

Secure Element

Secure Element on standardin mukainen varmennettu siru. Siinä toimii Java Card -alusta, joka täyttää rahoitusalan vaatimukset sähköiselle maksamiselle. Secure Element -mikropiiri ja Java Card -alusta on varmennettu EMVCo Security Evaluation -arviointiprosessin mukaisesti. Kun turvallisuusarviointi on suoritettu hyväksytysti, EMVCo antaa yksilölliset mikropiiri- ja alustavarmenteet.

Secure Element -mikropiiri on sertifioitu Common Criteria -standardin mukaisesti. Jos haluat lisätietoja, katso Secure Enclave -prosessorin tietoturvasertifioinnit Apple-alustojen sertifioinneissa.

NFC-ohjain

NFC-ohjain käsittelee NFC (Near Field Communication) -protokollia ja reitittää viestintää appeja suorittavan prosessorin ja Secure Elementin sekä Secure Elementin ja myyntipäätteen välillä.

Applen Lompakko

Applen Lompakko-appia käytetään luotto- ja pankkikorttien sekä kauppojen omien korttien lisäämiseen ja hallitsemiseen sekä maksujen suorittamiseen Apple Paylla. Käyttäjät voivat katsoa korttejaan ja mahdollisesti kortinmyöntäjän antamia lisätietoja, kuten kortinmyöntäjän tietosuojakäytännön tai viimeaikaiset tapahtumat, Applen Lompakossa. Käyttäjät voivat lisätä kortteja Apple Payhin myös seuraavissa:

- Käyttöönottoapuri ja Asetukset iOS:ssä ja iPadOS:ssä
- Watch-appi Apple Watchille
- Lompakko ja Apple Pay Touch ID:llä varustettujen Mac-tietokoneiden Järjestelmäasetuksissa

Lisäksi käyttäjät voivat lisätä ja hallita Applen Lompakossa muun muassa matkakortteja, kanta-asiakaskortteja, tarkastuskortteja, lippuja, lahjakortteja, opiskelijakortteja ja kulkukortteja.

Secure Enclave -alue

iPhonessa, iPadissa, Apple Watchissa, Touch ID:llä varustetuissa Mac-tietokoneissa sekä Apple siliconilla varustetuissa Mac-tietokoneissa, jotka käyttävät Touch ID:llä varustettua Magic Keyboardia, Secure Enclave hallitsee todennusprosessia ja sallii maksutapahtumat.

Käytettäessä Apple Watchia laitteen lukituksen tulee olla avattu ja käyttäjän tulee painaa sivupainiketta kahdesti. Kaksoispainallus tunnistetaan ja välitetään suoraan Secure Elementille tai Secure Enclavelle (jos käytettävissä). Tieto ei kulje appeja suorittavan prosessorin kautta.

Apple Pay -palvelimet

Apple Pay -palvelimet hallitsevat luotto-, pankki-, matka-, opiskelija- ja kulkukorttien käyttöönottoa ja niiden tietojen tuomista Applen Lompakkoon. Palvelimet hallitsevat myös Secure Elementiin tallennettuja laitteen tilinumeroita. Ne viestivät sekä laitteen että maksuverkon tai kortin myöntäjän palvelinten kanssa. Apple Pay -palvelimet vastaavat myös apeissa tai verkossa tehtävien maksujen tunnistetietojen uudelleensalaamisesta.

Miten Apple Pay suojaa käyttäjän ostot

Secure Element

Secure Elementissä on sovelma, joka on erityisesti suunniteltu hallitsemaan Apple Payta. Se sisältää myös maksuverkkojen tai kortin myöntäjien varmentamat sovelmat. Luotto-, pankki- tai prepaid-korttien tiedot lähetetään maksuverkosta tai kortin myöntäjältä salattuina näille sovelmille käyttäen avaimia, joista on tieto vain maksuverkolla tai kortin myöntäjällä ja sovelman suojaus-domainilla. Nämä tiedot on tallennettu kyseisiin sovelmiin ja suojattu käyttäen Secure Elementin suojausominaisuuksia. Maksutapahtuman aikana pääte viestii suoraan Secure Elementin kanssa NFC-ohjaimen kautta käyttäen tarkoitukseen varattua laitteistoväylää.

NFC-ohjain

Secure Elementin yhdyskäytävänä NFC-ohjain auttaa varmistamaan, että lähimaksutapahtumat suoritetaan käyttäen laitteen lähellä olevaa myyntipäätettä. NFC-ohjain merkitsee vain kentän sisällä olevasta päätteestä tulevat pyynnöt lähimaksuiksi.

Kun kortin haltija on valtuuttanut luotto-, pankki- tai prepaid-korttimaksun (mukaan lukien kauppojen omat kortit) Face ID:llä, Touch ID:llä tai pääsykoodilla tai lukitsemattomassa Apple Watchissa painamalla kahdesti sivupainiketta, maksusovelmien Secure Elementissä valmistelemat lähiluettavat vastaukset reititetään ainoastaan ohjaimen toimesta NFC-kenttään. Näin lähimaksutapahtuman valtuutustiedot rajataan paikalliseen NFC-kenttään, eivätkä ne missään vaiheessa paljastu appeja suorittavalle prosessorille. Sitä vastoin apeissa ja verkossa suoritettavien maksujen valtuutustiedot reititetään appeja suorittavaan prosessoriin, mutta vasta kun Secure Element on salannut ne Apple Pay -palvelimelle.

Luotto-, pankki- ja prepaid-kortit

Korttien tietojen tuomisen yleiskatsaus

Kun käyttäjä lisää luotto-, pankki- tai prepaid-kortin (mukaan lukien kauppojen omat kortit) Applen Lompakkoon, Apple lähettää suojattuina kortin tiedot sekä muita tietoja käyttäjän tilistä ja laitteesta kortin myöntäjälle tai kortin myöntäjän valtuuttamalle palveluntarjoajalle. Näiden tietojen perusteella kortin myöntäjä ratkaisee, hyväksytäänkö kortin lisääminen Apple Walletiin. Apple Pay käyttää kortin tietojen tuontiprosessissa viestien lähettämiseen ja vastaanottamiseen kortin myöntäjän kanssa kolmea palvelinpuolen kutsua:

- vaaditut kentät
- kortin tarkistus
- liittäminen ja tietojen tuominen

Kortin myöntäjä tai verkko käyttää näitä kutsuja vahvistukseen, hyväksymiseen ja korttien lisäämiseen Apple Walletiin. Näissä asiakas-palvelin-istunnoissa käytetään tiedonsiirtoon TLS 1.2:ta.

Korttien koko numeroita ei tallenneta laitteeseen tai Apple Pay -palvelimille. Sen sijaan luodaan yksilöllinen laitteen tilinumero ja se salataan ja tallennetaan Secure Elementiin. Tämä yksilöllinen laitteen tilinumero salataan siten, ettei Apple pääse siihen. Laitteen tilinumero on yksilöllinen ja erilainen kuin useimmat luotto- tai pankkikorttinumerot; kortin myöntäjä tai maksuverkko voi estää sen käytön magneettiraitakortissa, puhelimessa tai verkkosivustoilla. Secure Elementissä olevaa laitteen tilinumeroa ei koskaan tallenneta Apple Pay -palvelimille tai varmuuskopioida iCloudiin, ja se on erotettu iOS-, iPadOS- ja watchOS-laitteista sekä Mac-tietokoneista, joissa on Touch ID.

Apple Watchin kanssa käytettävien korttien tiedot tuodaan Apple Payta varten iPhonessa käyttäen joko Apple Watch -appia tai kortin myöntäjän iPhone-appia. Kortin lisääminen Apple Watchiin edellyttää, että kello on Bluetooth-yhteyden alueella. Kortit rekisteröidään nimenomaan Apple Watchilla käytettäviksi ja niillä on omat laitteen tilinumerot, jotka tallennetaan Secure Elementiin Apple Watchissa.

Kun luotto-, pankki- tai prepaid-kortit (mukaan lukien kauppojen omat kortit) on lisätty, ne näkyvät korttiluettelossa käyttöönottoapurissa laitteissa, jotka on kirjattu samalle iCloud-tilille. Kortit pysyvät tässä luettelossa niin kauan kuin ne ovat aktivoituina vähintään yhdessä laitteessa. Kortit poistetaan luettelosta sen jälkeen, kun niiden poistamisesta kaikista laitteista on kulunut seitsemän päivää. Tämä ominaisuus vaatii kaksiosaista todennusta kyseiselle iCloud-tilille.

Luotto- tai pankkikorttien lisääminen Apple Payhin

Luottokortteja voidaan lisätä käsin Apple Payhin Applen laitteissa.

Luotto- tai pankkikorttien lisääminen käsin

Kun kortti lisätään käsin, nimeä, kortin numeroa, vanhentumispäivää ja turvakoodia käytetään tietojentuontiprosessin sujuvoittamiseksi. Käyttäjät voivat syöttää nämä tiedot Asetuksissa, Applen Lompakossa tai Apple Watch -apissa kirjoittamalla tai käyttämällä laitteen kameraa. Kun kortin tiedot tallennetaan kameralla, Apple pyrkii täyttämään nimen, kortin numeron ja vanhentumispäivän. Kuvaa ei koskaan tallenneta laitteeseen tai kuvakirjastoon. Kun kaikki kentät on täytetty, kortin tarkistusprosessi tarkistaa muut kentät paitsi turvakoodin. Ne salataan ja lähetetään Apple Pay -palvelimelle.

Jos kortin tarkistusprosessi palauttaa ehtojen ID:n, Apple lataa ja näyttää kortin myöntäjän ehdot käyttäjälle. Jos käyttäjä hyväksyy ehdot, Apple lähettää hyväksyttyjen ehtojen ID:n sekä turvakoodin liittämis- ja tietojentuontiprosessiin. Lisäksi Apple jakaa osana liittämis- ja tietojentuontiprosessia kortin myöntäjälle tai verkolle tietoja laitteelta. Niihin sisältyy tietoja (a) käyttäjän iTunes- ja App Store -tilin toiminnasta (esimerkiksi onko käyttäjällä pitkä ostohistoria iTunesissa), (b) tietoja laitteesta (esimerkiksi käyttäjän laitteen puhelinnumero, nimi ja malli ja mahdollinen Apple Payn käyttöönottoon tarvittava kumppanilaite) sekä (c) käyttäjän likimääräinen sijainti kortin lisäämishetkellä (jos käyttäjä on ottanut sijaintipalvelut käyttöön). Kortin myöntäjä käyttää näitä tietoja ratkaistessaan, hyväksyykö se kortin lisäämisen Apple Payhin.

Liittämis- ja tietojentuontiprosessin tuloksena tapahtuu kaksi asiaa:

- Laite alkaa ladata luotto- tai pankkikorttia edustavaa Applen Lompakon korttitiedostoa.
- Laite aloittaa kortin sitomisen Secure Elementiin.

Korttitiedosto sisältää osoitteen kortin kuvan lataamista varten sekä kortin metadataa kuten yhteystiedot, siihen liittyvän kortin myöntäjän apin ja tuetut ominaisuudet. Se sisältää myös kortin tilan, johon kuuluu muun muassa tieto siitä, onko Secure Elementin personointi valmis, onko kortin myöntäjä parhaillaan keskeyttänyt kortin käytön tai tarvitaanko lisävahvistusta, ennen kuin korttia voidaan käyttää maksamiseen Apple Paylla.

Luotto- tai pankkikorttien lisääminen iTunes Store -tililtä

Kun kyseessä on iTunesiin arkistoitu luotto- tai pankkikortti, käyttäjän on ehkä syötettävä uudelleen Apple ID -salasanansa. Kortin numero noudetaan iTunesista ja kortin tarkistusprosessi aloitetaan. Jos kortti on kelvollinen Apple Payhin, laite lataa ja näyttää ehdot ja lähettää sitten ehtojen ID:n ja kortin turvakoodin liittämis- ja tietojentuontiprosessiin. iTunes-tilille arkistoiduille korteille saatetaan tehdä lisävahvistus.

Luotto- tai pankkikorttien lisääminen kortin myöntäjän apista

Kun appi rekisteröidään käytettäväksi Apple Payn kanssa, muodostetaan avaimet apille ja kortin myöntäjän palvelimelle. Näillä avaimilla salataan kortin myöntäjälle lähetettävät kortin tiedot. Tämä on suunniteltu estämään Applen laitetta lukemasta tietoja. Tietojen tuomisen kulku on samanlainen kuin lisättäessä kortteja käsin, mistä on kerrottu edellä, paitsi että turvakoodin sijasta käytetään kertakäyttöisiä salasanoja.

Luotto- tai pankkikorttien lisääminen kortin myöntäjän verkkosivustolta

Jotkin kortin myöntäjät tarjoavat mahdollisuuden aloittaa kortin tietojen tuominen Applen Lompakkoon suoraan omilta verkkosivustoiltaan. Tässä tapauksessa käyttäjä aloittaa tietojen tuonnin valitsemalla kortin myöntäjän verkkosivustolla sen kortin, jonka tiedot tuodaan. Sen jälkeen käyttäjä ohjataan itsenäiseen Applen sisäänkirjautumiseen (sisältö Applen domainilla) ja häntä kehotetaan kirjautumaan sisään Apple ID:llään. Onnistuneen sisäänkirjautumisen jälkeen käyttäjä valitsee yhden tai useamman laitteen, johon kortin tiedot tuodaan, ja häntä vaaditaan vahvistamaan tietojen tuonti kussakin kohdelaitteessa.

Lisävahvistuksen lisääminen

Kortin myöntäjä voi päättää, vaatiiko luotto- tai pankkikortti lisävahvistuksen. Kortin myöntäjän tarjoamista mahdollisuuksista riippuen käyttäjä voi valita lisävahvistuksen eri vaihtoehdoista, kuten tekstiviesti, sähköposti, asiakaspalvelun soitto tai hyväksytyn muun valmistajan apin vahvistusmenetelmä. Käytettäessä tekstiviestejä tai sähköpostia käyttäjä valitsee kortin myöntäjälle tallennetuista yhteystiedoista. Käyttäjälle lähetetään koodi, joka tulee syöttää Applen Lompakkoon, Asetuksiin tai Apple Watch -appiin. Käytettäessä asiakaspalvelua tai vahvistusta apissa kortin myöntäjä hoitaa viestintäprosessin.

Maksun valtuutus Apple Payn kanssa

Jos laitteessa on Secure Enclave, maksu voidaan maksaa vasta, kun sille on saatu valtuutus Secure Enclavelta. iPhonessa tai iPadissa tähän kuuluu sen vahvistaminen, että käyttäjä on suorittanut todennuksen Face ID:llä, Touch ID:llä tai laitteen pääsykoodilla. Jos Face ID tai Touch ID on käytettävissä, sitä käytetään oletusarvoisesti, mutta aina voidaan kuitenkin käyttää pääsykoodia. Pääsykoodia ehdotetaan automaattisesti, jos sormenjäljen tunnistaminen on epäonnistunut kolme kertaa tai kasvojen tunnistaminen on epäonnistunut kaksi kertaa. Viiden epäonnistuneen yrityksen jälkeen vaaditaan pääsykoodi. Pääsykoodia vaaditaan myös silloin, kun Face ID:tä tai Touch ID:tä ei ole määritetty tai se ei ole käytössä Apple Paylle. Maksettaessa Apple Watchilla laitteen lukituksen tulee olla avattu pääsykoodilla ja sivupainiketta tulee painaa kahdesti, jotta maksu suoritetaan.

Jaetun pariavaimen käyttäminen

Tiedonsiirto Secure Enclaven ja Secure Elementin välillä tapahtuu sarjaliitännän kautta siten, että Secure Element on yhdistetty NFC-ohjaimeen, joka puolestaan on yhdistetty appeja suorittavaan prosessoriin. Vaikka niitä ei ole yhdistetty suoraan, Secure Enclave ja Secure Element voivat viestiä suojatusti käyttäen jaettua pariavainta, jonka ne saavat valmistusprosessin aikana. Viestinnän salaus ja todennus perustuvat AES-menetelmään, jossa kumpikin puoli käyttää salauksessa satunnaisia lisämerkkejä (nonce) suojana toistohyökkäyksiltä. Pariavain luodaan Secure Enclavessa sen UID-avaimesta ja Secure Elementin yksilöllisestä tunnisteesta. Sen jälkeen pariavain siirretään tehtaalla suojatusti Secure Enclavesta laitteiston suojausmoduuliin, jossa on tarvittava avainmateriaali pariavaimen viemiseksi Secure Elementiin.

Suojatun maksutapahtuman valtuuttaminen

Kun käyttäjä valtuuttaa maksutapahtuman, joka sisältää suoraan Secure Enclavelle lähetetyn fyysisen eleen, Secure Enclave lähettää allekirjoitetun datan valtuutuksen tyypistä ja tiedot maksutapahtuman tyypistä (lähimaksu tai maksu apissa) Secure Elementille sidottuna AR (Authorization Random) -arvoon. AR-arvo luodaan Secure Enclavessa, kun käyttäjä ensimmäisen kerran tuo luottokortin tiedot, ja se säilyy niin kauan kuin Apple Pay on käytössä. Sitä suojaavat Secure Enclaven salaus ja heikennysten vastainen suojausmekanismi. Se toimitetaan Secure Elementille suojatusti pariavainta käyttäen. Jos Secure Element saa uuden AR-arvon, se merkitsee aiemmin lisätyt kortit poistetuiksi.

Maksukryptogrammin käyttäminen dynaamiseen suojaukseen

Maksusovelmista tuleviin maksutapahtumiin sisältyy maksukryptogrammi ja laitteen tilinumero. Tämä kryptogrammi on kertakäyttöinen koodi. Se lasketaan käyttäen tapahtumalaskuria ja avainta. Jokainen uusi tapahtuma kasvattaa tapahtumalaskurin lukemaa. Avaimen tiedot tuodaan maksusovelmassa personoinnin aikana ja ne ovat maksuverkon tai kortin myöntäjän tai molempien tiedossa. Maksumallista riippuen laskemiseen voidaan käyttää myös muita tietoja, kuten:

- Terminal Unpredictable Number NFC-tapahtumille
- Apple Pay -palvelimen nonce apeissa tapahtuville maksuille

Nämä suojakoodit annetaan maksuverkolle ja kortin myöntäjälle, jotta myöntäjä voi vahvistaa kunkin tapahtuman. Näiden suojakoodien pituus voi vaihdella riippuen tapahtuman tyypistä.

Maksaminen korteilla Apple Payta käyttäen

Apple Payta voidaan käyttää ostosten maksamiseen myymälöissä, apeissa ja verkkosivustoilla.

Maksaminen korteilla myymälöissä

Jos iPhone tai Apple Watch on päällä ja havaitsee NFC-kentän, se näyttää käyttäjälle pyydetyn kortin (jos kyseisen kortin automaattinen valinta on päällä) tai oletuskortin, jota hallitaan Asetuksissa. Käyttäjä voi myös avata Applen Lompakon ja valita kortin, tai kun laite on lukittu, käyttäjä voi:

- painaa kahdesti sivupainiketta Face ID:llä varustetuissa laitteissa
- painaa kahdesti Koti-painiketta Touch ID:llä varustetuissa laitteissa
- käyttää Apple Payn lukitulta näytöltä mahdollistavia käyttöapuominaisuuksia

Seuraavaksi käyttäjän on suoritettava todennus käyttäen Face ID:tä, Touch ID:tä tai pääsykoodiaan, ennen kuin maksutiedot välitetään. Kun Apple Watch on lukitsematon, sivupainikkeen painaminen kahdesti aktivoi oletuskortin maksua varten. Mitään maksutietoja ei lähetetä ilman käyttäjän todennusta.

Kun käyttäjä on suorittanut todennuksen, maksun käsittelyyn käytetään laitteen tilinumeroa ja tapahtumakohtaista dynaamista suojakoodia. Apple tai käyttäjän laite ei kumpikaan lähetä luotto- tai pankkikorttien koko numeroita myyjille. Apple voi saada tapahtumasta anonyymeja tietoja, kuten likimääräisen ajan ja sijainnin. Tiedot auttavat parantamaan Apple Payta ja muita Applen tuotteita ja palveluita.

Maksaminen korteilla apeissa

Apple Payta voidaan käyttää myös maksamiseen iPhonen, iPadin, Macin ja Apple Watchin apeissa. Kun käyttäjät maksavat apeissa käyttäen Apple Payta, Apple saa tapahtuman tiedot salattuina. Ennen kuin tiedot lähetetään kehittäjälle tai myyjälle, Apple salaa tapahtuman uudelleen kehittäjäkohtaisella avaimella. Apple Pay säilyttää anonyymeja tapahtumatietoja kuten oston likimääräisen summan. Näitä tietoja ei voi yhdistää käyttäjään, eikä niihin koskaan sisälly tietoa siitä, mitä käyttäjä ostaa.

Kun appi aloittaa Apple Pay -maksutapahtuman, Apple Pay -palvelimet vastaanottavat salatun tapahtuman laitteelta, ennen kuin myyjä saa sen. Apple Pay -palvelimet salaavat sitten tapahtuman uudelleen myyjäkohtaisella avaimella ennen kuin välittävät sen myyjälle.

Kun appi pyytää maksua, se kutsuu ohjelmointirajapintaa (API) selvittääkseen, tukeeko laite Apple Payta ja onko käyttäjällä luotto- tai pankkikortteja, joilla voidaan maksaa myyjän hyväksymässä maksuverkossa. Appi pyytää kaikkia tietoja, jotka se tarvitsee käsitelläkseen ja toteuttaakseen tapahtuman, kuten laskutus- ja toimitusosoitetta ja yhteystietoja. Sitten appi pyytää iOS:ää, iPadOS:ää tai watchOS:ää esittämään Apple Pay -lomakkeen, joka pyytää tietoja apille, sekä muita tarvittavia tietoja, kuten käytettävän kortin.

Tässä vaiheessa apille kerrotaan kaupunki-, valtio- ja postinumerotiedot, jotta se voi laskea lopulliset toimituskulut. Kaikkia pyydettyjä tietoja ei anneta apille, ennen kuin käyttäjä valtuuttaa maksun Face ID:llä, Touch ID:llä tai laitteen pääsykoodilla. Kun maksu on valtuutettu, Apple Pay -lomakkeessa olevat tiedot siirretään myyjälle.

Apin maksun valtuutus

Kun käyttäjä valtuuttaa maksun, Apple Pay -palvelimille lähetetään pyyntö saada salaus-nonce, joka on samanlainen kuin NFC-päätteen palauttama arvo myymälässä suoritettavissa maksutapahtumissa. Nonce ja muut tapahtuman tiedot annetaan Secure Elementille, jotta se laskee maksun tunnistetiedon, joka salataan Applen avaimella. Salattu maksun tunnistetieto palautetaan Apple Pay -palvelimille, jotka purkavat salauksen, vahvistavat tunnistetiedon noncen vertaamalla sitä Apple Pay -palvelimien alun perin lähettämään nonceen ja salaavat maksun tunnistetiedon uudelleen myyjän tunnukseen liitetyllä myyjän avaimella. Sitten maksu palautetaan laitteeseen, joka antaa sen takaisin apille ohjelmointirajapinnan kautta. Sen jälkeen appi antaa sen käsiteltäväksi myyjän järjestelmään. Myyjä voi purkaa maksun tunnistetiedon salauksen käsittelyä varten yksityisellä avaimellaan. Tämä yhdessä Applen palvelimilta saatavan allekirjoituksen kanssa mahdollistaa myyjälle sen varmistamisen, että tapahtuma oli tarkoitettu juuri tälle myyjälle.

Ohjelmointirajapinnat vaativat oikeutuksen, jossa on eritelty tuetut myyjän tunnukset. Appi voi lisätä myös muita tietoja (esimerkiksi tilausnumero tai asiakkaan identiteetti), jotka lähetetään Secure Elementille allekirjoitettaviksi ja joilla varmistetaan, ettei tapahtumaa voi suunnata toiselle asiakkaalle. Apin kehittäjä voi toteuttaa tämän määrittelemällä applicationData-ominaisuuden PKPaymentRequest-luokassa. Tämän datan tiiviste sisältyy salattuun maksudataan. On myyjän vastuulla tarkistaa, että myyjän applicationData-tiiviste vastaa maksudatassa olevaa.

Maksaminen korteilla verkkosivustoilla

Apple Payta voidaan käyttää maksamiseen verkkosivustoilla iPhonessa, iPadissa, Apple Watchissa ja Mac-tietokoneissa, joissa on Touch ID. Apple Pay -maksutapahtumat voidaan myös aloittaa Macilla ja viedä loppuun Apple Payta käyttävässä iPhonessa tai Apple Watchissa, jossa käytetään samaa iCloud-tiliä.

Apple Payn käyttäminen verkossa edellyttää kaikilta siihen osallistuvilta verkkosivustoilta rekisteröintiä Applelle. Kun domain on rekisteröity, domain-nimen validointi suoritetaan vasta, kun Apple on antanut TLS-asiakasvarmenteen. Apple Payta tukevia verkkosivustoja vaaditaan käyttämään sisällölleen HTTPS-protokollaa. Sivustot tarvitsevat jokaista maksutapahtumaa varten suojatun ja yksilöllisen myyjäistunnon Applen palvelimelta käyttäen Applen myöntämää TLS-asiakasvarmennetta. Apple allekirjoittaa myyjäistunnon datan. Kun myyjäistunnon allekirjoitus on vahvistettu, verkkosivusto voi kysyä, onko käyttäjällä Apple Payta tukeva laite ja onko hän aktivoinut luotto-, pankki- tai prepaid-kortin laitteessa. Muita tietoja ei jaeta. Jos käyttäjä ei halua jakaa näitä tietoja, hän voi estää Apple Pay -kyselyt Safarin yksityisyysasetuksissa iPhone-, iPad- ja Mac-laitteissa.

Kun myyjäistunto on validoitu, kaikki tietosuoja- ja suojaustoimet ovat samat kuin apissa maksettaessa.

Kun käyttäjä siirtää maksuun liittyviä tietoja Macista iPhoneen tai Apple Watchiin, Apple Pay Handoff käyttää päästä päähän salattua Apple Identity Service (IDS) -protokollaa maksuun liittyvien tietojen siirtämiseen käyttäjän Macin ja valtuuttavan laitteen välillä. IDS-asiakas Macissa käyttää käyttäjän laitteen avaimia salaamiseen, joten mikään muu laite ei voi purkaa tietojen salausta, eivätkä avaimet ole Applen käytettävissä. Apple Payn Handoffin laitteiden etsintä sisältää käyttäjän luottokorttien tyypin ja yksilöllisen tunnisteen sekä metadataa. Laitekohtaista käyttäjän kortin tilinumeroa ei jaeta, ja se pysyy suojatusti tallennettuna käyttäjän iPhonessa tai Apple Watchissa. Apple myös siirtää suojatusti käyttäjän äskettäin käytetyt yhteystiedot ja toimitus- ja laskutusosoitteen iCloud-avainnipun kautta.

Kun käyttäjä valtuuttaa maksun käyttämällä Face ID:tä, Touch ID:tä tai pääsykoodia tai painamalla kahdesti sivupainiketta Apple Watchissa, yksilöllisesti kunkin verkkosivuston myyjävarmenteelle salattu maksutunniste lähetetään suojatusti käyttäjän iPhonesta tai Apple Watchista hänen Maciinsa ja toimitetaan sitten myyjän verkkosivustolle.

Vain lähellä toisiaan olevat laitteet voivat pyytää maksua ja viedä maksutapahtuman loppuun. Läheisyys määritetään Bluetooth Low Energy (BLE) -mainoksilla.

Lähiluettavat kortit Apple Payssa

Apple käyttää Applen lisäarvopalveluprotokollaa (Apple Value Added Services, Apple VAS) datan lähettämiseksi tuetuista korteista yhteensopiviin NFC-päätteisiin. VAS-protokollaa voidaan käyttää lähilukupäätteissä tai iPhone-apeissa, ja se käyttää NFC-teknologiaa viestintään tuettujen Applen laitteiden kanssa. VAS-protokolla toimii lähietäisyydellä ja sitä voidaan käyttää lähiluettavien korttien esittämiseen itsenäisesti tai osana Apple Pay -tapahtumaa.

Kun laitetta pidetään lähellä NFC-päätettä, pääte käynnistää kortin tietojen vastaanottamisen lähettämällä korttipyynnön. Jos käyttäjällä on kortti, jolla on kortin tarjoajan tunniste, käyttäjää pyydetään valtuuttamaan sen käyttö Face ID:llä, Touch ID:llä tai pääsykoodilla. Käyttämällä kortin tietoja, aikaleimaa ja kertakäyttöistä satunnaista ECDH P-256 -avainta yhdessä kortin tarjoajan julkisen avaimen kanssa muodostetaan salausavain kortin datalle, joka lähetetään sitten päätteelle.

iOS 12.01:stä alkaen iOS 13:een saakka käyttäjät voivat valita kortin käsin ennen sen esittämistä myyjän NFC-päätteelle. iOS 13.1:ssä ja uudemmissa kortin tarjoajat voivat määrittää käsin valitut kortit joko vaatimaan käyttäjän todentamista tai toimimaan ilman todentamista.

Korttien Apple Pay -käytön estäminen

Secure Elementiin lisättyjä luotto-, pankki- ja prepaid-kortteja voidaan käyttää vain, jos Secure Elementille esitetään valtuutus käyttäen samaa pariavainta ja AR-arvoa (Authorization Random), joita käytettiin, kun kortti lisättiin. Jos Secure Element saa uuden AR-arvon, se merkitsee aiemmin lisätyt kortit poistetuiksi. Tämän ansiosta käyttöjärjestelmä voi ohjeistaa Secure Enclavea poistamaan kortit käytöstä merkitsemällä kopionsa AR-arvosta epäkelvoksi seuraavissa tilanteissa:

Menetelmä	Laite
Pääsykoodi otetaan pois käytöstä.	iPhone, iPad, Apple Watch
Salasana otetaan pois käytöstä.	Mac
Käyttäjä kirjautuu ulos iCloudista.	iPhone, iPad, Mac, Apple Watch
Käyttäjä valitsee komennon Poista kaikki sisältö ja asetukset.	iPhone, iPad, Mac, Apple Watch
Laite palautetaan palautustilasta.	iPhone, iPad, Mac, Apple Watch
Laiteparin poistaminen	Apple Watch

Korttien käytön keskeyttäminen, poistaminen ja tyhjentäminen

Käyttäjät voivat keskeyttää Apple Payn käytön iPhonessa, iPadissa ja Apple Watchissa asettamalla laitteen Kadonnut-tilaan Missä on…? -palvelulla. Käyttäjät voivat myös poistaa kortteja tai tyhjentää kortit Apple Paysta käyttäen Missä on…? -palvelua tai iCloud.com-sivustoa tai suoraan laitteessa käyttäen Applen Lompakkoa. Apple Watchista kortit voidaan poistaa käyttäen iCloud-asetuksia tai Apple Watch -appia iPhonessa tai suoraan kellossa. Kortin myöntäjä tai maksuverkko keskeyttää tai poistaa Apple Paysta mahdollisuuden suorittaa maksuja laitteessa kortteja käyttäen, vaikka laite ei olisi linjoilla eikä yhteydessä mobiilidata- tai Wi-Fi-verkkoon. Käyttäjät voivat myös soittaa kortin myöntäjälle ja pyytää tätä keskeyttämään korttien käytön tai poistamaan ne Apple Paysta.

Kun käyttäjä tyhjentää koko laitteen käyttämällä komentoa Poista kaikki sisältö ja asetukset tai Missä on…? -palvelua tai palauttamalla laitteen, iPhone, iPad, iPod touch, Mac ja Apple Watch ohjeistavat Secure Elementiä merkitsemään kaikki kortit poistetuiksi. Tämä astuu voimaan välittömästi ja korttien käyttö estetään, kunnes saadaan yhteys Apple Pay -palvelimiin, jotta kortit saadaan kokonaan poistettua Secure Elementistä. Secure Enclave merkitsee itsenäisesti AR-arvon epäkelvoksi, jotta aiemmin rekisteröityjen korttien maksuja ei enää voida valtuuttaa. Kun laite on yhteydessä verkkoon, se yrittää saada yhteyden Apple Pay -palvelimiin auttaakseen varmistamaan, että kaikki kortit Secure Elementissä poistetaan.

Apple Cardin suojaus

Tuetuissa iPhone- ja Mac-malleissa käyttäjät voivat hakea suojatusti Apple Cardia.

Apple Card -hakemus

iOS 12.4:ssä tai uudemmassa, macOS 10.14.6:ssa tai uudemmassa ja watchOS 5.3:ssa tai uudemmassa voidaan käyttää Apple Cardia Apple Payn kanssa maksamiseen myymälöissä, apeissa ja verkossa.

Voidakseen hakea Apple Cardia käyttäjän tulee olla kirjautunut sisään iCloud-tililleen Apple Payta tukevassa iOS- tai iPadOS-laitteessa, ja kaksiosaisen todennuksen tulee olla käytössä iCloud-tilille. Kun hakemus on hyväksytty, Apple Cardiin pääsee Applen Lompakossa tai valitsemalla Asetukset > Lompakko ja Apple Pay missä tahansa vaatimukset täyttävässä laitteessa, jossa käyttäjä on kirjautunut sisään Apple ID:llään.

Kun käyttäjä hakee Apple Cardia, Applen kumppaneina toimivat tunnistustietojen tarjoajat tarkistavat käyttäjän henkilöllisyyden suojatusti, ja sen jälkeen henkilöllisyyttä koskevat tiedot jaetaan Goldman Sachs Bank USA:lle henkilöllisyyttä ja luottokelpoisuuden arviointia varten.

Sellaiset hakemuksen yhteydessä annetut tiedot kuten henkilötunnus tai kuva henkilöllisyystodistuksesta toimitetaan suojatusti Applen kumppaneina toimiville tunnistustietojen tarjoajille ja/tai Goldman Sachs Bank USA:lle salattuina kunkin avaimilla. Apple ei voi purkaa näiden tietojen salausta.

Hakemisen yhteydessä annetut tiedot tuloista sekä laskujen maksamiseen käytettävän pankkitilin tiedot toimitetaan suojatusti Goldman Sachs Bank USA:lle salattuina sen avaimella. Pankkitilitiedot tallennetaan avainnippuun. Apple ei voi purkaa näiden tietojen salausta.

Kun Apple Card lisätään Applen Lompakkoon, samat tiedot kuin luotto- tai pankkikortin lisäämisen yhteydessä voidaan jakaa Applen kumppanipankille Goldman Sachs Bank USA:lle ja Apple Payments Inc:lle. Näitä tietoja käytetään ainoastaan vianmääritykseen, petosten torjuntaan ja virallisten määräysten noudattamiseen.

iOS 14.6:ssa tai uudemmissa, iPadOS 14.6:ssa tai uudemmissa ja watchOS 7.5:ssä tai uudemmissa iCloud-perheen järjestäjä, jolla on Apple Card, voi jakaa korttinsa yli 13-vuotiaiden iCloud-perheen jäsenten kanssa. Kutsun vahvistamiseen vaaditaan käyttäjän todennus. Applen Lompakko käyttää Secure Enclavessa olevaa avainta omistajan ja kutsunsaajan toisiinsa sitovan allekirjoituksen laskemiseen. Tämä allekirjoitus validoidaan Applen palvelimilla.

Järjestäjä voi halutessaan asettaa osallistujille maksurajan. Osallistujien kortit voidaan myös milloin tahansa lukita Applen Lompakon kautta niiden käytön keskeyttämiseksi. Kun yhteisomistaja tai yli 18-vuotias osallistuja hyväksyy kutsun ja hakee korttia, hän käy läpi saman hakuprosessin, josta on kerrottu Applen Lompakon Apple Card -hakemusta käsittelevässä osiossa.

Apple Cardin käyttö

Fyysisen kortin voi tilata Apple Cardista Applen Lompakossa. Kun käyttäjä on vastaanottanut fyysisen kortin, se aktivoidaan käyttäen NFC-tunnistetta, joka on kaksinkertaisessa kirjekuoressa kortin kanssa. Jokaiselle kortille on yksilöllinen tunniste, eikä tunnisteella voi aktivoida toisen käyttäjän korttia. Vaihtoehtoisesti kortin voi aktivoida käsin Applen Lompakon asetuksissa. Lisäksi käyttäjä voi lukita tai avata fyysisen kortin milloin tahansa Applen Lompakossa.

Apple Card -maksut ja Applen Lompakon korttien tiedot

Apple Card -tilin erääntyvät maksut voidaan maksaa Applen Lompakosta iOS:ssä Apple Cashilla ja pankkitilillä. Laskut voidaan ajastaa toistuvasti maksettaviksi tai maksettaviksi kerran tiettynä päivänä Apple Cashilla ja pankkitilillä. Kun käyttäjä maksaa, Apple Pay -palvelimille lähetetään kutsu, jolla pyydetään samanlainen salaus-nonce kuin Apple Cashilla. Nonce ja maksun tiedot annetaan Secure Elementille, jotta se laskee allekirjoituksen. Sitten allekirjoitus palautetaan Apple Pay -palvelimille. Apple Pay -palvelimet tarkistavat maksun todentamisen, eheyden ja oikeellisuuden käyttäen allekirjoitusta ja noncea, ja määräys annetaan Goldman Sachs Bank USA:lle käsiteltäväksi.

Applen Lompakko noutaa Apple Cardin numeron esittämällä varmenteen. Apple Pay -palvelin validoi varmenteen sen varmistamiseksi, että avain on muodostettu Secure Enclavessa. Sitten se käyttää tätä avainta Apple Cardin numeron salaamiseen ennen kuin palauttaa sen Applen Lompakkoon, jotta vain Apple Cardin numeroa pyytänyt iPhone voi purkaa salauksen. Salauksen purkamisen jälkeen Apple Cardin numero tallennetaan iCloud-avainnippuun.

Apple Cardin numeron tietojen näyttäminen kortissa Applen Lompakkoa käyttäen vaatii käyttäjän todennuksen Face ID:llä, Touch ID:llä tai pääsykoodilla. Käyttäjä voi korvata sen kortin tieto-osiossa, ja se poistaa edellisen käytöstä.

Edistyksellinen petossuojaus

iOS 15:ssä tai uudemmissa ja iPadOS 15:ssä tai uudemmissa Apple Cardin käyttäjä voi ottaa Applen Lompakossa käyttöön edistyksellisen petossuojauksen. Kun se on käytössä, kortin turvakoodi päivittyy muutaman päivän välein.

Apple Cashin suojaus

iOS 11.2:ssa tai uudemmissa, iPadOS 13.1:ssä tai uudemmissa ja watchOS 4.2:ssa tai uudemmissa Apple Payta voidaan käyttää rahan lähettämiseen, vastaanottamiseen ja pyytämiseen toisilta käyttäjiltä iPhonessa, iPadissa tai Apple Watchissa. Kun käyttäjä vastaanottaa rahaa, se lisätään Apple Cash -tilille, johon pääsee Applen Lompakossa tai valitsemalla Asetukset > Lompakko ja Apple Pay missä tahansa vaatimukset täyttävässä laitteessa, jossa käyttäjä on kirjautunut sisään Apple ID:llään.

iOS 14:ssä, iPadOS 14:ssä ja watchOS 7:ssä iCloud-perheen järjestäjä, joka on vahvistanut henkilöllisyytensä Apple Cashille, voi ottaa Apple Cashin käyttöön alle 18-vuotiaille perheenjäsenilleen. Järjestäjä voi halutessaan rajoittaa näille perheenjäsenille sallittua rahan lähettämistä siten, että rahaa voi lähettää vain perheenjäsenille tai vain yhteystiedoissa oleville henkilöille. Jos alle 18-vuotiaan perheenjäsenen Apple ID -tili palautetaan, perheen järjestäjän on otettava uudelleen Apple Cash -kortti käyttöön kyseiselle käyttäjälle käsin. Jos alle 18-vuotias perheenjäsen ei enää ole iCloud-perheen jäsen, hänen Apple Cash -saldonsa siirretään automaattisesti järjestäjän tilille.

Kun käyttäjä ottaa Apple Cashin käyttöön, samat tiedot kuin luotto- ja pankkikortteja lisättäessä voidaan jakaa kumppanipankillemme Green Dot Bankille sekä Apple Payments Inc:lle. Apple Payments Inc. on Applen kokonaan omistama tytäryhtiö, joka on luotu varmistamaan käyttäjän tietosuoja säilyttämällä ja käsittelemällä tiedot erillään muusta Applen toiminnasta ja tavalla, jota muut Applen yksiköt eivät tiedä. Näitä tietoja käytetään ainoastaan vianmääritykseen, petosyritysten torjuntaan ja virallisten määräysten noudattamiseen.

Apple Cashin käyttäminen iMessagessa

Voidakseen käyttää rahansiirtoja yksityishenkilöiden välillä ja Apple Cashia käyttäjän tulee olla kirjautunut sisään iCloud-tililleen Apple Cashia tukevassa laitteessa ja kaksiosaisen todennuksen tulee olla käytössä iCloud-tilille. Rahapyynnöt ja käyttäjien väliset siirrot aloitetaan Viestit-apista tai pyytämällä Siriltä. Kun käyttäjä yrittää lähettää rahaa, iMessage näyttää Apple Pay -lomakkeen. Ensimmäisenä käytetään aina Apple Cash -saldoa. Tarvittaessa rahaa nostetaan lisäksi toiselta luotto- tai pankkikortilta, jonka käyttäjä on lisännyt Applen Lompakkoon.

Apple Cashin käyttäminen myymälöissä, apeissa ja verkossa

Apple Cash -korttia Applen Lompakossa voidaan käyttää Apple Payn kanssa maksamiseen myymälöissä, apeissa ja verkossa. Apple Cash -tililtä voidaan myös siirtää rahaa pankkitilille. Toiselta käyttäjältä vastaanotetun rahan lisäksi Apple Cash -tilille voidaan lisätä rahaa pankki- tai prepaid-kortilta Applen Lompakossa.

Apple Payments Inc. tallentaa ja voi käyttää käyttäjän tilitapahtumatietoja vianmääritykseen, petosten torjuntaan ja virallisten määräysten noudattamiseen, kun tapahtuma on suoritettu. Applen muut yksiköt eivät tiedä, kenelle käyttäjä on lähettänyt rahaa tai keneltä hän on saanut rahaa tai missä hän on tehnyt ostoksia Apple Cash -kortilla.

Kun käyttäjä lähettää rahaa Apple Paylla, lisää rahaa Apple Cash -tilille tai siirtää rahaa pankkitilille, Apple Pay -palvelimille lähetetään kutsu, jossa pyydetään arvoltaan samanlaista salaus-noncea kuin käytettäessä Apple Payta apeissa. Nonce ja muu tapahtuman data annetaan Secure Elementille, jotta se laskee maksun allekirjoituksen. Allekirjoitus palautetaan Apple Pay -palvelimille. Apple Pay -palvelimet tarkistavat tapahtuman todentamisen, eheyden ja oikeellisuuden käyttäen allekirjoitusta ja noncea. Sen jälkeen rahansiirto aloitetaan, ja käyttäjä saa ilmoituksen suoritetusta tapahtumasta.

Jos maksutapahtuman osana on:

- pankkikortti, jolla lisätään rahaa Apple Cashiin
- lisärahan antaminen mikäli Apple Cashin saldo ei riitä

tuotetaan myös salattu maksun tunnistetieto, joka lähetetään Apple Pay -palvelimille samalla tavoin kuin Apple Pay toimii apeissa ja verkkosivustoilla.

Kun Apple Cash -tilin saldo ylittää tietyn summan tai jos havaitaan epätavallista toimintaa, käyttäjää kehotetaan vahvistamaan henkilöllisyytensä. Käyttäjän henkilöllisyyden vahvistamiseksi annetut tiedot, kuten henkilötunnus tai vastaukset kysymyksiin (esimerkiksi aikaisemman asuinosoitteen kadunnimi) toimitetaan suojattuina Applen kumppanille ja salataan kumppanin avaimella. Apple ei voi purkaa näiden tietojen salausta. Jos käyttäjä tekee Apple ID -tilin palautuksen, häntä pyydetään vahvistamaan henkilöllisyytensä uudelleen ennen kuin hän pääsee Apple Cash -saldoonsa.

Tap to Pay on iPhone -ominaisuuden suojaus

Tap to Pay on iPhone on saatavilla iOS 15.4:ssä, ja sen ansiosta myyjät Yhdysvalloissa voivat hyväksyä Apple Pay -maksuja ja muita lähimaksuja käyttämällä iPhonea ja kumppanin mahdollistamaa iOS-appia. Tällä palvelulla tuettujen iPhone-laitteiden käyttäjät voivat hyväksyä suojatusti lähimaksuja ja *Apple Payn* NFC:tä tukevia kortteja. Tap to Pay on iPhone -ominaisuutta käytettäessä myyjät eivät tarvitse lisälaitteita lähimaksujen hyväksymistä varten.

Tap to Pay on iPhone on suunniteltu suojaamaan maksajan henkilötietoja. Tämä palvelu ei kerää mitään sellaisia maksutapahtumatietoja, jotka voidaan yhdistää takaisin käyttäjään. Secure Element suojaa maksukorttitiedot, kuten luotto-/pankkikortin numeron (PAN), eivätkä ne ole myyjän saatavilla. Maksukortin tiedot jäävät myyjän maksupalvelun tarjoajan, maksajan ja kortin myöntäjän välisiksi. Tap to Pay -palvelu ei myöskään kerää maksajien nimiä, osoitteita tai puhelinnumeroita.

Tap to Pay on iPhone on läpikäynyt akkreditoidun turvallisuustutkimuslaitoksen ulkopuolisen arvioinnin ja saanut hyväksynnän American Expressiltä, Discoverilta, Mastercardilta ja Visalta.

Lähimaksua suojaavat komponentit

- *Secure Element:* Secure Elementissä [Linkki Apple Payn Secure Element -osioon] ovat maksukernelit, jotka lukevat ja suojaavat lähimaksukortin tiedot.
- *NFC-ohjain:* NFC-ohjain käsittelee NFC (Near Field Communication) -protokollia ja reitittää viestintää appeja suorittavan prosessorin ja Secure Elementin sekä Secure Elementin ja lähimaksukortin välillä.
- *Tap to Pay on iPhone -palvelimet:* Tap to Pay on iPhone -palvelimet hallitsevat maksukernelien käyttöönottoa ja provisiointia laitteessa. Nämä palvelimet myös valvovat Tap to Pay on iPhone -laitteiden turvallisuutta tavalla, joka vastaa Payment Card Industry Security Standards Council (PCI SSC) -neuvoston Contactless Payments on COTS (CPoC) -standardia, ja ne ovat PCI DSS:n vaatimusten mukaisia.

Miten Tap to Pay lukee luotto-, pankki- ja prepaid-kortteja

Provisioinnin suojauksen yleiskatsaus

Kun Tap to Pay on iPhone -ominaisuutta käytetään ensimmäisen kerran apilla, jolla on riittävät oikeudet, Tap to Pay on iPhone -palvelin selvittää, täyttääkö laite kelpoisuusvaatimukset, joita ovat esimerkiksi laitemalli, iOS-versio ja pääsykoodin asettaminen. Kun tämä tarkistus on valmis, maksunhyväksymissovelma ladataan Tap to Pay on iPhone -palvelimelta ja asennetaan Secure Elementiin siihen liittyvän maksukernelmäärityksen kanssa. Tämä operaatio suoritetaan suojatusti Tap to Pay on iPhone -palvelinten ja Secure Elementin kesken. Secure Element tarkistaa näiden tietojen eheyden ja aitouden ennen asennusta.

Korttien lukemisen suojauksen yleiskatsaus

Kun jokin Tap to Pay on iPhone -appi pyytää kortin lukemista ProximityReader-sovelluskehykseltä, näytetään (iOS:n hallitsema) lomake, joka kehottaa käyttäjää napauttamaan maksukorttia. iOS valmistelee maksukortinlukijan ja pyytää sitten maksukerneleitä Secure Elementissä käynnistämään kortin lukemisen.

Tässä kohden Secure Element ottaa NFC-ohjaimen hallintaansa lukijatilassa. Tämä tila sallii ainoastaan korttitietojen siirron maksukortin ja Secure Elementin välillä NFC-ohjaimen kautta. Maksukortteja voidaan lukea ainoastaan tässä tilassa.

Kun maksujenhyväksymissovelma Secure Elementissä on lukenut kortin, se salaa ja allekirjoittaa kortin tiedot. Kortin tiedot pysyvät salattuina ja todennettuina, kunnes ne päätyvät maksupalvelun tarjoajalle asti. Ainoastaan maksupalvelun tarjoaja, jota appi käytti pyytääkseen kortin lukemista, voi purkaa kortin tietojen salauksen. Maksupalvelun tarjoajan täytyy pyytää avain kortin tietojen salauksen purkamiseen Tap to Pay on iPhone -palvelimelta. Tap to Pay on iPhone -palvelin lähettää avaimet salauksen purkamiseen maksupalvelun tarjoajalle sen jälkeen, kun tietojen eheys ja aitous on tarkistettu ja on varmistettu, että kortin lukeminen tapahtui 60 sekunnin sisällä kortin lukemisesta laitteella.

Tämä malli auttaa varmistamaan, ettei kortin tietojen salausta voi purkaa kukaan muu kuin maksupalvelun tarjoaja, joka prosessoi maksutapahtuman myyjän puolesta.

Applen Lompakon käyttäminen

Pääsy Applen Lompakkoa käyttäen

Käyttäjät voivat tallentaa kodin, auton ja hotellihuoneen avaimia Applen Lompakkoon tuetuissa iPhone- ja Apple Watch -laitteissa. He voivat jopa tallentaa yritysten kulkukortteja ja opiskelijakortteja. Kun käyttäjä saapuu ovelle, oikea avain esitetään automaattisesti ja hän pääsee sisään yksinkertaisesti napauttamalla hyödyntäen lähilukuteknologiaa (NFC).

Kätevä käyttäjälle

Kun avain, kortti, opiskelijakortti tai yrityksen kulkukortti lisätään Applen Lompakkoon, sen pikatila on oletuksena käytössä. Pikatilassa olevat kortit toimivat hyväksyvien päätteiden kanssa ilman Face ID:tä, Touch ID:tä, pääsykooditodentamista tai Apple Watchin sivupainikkeen painamista kahdesti. Käyttäjät voivat ottaa tämän ominaisuuden pois käytöstä laittamalla pikatilan pois päältä napauttamalla Applen Lompakossa kortin edessä Lisää-painiketta. Pikatilan laittaminen takaisin päälle edellyttää Face ID:n, Touch ID:n tai pääsykoodin käyttämistä.

Tietosuoja ja tietoturva

Applen Lompakossa olevat avaimet hyödyntävät täysimääräisesti iPhoneen ja Apple Watchiin sisältyviä tietosuoja- ja tietoturvaratkaisuja. Tietoa siitä, milloin ja missä henkilö käyttää Applen Lompakossa olevia avaimiaan, ei koskaan jaeta Applelle tai tallenneta Applen palvelimille, ja tunnistetiedot tallennetaan suojatusti tuettujen laitteiden Secure Elementiin (SE). Secure Elementissä on erityiset sovelmat pääsyavainten suojattua hallintaa ja tallentamista varten, millä varmistetaan, ettei avaimia saa esiin.

Ennen minkään pääsyavainten tietojen tuomista käyttäjän täytyy olla kirjautunut iCloud-tililleen yhteensopivassa iPhonessa ja kaksiosaisen todennuksen täytyy olla päällä tälle iCloud-tilille. Poikkeuksena ovat opiskelijakortit, jotka eivät vaadi, että kaksiosainen todennus on päällä.

Kun käyttäjä aloittaa tietojen tuomisen prosessin, seuraavat samanlaiset vaiheet kuin tuotaessa luotto- ja pankkikorttien tietoja, kuten liittäminen ja tietojen tuominen. Tapahtuman aikana lukija viestii Secure Elementin kanssa NFC-ohjaimen kautta käyttäen muodostettua suojattua kanavaa.

Kukin kumppani määrittelee ja hallitsee sitä, kuinka moneen laitteeseen, (mukaan lukien iPhone ja Apple Watch) pääsyavaimen tiedot voidaan tuoda, ja määrä voi vaihdella eri kumppaneilla. Tämän ansiosta kukin kumppani voi hallita laitteille tuotujen pääsyavainten laitetyyppikohtaista enimmäismäärää omien tarpeidensa mukaan. Apple toimittaa kumppaneille tätä tarkoitusta varten laitetyypin ja anonymisoidut laitetunnisteet. Tietosuojan ja tietoturvan vuoksi tunnisteet ovat erilaiset jokaiselle kumppanille.

Avaimet voidaan poistaa käytöstä tai poistaa

- etätyhjentämällä laite Missä on…? -palvelulla
- ottamalla käyttöön Kadonnut-tilan Missä on…? -apilla
- vastaanottamalla mobiililaitteiden hallinnan (MDM) etätyhjennyskomento
- poistamalla kaikki kortit niiden Apple ID -tilisivulta
- poistamalla kaikki kortit iCloud.comista
- poistamalla kaikki kortit Applen Lompakosta
- poistamalla kortti kortin myöntäjän apissa

Kun käyttäjä iOS 15.4:ssä tai uudemmissa painaa kahdesti Face ID:llä varustetun iPhonen sivupainiketta tai Touch ID:llä varustetun iPhonen Koti-painiketta, hänen korttiensa ja pääsyavaintensa tietoja ei näytetä, ennen kuin hän suorittaa todennuksen laitteelle. Ennen kuin korttikohtaisia tietoja, kuten hotellivarauksen tiedot, näytetään Applen Lompakossa, vaaditaan todennus joko Face ID:llä, Touch ID:llä tai pääsykoodilla.

Pääsytunnistetietojen tyypit

Applen Lompakossa toimivat erilaiset pääsykortit majoitusliikkeiden korteista yritysten kulkukortteihin, opiskelijakortteihin, kotiavaimiin ja auton avaimiin.

Majoitusliikkeet

Hotellihuoneiden avaimet Applen Lompakossa auttavat toteuttamaan helpon ja kontaktittoman kokemuksen sisäänkirjautumisesta uloskirjautumiseen saakka, ja samalla ne tarjoavat vieraille yksityisyyteen ja turvallisuuteen liittyviä lisäetuja verrattuna hotellien perinteisiin muovisiin avainkortteihin. Tuetuissa paikoissa hotellivieraat voivat avata oven napauttamalla, kun heillä on hotelliavaimet Applen Lompakossa yhteensopivassa iPhonessa tai Apple Watch Series 4:ssä tai uudemmassa.

Applen Lompakon ominaisuudet on nimenomaisesti suunniteltu parantamaan asiakaskokemuksen sujuvuutta:

- Kortin tietojen tuominen hotellin apista ennen saapumista mahdollistaa kortin lisäämisen Applen Lompakkoon ennen vierailua
- Sisäänkirjautumiskorttiruudut sisäänkirjautumisen ja huoneiden antamisen aloittamiseen Applen Lompakosta
- Avainten päivitykset tietojen tuomisen jälkeen meneillään olevan majoituksen jatkamista tai muokkaamista varten
- Tuki usean huoneen avaimelle yhdellä kortilla Applen Lompakossa
- Vanhentuneiden avainten automaattinen arkistointi Applen Lompakossa

Yritysten kulkukortit

Tuettujen kumppaneiden työntekijöiden kulkukortteja voidaan lisätä Applen Lompakkoon iPhonessa ja Apple Watchissa. Tämä mahdollistaa työntekijöille ympäri maailmaa kontaktittoman kulun työpaikoilleen. Kulkukortin lisääminen edellyttää, että työntekijällä on käytössä moniosainen todennus sille tilille, jota hän käyttää kirjautuakseen sisään työnantajan tarjoamaan appiin.

Työntekijän kulkukortti hyödyntää Applen pääsykorttiominaisuuksia, ja käyttäjät voivat tehdä sillä seuraavia asioita:

- lisätä automaattisesti työntekijän kulkukortin pariksi asetettuun Apple Watchiinsa käyttäen tietojen tuomiseen push-toimintoa, joka ei edellytä kumppanin apin asentamista
- kulkea sujuvasti toimiston tiloihin pikatilaa hyödyntäen
- päästä työpaikalle silloinkin, kun iPhonen akku on tyhjentynyt

Opiskelijakortit

iOS 12:ssa tai uudemmissa mukana olevien kampusten opiskelijat, opetushenkilöstö ja muu henkilökunta voivat lisätä opiskelijakorttinsa Applen Lompakkoon tuetuissa iPhone- ja Apple Watch -malleissa ja käyttää sitä kulkukorttina ja maksaakseen kaikkialla, missä kortti hyväksytään maksuvälineenä.

Käyttäjä lisää opiskelijakorttinsa Applen Lompakkoon kortin myöntäjän tai mukana olevan oppilaitoksen tarjoaman apin kautta. Tässä käytettävä tekninen prosessi on samanlainen kuin osiossa Luotto- tai pankkikorttien lisääminen kortin myöntäjän apista kuvattu prosessi. Lisäksi myöntävien appien on tuettava kaksiosaista todennusta tileille, jotka suojelevat pääsyä opiskelijakortteihin. Kortti voidaan ottaa samanaikaisesti käyttöön enimmillään kahdessa tuetussa Applen laitteessa, joihin on kirjauduttu samalla Apple ID:llä.

Useita asuinhuoneistoja sisältävät rakennukset

Tuettujen kumppaneiden rakennusten asukkaat ja työntekijät voivat käyttää kotiavaintaan Applen Lompakossa päästäkseen rakennukseen, omaan huoneistoonsa ja yhteistiloihin. Kotiavaimen tiedot voidaan tuoda kumppanin tarjoamasta apista. Kitkatonta tietojen tuomista tukevien kumppaneiden isännöitsijät voivat lähettää asukkaille linkin tietojen tuomisen aloittamista varten käyttäen haluamaansa viestintäkanavaa (esimerkiksi sähköposti tai tekstiviesti), jolloin asukkaan tarvitsee vain klikata linkkiä lunastaakseen avaimen. Lisäksi appiklipit tarjoavat suojatun ja saumattoman kokemuksen, joka mahdollistaa avaimen tietojen tuomisen ilman kumppanin apin asentamista. Jos haluat lisätietoja, katso Applen tukiartikkeli Appiklippien käyttäminen iPhonessa.

Kotiavain

Applen Lompakossa olevaa kotiavainta voidaan käyttää tuettuihin NFC-ominaisuudella varustettuihin ovien lukkoihin helposti iPhonella tai Apple Watchilla napauttamalla. Jos haluat lisätietoja siitä, miten käyttäjä voi ottaa käyttöön kotiavaimen ja käyttää sitä, katso Applen tukiartikkeli Oven avaaminen kotiavaimella iPhonella.

Kun käyttäjä ottaa kotiavaimen käyttöön, kaikki talouden asukkaat saavat myös automaattisesti kotiavaimen. Jos kodin omistaja haluaa jakaa kotiavaimen myös muille tai poistaa jäsenen jaetusta kodista, hän voi käyttää Koti-appia kutsujen ja jäsenten hallitsemiseen. Kun käyttäjä hyväksyy kutsun liittyä kotiin, jossa on käytössä kotiavain, se käynnistää kotiavaimen tietojen tuomisen Applen Lompakkoon hänen laitteissaan. Jos käyttäjä lähtee kodista tai jos kodin omistaja lopettaa käyttäjän pääsyn, nämä toiminnot poistavat samalla kotiavaimen Applen Lompakosta.

Auton avain

Auton avainten tallentamiselle digitaalisessa muodossa Applen Lompakkoon on natiivituki tuetuissa iPhone-laitteissa ja niiden pariksi asetetuissa Apple Watch -laitteissa. Auton avaimet ovat Applen Lompakossa kortteina (jotka Apple on luonut autovalmistajan puolesta), ja ne tukevat koko Apple Pay -kortin elinkaarta (johon sisältyvät iCloudin Kadonnut-tila, etätyhjennys, paikallinen kortin poisto sekä Poista kaikki sisältö ja asetukset -komento). Tavallisten Apple Pay -kortin hallintaominaisuuksien lisäksi jaetut auton avaimet voidaan poistaa omistajan iPhonesta, Apple Watchista ja auton käyttöliittymässä (HMI).

Auton avaimia voidaan käyttää auton avaamiseen ja lukitsemiseen sekä moottorin käynnistämiseen ja auton ajotilaan asettamiseen. ”Tavalliseen tapahtumaan” kuuluu molemminpuolinen todentaminen, ja se vaaditaan moottorin käynnistämistä varten. Avaamiseen ja lukitsemiseen voidaan käyttää ”pikatapahtumaa”, jos se on tarpeen suorituskykysyistä.

Avaimet voidaan luoda asettamalla iPhone pariksi sen käyttäjän omistamalle tuetulle autolle. Kaikki avaimet luodaan upotetussa Secure Elementissä perustuen elliptisen käyrän (NIST P-256) avaimen muodostamiseen laitteessa (ECC-OBKG), eivätkä yksityiset avaimet koskaan poistu Secure Elementistä. Laitteiden ja auton välisessä viestinnässä käytetään joko NFC:tä tai Bluetooth LE:n ja UWB:n yhdistelmää, ja avaimen hallinta käyttää Apple–autovalmistajan palvelin -rajapintaa molempien todentamalla TLS:llä. Kun avaimesta ja iPhonesta on tehty pari, myös kyseisen iPhonen pariksi asetettu Apple Watch voi saada avaimen. Kun avain on poistettu joko autossa tai laitteessa, sitä ei voi palauttaa. Kadonneissa tai varastetuissa laitteissa olevien avainten käyttö voidaan keskeyttää ja sitä voidaan jatkaa, mutta avainten tietojen tuominen uudelleen uuteen laitteeseen vaatii uuden parinmuodostuksen tai jakamisen.

Auton avaimen suojaus iOS:ssä

Kehittäjät voivat tukea auton avaamista turvallisesti ilman fyysistä avainta tuetulla iPhonella ja sen pariksi asetetulla Apple Watchilla.

Omistajan tekemä laiteparin muodostus

Omistajan on todistettava auton hallintaoikeutensa (menetelmä riippuu autovalmistajasta), ja hän voi aloittaa laiteparin muodostusprosessin autovalmistajan apissa käyttäen autovalmistajalta saatua sähköpostilinkkiä tai auton valikosta. Kaikissa tapauksissa omistajan on annettava luottamuksellinen kertakäyttöinen parinmuodostussalasana iPhonelle. Sitä käytetään suojatun parinmuodostuskanavan muodostamiseen käyttäen SPAKE2+-protokollaa ja NIST P-256 -käyrää. Appia tai sähköpostilinkkiä käytettäessä salasana siirretään automaattisesti iPhoneen. Kun parinmuodostus aloitetaan autosta, salasana on syötettävä iPhoneen käsin.

Avaimen jakaminen

Auton pariksi asetettu omistajan iPhone voi jakaa avaimia ehdot täyttäville perheenjäsenten ja ystävien iPhone-laitteille (ja niiden pariksi asetetuille Apple Watch -laitteille) lähettämällä laitekohtaisen kutsun käyttäen iMessagea ja Applen IDS-palvelua. Kaikki jakamiskomennot vaihdetaan käyttäen päästä päähän salattua IDS-ominaisuutta. Auton pariksi asetettu omistajan iPhone estää IDS-kanavan vaihtumisen jakamisprosessin aikana. Tämän tarkoitus on suojata kutsun välittämiseltä eteenpäin.

Kun kutsu on hyväksytty, perheenjäsenen tai ystävän iPhone luo digitaalisen avaimen ja lähettää avaimen luomisen varmenneketjun takaisin auton pariksi asetettuun omistajan iPhoneen sen varmistamiseksi, että avain on muodostettu aidolla Apple-laitteella. Auton pariksi asetettu omistajan iPhone allekirjoittaa toisen perheenjäsenen tai ystävän iPhonessa olevan julkisen ECC-avaimen ja lähettää allekirjoituksen takaisin perheenjäsenen tai ystävän iPhoneen. Allekirjoitusoperaatio omistajan laitteessa vaatii käyttäjän todentamisen (Face ID, Touch ID tai pääsykoodin syöttäminen) ja turvallisen käyttäjän aikeen vahvistuksen, joka on kuvattu osiossa Face ID:n ja Touch ID:n käyttötarkoitukset. Valtuutus pyydetään kutsun lähettämisen yhteydessä, ja se tallennetaan Secure Elementiin käytettäväksi sitten kun ystävän laite lähettää allekirjoituspyynnön takaisin. Avaimen oikeudet annetaan autolle joko verkossa auton alkuperäisen laitevalmistajan (OEM) palvelimen toimesta tai kun jaettua avainta käytetään ensimmäisen kerran autossa.

Avaimen poistaminen

Avaimet voidaan poistaa avaimenhaltijan laitteessa, omistajan laitteella ja autossa. Poisto avaimenhaltijan iPhonessa on voimassa välittömästi, vaikka avaimenhaltija käyttäisi parhaillaan avainta. Siksi ennen poistamista näytetään selkeä varoitus. Avainten poistaminen autossa voi olla mahdollista milloin tahansa, tai se voi olla mahdollista vain, kun auto on verkkoyhteydessä.

Poisto sekä avaimenhaltijan laitteessa että autossa ilmoitetaan autovalmistajan puolelle avainluettelopalvelimelle (KIS), johon myönnetyt avaimet kirjataan vakuutusta varten.

Omistaja voi pyytää poistoa omistajan kortin taustapuolelta. Pyyntö lähetetään ensin autovalmistajalle, jotta avain poistetaan autossa. Autovalmistaja määrittää ehdot avaimen poistamiselle autosta. Vasta kun avain on poistettu autossa, autovalmistajan palvelin lähettää etäkuoletuspyynnön avaimenhaltijan laitteelle.

Kun avain on kuoletettu laitteessa, digitaalisia auton avaimia hallitseva sovelma luo kryptografisesti allekirjoitetun vahvistuksen kuolettamisesta. Autovalmistaja käyttää sitä todisteena poistosta, ja sitä käytetään avaimen poistamiseen KIS-palvelimelta.

Tavalliset NFC-tapahtumat

NFC-avainta käyttävissä autoissa suojatun kanavan muodostaminen lukijan ja iPhonen välillä aloitetaan muodostamalla lyhytaikaiset avainparit sekä lukijan että iPhonen puolella. Avaintensopimismenetelmää käyttäen molemmilla puolilla voidaan muodostaa jaettu salaisuus ja käyttää sitä jaetun symmetrisen avaimen muodostamiseen käyttäen Diffie-Hellman-menetelmää, avaimenmuodostamisfunktiota ja allekirjoituksia parinmuodostuksen aikana asetetusta pitkäaikaisesta avaimesta.

Auton puolella muodostettu lyhytaikainen julkinen avain allekirjoitetaan lukijan pitkäaikaisella yksityisellä avaimella, minkä tuloksena iPhone todentaa lukijan. iPhonen kannalta tämä protokolla on suunniteltu estämään arkaluontoisten yksityisten tietojen paljastumista tiedonsiirtoa salakuuntelevalle vastapuolelle.

Lopuksi iPhone käyttää muodostettua suojattua kanavaa salatakseen julkisen avaimen tunnisteensa sekä allekirjoituksen, joka on laskettu lukijan tiedoista muodostetusta haasteesta ja lisäksi käytettävistä appikohtaisista tiedoista. Tämä lukijan suorittama iPhonen allekirjoituksen tarkistus mahdollistaa laitteen todentamisen lukijalle.

Pikatapahtumat

iPhone muodostaa kryptogrammin aikaisemmin tavallisessa tapahtumassa jaetun salaisuuden pohjalta. Tällä kryptogrammilla auto voi todentaa laitteen nopeasti tilanteissa, joissa keskeistä on tehokkuus. Valinnaisesti voidaan muodostaa suojattu kanava auton ja laitteen välillä muodostamalla istuntoavaimet aikaisemmin tavallisessa tapahtumassa jaetusta salaisuudesta ja uudesta lyhytaikaisesta avainparista. Se, että auto pystyy muodostamaan suojatun kanavan, toimii auton todennuksena iPhonelle.

Tavalliset BLE/UWB-tapahtumat

UWB-avainta käyttävissä autoissa muodostetaan Bluetooth LE -istunto auton ja iPhonen välille. Samoin kuin NFC-tapahtumassa, molemmilla puolilla muodostetaan jaettu salaisuus, jota käytetään suojatun istunnon muodostamiseen. Tätä istuntoa käytetään sen jälkeen UWB-etäisyysmittauksen salaisen avaimen (UWB Ranging Secret Key, URSK) muodostamiseen ja siitä sopimiseen. URSK annetaan UWB-radioille käyttäjän laitteessa ja autossa, jotta käyttäjän laite voidaan paikallistaa tarkasti tiettyyn sijaintiin auton lähellä tai sen sisällä. Sitten auto käyttää laitteen sijaintia sen ratkaisemiseen, sallitaanko lukituksen avaus tai auton käynnistäminen. URSK-avaimilla on ennalta määritetty elinaika (TTL). Jotta etäisyysmittaus ei keskeytyisi, kun TTL-aika umpeutuu, URSK-avaimia voidaan muodostaa ennakkoon laitteen SE:ssä ja auton HSM-moduulissa/SE:ssä, kun suojattu etäisyysmittaus ei ole aktiivinen mutta BLE on yhdistetty. Tällä vältetään tarve tavalliselle tapahtumalle uuden URSK-avaimen muodostamiseksi tilanteessa, jossa aika on kriittinen tekijä. Ennakkoon muodostettu URSK voidaan siirtää hyvin nopeasti auton ja laitteen UWB-radioihin, jotta UWB-etäisyysmittaus ei keskeydy.

Tietosuoja

Autovalmistajan avainluettelopalvelin (KIS) ei tallenna laitteen tunnusta, SEID:tä tai Apple ID:tä. Se tallentaa ainoastaan varmenteen myöntäjän tunnisteen ilmentymälle, joka on muuttuva tunniste. Tämä tunniste ei ole sidoksissa mihinkään yksityisiin tietoihin laitteella tai palvelimen toimesta, ja se poistetaan, kun käyttäjä tyhjentää laitteensa kokonaan (käyttäen komentoa Poista kaikki sisältö ja asetukset).

Matka- ja eMoney-korttien lisääminen Applen Lompakkoon

Monissa paikoissa ympäri maailmaa käyttäjät voivat lisätä tuettuja matka- ja eMoney-kortteja Applen Lompakkoon tuetuissa iPhone- ja Apple Watch -malleissa. Toiminnanharjoittajasta riippuen tämä voidaan tehdä joko siirtämällä fyysinen matkakortti tai sillä oleva arvo (tai molemmat) digitaaliseksi Applen Lompakkoon tai tuomalla uuden matka- tai eMoney-kortin tiedot joko Applen Lompakon tai kortin myöntäjän apin kautta. Kun matkakortit on lisätty Applen Lompakkoon, käyttäjät voivat käyttää joukkoliikennettä yksinkertaisesti pitämällä iPhonea tai Apple Watchia lähellä matkakortinlukijaa. Joillakin matkakorteilla voi myös suorittaa maksuja.

Miten matka- ja eMoney-kortit toimivat

Lisätyt matka- ja eMoney-kortit liitetään käyttäjän iCloud-tiliin. Jos käyttäjä lisää enemmän kuin yhden kortin Applen Lompakkoon, Apple tai kortin myöntäjä voi ehkä liittää käyttäjän henkilötiedot ja korttiin yhdistetyn tilin tiedot korttien välillä. Matka- ja eMoney-kortteja ja tapahtumia suojaa sarja hierarkkisia salausavaimia.

Kun saldo siirretään fyysiseltä kortilta Applen Lompakkoon, käyttäjän on annettava korttikohtaiset tiedot. Käyttäjän on myös mahdollisesti annettava henkilötietoja todisteeksi kortin haltijuudesta. Kun kortteja siirretään iPhonesta Apple Watchiin, molempien laitteiden on oltava verkossa.

Saldoa voidaan lisätä luotto-, pankki- tai prepaid-korteilta Applen Lompakon kautta tai matka- tai eMoney-kortin myöntäjän apista. Jos haluat tietoa lisäsaldon lataamisen suojauksesta käytettäessä Apple Payta, katso Maksaminen korteilla apeissa. Jos haluat ohjeita kortin tietojen tuomiseen kortin myöntäjän apissa, katso Luotto- tai pankkikorttien lisääminen kortin myöntäjän apista.

Jos tietojen tuomista fyysiseltä kortilta tuetaan, matka- tai eMoney-kortin myöntäjällä on tarvittavat salausavaimet fyysisen kortin todentamiseen ja käyttäjän syöttämien tietojen vahvistamiseen. Tietojen vahvistamisen jälkeen järjestelmä voi luoda laitteen tilinumeron Secure Elementiä varten ja aktivoida juuri lisätyn kortin Applen Lompakossa siten, että siirretty saldo on kortilla. Joissakin tapauksissa fyysinen kortti lakkaa toimimasta, kun sen tiedot on tuotu.

Kun tietojen tuominen kummalla tahansa tavalla on valmis, jos kortin saldo tallennetaan laitteeseen, se salataan ja tallennetaan sitä varten olevaan sovelmaan Secure Elementissä. Toiminnanharjoittajalla on kortin datan salaustoimintoihin tarvittavat avaimet saldotapahtumia varten.

Oletuksena matkakorttien käyttäjät saavat saumattoman pikamatkakokemuksen, jolloin matka voidaan maksaa ilman Face ID:tä, Touch ID:tä tai pääsykoodia. Kun pikatila on käytössä, sellaiset tiedot kuten äskettäiset asemat, tapahtumahistoria ja lisäliput ovat kaikkien lähietäisyydellä olevien lähilukulaitteiden saatavilla. Käyttäjät voivat laittaa päälle Face ID-, Touch ID- tai pääsykoodivaltuutuksen vaatimisen Lompakko ja Apple Pay -asetuksissa poistamalla Pikamatka-asetuksen käytöstä. Pikatilaa ei tueta eMoney-korteille.

Muiden Apple Pay -korttien tavoin eMoney-korttien käyttö voidaan keskeyttää tai ne voidaan poistaa

- etätyhjentämällä laite Missä on…? -palvelulla
- ottamalla käyttöön Kadonnut-tilan Missä on…? -apilla
- antamalla mobiililaitteiden hallinnan (MDM) etätyhjennyskomento
- poistamalla kaikki kortit niiden Apple ID -tilisivulta
- poistamalla kaikki kortit iCloud.comista
- poistamalla kaikki kortit Applen Lompakosta
- poistamalla kortti kortin myöntäjän apissa

Apple Pay -palvelimet ilmoittavat korttitoiminnan harjoittajalle, että korttien käyttö pitää keskeyttää tai että ne pitää poistaa käytöstä. Jos käyttäjä poistaa matka- tai eMoney-kortin verkossa olevasta laitteesta, saldon saa palautettua lisäämällä sen takaisin laitteeseen, joka on kirjattu sisään samalla Apple ID:llä. Jos laitteella ei ole verkkoyhteyttä, se ei ole päällä tai sitä ei pysty käyttämään, palauttaminen ei ehkä ole mahdollista.

Matka- ja eMoney-korttien lisääminen perheenjäsenen Apple Watchiin

iOS 15:ssä ja watchOS 8:ssa iCloud-perheen järjestäjä voi lisätä matka- ja eMoney-kortteja perheenjäsenten Apple Watch -laitteisiin iPhonensa Watch-apin kautta. Kun tällaisen kortin tiedot tuodaan perheenjäsenen Apple Watchiin, sen täytyy olla lähellä ja yhdistetty järjestäjän iPhoneen Wi-Fillä tai Bluetoothilla. Perheenjäsenillä täytyy olla kaksiosainen todennus käytössä Apple ID:lleen, jotta tämä onnistuu.

Perheenjäsenet voivat lähettää pyynnön lisätä rahaa matka- tai eMoney-kortille Apple Watchistaan käyttäen iMessagea. Viestin sisältö on suojattu päästä päähän -salauksella, joka on kuvattu osiossa iMessagen suojauksen yleiskatsaus. Rahaa voidaan lisätä perheenjäsenen Apple Watchissa olevalle kortille etänä Wi-Fi- tai mobiilidatayhteyttä käyttäen. Laitteiden ei tarvitse olla lähellä toisiaan.

Huomaa: Tämä ominaisuus ei välttämättä ole käytettävissä kaikissa maissa tai kaikilla alueilla.

Luotto- ja pankkikortit

Joissakin kaupungeissa julkisen liikenteen matkoja voi maksaa matkakortinlukijoissa EMV-sirukorteilla. Kun käyttäjä esittää tällaiselle lukijalle EMV-luotto-/pankkikortin, käyttäjän todentamista vaaditaan samalla tavoin kuin maksettaessa luotto- ja pankkikorteilla myymälöissä.

iOS 12.3:ssa tai uudemmissa jotkin Applen Lompakossa jo olevat EMV-luotto-/pankkikortit voidaan ottaa käyttöön pikamatkakortteina. Pikamatkaominaisuutta käytettäessä käyttäjät voivat maksaa tuettujen joukkoliikenteen järjestäjien matkoja ilman, että siihen vaaditaan Face ID:tä, Touch ID:tä tai pääsykoodia. Kun käyttäjä tuo EMV-luotto-/pankkikortin tiedot, ensimmäinen kortti, jonka tiedot on tuotu Applen Lompakkoon, otetaan pikamatkakäyttöön. Käyttäjä voi napauttaa kortin edessä Applen Lompakossa Lisää-painiketta ja ottaa pikamatkan pois käytöstä kyseiseltä kortilta valitsemalla Pikamatka-asetukseksi Ei mitään. Käyttäjä voi myös valita toisen luotto- tai pankkikortin pikamatkakortikseen Applen Lompakossa. Pikamatkakorttikäytön salliminen uudelleen tai toisen kortin valitseminen pikamatkakortiksi vaatii Face ID:tä, Touch ID:tä tai pääsykoodia.

Apple Cardia ja Apple Cashia voi käyttää pikamatkaan.

Henkilökortit Applen Lompakossa

iPhone 8:ssa tai uudemmissa, joissa on iOS 15.4 tai uudempi, ja Apple Watch Series 4:ssä tai uudemmissa, joissa on watchOS 8.4 tai uudempi, käyttäjät voivat lisätä virallisen henkilökorttinsa tai ajokorttinsa Applen Lompakkoon ja esittää sen mukana olevissa paikoissa sujuvasti ja suojatusti napauttamalla iPhoneaan tai Apple Watchiaan.

Huomaa: Tämä ominaisuus on saatavilla ainoastaan mukana olevissa Yhdysvaltain osavaltioissa.

Applen Lompakossa olevat henkilökortit käyttävät käyttäjän laitteen laitteistoon ja ohjelmistoon sisältyviä suojausominaisuuksia apuna hänen henkilöllisyytensä ja henkilötietojensa suojaamisessa.

Ajokortin tai virallisen henkilökortin lisääminen Applen Lompakkoon

iPhonessa käyttäjä voi aloittaa ajokortin tai henkilökortin lisäämisen yksinkertaisesti napauttamalla Applen Lompakossa näytön yläosassa lisäyspainiketta (+). Jos käyttäjillä on tämän käyttöönoton aikaan pariksi asetettu Apple Watch, he saavat kehotuksen lisätä ajokortti tai henkilökortti myös Applen Lompakkoon Apple Watchissa.

Ensin käyttäjiä kehotetaan skannaamaan iPhonella fyysisen ajokortin tai henkilökortin etu- ja taustapuoli. iPhone arvioi kuvien laadun ja tyypin auttaakseen varmistamaan, että osavaltion myöntäjäviranomainen voi hyväksyä ne. Henkilökortin kuvat salataan laitteessa osavaltion myöntäjäviranomaisen avaimelle ja lähetetään sitten osavaltion myöntäjäviranomaiselle.

Seuraavaksi käyttäjää pyydetään suorittamaan sarja kasvojen ja pään liikkeitä. Käyttäjän laite ja Apple arvioivat nämä liikkeet auttaakseen pienentämään riskiä, että joku käyttäisi valokuvaa, videota tai naamiota yrittääkseen lisätä jonkun toisen henkilökortin Applen Lompakkoon. Näiden liikkeiden analyysin tulokset lähetetään sitten osavaltion myöntäjäviranomaiselle, mutta videota itse liikkeistä ei lähetetä.

Käyttäjiä pyydetään ottamaan selfie-kuva avuksi sen varmistamisessa, että henkilökortin Applen Lompakkoon lisäävä henkilö on sama kuin henkilökortin haltija. Ennen kuin käyttäjän kuva lähetetään osavaltion myöntäjäviranomaiselle, Applen palvelimet ja käyttäjän laite vertaavat kuvan yhdennäköisyyttä henkilöön, joka suoritti kasvojen ja pään liikkeet auttaakseen varmistamaan, että lähetetty kuva on todellisesta henkilöstä, joka on yhdennäköinen henkilökortin henkilön kanssa. Kun vertailu on tehty, kuva salataan laitteessa ja lähetetään osavaltion myöntäjäviranomaiselle verrattavaksi heidän kuvaansa, joka on arkistoitu heidän henkilökorttiaan varten.

Lopuksi käyttäjiä pyydetään suorittamaan todennus Face ID:llä tai Touch ID:llä. Käyttäjän laite sitoo tämän yhden täsmäävän Face ID:n tai Touch ID:n biometrisen tiedon viralliseen henkilökorttiin auttaakseen varmistamaan, että vain henkilö, joka lisäsi henkilökortin kyseiseen iPhoneen, voi esittää sen. Henkilökortin esittämistä ei voida valtuuttaa muilla laitteeseen rekisteröidyillä biometrisillä tiedoilla. Tämä tapahtuu tiukasti laitteessa eikä näitä tietoja lähetetä osavaltion myöntäjäviranomaiselle.

Osavaltion myöntäjäviranomainen saa tarvitsemansa tiedot digitaalisen henkilökortin käyttöönottoa varten. Niihin sisältyvät kuvat käyttäjän henkilökortin etu- ja taustapuolesta, PDF417-viivakoodista luetut tiedot sekä selfie-kuva, jonka käyttäjä otti osana henkilökortin tarkistusprosessia. Myöntäjäosavaltio saa myös yksinumeroisen arvon, jota käytetään apuna petosten ehkäisemisessä. Se perustuu käyttäjän laitteen käyttökaavoihin, asetustietoihin ja tietoihin hänen henkilökohtaisesta Apple ID:stään. Tämän kaiken jälkeen myöntäjäosavaltio päättää viime kädessä, hyväksytäänkö vai kielletäänkö henkilökortin lisääminen Applen Lompakkoon.

Kun osavaltion myöntäjäviranomainen valtuuttaa virallisen henkilökortin tai ajokortin lisäämisen Applen Lompakkoon, iPhone muodostaa Secure Elementissä avainparin, joka kiinnittää käyttäjän henkilökortin tiettyyn laitteeseen. Apple Watchiin lisättäessä Apple Watch muodostaa avainparin Secure Elementissä.

Kun henkilökortti on iPhonessa, käyttäjän henkilökortissa Applen Lompakossa olevat tiedot tallennetaan salatussa muodossa Secure Enclaven suojaamina.

Applen Lompakossa olevan ajokortin tai virallisen henkilökortin käyttäminen

Käyttääkseen Applen Lompakossa olevaa henkilökorttiaan käyttäjien on suoritettava todennus Face ID:llä tai Touch ID:llä, jonka laite yhdisti henkilökorttiin Applen Lompakossa, ennen kuin iPhone esittää tiedot henkilöllisyystodistuksen lukulaitteelle.

Käyttääkseen henkilökorttiaan Applen Lompakossa Apple Watchissa käyttäjän on avattava iPhonensa lukitus käyttäen korttiin yhdistettyä Face ID -otosta tai Touch ID -sormenjälkeä joka kerta, kun hän laittaa Apple Watchin ranteeseensa. Sen jälkeen hän voi käyttää henkilökorttiaan Applen Lompakossa ilman todennusta siihen saakka, kunnes ottaa taas Apple Watchin pois ranteestaan. Tämä ominaisuus hyödyntää perusominaisuuksiin kuuluvaa automaattista lukituksen avausta, josta kerrotaan tarkemmin osiossa watchOS-järjestelmän suojaus.

Kun käyttäjät pitävät iPhonea tai Apple Watchia lähellä henkilöllisyystodistuksen lukulaitetta, laitteessa näkyy käyttäjälle kehotus, jossa kerrotaan, mitä tietoja tarkalleen pyydetään, kuka niitä pyytää ja onko ne tarkoitus tallentaa. Kun valtuutus on annettu korttiin yhdistetyllä Face ID:llä tai Touch ID:llä, pyydetyt henkilöllisyystiedot päästetään laitteesta.

Tärkeää: Käyttäjien ei tarvitse avata lukitusta, näyttää laitetta tai luovuttaa sitä henkilökortin esittämiseksi.

Jos käyttäjillä on käyttöapuominaisuus kuten Ääniohjaus, Kytkinohjaus tai AssistiveTouch Face ID:n tai Touch ID:n käytön sijaan, he voivat päästä tietoihinsa ja esittää ne käyttäen pääsykoodia.

Henkilöllisyystietojen lähettäminen henkilöllisyystodistuksen lukulaitteelle noudattaa standardia ISO/IEC 18013-5. Siihen kuuluu useita suojausmekanismeja, joilla voidaan havaita, estää ja pienentää turvallisuusriskejä. Niitä ovat henkilöllisyystietojen eheys ja väärennösten torjuminen, sitominen laitteeseen, tietoinen suostumus ja käyttäjätietojen luottamuksellisuus radiolinkkisiirroissa.

Henkilötietojen eheys ja väärennösten torjuminen

Applen Lompakossa olevat henkilökortit käyttävät myöntäjältä saatua allekirjoitusta, joka mahdollistaa ISO/IEC 18013-5:n mukaiselle lukulaitteelle käyttäjän Applen Lompakossa olevan henkilökortin tarkistamisen. Lisäksi kaikki henkilökortin dataelementit Lompakossa on suojattu yksitellen väärentämiseltä. Tämän ansiosta henkilöllisyystodistuksen lukulaite voi pyytää tiettyä dataelementtien alijoukkoa, joka on henkilökortissa Applen Lompakossa, ja henkilökortti Applen Lompakossa voi vastata samalla alijoukolla ja siis jakaa ainoastaan pyydetyt tiedot. Tämä maksimoi käyttäjän tietosuojan.

Sitominen laitteeseen

Applen Lompakossa olevien henkilökorttien todennus käyttää laitteen allekirjoitusta suojaamaan henkilökortin kloonaamiselta ja henkilöllisyystietotapahtuman uudelleentoistolta. Tallentamalla henkilökortin todennuksen yksityisen avaimen iPhonen Secure Elementiin henkilökortti sidotaan siihen samaan laitteeseen, jolle osavaltion myöntäjäviranomainen loi henkilökortin.

Tietoinen suostumus

Applen Lompakossa olevien henkilökorttien lukulaitteen todennus todentaa henkilöllisyystodistuksen lukulaitteen käyttäen ISO/IEC 18013-5 -standardissa määriteltyä protokollaa. Tietojen esittämisen yhteydessä näytetään lukulaitteen varmenteesta saatu kuvake, joka vakuuttaa käyttäjälle, että hän on tekemisissä aiotun tahon kanssa.

Käyttäjän tietojen luottamuksellisuus radiolinkkisiirroissa

Istunnon salaus auttaa varmistamaan, että kaikki henkilöllisyyden määrittämistä koskevien tietojen siirto Applen Lompakossa olevan henkilökortin ja henkilöllisyystodistuksen lukulaitteen välillä on salattua. Salauksen suorittaa sovelluskerros. Näin ollen istunnon salauksen suojaus ei ole riippuvainen kuljetuskerroksesta (esimerkiksi NFC, Bluetooth ja Wi-Fi).

Applen Lompakossa olevat henkilökortit auttavat pitämään käyttäjän tiedot yksityisinä

Henkilökortit Applen Lompakossa ovat ISO/IEC 18013-5 -standardissa määritellyn laitteesta hakemisen prosessin (”device retrieval”) mukaisia. Laitteesta hakeminen poistaa tarpeen tehdä palvelinkutsuja kortin esittämisen aikana ja suojaa näin käyttäjiä Applen tai kortin myöntäjän seurannalta.

iMessage

iMessagen suojauksen yleiskatsaus

Applen iMessage on viestipalvelu iOS- ja iPadOS-laitteille, Apple Watchille ja Mac-tietokoneille. iMessage tukee tekstiä ja liitteitä kuten kuvia, yhteystietoja, sijainteja, linkkejä ja suoraan viestiin lisättäviä liitteitä kuten peukutuskuvaketta. Viestit näkyvät kaikissa käyttäjän rekisteröidyissä laitteissa, joten käyttäjä voi jatkaa keskustelua millä tahansa laitteellaan. iMessage käyttää laajasti Applen push-ilmoituspalvelua (APNs). Apple ei kirjaa lokia viestien tai liitteiden sisällöstä. Ne on suojattu päästä-päähän-salauksella, joten ainoastaan lähettäjä ja vastaanottaja pääsevät niihin. Apple ei voi purkaa näiden tietojen salausta.

Kun käyttäjä laittaa iMessagen päälle laitteessa, laite luo salaus- ja allekirjoitusavainparit palvelun kanssa käytettäviksi. Salaukseen on 1280-bittinen RSA-salausavain sekä 256-bittinen elliptisen käyrän salausavain NIST P-256 -käyrällä. Allekirjoituksille käytetään 256-bittisiä elliptisten käyrien allekirjoitusalgoritmin (ECDSA) allekirjoitusavaimia. Yksityiset avaimet tallennetaan laitteen avainnippuun ja ne ovat käytettävissä vain, kun lukitus on ensin avattu. Julkiset avaimet lähetetään Apple Identity Service (IDS) -palvelulle, missä ne liitetään käyttäjän puhelinnumeroon tai sähköpostiosoitteeseen yhdessä laitteen APNs-osoitteen kanssa.

Kun käyttäjät ottavat iMessagen käyttöön useammilla laitteilla, niiden julkiset salaus- ja allekirjoitusavaimet, APNs-osoitteet ja liitetyt puhelinnumerot lisätään hakemistopalveluun. Käyttäjät voivat myös lisätä useampia sähköpostiosoitteita, jotka vahvistetaan lähettämällä vahvistuslinkki. Puhelinnumerot vahvistetaan käyttäen operaattorin verkkoa ja SIM-korttia. Joissakin verkoissa tämä vaatii tekstiviestin käyttämistä (käyttäjälle näytetään vahvistusvalintaikkuna, jos tekstiviesti ei ole ilmainen). Puhelinnumeron vahvistamista voidaan vaatia iMessagen lisäksi useille järjestelmäpalveluille, kuten FaceTimelle ja iCloudille. Kaikissa käyttäjän rekisteröidyissä laitteissa näkyy varoitusviesti, kun uusi laite, puhelinnumero tai sähköpostiosoite lisätään.

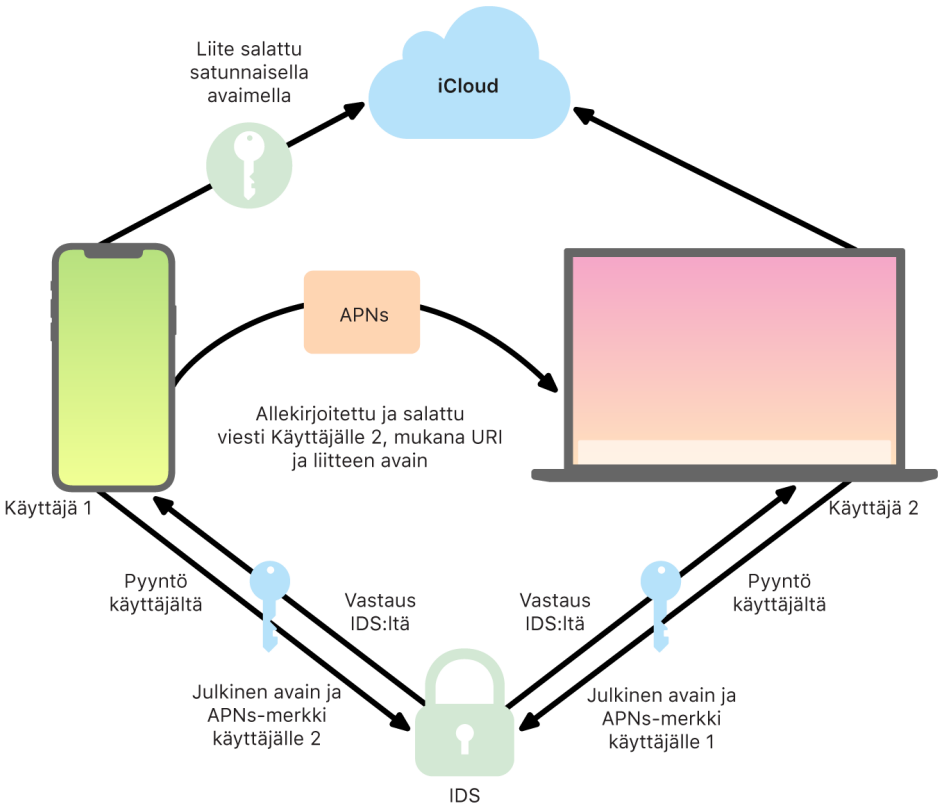
Miten iMessage lähettää ja vastaanottaa viestejä suojatusti

Käyttäjät aloittavat uuden iMessage-keskustelun syöttämällä osoitteen tai nimen. Jos he syöttävät puhelinnumeron tai sähköpostiosoitteen, laite ottaa yhteyttä Applen IDS-palveluun noutaakseen julkiset avaimet ja APNs-osoitteet kaikille vastaanottajaan liitetyille laitteille. Jos käyttäjä syöttää nimen, laite kerää ensin käyttäjän Yhteystiedot-apista nimeen liittyvät puhelinnumerot ja sähköpostiosoitteet ja hankkii sitten julkiset avaimet ja APNs-osoitteet IDS-palvelusta.

Käyttäjän lähtevä viesti salataan yksilöllisesti jokaiselle vastaanottajan laitteelle. Vastaanottavien laitteiden julkiset salausavaimet ja allekirjoitusavaimet noudetaan IDS-palvelusta. Lähettävä laite luo jokaiselle vastaanottavalle laitteelle satunnaisen 88-bittisen arvon ja käyttää sitä HMAC-SHA256-avaimena muodostaakseen 40-bittisen arvon lähettäjän ja vastaanottajan julkisesta avaimesta ja ilmitekstistä. Yhdistämällä 88-bittinen ja 40-bittinen arvo saadaan 128-bittinen avain, joka salaa viestin AES-salauksella laskuritilassa (CTR). Vastaanottajapuoli käyttää 40-bittistä arvoa salauksesta puretun ilmitekstin eheyden tarkistukseen. Tämä viestikohtainen AES-avain salataan käyttäen RSA-OAEP:tä vastaanottavan laitteen julkiseen avaimeen. Salatun viestitekstin ja salatun viestiavaimen yhdistelmä tiivistetään käyttäen SHA-1:tä, ja tiiviste allekirjoitetaan elliptisten käyrien allekirjoitusalgoritmilla (ECDSA) käyttäen lähettävän laitteen yksityistä allekirjoitusavainta. iOS 13:ssa tai uudemmissa ja iPadOS 13.1:ssä tai uudemmissa laitteet voivat käyttää ECIES-salausta (Elliptic Curve Integrated Encryption Scheme) RSA-salauksen sijaan.

Tuloksena oleva oma viesti jokaiselle vastaanottavalle laitteelle koostuu salatusta viestitekstistä, salatusta viestiavaimesta ja lähettäjän digitaalisesta allekirjoituksesta. Ne lähetetään APNs-palvelun toimitettaviksi. Metadataa, kuten aikaleimaa ja APNs:n reititystietoja, ei salata. Viestintä APNs-palvelun kanssa salataan käyttäen TLS-kanavaa, jossa paljastuneella avaimella ei voi purkaa aiemmin salattuja viestejä (forward secrecy).

APNs-palvelu voi välittää vain enintään 4 tai 16 Kt kokoisia viestejä riippuen iOS- tai iPadOS-versiosta. Jos viestin teksti on liian pitkä tai jos siihen sisältyy liite, kuten kuva, liite salataan käyttäen AES-salausta CTR-tilassa satunnaisesti generoidulla 256-bittisellä avaimella ja ladataan iCloudiin. Liitteen AES-avain, sen URI (Uniform Resource Identifier) ja sen salatun muodon SHA-1-tiiviste lähetetään sitten vastaanottajalle iMessage-viestin sisältönä, jossa niiden luottamuksellisuus ja eheys on suojattu iMessagen tavallisella salauksella seuraavan kaavion mukaisesti.



Ryhmäkeskusteluissa tämä prosessi toistetaan kullekin vastaanottajalle ja heidän laitteilleen.

Vastaanottajapuolella kukin laite vastaanottaa oman kopionsa viestistä APNs-palvelulta ja tarvittaessa noutaa liitteen iCloudista. Lähettäjän saapuvaa puhelinnumeroa tai sähköpostiosoitetta verrataan vastaanottajan yhteystietoihin, jotta nimi voidaan näyttää, jos se on mahdollista.

Kuten kaikki push-ilmoitukset, viesti poistetaan APNs-palvelusta, kun se on toimitettu. Kuitenkin toisin kuin muut APNs-ilmoitukset, iMessage-viestit laitetaan jonoon odottamaan toimittamista poissa linjoilta oleviin laitteisiin. Viestejä säilytetään Applen palvelimilla enimmillään 30 päivää.

Nimen ja kuvan suojattu jakaminen iMessagessa

iMessagen nimen ja kuvan jakamisominaisuus mahdollistaa käyttäjälle nimen ja kuvan jakamisen iMessagessa. Käyttäjä voi valita oman korttinsa tiedot tai muokata nimeä ja sisällyttää vapaasti valitsemansa kuvan. iMessagen nimen ja kuvan jakamisominaisuus käyttää kaksivaiheista järjestelmää nimen ja kuvan jakelemiseen.

Data jaetaan pienempiin kenttiin, joista jokainen salataan ja todennetaan erikseen sekä todennetaan yhdessä alla kuvatussa prosessissa. Kenttiä on kolme:

- Nimi
- Kuva
- Kuvan tiedostonimi

Yksi ensimmäisistä toimenpiteistä datan luomisessa on satunnaisen 128-bittisen tietueavaimen muodostaminen laitteessa. Tästä tietueavaimesta muodostetaan sitten HKDF-HMAC-SHA256:ta käyttäen kolme aliavainta: avain 1:avain 2:avain 3 = HKDF(tietueavain, ”lempinimet”). Kullekin kentälle luodaan satunnainen 96-bittinen alkuarvo (Initialization Vector, IV) ja data salataan käyttäen AES-CTR:ää ja avainta 1. Sen jälkeen lasketaan sanoman autentikointikoodi (MAC) HMAC-SHA256:lla käyttäen avainta 2. Se kattaa kentän nimen, kentän alkuarvon ja kentän salatekstin. Lopuksi yksittäisten MAC-arvojen sarja yhdistetään ja niiden MAC lasketaan HMAC-SHA256:lla käyttäen avainta 3. 256-bittinen MAC tallennetaan salattujen tietojen rinnalla. Tämän MAC-koodin ensimmäisiä 128 bittiä käytetään RecordID:nä.

Tämä salattu tietue tallennetaan sitten CloudKitin julkiseen tietokantaan RecordID:n alle. Tätä tietuetta ei koskaan muuteta, ja joka kerta kun käyttäjä päättää muuttaa nimi- ja kuvatietojaan, luodaan uusi salattu tietue. Kun käyttäjä 1 valitsee jakaa nimensä ja kuvansa käyttäjän 2 kanssa, hän lähettää tietueavaimen recordID:n kanssa iMessagen tietosisällössä, joka on salattu.

Kun käyttäjä 2:n laite vastaanottaa tämän iMessage-tietosisällön, se havaitsee, että tietosisältö sisältää lempinimen ja kuvan recordID:n ja avaimen. Käyttäjä 2:n laite noutaa salatun nimen ja kuvan recordID:n alta julkisesta CloudKit-tietokannasta ja lähettää ne iMessagella.

Kun viesti on noudettu, käyttäjän 2 laite purkaa tietosisällön salauksen ja vahvistaa allekirjoituksen käyttäen itse recordID:tä. Jos se hyväksytään, käyttäjälle 2 näytetään nimi ja kuva, ja hän voi valita lisätä ne yhteystietoihinsa tai käyttää niitä Viesteissä.

Suojatut Apple Messages for Business -viestit

Apple Messages for Business on viestipalvelu, jolla käyttäjät voivat kommunikoida yritysten kanssa Viestit-apilla. Apple Messages for Business -palvelua käytettäessä käyttäjä hallitsee aina keskustelua. Hän voi myös poistaa keskustelun ja estää yritystä lähettämästä itselleen viestejä jatkossa. Yksityisyyden turvaamiseksi yritys ei saa käyttäjän puhelinnumeroa, sähköpostiosoitetta tai iCloud-tilin tietoja. Niiden sijaan Applen identiteettipalvelu (Apple Identity Service, IDS) luo juuri tähän tarkoitukseen yksilöllisen tunnisteen, jota kutsutaan *läpinäkymättömäksi tunnukseksi*, ja se jaetaan yrityksen kanssa. Läpinäkymätön tunnus on käytössä ainoastaan käyttäjän Apple ID:n ja kyseisen yrityksen yritystunnuksen välisessä suhteessa. Käyttäjällä on erillinen läpinäkymätön tunnus jokaiselle yritykselle, johon hän on yhteydessä Apple Messages for Business -palvelua käyttäen. Käyttäjä päättää, jakaako hän yrityksen kanssa tietoja, joista hänet voi tunnistaa, ja missä vaiheessa hän tekee sen, eikä Apple Messages for Business -palvelu koskaan tallenna keskusteluhistoriaa.

Apple Messages for Business tukee Apple Business Managerissa luotuja hallittuja Apple ID:itä ja tarkistaa, ovatko iMessage ja FaceTime käytössä Apple School Managerissa luoduille hallituille Apple ID:ille.

Yrityksille lähetettävät viestit salataan, kun ne siirtyvät käyttäjän laitteen ja Applen viestipalvelinten välillä, ja ne käyttävät samaa suojausta ja samoja Applen viestipalvelimia kuin iMessage. Applen viestipalvelimet purkavat näiden viestien salauksen RAM-muistissa ja välittävät ne yritykselle TLS 1.2:ta käyttävän salatun linkin avulla. Viestejä ei koskaan tallenneta salaamattomassa muodossa matkalla Apple Messages for Business -palvelun läpi. Myös yritysten vastaukset lähetetään TLS 1.2:ta käyttäen Applen viestipalvelimille, missä ne salataan käyttäen kunkin vastaanottavan laitteen yksilöllisiä julkisia avaimia.

Jos käyttäjän laitteet ovat verkossa, viesti toimitetaan välittömästi, eikä sitä tallenneta välimuistiin Applen viestipalvelimille. Jos käyttäjän laite ei ole verkossa, salattu viesti tallennetaan välimuistiin enintään 30 päiväksi, jotta käyttäjä voi saada sen, kun laite on jälleen verkossa. Heti kun laite on taas verkossa, viesti toimitetaan ja poistetaan välimuistista. 30 päivän jälkeen toimittamaton välimuistissa oleva viesti vanhenee ja se poistetaan pysyvästi.

FaceTimen suojaus

FaceTime on Applen video- ja äänipuhelupalvelu. iMessagen tavoin FaceTime-puhelut käyttävät Applen push-ilmoituspalvelua (APNs) alkuyhteyden muodostamiseksi käyttäjän rekisteröityihin laitteisiin. FaceTime-puheluiden ääni-/videosisällöt on suojattu päästä-päähän-salauksella, joten ainoastaan lähettäjä ja vastaanottaja pääsevät niihin. Apple ei voi purkaa näiden tietojen salausta.

FaceTimen alkuyhteys muodostetaan käyttäen Applen palvelininfrastruktuuria, joka välittää datapaketteja käyttäjien rekisteröityjen laitteiden välillä. Käyttäen APNs-ilmoituksia ja STUN-viestejä (Session Traversal Utilities for NAT) välitetyn yhteyden yli laitteet tarkistavat identiteettivarmenteensa ja muodostavat jaetun salaisuuden kullekin istunnolle. Jaettua salaisuutta käytetään istuntoavainten muodostamiseen mediakanaville, jotka suoratoistetaan käyttäen SRTP-protokollaa (Secure Real-time Transport Protocol). SRTP-paketit salataan käyttäen AES256:ta laskuritilassa ja todennetaan HMAC-SHA1:llä. Alkuyhteyden ja suojauksen käyttöönoton jälkeen FaceTime käyttää STUN:ia ja ICE:tä (Internet Connectivity Establishment) vertaisyhteyden muodostamiseen laitteiden välillä, jos se on mahdollista.

Ryhmä-FaceTime laajentaa FaceTimen tukemaan jopa 33 samanaikaista osallistujaa. Tavallisten kahdenkeskisten FaceTime-puheluiden tavoin puhelut ovat päästä päähän salattuja kutsuttujen osallistujien laitteiden välillä. Vaikka ryhmä-FaceTime-puheluissa käytetyt infrastruktuuri ja suunnittelu ovat pitkälti samat kuin kahdenkeskisissä FaceTime-puheluissa, näissä ryhmäpuheluissa on avaimenmuodostusmekanismi, joka rakentuu Applen IDS-palvelun todentamisen päälle. Tämä protokolla turvaa, että käyttäjän laitteen vaarantuminen ei johda aikaisempien puheluiden sisällön vuotamiseen (forward secrecy). Istuntoavaimet salataan käyttäen AES-SIV:tä ja jaellaan käyttäjille käyttäen ECIES-rakennetta lyhytaikaisilla P-256 ECDH -avaimilla.

Kun uusi puhelinnumero tai sähköpostiosoite lisätään käynnissä olevaan ryhmä-FaceTime-puheluun, aktiiviset laitteet muodostavat uudet media-avaimet eivätkä koskaan jaa aiemmin käytettyjä avaimia uusille kutsutuille laitteille.

Missä on…?

Missä on…? -palvelun suojaus

Apple-laitteiden Missä on…? -appi on rakennettu edistyksellisen julkisen avaimen salauksen perustalle.

Yleiskatsaus

Missä on…? -appi yhdistää Etsi iPhoneni- ja Etsi ystäväni -toiminnot yhteen appiin iOS:ssä, iPadOS:ssä ja macOS:ssä. Missä on…? voi auttaa käyttäjiä löytämään kadonneen laitteen, jopa Macin, jolla ei ole verkkoyhteyttä. Verkkoyhteydessä oleva laite voi ilmoittaa sijaintinsa käyttäjälle iCloudin kautta. Missä on...? toimii ilman verkkoyhteyttä lähettämällä kadonneesta laitteesta lyhyen kantaman Bluetooth-signaaleita, jotka muut lähistöllä käytössä olevat Apple-laitteet voivat havaita. Nämä lähistöllä olevat laitteet voivat sitten välittää havaitun sijainnin iCloudiin, jotta käyttäjät voivat löytää sen Missä on…? -apilla. Kaikkien käyttäjien yksityisyys ja tietosuoja on koko prosessin ajan turvattuna. Missä on…? -apilla voidaan löytää jopa Mac, jolla ei ole verkkoyhteyttä ja joka on nukkumassa.

Bluetoothin ja satojen miljoonien ympäri maailmaa aktiivisessa käytössä olevien iOS-, iPadOS- ja macOS-laitteiden avulla käyttäjä voi paikantaa kadonneen laitteensa, vaikka se ei saisikaan yhteyttä Wi-Fi- tai mobiilidataverkkoon. Kaikki iOS-, iPadOS- tai macOS-laitteet, joiden Missä on…? -asetuksissa on sallittu yhteydettömien laitteiden etsiminen, voivat toimia löytäjälaitteena. Tämä tarkoittaa, että laite voi havaita toisen kadonneen ja yhteydettömän laitteen läheisyyden Bluetoothia käyttäen ja raportoida sitten omaa verkkoyhteyttään käyttäen likimääräisen sijainnin omistajalle. Kun yhteydettömien laitteiden etsiminen on käytössä laitteella, se myös tarkoittaa, että muut ominaisuuden käyttäjät voivat samalla tavoin paikantaa sen. Koko tämä vuorovaikutus on päästä päähän salattua, anonyymia ja suunniteltu käyttämään akkuvirtaa ja dataa säästeliäästi. Vaikutus akunkestoon ja mobiilidatan käyttöön on minimaalinen, ja käyttäjän tietosuoja on parempi.

Huomaa: Missä on…? ei välttämättä ole saatavilla kaikissa maissa tai kaikilla alueilla.

Päästä-päähän-salaus

Missä on…? -palvelu on rakennettu edistyksellisen julkisen avaimen salauksen perustalle. Kun yhteydettömien laitteiden löytäminen on käytössä Missä on…? -asetuksissa, suoraan laitteessa luodaan elliptisen käyrän yksityinen P-224-salausavainpari merkinnällä {d,P}, jossa *d* on yksityinen avain ja *P* on julkinen avain. Lisäksi 256-bittinen salainen SK_0 ja laskuri $_i$ nollataan. Tätä yksityistä avainparia ja salaisuutta ei koskaan lähetetä Applelle, ja ne synkronoidaan ainoastaan käyttäjän muiden laitteiden kanssa päästä päähän salattuina käyttäen iCloud-avainnippua. Salaisuutta ja laskuria käytetään nykyisen symmetrisen avaimen SK_i:n muodostamiseen seuraavalla rekursiivisella rakenteella: $SK_i = KDF(SK_{i-1}, \text{"päivitä"})$.

SK_i:n perusteella lasketaan kaksi suurta kokonaislukua, u_i ja v_i, kaavalla $(u_i,v_i) = KDF(SK_i, \text{"hajauta"})$. Sekä yksityinen P-224-avain, jonka merkintä on *d*, että vastaava julkinen avain, johon viitataan *P*:llä, muodostetaan käyttäen affiinista suhdetta, jossa kahdesta edellä mainitusta kokonaisluvusta lasketaan lyhytikäinen avainpari: muodostettu yksityinen avain on d_i, jossa $d_i = u_i * d + v_i$ (lukuun ottamatta P-224-käyrän järjestystä) ja vastaava julkinen osa on P_i ja varmistaa, että $P_i = u_i*P + v_i*G$.

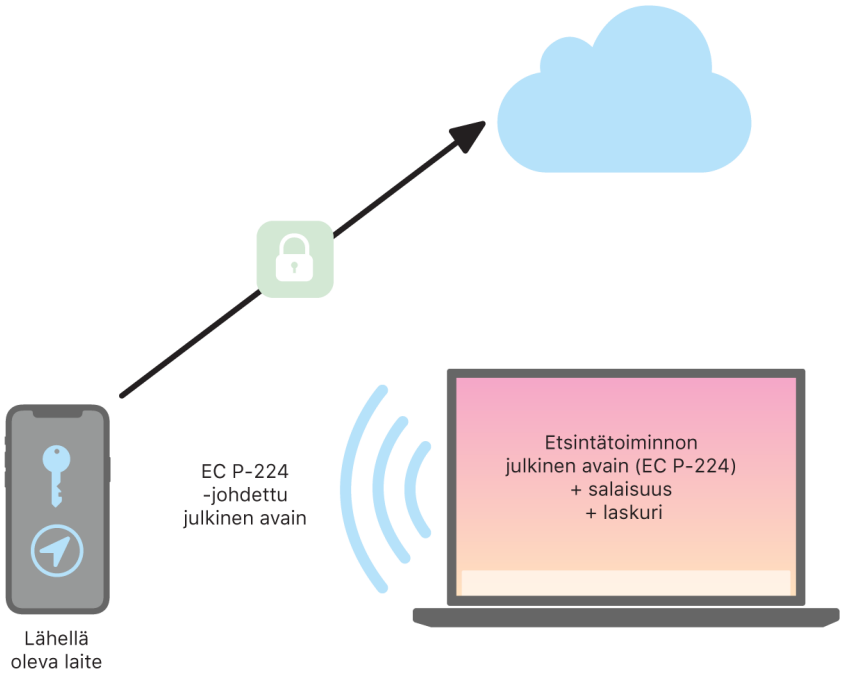
Kun laite katoaa eikä saa yhteyttä Wi-Fi- tai mobiilidataverkkoon – esimerkiksi jos MacBook Pro jää penkille puistoon – se alkaa ajoittain lähettää muodostettua julkista avainta P_i rajoitetun ajan Bluetooth-tietosisällössä. P-224:ää käyttäen julkisen avaimen esitys mahtuu yhteen Bluetooth-tietosisältöön. Ympäröivät laitteet voivat auttaa löytämään yhteydettömän laitteen salaamalla sijaintinsa julkiseen avaimeen. Noin 15 minuutin välein julkinen avain korvataan uudella, jossa käytetään laskurin kasvavaa arvoa ja yllä kuvattua prosessia, jotta käyttäjää ei voida seurata pysyvällä tunnisteella. Muodostamismekanismi on suunniteltu estämään yhdistämästä eri julkisia avaimia P_i samaan laitteeseen.

Käyttäjien ja laitteiden anonymiteetin säilyttäminen

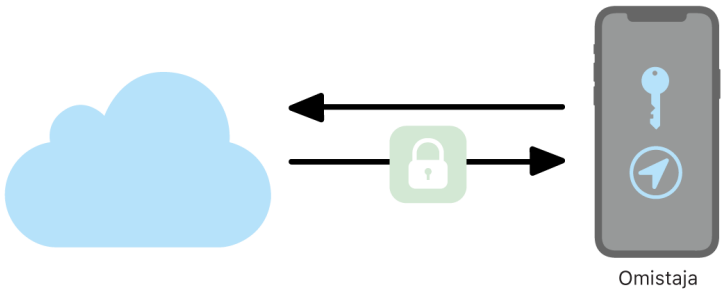
Sijaintitietojen ja muun datan täydellisen salaamisen lisäksi huolehditaan siitä, että käyttäjien henkilöllisyydet eivät tule toisten käyttäjien tai Applen tietoon. Löytäjälaitteiden Applelle lähettämä liikenne ei sisällä todentamistietoja sisällössä eikä otsakkeissa. Näin ollen Apple ei tiedä, kuka löytäjä on tai kenen laite on löydetty. Lisäksi Apple ei kirjaa lokiin tietoja, jotka paljastaisivat löytäjän henkilöllisyyden eikä säilytä tietoja, joista kukaan voisi yhdistää löytäjän ja omistajan. Laitteen omistaja saa ainoastaan salatun sijaintitiedon, jonka salaus puretaan ja joka näytetään Missä on…? -apissa ilman mitään tietoa siitä, kuka laitteen on löytänyt.

Missä on...? -apin käyttäminen kadonneiden Applen laitteiden paikantamiseen

Kaikki Bluetoothin kantaman sisällä olevat Applen laitteet, joissa yhteydettömien laitteiden löytäminen on käytössä, voivat havaita signaalin toisesta laitteesta, jossa on käytössä Missä on...? ja lukea sillä hetkellä lähetettävän avaimen P_i. Käyttäen ECIES-rakennetta ja julkista avainta P_i lähetyksestä, löytäjälaite salaa senhetkisen sijaintinsa tiedot ja välittää ne Applelle. Salattu sijainti liitetään palvelinindeksiin, joka lasketaan SHA256-tiivisteenä julkisesta P-224-avaimesta P_i, joka on saatu Bluetooth-tietosisällöstä. Applella ei ole koskaan avainta salauksen purkamiseen, joten Apple ei voi lukea löytäjän salaamaa sijaintia. Kadonneen laitteen omistaja voi rekonstruoida indeksin ja purkaa sijainnin salauksen.



Yritettäessä paikantaa kadonnutta laitetta laskurin arvojen odotettu alue arvioidaan sijainnin etsintäjaksosta. Kun tiedetään alkuperäinen yksityinen P-224-avain *d* ja salaiset arvot SK_i laskuriarvojen alueella etsintäjaksolla, omistaja voi rekonstruoida sarjan arvoja $\{d_i, SHA256(P_i)\}$ koko etsintäjaksolle. Omistajan laitteella, jota käytetään kadonneen laitteen paikantamiseen, voidaan suorittaa kyselyitä palvelimelle käyttäen indeksiarvojen $SHA256(P_i)$ sarjaa ja ladata salatut sijainnit palvelimelta. Sen jälkeen Missä on...? -appi purkaa paikallisesti sijaintien salauksen vastaavilla yksityisillä avaimilla d_i ja näyttää kadonneen laitteen likimääräisen sijainnin apissa. Omistajan appi yhdistää useiden etsijälaitteiden sijaintiraportit tarkentaakseen sijaintia.



Yhteydettömien laitteiden paikantaminen

Jos Etsi iPhoneni on otettu käyttöön käyttäjän laitteelle, yhteydettömien laitteiden etsiminen otetaan oletuksena käyttöön, kun laite päivitetään iOS 13:een tai uudempaan, iPadOS 13.1:een tai uudempaan tai macOS 10.15:een tai uudempaan. Tämä on suunniteltu varmistamaan jokaiselle käyttäjälle mahdollisimman hyvä todennäköisyys paikantaa laitteensa, jos se katoaa. Jos kuitenkaan käyttäjä ei halua osallistua, hän voi milloin tahansa ottaa yhteydettömien laitteiden etsimisen pois käytöstä laitteensa Missä on…? -asetuksissa. Kun yhteydettömien laitteiden etsiminen on pois käytöstä, laite ei enää toimi löytäjänä eivätkä muut laitteet enää voi havaita sitä. Käyttäjä voi kuitenkin edelleen paikantaa laitteen edellyttäen, että se saa yhteyden Wi-Fi- tai mobiilidataverkkoon.

Kun kadonnut yhteydetön laite paikannetaan, käyttäjä saa ilmoituksen ja sähköpostiviestin, joissa kerrotaan, että laite on löytynyt. Löytäjä voi näyttää kadonneen laitteen sijainnin avaamalla Missä on…? -apin ja valitsemalla Laitteet-välilehden. Sen sijaan, että laite näkyisi tyhjällä kartalla kuten ennen sen paikantamista, Missä on…? -appi näyttää nyt karttasijainnin ja likimääräisen osoitteen sekä tiedon siitä, kuinka paljon aikaa on kulunut laitteen havaitsemisesta. Jos sijaintiraportteja saapuu lisää, sekä nykyinen sijainti että aikaleima päivittyvät automaattisesti. Vaikka käyttäjät eivät voi toistaa ääntä yhteydettömässä laitteessa tai etätyhjentää sitä, he voivat käyttää sijaintitietoja palatakseen paikkaan, johon laite jäi, tai ryhtyäkseen muihin toimiin saadakseen sen takaisin.

Jatkuvuus

Jatkuvuuden suojauksen yleiskatsaus

Jatkuvuus hyödyntää teknologioita kuten iCloud, Bluetooth ja Wi-Fi, jotta käyttäjät voivat siirtää toimintansa laitteesta toiseen, soittaa ja vastaanottaa puheluita, lähettää ja vastaanottaa tekstiviestejä ja jakaa mobiilidataa käyttävän internet-yhteyden.

Handoffin suojaus

Apple suojaa handoff-siirrot niin laitteiden välillä, natiiviappien ja verkkosivustojen välillä kuin myös suuria tietomääriä siirrettäessä.

Miten Handoff toimii suojatusti

Kun käyttäjän iOS-, iPadOS- ja macOS-laitteet ovat lähekkäin, käyttäjä voi Handoffilla siirtää automaattisesti työskentelynsä laitteelta toiselle. Handoffilla käyttäjät voivat vaihtaa laitetta ja jatkaa työskentelyä välittömästi.

Kun käyttäjä kirjautuu sisään iCloudiin toisella Handoffia tukevalla laitteella, laitteet muodostavat kaistan ulkopuolisen Bluetooth Low Energy (BLE) 4.2 -parin käyttäen APNs-palvelua. Yksittäiset viestit ovat iMessage-viestien tapaan salattuja. Kun laitteet on liitetty pariksi, kukin laite luo symmetrisen 256-bittisen AES-avaimen, joka tallennetaan laitteen avainnippuun. Tämä avain voi salata ja todentaa BLE-mainokset, jotka viestivät laitteen nykyisen toiminnan toisille iCloud-parilaitteille käyttäen AES256:ta GCM-tilassa ja suojaustoimia toistohyökkäyksiä vastaan.

Kun laite ensimmäisen kerran vastaanottaa mainoksen uudelta avaimelta, se muodostaa BLE-yhteyden lähettäjälaitteeseen ja suorittaa mainoksen salauksen purkamisen avainten vaihdon. Tämä yhteys suojataan BLE 4.2:n standardin mukaisella salauksella sekä salaamalla yksittäiset viestit samalla tavoin kuin iMessagessa. Joissakin tilanteissa nämä viestit lähetetään käyttäen BLE:n sijasta APNs-palvelua. Toimintatietosisältö suojataan ja siirretään samalla tavoin kuin iMessage-viesti.

Handoff natiiviappien ja verkkosivustojen välillä

Handoff sallii iOS:n, iPadOS:n tai macOS:n natiiviapin jatkaa käyttäjän toimintaa sellaisten domainien verkkosivuilla, joihin apin kehittäjällä on hallintaoikeus. Se myös sallii käyttäjän natiiviappitoiminnan jatkamisen verkkoselaimessa.

Apin on osoitettava hallitsevansa oikeutetusti verkkodomaineja, joiden toimintaa se haluaa jatkaa. Tämä auttaa estämään sitä, että natiiviapit voisivat vaatia jatkettavikseen verkkosivustoja, jotka eivät ole niiden kehittäjän hallitsemia. Verkkosivuston domainin hallinta vahvistetaan jaettujen verkkotunnistetietojen mekanismilla. Jos haluat lisätietoja, katso Appien pääsy tallennettuihin salasanoihin. Järjestelmän on varmistettava, että domain-nimi on apin hallinnassa, ennen kuin appi saa hyväksyä käyttäjän toiminnan Handoffin.

Verkkosivun Handoffin lähde voi olla mikä tahansa selain, jossa käytetään Handoff-ohjelmointirajapintoja (API). Kun käyttäjä näyttää verkkosivun, järjestelmä mainostaa verkkosivun domain-nimeä salatuissa Handoff-mainostavuissa. Vain käyttäjän muut laitteet voivat purkaa mainostavujen salauksen.

Vastaanottavassa laitteessa järjestelmä havaitsee, että asennettu natiiviappi hyväksyy Handoffin mainostetulta domain-nimeltä, ja näyttää natiiviapin kuvakkeen Handoff-valintana. Kun natiiviappi avataan, se saa verkkosivun koko osoitteen ja otsikon. Muita tietoja ei anneta selaimesta natiiviappiin.

Toiseen suuntaan vaihdettaessa natiiviappi voi määrittää verkko-osoitteen sen varalle, että Handoffin vastaanottavassa laitteessa ei ole asennettuna samaa natiiviappia. Tässä tapauksessa järjestelmä näyttää käyttäjän oletusselaimen Handoffin appivalintana (jos selaimessa käytetään Handoffin ohjelmointirajapintoja). Kun Handoffia pyydetään, selain avataan ja se saa lähdeapin antaman varaosoitteen. Varaosoitteen ei välttämättä tarvitse olla natiiviapin kehittäjän hallitsemalla domain-nimellä.

Suuremman datamäärän Handoff

Handoffin perusominaisuuden käytön lisäksi jotkin apit voivat käyttää ohjelmointirajapintoja, jotka tukevat suurempien datamäärien lähettämistä Applen luomalla vertais-Wi-Fi-teknologialla (pitkälti samalla tavoin kuin AirDropissa). Esimerkiksi Mail-appi käyttää näitä ohjelmointirajapintoja mahdollisesti suuriakin liitteitä sisältävän sähköpostiluonnoksen Handoffin tukemiseksi.

Kun appi käyttää näitä ohjelmointirajapintoja, laitteiden välinen vaihto alkaa aivan samoin kuin Handoffissa. Sen jälkeen kun vastaanottava laite on vastaanottanut ensimmäisen tietosisällön BLE:llä, se kuitenkin aloittaa uuden yhteyden Wi-Fillä. Tämä yhteys salataan (TLS:llä), ja se johtaa luottamuksen iCloud-avainnipun kautta jaetun identiteetin kautta. Varmenteiden identiteetti vahvistetaan vertaamalla käyttäjän identiteettiin. Loppu tietosisältödata lähetetään tällä salatulla yhteydellä, kunnes siirto on valmis.

Universaali leikepöytä

Universaali leikepöytä hyödyntää Handoffia käyttäjän leikepöydän suojattuun siirtämiseen laitteiden välillä, jotta sisältö voidaan kopioida yhdessä laitteessa ja sijoittaa toisessa. Sisältö suojataan samoin kuten muukin Handoffin data ja jaetaan oletuksena universaalille leikepöydälle, ellei apin kehittäjä päätä kieltää jakamista.

Apit pääsevät leikepöydän dataan riippumatta siitä, onko käyttäjä sijoittanut leikepöydän appiin. Universaalin leikepöydän käyttäminen laajentaa tämän pääsyn käyttäjän muihin laitteisiin (iCloud-sisäänkirjautumisen perusteella).

Suojaus puheluiden välittämisessä iPhonen kautta

Kun käyttäjän Mac, iPad, iPod touch tai HomePod on samassa Wi-Fi-verkossa kuin hänen puhelimensa, se voi soittaa ja vastaanottaa puheluita käyttäen iPhonen matkapuhelinliittymää. Edellytyksenä on, että molemmat laitteet on kirjattu sekä iCloudiin että FaceTimeen käyttäen samaa Apple ID -tiliä.

Kun puhelu saapuu, kaikki määritetyt laitteet saavat ilmoituksen Applen push-ilmoituspalvelua (APNs) käyttäen; jokaisessa ilmoituksessa käytetään samaa päästä-päähän-salausta kuin iMessagessa. Samassa verkossa olevat laitteet esittävät käyttäjälle ilmoituksen saapuvasta puhelusta. Kun käyttäjä vastaa puheluun, ääni siirtyy saumattomasti käyttäjän iPhonesta käyttäen suojattua vertaisyhteyttä kahden laitteen välillä.

Kun puheluun vastataan yhdellä laitteella, lähellä olevien iCloud-parilaitteiden hälytysääni lopetetaan lyhyellä Bluetooth Low Energy (BLE) -mainoksella. Mainostavut salataan samalla menetelmällä kuin Handoff-mainokset.

Myös lähtevät puhelut välitetään iPhoneen käyttäen APNs-palvelua, ja ääni lähetetään samalla tavoin laitteiden välisellä suojatulla vertaisyhteydellä. Käyttäjät voivat estää puheluiden välittämisen laitteessa laittamalla FaceTime-asetuksissa Puhelut iPhonen kautta pois päältä.

iPhonen tekstiviestien välityksen suojaus

Tekstiviestien välitys lähettää automaattisesti iPhonen vastaanottamat tekstiviestit (SMS) käyttäjän rekisteröityyn iPadiin, iPod touchiin tai Maciin. Kukin laite tulee olla kirjattu iMessage-palveluun käyttäen samaa Apple ID -tiliä. Kun tekstiviestien välitys on käytössä, käyttäjän luottamusverkostoon kuuluvat laitteet, joissa kaksiosainen todennus on käytössä, rekisteröidään siihen automaattisesti. Muussa tapauksessa kunkin laitteen rekisteröinti vahvistetaan syöttämällä iPhonen luoma satunnainen kuusinumeroinen koodi.

Kun laitteet on yhdistetty, iPhone salaa saapuvat tekstiviestit ja välittää ne kullekin laitteelle käyttäen iMessagen suojauksen yleiskatsauksessa kuvattuja menetelmiä. Vastaukset lähetetään iPhonelle samalla menetelmällä, jonka jälkeen iPhone lähettää vastauksen tekstiviestinä käyttäen operaattorin tekstiviestimekanismia. Tekstiviestien välitys voidaan laittaa päälle tai pois Viestit-asetuksissa.

Instant Hotspotin suojaus

Instant Hotspot yhdistää muut Applen laitteet henkilökohtaiseen iOS- tai iPadOS-hotspotiin. Instant Hotspotia tukevat iOS- ja iPadOS-laitteet käyttävät Bluetooth Low Energy (BLE) -teknologiaa löytääkseen samalle yksittäiselle iCloud-tilille tai Perhejaon kanssa käytettäville tilileille (iOS 13:ssa ja iPadOS:ssä) kirjattuja laitteita ja viestiäkseen niiden kanssa. Yhteensopivat Mac-tietokoneet, joissa on OS X 10.10 tai uudempi, käyttävät samaa teknologiaa löytääkseen Instant Hotspotia tarjoavia iOS- ja iPadOS-laitteita ja viestiäkseen niiden kanssa.

Aluksi kun käyttäjä avaa iOS-laitteessa Wi-Fi-asetukset, laite lähettää BLE-mainosta, joka sisältää kaikkien samalle iCloud-tilille kirjattujen laitteiden yhteisen tunnisteen. Tunniste luodaan iCloud-tiliin sidotusta DSID:stä (Destination Signaling Identifier), ja sitä kierrätetään aika ajoin. Kun muut samalle iCloud-tilille kirjatut laitteet ovat lähellä ja tukevat omaa hotspotia, ne havaitsevat signaalin ja vastaavat, mikä kertoo niiden olevan saatavilla Instant Hotspotia varten.

Kun käyttäjä, joka ei kuulu Perhejakoon, valitsee iPhonen tai iPadin omaa hotspotia varten, kyseiselle laitteelle lähetetään pyyntö laittaa oma hotspot päälle. Pyyntö lähetetään käyttäen yhteyttä, joka on salattu BLE:n salauksella, ja pyyntö salataan samalla tavoin kuin iMessagea käytettäessä. Laite vastaa Oma hotspot -yhteyden tiedoilla käyttäen samaa BLE-yhteyttä ja samaa viestikohtaista salausta.

Perhejakoon kuuluvien käyttäjien oman hotspot-yhteyden tiedot jaetaan suojatusti käyttäen vastaavaa mekanismia kuin mitä HomeKit-laitteet käyttävät tietojen synkronoimiseen. Yhteys, joka jakaa hotspot-tiedot käyttäjien välillä, suojataan käyttäen lyhytaikaista ECDH (Curve25519) -avainta, joka todennetaan käyttäjien vastaavilla laitekohtaisilla julkisilla Ed25519-avaimilla. Käytettävät julkiset avaimet ovat ne avaimet, jotka synkronoitiin Perhejaon jäsenten kesken IDS:ää käyttäen aikaisemmin silloin, kun Perhejako muodostettiin.

Verkkoliikenteen suojaus

Verkkoliikenteen suojauksen yleiskatsaus

Apple suojaa Applen laitteille tallennettuja tietoja sisäänrakennettujen suojausominaisuuksien avulla. Niiden lisäksi organisaatiot voivat käyttää monenlaisia toimenpiteitä, jotka pitävät laitteisiin tulevat ja niistä lähtevät tiedot suojattuina. Kaikki nämä suojausominaisuudet ja toimenpiteet kuuluvat verkkoliikenteen suojaukseen.

Koska käyttäjillä täytyy olla pääsy yritysverkkoihin mistä päin maailmaa tahansa, on tärkeää auttaa varmistamaan, että he ovat valtuutettuja ja että heidän tietonsa on suojattu siirron aikana. Näiden tietoturvatavoitteiden saavuttamiseksi iOS:ssä, iPadOS:ssä ja macOS:ssä integroituvat tehokkaiksi todetut teknologiat ja uusimmat standardit Wi-Fi- ja mobiilidataverkkoyhteyksiä varten. Tästä syystä käyttöjärjestelmämme käyttävät standardien mukaisia verkkoprotokollia todennettuun, valtuutettuun ja salattuun viestintään ja tarjoavat kehittäjille pääsyn niihin.

TLS-suojaus

iOS, iPadOS ja macOS tukevat TLS-versioita (Transport Layer Security) 1.0, 1.1, 1.2 ja 1.3 sekä DTLS:ää (Datagram Transport Layer Security). TLS-protokolla tukee AES-128:aa ja AES-256:ta ja suosii salausmenetelmiä, joissa on forward secrecy -ominaisuus. Safarin, Kalenterin ja Mailin kaltaiset internet-apit muodostavat automaattisesti tällä protokollalla salatun tiedonsiirtokanavan laitteen ja verkkopalveluiden välille. Korkeamman tason rajapinnat (kuten CFNetwork) auttavat kehittäjiä ottamaan TLS:n käyttöön omissa apeissaan. Alemman tason rajapinnat (kuten Network.framework) puolestaan tarjoavat tarkan valvonnan. CFNetwork hylkää SSL 3:n, ja appeja, jotka käyttävät WebKitiä (kuten Safari), estetään muodostamasta SSL 3 -yhteyttä.

iOS 11:ssä ja uudemmissa ja macOS 10.13:ssa ja uudemmissa SHA-1-varmenteita ei enää sallita TLS-yhteyksille, jollei käyttäjä luota niihin. Myöskään varmenteita, joiden RSA-avaimet ovat alle 2048 bittiä, ei sallita. Symmetrinen RC4-salausmenetelmä poistetaan käytöstä iOS 10:ssä ja macOS 10.12:ssa. SecureTransport API -rajapinnoilla toteutetuilla TLS-asiakkailla tai -palvelimilla ei oletusarvoisesti ole käytössä RC4-salausmenetelmää, eivätkä ne voi muodostaa yhteyttä, jos RC4 on ainoa saatavilla oleva vaihtoehto. Suojauksen parantamiseksi RC4:ää vaativia palveluita tai appeja tulisi päivittää käyttämään turvallisia salausmenetelmiä. iOS 12.1:ssä 15.10.2018 jälkeen järjestelmän luottamasta juurivarmenteesta myönnettyjen varmenteiden täytyy kirjautua sisään luotettuun varmenteen läpinäkyvyyslokiin TLS-yhteyksien sallimiseksi. iOS 12.2:ssa TLS 1.3 on oletuksena käytössä Network.framework- ja NSURLSession-rajapinnoille. TLS-asiakkaat, jotka käyttävät SecureTransport-rajapintoja, eivät voi käyttää TLS 1.3:a.

ATS (App Transport Security)

ATS (App Transport Security) tarjoaa oletusarvoiset yhteysvaatimukset niin, että apit noudattavat parhaita käytäntöjä turvallisten yhteyksien suhteen käyttäessään NSURLConnection-, CFURL- tai NSURLSession-rajapintoja. ATS rajaa oletusarvoisesti salauksen valinnan sisältämään ainoastaan ratkaisut, jotka tarjoavat forward secrecy -ominaisuuden, erityisesti:

- ECDHE_ECDSA_AES ja ECDHE_RSA_AES Galois-/laskuritilassa (GCM)
- Salauslohkoketjutus (CBC) -tila

Apit voivat poistaa forward secrecy -vaatimuksen käytöstä domain-kohtaisesti. Tässä tapauksessa RSA_AES lisätään käytettävissä olevien koodipakettien sarjaan.

Palvelimien tulee tukea TLS 1.2:ta ja forward secrecy -ominaisuutta. Lisäksi varmenteiden tulee olla voimassa ja allekirjoitettu käyttäen SHA256:ta tai mieluummin minimissään 2048-bittistä RSA-avainta tai 256-bittistä elliptisen käyrän avainta.

Sellaisten verkkoyhteyksien muodostaminen ei onnistu, jotka eivät täytä näitä vaatimuksia, ellei appi ohita ATS:ää. Virheellisistä varmenteista on aina seurauksena laitteistovirhe tai se, ettei yhteyttä muodostu. ATS:ää käytetään automaattisesti appeihin, jotka on rakennettu iOS 9:lle tai uudemmalle ja macOS 10.11:lle tai uudemmalle.

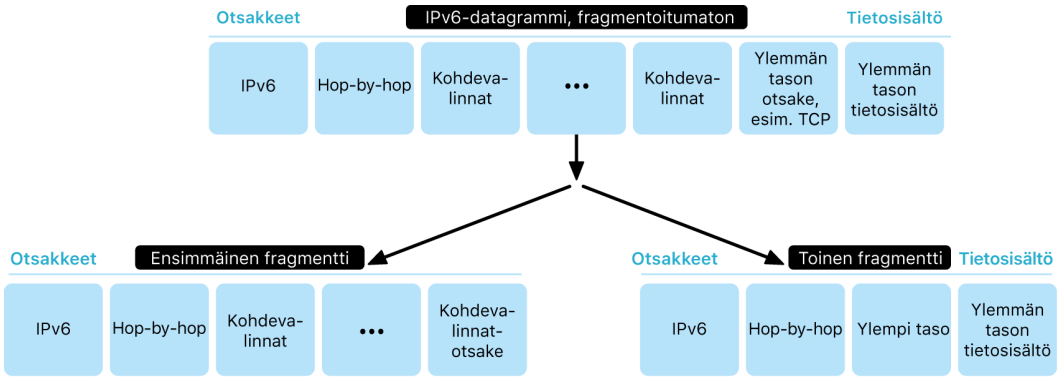
Varmenteen tarkistus

TLS-varmenteen luotetun tilan arviointi tehdään alan vakiintuneiden standardien mukaisesti, kuten on määritetty standardissa RFC 5280, ja siihen sisältyy uusia standardeja, kuten RFC 6962 (varmenteen läpinäkyvyys). iOS 11:ssä tai uudemmissa ja macOS 10.13:ssa tai uudemmissa Applen laitteisiin päivitetään säännöllisesti nykyinen luettelo perutuista ja rajoitetuista varmenteista. Luettelo on peräisin varmenteen sulkulistoista (CRL-listat), joita julkaisevat jokainen Applen luottama vakiojuurivarmentaja sekä niiden alapuoliset varmenteen myöntäjät. Luettelo voi myös sisältää muita rajoituksia Applen harkinnan mukaisesti. Tietoja kysytään aina, kun verkkorajapintatoimintoa käytetään salatun yhteyden muodostamista varten. Jos varmenteen myöntäjältä on saatu liian monta peruttua varmennetta luetteloitaviksi yksitellen, luottamuksen arviointi voi edellyttää, että tarvitaan OCSP-vastaus, ja arviointi voi epäonnistua, jos vastausta ei ole saatavilla.

IPv6:n suojaus

Kaikki Applen käyttöjärjestelmät tukevat IPv6:ta käyttäen useita mekanismeja käyttäjän yksityisyyden ja verkkopinon vakauden suojaamiseen. Kun käytetään osoitteen tilatonta autokonfiguraatiota (Stateless Address Autoconfiguration, SLAAC), kaikkien rajapintojen IPv6-osoitteet muodostetaan tavalla, joka auttaa estämään laitteiden seuraamista verkosta toiseen ja samalla mahdollistaa hyvän käyttäjäkokemuksen varmistamalla, että osoitteet pysyvät vakaina, kun verkko ei muutu. Osoitteenmuodostusalgoritmi perustuu kryptografisesti generoituihin osoitteisiin RFC 3972:n mukaisesti, ja sitä on parannettu rajapintakohtaisella muuntelijalla, jolla varmistetaan, että myös saman verkon eri rajapinnoilla on lopulta eri osoitteet. Lisäksi luodaan väliaikaisia osoitteita, joiden haluttu elinaika on 24 tuntia, ja kaikille uusille yhteyksille käytetään oletuksena niitä. iOS 14:ssä, iPadOS 14:ssä ja watchOS 7:ssä esitellyn yksityinen Wi-Fi-osoite -ominaisuuden mukaisesti jokaiselle Wi-Fi-verkolle, johon laite liittyy, luodaan yksilöllinen paikallinen osoite. Verkon SSID:tä käytetään lisäelementtinä osoitteen muodostamisessa kuten Network_ID-parameteria RFC 7217:ssä. Tätä tapaa käytetään iOS 14:ssä, iPadOS 14:ssä ja watchOS 7:ssä.

IPv6:n laajennusotsakkeisiin ja osioimiseen pohjautuvilta hyökkäyksiltä suojautumista varten Applen laitteet toteuttavat suojaustoimia, jotka on käsitelty RFC 6980:ssä, RFC 7112:ssa ja RFC 8021:ssä. Nämä estävät muun muassa hyökkäyksiä, joissa ylemmän kerroksen otsake löytyy vain toisesta osasta (alla näkyvällä tavalla), mikä voisi aiheuttaa epäselvyyttä sellaisille suojauskeinoille kuten tilaton pakettisuodatus.



Lisäksi Applen laitteet rajoittavat eri tavoin IPv6:een liittyviä tietorakenteita, kuten etuliitteiden määrää rajapintaa kohden, auttaakseen varmistamaan IPv6-pinon luotettavuuden Applen käyttöjärjestelmissä.

VPN-suojaus

Suojatut verkkopalvelut, kuten VPN (virtual private networking), edellyttävät tavallisesti vain vähimmäiskäyttöönottoa ja -määrityksiä toimiakseen iOS-, iPadOS- ja macOS-laitteiden kanssa.

Tuetut protokollat

Nämä laitteet toimivat VPN-palvelinten kanssa, jotka tukevat seuraavia protokollia ja todentamismenetelmiä:

- IKEv2/IPSec, jossa todentaminen jaetulla salaisuudella, RSA-varmenteilla, ECDSA (Elliptic Curve Digital Signature Algorithm) -varmenteilla, EAP-MSCHAPv2:lla tai EAP-TLS:llä
- SSL-VPN käyttäen sopivaa App Storen asiakasappia
- L2TP/IPSec, jossa käyttäjän todentautuminen MS-CHAPV2-salasanalla ja koneellinen todentautuminen jaetulla salaisuudella (iOS, iPadOS ja macOS) sekä RSA SecurID:llä tai CRYPTOCardilla (vain macOS)
- Cisco IPSec, jossa käyttäjän todentautuminen salasanalla, RSA SecurID:llä tai CRYPTOCardilla ja koneellinen todentautuminen jaetulla salaisuudella ja varmenteilla (vain macOS)

Tuetut VPN:n käyttötavat

iOS, iPadOS ja macOS tukevat seuraavia:

- *VPN On Demand:* Varmennepohjaista todentamista käyttäville verkoille. IT-käytännöt määrittävät, mitkä domainit edellyttävät VPN-yhteyttä käyttämällä VPN-asetusprofiilia.
- *Appikohtainen VPN:* VPN-yhteyksien helpottamiseen paljon tarkemmalta pohjalta. Mobiililaitteen hallintaratkaisut (MDM) voivat määrittää yhteyden kullekin hallitulle apille ja tietylle domainille Safarissa. Tämä auttaa varmistamaan, että suojatut tiedot siirtyvät aina yrityksen verkossa ja että käyttäjän henkilökohtaiset tiedot eivät siirry.

iOS ja iPadOS tukevat seuraavia:

- *Aina päällä -VPN:* Laitteille, joita hallitaan MDM-ratkaisulla ja valvotaan Apple Configuratorilla Macille, Apple School Managerilla tai Apple Business Managerilla. Aina päällä -VPN:ää käytettäessä käyttäjän ei tarvitse suojauksen vuoksi laittaa VPN:ää erikseen päälle muodostaessaan yhteyttä mobiili- ja Wi-Fi-verkkoihin. Sen avulla organisaatio voi myös hallita täydellisesti laiteliikennettä tunneloimalla kaiken IP-liikenteen takaisin organisaatioon. IKEv2 on parametrien ja avainten oletusarvoinen vaihto salausta varten, ja se suojaa tietoliikenteen salaamalla datan. Organisaatiot voivat tarkkailla ja suodattaa laitteidensa liikennettä, suojata organisaation verkossa olevia tietoja ja rajoittaa laitteiden pääsyä internetiin.

Wi-Fin suojaus

Suojattu langattomien verkkojen käyttö

Kaikki Applen alustat tukevat alan standardien mukaisia Wi-Fi-todentamis- ja -salaamisprotokollia ja tarjoavat näin todennetun pääsyn ja luottamuksellisuuden yhdistettäessä seuraaviin suojattuihin langattomiin verkkoihin:

- WPA2 Personal
- WPA2 Enterprise
- WPA2/WPA3 Transitional
- WPA3 Personal
- WPA3 Enterprise
- WPA3 Enterprise, 192-bittinen suojaus

WPA2 ja WPA3 todentavat jokaisen yhteyden ja tarjoavat 128-bittisen AES-salauksen auttaakseen varmistamaan langattomasti lähetetyn tiedon luottamuksellisuuden. Tämä antaa käyttäjille parhaan varmuuden siitä, että heidän tietonsa pysyvät suojattuina heidän lähettäessään ja vastaanottaessaan tietoja Wi-Fi-verkkoyhteyden kautta.

WPA3:n tuki

WPA3:a tuetaan seuraavissa Applen laitteissa:

- iPhone 7 tai uudempi
- iPad, 5. sukupolvi tai uudempi
- Apple TV 4K tai uudempi
- Apple Watch Series 3 tai uudempi
- Mac-tietokoneet (loppuvuosi 2013 tai uudemmat, joissa on 802.11ac tai uudempi)

Uudemmat laitteet tukevat todentamista WPA3 Enterprise (192-bittinen suojaus) -protokollalla, mukaan lukien tuki 256-bittiselle AES-salaukselle, kun muodostetaan yhteys yhteensopiviin langattomiin tukiasemiin. Tämä tarjoaa entistä vahvemmat luottamuksellisuussuojaukset langattomasti lähetetylle tietoliikenteelle. 192-bittistä WPA3 Enterprise -suojausta tuetaan iPhone 11:ssä, iPhone 11 Prossa, iPhone 11 Pro Maxissa ja uudemmissa iOS- ja iPadOS-laitteissa.

PMF-tuki

Sen lisäksi, että Applen alustat suojaavat langattomasti lähetettyjä tietoja, ne myös laajentavat WPA2- ja WPA3-tason suojauksia täsmälähetysten ja monilähetyksen hallintakehyksiin PMF-palvelulla (Protected Management Frame), joka on määritetty 802.11w:ssä. PMF-tuki on saatavilla seuraavissa Apple-laitteissa:

- iPhone 6 tai uudempi
- iPad Air 2 tai uudempi
- Apple TV HD tai uudempi
- Apple Watch Series 3 tai uudempi
- Mac-tietokoneet (loppuvuosi 2013 tai uudemmat, joissa on 802.11ac tai uudempi)

802.1X-tuella Apple-laitteet voidaan integroida moniin eri RADIUS-todentamisympäristöihin. 802.1X:n langattoman todentamisen menetelmiin sisältyvät EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 ja PEAPv1.

Alustasuojaukset

Applen käyttöjärjestelmät suojaavat laitetta haavoittuvuuksilta verkkoprosessorin laiteohjelmistossa. Tämä tarkoittaa, että verkko-ohjaimilla, joissa on Wi-Fi, on rajoitettu pääsy appeja suorittavan prosessorin muistiin.

- Kun USB:tä tai SDIO:ta (Secure Digital Input Output) käytetään verkkoprosessorin liitäntään, verkkoprosessori ei voi käynnistää DMA-toimintoja appeja suorittavaan prosessoriin.
- Kun PCIe:tä käytetään, jokainen verkkoprosessori on sen omassa eristetyssä PCIe-väylässä. Jokaisessa PCIe-väylässä oleva I/O-muistinhallintayksikkö (IOMMU) rajoittaa lisää verkkoprosessorin DMA-pääsyä vain muistiin ja resursseihin, jotka sisältävät sen verkkopaketit ja ohjainrakenteet.

Vanhentuneet protokollat

Applen tuotteet tukevat seuraavia vanhentuneita Wi-Fi-todentamis- ja -salausprotokollia:

- Avoin WEP 40-bittisillä ja 104-bittisillä avaimilla
- Jaettu WEP 40-bittisillä ja 104-bittisillä avaimilla
- Dynaaminen WEP
- TKIP-protokolla (Temporal Key Integrity Protocol)
- WPA
- WPA/WPA2 Transitional

Näitä protokollia ei enää pidetä turvallisina ja niiden käytön lopettamista suositellaan vahvasti yhteensopivuus-, luotettavuus-, suorituskyky- ja turvallisuussyiden vuoksi. Niitä tuetaan vain aiempien versioiden yhteensopivuuden vuoksi, ja ne saatetaan poistaa tulevista ohjelmistoversioista.

Kaikkia Wi-Fi-toteutuksia suositellaan siirtymään WPA3 Personal- tai WPA3 Enterprise -protokollaan, jotta käytössä on mahdollisimman vakaat, turvalliset ja yhteensopivat Wi-Fi-yhteydet.

Wi-Fin yksityisyys

MAC-osoitteen satunnaistaminen

Applen alustat käyttävät satunnaista MAC-osoitetta (Media Access Control address), kun ne tekevät Wi-Fi-hakuja silloin, kun ne eivät ole yhteydessä Wi-Fi-verkkoon. Hakujen avulla voidaan löytää ja yhdistää tunnettuun Wi-Fi-verkkoon tai auttaa sijaintipalveluja sellaisia appeja varten, jotka käyttävät aluerajoja, kuten sijaintiperusteisia muistutuksia tai sijainnin korjaamista Applen Kartoissa. Huomaa, että Wi-Fi-hakuja, jotka tapahtuvat, kun yritetään muodostaa yhteyttä haluttuun Wi-Fi-verkkoon, ei satunnaisteta. Wi-Fin MAC-osoitteen satunnaistamista tuetaan iPhone 5:ssä ja uudemmissa.

Applen alustat käyttävät satunnaista MAC-osoitetta myös, kun ne suorittavat ePNO (enhanced Preferred Network Offload) -hakuja silloin, kun laitetta ei ole yhdistetty Wi-Fi-verkkoon tai kun sen prosessori nukkuu. ePNO-haut suoritetaan, kun laite käyttää sijaintipalveluja aluerajoja käyttäville apeille, kuten sijaintiperusteisille muistutuksille, jotka määrittävät, onko laite lähellä tiettyä sijaintia.

Koska laitteen MAC-osoite muuttuu, kun sen yhteys Wi-Fi-verkkoon katkaistaan, passiiviset Wi-Fi-tietoliikenteen tarkkailijat eivät voi käyttää osoitetta laitteen jatkuvaan tarkkailuun silloinkaan, kun laite on yhdistettynä mobiiliverkkoon. Apple on ilmoittanut Wi-Fi-valmistajille, että iOS:n ja iPadOS:n Wi-Fi-haut käyttävät satunnaista MAC-osoitetta ja että Apple tai valmistajat eivät voi ennustaa näitä satunnaisia MAC-osoitteita.

iOS 14:ssä tai uudemmissa, iPadOS 14:ssä tai uudemmissa ja watchOS 7:ssä tai uudemmissa kun iPhone, iPad, iPod touch tai Apple Watch muodostaa yhteyden Wi-Fi-verkkoon, se tunnistautuu jokaiseen verkkoon erilaisella (satunnaisella) MAC-osoitteella. Käyttäjä voi poistaa tämän ominaisuuden käytöstä, tai se voidaan poistaa Wi-Fi-tietosisällön uudella valinnalla. Tietyissä tilanteissa laite palaa käyttämään varsinaista MAC-osoitetta.

Saat lisätietoja Applen tukiartikkelista Yksityisten Wi-Fi-osoitteiden käyttäminen iPhonessa, iPadissa, iPod touchissa ja Apple Watchissa.

Wi-Fi-kehyksen järjestysnumerojen satunnaistaminen

Wi-Fi-kehykset sisältävät sarjanumeron, jota alemman tason 802.11-protokolla käyttää tehokkaaseen ja luotettavaan Wi-Fi-tietoliikenteeseen. Koska nämä sarjanumerot kasvavat jokaisen lähetetyn kehyksen myötä, niitä voisi käyttää Wi-Fi-hauissa lähetettyjen tietojen vertaamiseen muiden saman laitteen lähettämien kehysten kanssa.

Tältä suojaamiseksi Apple-laitteet satunnaistavat sarjanumerot aina, kun MAC-osoite muutetaan uudeksi satunnaiseksi osoitteeksi. Tämä sisältää myös sarjanumeroiden satunnaistamisen jokaiselle uudelle hakupyynnölle, joka aloitetaan, kun laite ei ole yhdistettynä. Satunnaistamista tuetaan seuraavissa laitteissa:

- iPhone 7 tai uudempi
- iPad, 5. sukupolvi tai uudempi
- Apple TV 4K tai uudempi
- Apple Watch Series 3 tai uudempi
- iMac Pro (Retina 5K, 27 tuumaa, 2017) tai uudempi
- MacBook Pro (13 tuumaa, 2018) tai uudempi
- MacBook Pro (15 tuumaa, 2018) tai uudempi
- MacBook Air (Retina, 13 tuumaa, 2018) tai uudempi
- Mac mini (2018) tai uudempi
- iMac (Retina 4K, 21,5 tuumaa, 2019) tai uudempi
- iMac (Retina 5K, 27 tuumaa, 2019) tai uudempi
- Mac Pro (2019) tai uudempi

Wi-Fi-yhteydet

Apple luo satunnaisia MAC-osoitteita Wi-Fi-vertaisverkoille AirDropia ja AirPlayta varten. Satunnaisia osoitteita käytetään myös omaan hotspotiin iOS:ssä ja iPadOS:ssä (jossa on SIM-kortti) ja internet-jakoon macOS:ssä.

Uudet satunnaiset osoitteet luodaan aina, kun nämä verkkoliitännät käynnistetään, ja ainutkertainen osoite luodaan erikseen jokaista liitäntää varten tarpeen mukaan.

Kätketyt verkot

Wi-Fi-verkot tunnistetaan niiden verkkonimestä, jota kutsutaan *palvelutunnisteeksi (SSID, service set identifier)*. Jotkin Wi-Fi-verkot on määritetty kätkemään niiden SSID-tunniste, minkä vuoksi langaton tukiasema ei lähetä verkon nimeä. Näitä kutsutaan *kätketyiksi verkoiksi*. iPhone 6s ja uudemmat laitteet havaitsevat automaattisesti, kun verkko on kätketty. Jos verkko on kätketty, iOS- tai iPadOS-laite lähettää tiedustelun, jonka pyyntö sisältää SSID:n. Tämä auttaa estämään laitetta lähettämästä aiemmin kätkettyjen verkkojen nimiä, joihin käyttäjä oli yhteydessä, ja auttaa siten osaltaan varmistamaan yksityisyyttä.

Bluetooth-suojaus

Applen laitteissa on kahdentyyppisiä Bluetootheja: Bluetooth Classic ja Bluetooth Low Energy (BLE). Molempien versioiden Bluetooth-suojausmalli sisältää seuraavat eri suojausominaisuudet:

- *Parinmuodostus:* Yhden tai useamman jaetun salaisuusavaimen luontiprosessi
- *Yhdistäminen:* Parinmuodostuksen aikana luotujen avainten säilyttäminen käytettäväksi seuraavissa yhteyksissä luotetun laiteparin muodostamista varten
- *Todentaminen:* Sen varmistaminen, että kahdella laitteella on samat avaimet
- *Salaaminen:* Viestin luottamuksellisuus
- *Viestin eheys:* Suojaaminen viestien väärentämiseltä
- *SSP (Secure Simple Pairing):* Suojaaminen passiiviselta salakuuntelulta ja suojaaminen man in the middle -hyökkäyksiltä

Bluetoothin versio 4.1 lisäsi Secure Connections -ominaisuuden Bluetooth Classicin fyysiseen BR/EDR-siirtoon.

Jokaisen Bluetooth-tyypin suojausominaisuuksia ovat alla olevat.

Tuki	Bluetooth Classic	Bluetooth Low Energy
Parinmuodostus	P-256 elliptinen käyrä	FIPS-hyväksytyt algoritmit (AES-CMAC ja P-256 elliptinen käyrä)
Yhdistäminen	Parinmuodostustiedot tallennetaan suojattuun sijaintiin iOS-, iPadOS-, macOS-, tvOS- ja watchOS-laitteissa	Parinmuodostustiedot tallennetaan suojattuun sijaintiin iOS-, iPadOS-, macOS-, tvOS- ja watchOS-laitteissa
Todentaminen	FIPS-hyväksytyt algoritmit (HMAC-SHA256 ja AES-CTR)	FIPS-hyväksytyt algoritmit
Salaaminen	Ohjaimessa suoritettava AES-CCM-salaus	Ohjaimessa suoritettava AES-CCM-salaus

Tuki	Bluetooth Classic	Bluetooth Low Energy
Viestin eheys	Viestin eheyteen käytettävä AES-CCM-salaus	Viestin eheyteen käytettävä AES-CCM-salaus
SSP (Secure Simple Pairing): Suojaaminen passiiviselta salakuuntelulta	Elliptisen käyrän Diffie-Hellman -avaimenvaihto lyhytaikaisella avaimella (ECDHE)	Elliptisen käyrän Diffie-Hellman -avaimenvaihto (ECDHE)
SSP (Secure Simple Pairing): Suojaaminen MITM-hyökkäyksiltä (man-in-the-middle)	Kaksi käyttäjän avustamaa numeromenetelmää: numerovertailu tai pääsyavaimen syöttö	Kaksi käyttäjän avustamaa numeromenetelmää: numerovertailu tai pääsyavaimen syöttö Parinmuodostukset vaativat käyttäjän vastauksen, mukaan lukien kaikki ei-MITM-parinmuodostustilat
Bluetooth 4.1 tai uudempi	iMac (loppuvuosi 2015 tai uudempi) MacBook Pro (alkuvuosi 2015 tai uudempi)	iOS 9 tai uudempi iPadOS 13.1 tai uudempi macOS 10.12 tai uudempi tvOS 9 tai uudempi watchOS 2.0 tai uudempi
Bluetooth 4.2 tai uudempi	iPhone 6 tai uudempi	iOS 9 tai uudempi iPadOS 13.1 tai uudempi macOS 10.12 tai uudempi tvOS 9 tai uudempi watchOS 2.0 tai uudempi

Bluetooth Low Energyn yksityisyyden suoja

BLE:ssä on käyttäjän yksityisyyden suojaamista varten seuraavat kaksi ominaisuutta: osoitteen satunnaistaminen ja poikittaisen liikenteen avaimenluonti.

Osoitteen satunnaistaminen -ominaisuudella vähennetään BLE-laitteen seurantamahdollisuutta ajan myötä muuttamalla Bluetooth-laitteen osoitetta säännöllisesti. Jotta laite voi käyttää yksityisyysominaisuutta tunnettuihin laitteisiin uudelleenyhdistämiseen, laitteen osoitteen, jota kutsutaan *yksityiseksi osoitteeksi*, täytyy olla toisen laitteen ratkaistavissa. Yksityinen osoite luodaan käyttämällä laitteen identiteetin ratkaisevaa avainta (IRK), joka vaihdettiin parinmuodostuksen aikana.

iOS 13:ssa ja uudemmissa ja iPadOS 13.1:ssä ja uudemmissa on mahdollisuus johtaa linkkiavaimia siirtojen välillä ominaisuudella, jonka nimi on *poikittaisen liikenteen avaimenluonti*. Esimerkiksi BLE:llä luotua linkkiavainta voidaan käyttää Bluetooth Classic -linkkiavaimen johtamiseen. Lisäksi Apple lisäsi Bluetooth Classic to BLE -tuen Secured Connections -ominaisuutta tukeviin laitteisiin. Ominaisuus esiteltiin Bluetooth Core Specification -versiossa 4.1 (katso Bluetooth Core Specification 5.1).

Ultra Wideband -teknologian suojaus iOS:ssä

Uusi Applen suunnittelema U1-siru käyttää Ultra Wideband -teknologiaa sijainnin havaitsemiseen. Sen ansiosta iPhone 11, iPhone 11 Pro ja iPhone 11 Pro Max tai uudemmat iPhone-mallit voivat paikantaa tarkasti muut U1-varustetut Applen laitteet. Ultra Wideband -teknologia käyttää samaa teknologiaa tietojen satunnaistamiseen kuin muut tuetut Applen laitteet:

- MAC-osoitteen satunnaistaminen
- Wi-Fi-kehyksen sarjanumerojen satunnaistaminen

Kertakirjautuminen

Kertakirjautumisen suojaus

Kertakirjautuminen

iOS ja iPadOS tukevat todentamista yritysverkkoihin kertakirjautumisella (SSO, Single sign-on). Kertakirjautuminen toimii yhdessä Kerberos-pohjaisten verkkojen kanssa ja todentaa käyttäjät palveluihin, joihin heille on valtuutettu pääsy. Kertakirjautumista voidaan käyttää useisiin verkkotoimintoihin aina suojatuista Safari-istunnoista muiden valmistajien appeihin. Myös varmennepohjaista todentamista, kuten PKINIT, tuetaan.

macOS tukee todentautumista yritysverkkoihin Kerberoksella. Apit voivat todentaa käyttäjät Kerberoksella palveluihin, joihin heille on valtuutettu pääsy. Kerberosta voidaan myös käyttää useisiin verkkotoimintoihin aina suojatuista Safari-istunnoista ja verkon tiedostojärjestelmän todentamisesta muiden valmistajien appeihin. Varmennepohjaista todentamista tuetaan, mutta apilta vaaditaan tällöin kehittäjän rajapinnan käyttöönottoa.

iOS:n, iPadOS:n ja macOS:n kertakirjautumisten SPNEGO-suojaustunnukset ja HTTP Negotiate -protokolla toimivat Kerberos-pohjaisten todentamisen yhdyskäytävien ja Kerberos-lippuja tukevien Windows Integrated Authentication -järjestelmien kanssa. Kertakirjautumisen tuki perustuu avoimen lähdekoodin Heimdal-projektiin.

Seuraavia salaustyyppejä tuetaan iOS:ssä, iPadOS:ssä ja macOS:ssä:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari tukee kertakirjautumista, ja myös muiden valmistajien standardien mukaisia iOS- ja iPadOS-verkkoyhteysrajapintoja käyttävät apit voidaan määrittää käyttämään kertakirjautumista. Kertakirjautumisen määrittämistä varten iOS ja iPadOS tukevat asetusprofiileja, joiden avulla mobiilinhallintaratkaisut (MDM) voivat lähettää tarvittavat asetukset. Näissä määritetään käyttäjän ensisijainen nimi (eli Active Directory -käyttäjätili) ja Kerberos-alueen asetukset ja määritetään, minkä appien ja Safarin verkko-osoitteiden sallitaan käyttää kertakirjautumista.

macOS:ssä Kerberos voidaan määrittää hankkimalla liput Ticket Viewerin avulla, kirjautumalla Windows Active Directory-domainiin tai käyttämälllä `kinit`-komentorivityökalua.

Laajennettava kertakirjautuminen

Appien kehittäjät voivat tarjota omia kertakirjautumistoteutuksia kertakirjautumisen laajennuksilla. Kertakirjautumisen laajennukset otetaan käyttöön, kun natiivi- tai verkkoapin tarvitsee käyttää jotain identiteetin tarjoajaa käyttäjän todentamiseen. Kehittäjät voivat tarjota kahdentyyppisiä laajennuksia: sellaisia, jotka uudelleenohjaavat HTTPS:ään, ja sellaisia, jotka käyttävät haaste/vastaus-mekanismia, kuten Kerberos. Tämän ansiosta laajennettava kertakirjautuminen voi tukea OpenID-, OAuth-, SAML2- ja Kerberos-todentamismalleja.

Appi voi käyttää kertakirjautumisen laajennusta joko käyttämällä AuthenticationServices API:a tai osoitteen sieppausmekanismia, jonka käyttöjärjestelmä tarjoaa. WebKit ja CFNetwork tarjoavat sieppauskerroksen, joka sallii kertakirjautumisen saumattoman tuen mille tahansa natiivi- tai WebKit-apille. Jotta kertakirjautumisen laajennus otetaan käyttöön, ylläpitäjän tarjoama määritys täytyy asentaa mobiililaitteenhallintaprofiilin (MDM) avulla. Tämän lisäksi uudelleenohjaustyyppisten laajennusten täytyy käyttää Yhdistetyt domainit -tietosisältöä sen varmistamiseen, että niiden tukema identiteettipalvelin tietää niiden olemassaolosta.

Ainoa käyttöjärjestelmän tarjoama laajennus on Kerberos-kertakirjautumislaajennus.

AirDropin suojaus

AirDropia tukevat Apple-laitteet käyttävät Bluetooth Low Energy (BLE) -teknologiaa ja Applen luomaa Wi-Fi-vertaisverkkoteknologiaa tiedostojen ja tietojen lähettämiseen lähellä oleviin laitteisiin, mukaan lukien AirDrop-yhteensopivat iOS-laitteet ja iPad-laitteet, joissa on iOS 7 tai uudempi, ja Mac-tietokoneet, joissa on OS X 10.11 tai uudempi. Wi-Fi-radiota käytetään laitteiden väliseen suoraan kommunikaatioon ilman internet-yhteyttä tai langatonta tukiasemaa (AP). Tämä yhteys salataan TLS:llä.

AirDrop on oletuksena asetettu jakamaan vain yhteystiedoille. Käyttäjät voivat jakaa AirDropilla kaikille tai laittaa ominaisuuden kokonaan pois päältä. Organisaatiot voivat rajoittaa hallittujen laitteiden tai appien AirDropin käyttöä mobiililaitteiden hallintaratkaisulla (MDM).

AirDropin toiminta

AirDrop käyttää iCloud-palveluita käyttäjien todentamiseen. Kun käyttäjä kirjautuu iCloudiin, 2048-bittinen RSA-identiteetti tallennetaan laitteeseen, ja kun käyttäjä laittaa AirDropin päälle, AirDropin lyhyt identiteettitunniste luodaan perustuen sähköpostiosoitteisiin ja puhelinnumeroihin, jotka on liitetty käyttäjän Apple ID:hen.

Kun käyttäjä valitsee kohteen jakotavaksi AirDropin, lähettävä laite lähettää BLE:llä AirDrop-signaalin, joka sisältää käyttäjän lyhyen AirDrop-identiteettitunnisteen. Muut päällä ja lähellä olevat Applen laitteet, joiden AirDrop on päällä, havaitsevat signaalin ja vastaavat käyttäen Wi-Fi-vertaisverkkoa, jolloin lähettävä laite saa tietoonsa vastaanottavien laitteiden identiteetin.

Vain yhteystiedot -tilassa vastaanotettua lyhyttä AirDrop-identiteettitunnistetta verrataan henkilöiden tunnisteisiin vastaanottavan laitteen Yhteystiedot-apissa. Jos löydetään täsmäävä tieto, vastaanottava laite vastaa Wi-Fi-vertaisverkon kautta sen identiteettitiedoilla. Jos täsmääviä tietoja ei ole, laite ei vastaa.

Kaikki-tilassa käytetään samaa yleistä prosessia. Vastaanottava laite kuitenkin vastaa myös, jos tiedot eivät täsmää laitteen Yhteystiedot-apin tietojen kanssa.

Lähettävä laite muodostaa AirDrop-yhteyden Wi-Fi-vertaisverkolla ja käyttää tätä yhteyttä pitkän identiteettitunnisteen lähettämiseen vastaanottavaan laitteeseen. Jos pitkä identiteettitunniste täsmää vastaanottajan Yhteystiedot-apin tunnetun henkilön tunnisteen kanssa, vastaanottaja vastaa pitkillä identiteettitunnisteilla.

Jos tunnisteet varmistetaan, vastaanottajan etunimi ja kuva (jos saatavilla Yhteystiedoissa) näytetään lähettäjän AirDrop-jakoikkunassa. iOS:ssä ja iPadOS:ssä ne näytetään Ihmiset- tai Laitteet-osiossa. Varmistamattomat ja todentamattomat laitteet näkyvät lähettäjän AirDrop-jakoikkunassa. Niissä näkyy siluettikuvake ja laitteen nimi, joka on määritetty kohdassa Asetukset > Yleiset > Tietoja > Nimi. iOS:ssä ja iPadOS:ssä ne ovat AirDrop-jakoikkunan Muut henkilöt -osiossa.

Lähettävä käyttäjä voi sen jälkeen valita, kenelle hän haluaa jakaa. Käyttäjän valinnan mukaisesti lähettävä laite muodostaa salatun (TLS-) yhteyden vastaanottavaan laitteeseen, joka vaihtaa niiden iCloud-henkilövarmenteita. Varmenteiden identiteetti varmistetaan jokaisen käyttäjän Yhteystiedot-apista.

Jos varmenteet on varmistettu, vastaanottavaa käyttäjää pyydetään hyväksymään siirto tunnistetulta käyttäjältä tai laitteelta. Jos valittuna on useita vastaanottajia, prosessi toistetaan jokaiselle kohteelle.

Wi-Fi-salasanan jakamisen suojaus iPhonessa ja iPadissa

iOS- ja iPadOS-laitteet, jotka tukevat Wi-Fi-salasanan jakoa, käyttävät AirDropia muistuttavaa menetelmää Wi-Fi-salasanan lähettämiseen laitteesta toiseen.

Kun käyttäjä valitsee Wi-Fi-verkon (pyytäjä) ja käyttäjältä pyydetään Wi-Fi-salasanaa, Apple-laite aloittaa BLE-mainoksen, joka ilmoittaa, että se haluaa Wi-Fi-salasanan. Muut päällä ja lähellä olevat Applen laitteet, joilla on valitun Wi-Fi-verkon salasana, muodostavat yhteyden BLE:llä pyytävään laitteeseen.

Laite, jolla on Wi-Fi-salasana (myöntäjä) vaatii pyytäjän yhteystiedot, ja pyytäjän täytyy todistaa identiteettinsä vastaavalla tavalla kuin AirDrop. Kun identiteetti on varmistettu, myöntäjä lähettää pyytäjälle pääsykoodin, jolla voidaan liittyä verkkoon.

Organisaatiot voivat rajoittaa hallittujen laitteiden tai appien Wi-Fi-salasanan jakamista mobiililaitteiden hallintaratkaisulla (MDM).

Palomuurisuojaus macOS:ssä

macOS:ssä on sisäinen palomuuri, jolla suojataan Macia verkosta tulevilta hyökkäyksiltä ja palvelunestohyökkäyksiltä. Se voidaan määrittää Järjestelmäasetusten Suojaus ja yksityisyys -osiossa, ja se tukee seuraavia määrityksiä:

- Kaikki saapuvat yhteydet estetään apista riippumatta.
- Vakio-ohjelmistoille sallitaan automaattisesti saapuvien yhteyksien vastaanottaminen.
- Ladatuille ja allekirjoitetuille ohjelmistoille sallitaan automaattisesti saapuvien yhteyksien vastaanottaminen.
- Pääsy lisätään tai kielletään käyttäjän määrittämien appien pohjalta.
- Macia estetään vastaamasta ICMP (Internet Control Message Protocol) -tiedusteluihin ja porttiskannauspyyntöihin.

Kehittäjäpaketin suojaus

Kehittäjäpaketin suojauksen yleiskatsaus

Apple tarjoaa useita pakettisovelluskehyksiä, joilla muiden valmistajien kehittäjät voivat laajentaa Applen palveluita. Käyttäjän yksityisyys ja suojaus ovat näiden sovelluskehysten ytimessä:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

HomeKitin suojaus

HomeKit-tietoliikenteen suojaus

HomeKit tarjoaa kodin automaatioille infrastruktuurin, jossa hyödynnetään iCloudin ja iOS:n, iPadOS:n ja macOS:n suojausta yksityisten tietojen suojaamiseen ja synkronoimiseen ilman, että ne tulevat Applen tietoon.

HomeKitin identiteetti ja suojaus perustuvat julkisen ja yksityisen Ed25519-avaimen pareihin. iOS-, iPadOS- ja macOS-laitteessa luodaan Ed25519-avainpari kullekin HomeKitin käyttäjälle, ja siitä tulee käyttäjän HomeKit-identiteetti. Sitä käytetään viestinnän todentamiseen iOS-, iPadOS- ja macOS-laitteiden välillä sekä iOS-, iPadOS- ja macOS-laitteiden ja lisälaitteiden välillä.

Avaimet, jotka tallennetaan avainnippuun ja sisällytetään ainoastaan salattuihin avainnippuvarmuuskopioihin, pidetään ajantasaisina laitteiden välillä käyttäen iCloud-avainnippua, jos se on käytössä. HomePod ja Apple TV saavat avaimet käyttäen käyttöönottoa napautuksella tai käyttöönottotilaa, josta kerrotaan jäljempänä. Avaimet jaetaan iPhonesta sen parina olevaan Apple Watchiin käyttäen Apple Identity Service (IDS) -palvelua.

Viestintä HomeKit-lisälaitteiden välillä

HomeKit-lisälaitteet luovat oman Ed25519-avainparinsa käytettäväksi viestinnässä iOS-, iPadOS- ja macOS-laitteiden kanssa. Jos lisälaite palautetaan tehdasasetuksiinsa, luodaan uusi avainpari.

Kun iOS-, iPadOS- ja macOS-laite muodostavat suhteen HomeKit-lisälaitteen kanssa, ne vaihtavat avaimia käyttäen Secure Remote Password -protokollaa (3072-bittinen), jossa hyödynnetään lisälaitteen valmistajalta saatua kahdeksannumeroista koodia. Käyttäjä syöttää koodin iOS- tai iPadOS-laitteeseen, ja sitten se salataan käyttäen ChaCha20-Poly1305 AEAD:tä ja HKDF-SHA512:lla muodostettuja avaimia. Myös lisälaitteen MFi-hyväksyntä tarkistetaan käyttöönoton yhteydessä. Lisälaitteisiin, joilla ei ole MFi-sirua, voidaan sisällyttää tuki ohjelmistotodennukselle iOS 11.3:ssa tai uudemmissa.

Kun iOS-, iPadOS- ja macOS-laite ja HomeKit-lisälaite viestivät käytön aikana, kumpikin todentaa toisen käyttäen edellä kuvatussa prosessissa vaihdettuja avaimia. Jokaisen istunnon luomiseen käytetään Station-to-Station-protokollaa (STS), ja istunnot salataan käyttäen HKDF-SHA512:lla muodostettuja avaimia, jotka perustuvat istuntokohtaisiin Curve25519-avaimiin. Tämä koskee sekä IP-pohjaisia että Bluetooth Low Energy (BLE) -lisälaitteita.

Jos BLE-laite tukee ilmoitusten yleislähetystä, lisälaite saa yleislähetyksen salausavaimen pariksi asetetulta iOS-, iPadOS- ja macOS-laitteelta suojatussa istunnossa. Tätä avainta käytetään lisälaitteen tilamuutostietojen salaamiseen, kun muutoksista ilmoitetaan BLE-mainoksilla. Yleislähetyksen salausavain muodostetaan käyttäen HKDF-SHA512:ta, ja tiedot salataan käyttäen ChaCha20-Poly1305 AEAD -algoritmia. iOS-, iPadOS- ja macOS-laite vaihtaa yleislähetyksen salausavaimen ajoittain ja päivittää sen muihin laitteisiin käyttäen iCloudia. Tästä kerrotaan osiossa HomeKitin tietojen suojaus.

HomeKit ja Siri

Siriä voidaan käyttää lisälaitteiden kyselyihin ja hallintaan, ja sillä voidaan aloittaa tilanteita. Sirille annetaan tietoja kodin määrityksistä mahdollisimman niukasti ja anonyymissa muodossa. Siri saa tiedoista komentojen tunnistamista varten tarvittavat huoneiden, lisälaitteiden ja tilanteiden nimet. Sirille lähetettävässä äänisisällössä saatetaan ilmaista tiettyjä lisälaitteita tai komentoja, mutta näitä Siri-tietoja ei yhdistetä muihin Applen ominaisuuksiin kuten HomeKitiin.

Siriä tukevat HomeKit-lisälaitteet

Käyttäjät voivat ottaa käyttöön uusia ominaisuuksia kuten Sirin sekä muita HomePodin ominaisuuksia kuten ajastimet, herätykset, intercomin ja ovikellon Siriä tukevissa lisälaitteissa Koti-appia käyttäen. Kun nämä ominaisuudet on otettu käyttöön, lisälaite tekee yhteistyötä sen parina olevan HomePodin kanssa lähiverkossa, jossa nämä Applen ominaisuudet toimivat. Ääni siirretään laitteiden välillä salattujen kanavien kautta käyttäen sekä HomeKit- että AirPlay-protokollia.

Kun ”Reagoi Hei Siri -kutsuun” on päällä, lisälaite kuuntelee ”Hei Siri” -lausahdusta käyttäen paikallisesti toimivaa käynnistyslausahduksen tunnistusohjelmaa. Jos tämä ohjelma tunnistaa lausahduksen, se lähettää äänikehykset suoraan parina olevalle HomePodille käyttäen HomeKitiä. HomePod tarkistaa äänimateriaalin uudestaan ja voi kumota ääni-istunnon, jos lausahdus ei vaikuta sisältävän käynnistyslausahdusta.

Kun Sirin käyttö koskettamalla on päällä, käyttäjä voi aloittaa keskustelun Sirin kanssa painamalla lisälaitteessa tätä tarkoitusta varten olevaa painiketta. Äänikehykset lähetetään suoraan parina olevaan HomePodiin.

Kun onnistunut Siri-kutsu tunnistetaan, HomePod lähettää äänen Siri-palvelimille ja toteuttaa käyttäjän aikeen käyttäen samoja suojauksen, yksityisyyden ja salauksen suojakeinoja kuin silloin, jos käyttäjän kutsut tehdään HomePodille itselleen. Jos Siri vastaa äänellä, Sirin vastaus lähetetään lisälaitteeseen AirPlay-äänikanavan kautta. Jotkin Siri-pyynnöt vaativat käyttäjältä lisätietoja (esimerkiksi kysymys, haluaako käyttäjä kuulla lisää vaihtoehtoja). Tässä tapauksessa lisälaite saa merkin, että käyttäjän toimintaa tarvitaan, ja uusi äänimateriaali striimataan HomePodiin.

Lisälaitteessa täytyy olla näkyvä merkki, joka kertoo käyttäjälle, milloin se kuuntelee aktiivisesti (esimerkiksi merkkivalo). Lisälaitteella ei ole tietoa Siri-pyynnön aikeesta lukuun ottamatta pääsyä äänivirtoihin, eikä käyttäjän tietoja tallenneta lisälaitteeseen.

HomeKitin tietojen suojaus

HomeKitin tiedot voidaan päivittää suojatusti käyttäjän iOS-, iPadOS- ja macOS-laitteiden välillä käyttäen iCloudia ja iCloud-avainnippua. Tämän prosessin aikana HomeKitin tiedot salataan käyttäen käyttäjän HomeKit-identiteetistä muodostettuja avaimia ja satunnaista noncea ja niitä käsitellään läpinäkymättömänä ja binäärisenä suurena kokonaisuutena (*blob*). Viimeisin datakokonaisuus tallennetaan iCloudiin, mutta sitä ei käytetä mihinkään muuhun tarkoitukseen. Koska se on salattu käyttäen avaimia, jotka ovat saatavilla vain käyttäjän iOS-, iPadOS- ja macOS-laitteissa, sen sisältö ei ole käytettävissä siirron aikana tai iCloud-tallennustilassa.

HomeKitin tietoja synkronoidaan myös saman kodin useiden käyttäjien välillä. Tässä prosessissa käytetään samaa todennusta ja salausta kuin iOS-, iPadOS- ja macOS-laitteen ja HomeKit-lisälaitteen välillä. Todennus perustuu julkisiin Ed25519-avaimiin, jotka laitteet vaihtavat, kun käyttäjä lisätään kotiin. Kun uusi käyttäjä on lisätty kotiin, kaikki sen jälkeinen viestintä todennetaan ja salataan käyttäen Station-to-Station-protokollaa ja istuntokohtaisia avaimia.

Uusia käyttäjiä voi lisätä se käyttäjä, joka alun perin loi kodin HomeKitissä, tai toinen käyttäjä, jolla on muokkausoikeudet. Omistajan laite määrittää uuden käyttäjän julkisen avaimen lisälaitteisiin, jotta lisälaite voi todentaa uuden käyttäjän ja hyväksyä komentoja tältä. Kun käyttäjä, jolla on muokkausoikeudet, lisää uuden käyttäjän, prosessi delegoidaan kodin keskittimeen toiminnon loppuunviemistä varten.

HomeKit ja Apple TV

Apple TV valmistellaan automaattisesti HomeKitin kanssa käyttöä varten, kun käyttäjä kirjautuu sisään iCloudiin. iCloud-tilillä on oltava käytössä kaksiosainen todennus. Apple TV ja omistajan laite vaihtavat tilapäiset julkiset Ed25519-avaimet iCloudin kautta. Kun omistajan laite ja Apple TV ovat samassa lähiverkossa, tilapäisiä avaimia käytetään paikallisessa verkossa toimivan yhteyden suojaamiseen Station-to-Station-protokollaa ja istuntokohtaisia avaimia käyttäen. Tässä prosessissa käytetään samaa todennusta ja salausta kuin iOS-, iPadOS- ja macOS-laitteen ja HomeKit-lisälaitteen välillä. Tätä suojattua paikallista yhteyttä käyttäen omistajan laite siirtää käyttäjän julkisen ja yksityisen Ed25519-avaimen parit Apple TV:lle. Sen jälkeen näitä avaimia käytetään suojaamaan viestintä Apple TV:n ja HomeKit-lisälaitteiden välillä sekä myös Apple TV:n ja muiden HomeKit-kotiin kuuluvien iOS-, iPadOS- ja macOS-laitteiden välillä.

Jos käyttäjällä ei ole useita laitteita eikä hän salli muille käyttäjille pääsyä kotiinsa, mitään HomeKitin tietoja ei siirretä iCloudiin.

Kotitiedot ja apit

Appien oikeutta käyttää kotitietoja hallitaan käyttäjän Tietosuoja-asetuksissa. Kun apit pyytävät kotitietoja, käyttäjää pyydetään sallimaan käyttö samoin kuten Yhteystietojen, Kuvien ja muiden iOS:n, iPadOS:n ja macOS:n tietolähteiden kanssa. Jos käyttäjä hyväksyy pyynnön, apit pääsevät huoneiden nimiin, lisälaitteiden nimiin, tietoon siitä, missä huoneessa mikäkin lisälaite on, sekä muihin tietoihin, jotka on lueteltu HomeKitin kehittäjädokumentaatiossa osoitteessa https://developer.apple.com/homekit/.

Paikallinen tietojen tallennus

HomeKit tallentaa tietoja kodeista, lisälaitteista, tilanteista ja käyttäjistä käyttäjän iOS-,iPadOS- ja macOS-laitteisiin. Nämä tallennettavat tiedot salataan käyttäen käyttäjän HomeKit-identiteetin avaimista johdettuja avaimia ja satunnaista noncea. Lisäksi HomeKit-tietojen tallennuksessa käytetään tietojen suojausluokkaa Suojattu ensimmäiseen käyttäjän todentamiseen saakka. HomeKitin tiedot varmuuskopioidaan ainoastaan salattuihin varmuuskopioihin, joten esimerkiksi USB:llä tallennetut salaamattomat varmuuskopiot Finderiin (macOS 10.15:ssä tai uudemmissa) tai iTunesiin (macOS 10.14:ssä tai vanhemmissa) eivät sisällä HomeKitin tietoja.

Reitittimien suojaaminen HomeKitiä käyttäen

HomeKitiä tukevien reitittimien avulla käyttäjät voivat parantaa kotiverkkonsa suojausta hallitsemalla HomeKit-lisälaitteiden Wi-Fi-yhteyttä paikallisverkkoon ja internetiin. Reitittimet myös tukevat todentamista PPSK-avaimella (yksityinen PSK), joten lisälaitteita voidaan lisätä Wi-Fi-verkkoon käyttämällä avainta, joka on lisälaitekohtainen ja joka voidaan perua tarpeen vaatiessa. PPSK-todentaminen parantaa suojausta, sillä Wi-Fin pääsalasanaa ei paljasteta lisälaitteille, ja reititin voi tunnistaa lisälaitteen suojatusti, vaikka se muuttaisi MAC-osoitteensa.

Koti-apilla käyttäjä voi määrittää pääsyrajoituksia lisälaiteryhmille seuraavasti:

- *Ei rajoitusta:* Rajoittamaton pääsy sallitaan internetiin ja paikallisverkkoon.
- *Automaattinen:* Tämä on oletusasetus. Pääsy internetiin ja paikallisverkkoon sallitaan lisälaitteen valmistajan Applelle toimittaman internetsivustojen ja paikallisporttien luettelon perusteella. Tämä luettelo sisältää kaikki sivustot ja portit, joita lisälaite tarvitsee toimiakseen normaalisti. (Ei rajoitusta -asetus on voimassa, kunnes tällainen luettelo on satavilla.)
- *Rajoita Kotiin:* Pääsy internetiin tai paikallisverkkoon sallitaan ainoastaan yhteyksille, joita HomeKit tarvitsee lisälaitteen löytämiseen ja hallitsemiseen paikallisverkosta (mukaan lukien kodin keskittimestä etäohjauksen tukemiseksi).

PPSK on vahva lisälaitekohtainen WPA2 Personal -salauslause, jonka HomeKit generoi automaattisesti. Se perutaan jos ja kun lisälaite myöhemmin poistetaan kodista. PPSK:ta käytetään, kun lisälaite lisätään HomeKitillä Wi-Fi-verkkoon kodissa, johon on määritetty HomeKit-reititin; tästä lisäyksestä kertoo Wi-Fi-tunnistetieto: Hallitaan HomeKitillä lisälaitteen asetusnäytössä Koti-apissa. Lisälaitteet, jotka on lisätty Wi-Fi-verkkoon ennen reitittimen lisäämistä, määritetään uudelleen käyttämään PPSK:ta, jos lisälaite tukee sitä. Muussa tapauksessa ne pitävät olemassa olevat tunnistetietonsa.

Lisäsuojaustoimena käyttäjien täytyy määrittää HomeKit-reititin reitittimen valmistajan apilla, jotta appi voi vahvistaa, että käyttäjillä on pääsy reitittimeen ja että he voivat lisätä sen Koti-appiin.

HomeKit-kameran suojaus

Kamerat, joilla on HomeKitissä IP-osoite, lähettävät suoratoistona videota ja ääntä suoraan lähiverkossa olevalle, suoratoistovirtaan pääsevälle iOS-, iPadOS-, tvOS- ja macOS-laitteelle. Suoratoistovirrat salataan käyttäen laitteessa ja IP-kamerassa satunnaisesti muodostettuja avaimia, ja avaimet vaihdetaan suojatussa HomeKit-istunnossa kameran kanssa. Kun laite ei ole lähiverkossa, salatut suoratoistovirrat välitetään laitteelle kodin keskittimen kautta. Kodin keskitin ei pura salausta, vaan se toimii vain välittäjänä laitteen ja IP-kameran välillä. Kun appi näyttää HomeKit-IP-kameran videonäkymän käyttäjälle, HomeKit hahmontaa videokehykset suojatusti erillisestä järjestelmäprosessista. Näin ollen appi ei pääse videovirtaan eikä voi tallentaa sitä. Appien ei myöskään sallita tehdä kuvakaappauksia suoratoistovirrasta.

HomeKitin suojattu video

HomeKit tarjoaa päästä päähän suojatun ja yksityisen tavan tallentaa, analysoida ja katsella klippejä HomeKit-IP-kameroiden avulla siten, että Apple tai kolmannet osapuolet eivät voi nähdä tätä videosisältöä. Kun IP-kamera havaitsee liikettä, videoklipit lähetetään suoraan kodin keskittimenä toimivaan Apple-laitteeseen keskittimen ja IP-kameran välisen, erillisen paikallisverkkoyhteyden kautta. Lähiverkkoyhteys salataan istuntokohtaisella HKDF-SHA512:lla muodostetulla avainparilla, joka neuvotellaan HomeKit-istunnossa kodin keskittimen ja IP-kameran välillä. HomeKit purkaa ääni- ja videovirran salauksen kodin keskittimessä ja analysoi videokehykset paikallisesti merkittävien tapahtumien havaitsemiseksi. Jos merkittävä tapahtuma havaitaan, HomeKit salaa videoklipin AES-256-GCM:llä ja satunnaisesti generoidulla AES256-avaimella. HomeKit myös generoi jokaiselle klipille tunnistekuvan, jotka salataan samalla AES256-avaimella. Salattu tunnistekuva sekä ääni- ja videotiedot lähetetään iCloud-palvelimille. Jokaisen klipin metadata, salausavain mukaan lukien, lähetetään CloudKitiin iCloudin päästä-päähän-salauksella.

HomeKit tallentaa kaikki tietyn henkilön kasvojen luokittelua varten käytettävät tiedot CloudKitiin käyttäen päästä päähän -salausta. Tallennetut tiedot sisältävät tietoja jokaisesta henkilöstä, kuten nimen, sekä henkilön kasvoja edustavia kuvia. Näitä kasvokuvia voidaan hankkia käyttäjän Kuvat-apista, jos hän valitsee niin, tai niitä voidaan kerätä aikaisemmin analysoidusta IP-kameran videomateriaalista. HomeKitin suojatun videon analyysi-istunto käyttää tätä luokittelutietoa kasvojen tunnistamiseen suojatusta videovirrasta, jonka se saa suoraan IP-kamerasta, ja sisällyttää tunnistustiedon edellä käsiteltyyn leikkeen metadataan.

Kun Koti-appia käytetään tietyn kameran klippien katselemiseen, tiedot ladataan iCloudista ja virtojen salauksen purkamiseen tarvittavat avaimet avataan paikallisesti iCloudin päästä-päähän-salauksella. Salattu videosisältö suoratoistetaan palvelimilta, ja sen salaus puretaan paikallisesti iOS-laitteessa ennen kuin sisältö näytetään katseluikkunassa. Jokainen videoklippi-istunto voidaan jakaa alaosioihin siten, että kukin alaosio salaa sisällön omalla yksilöllisellä avaimellaan.

HomeKitin suojaus Apple TV:n kanssa

HomeKit yhdistää suojatusti joitakin muiden valmistajien kaukosäädinlisälaitteita Apple TV:hen ja tukee käyttäjäprofiilien lisäämistä kodin omistajan Apple TV:hen.

Muiden valmistajien kaukosäädinlisälaitteiden käyttäminen Apple TV:n kanssa

Jotkin muiden valmistajien kaukosäädinlisälaitteet toimittavat HID-laitetapahtumia (Human Interface Design) ja Siri-ääntä yhdistetylle Apple TV:lle, joka on lisätty käyttäen Koti-appia. Kaukosäädin lähettää HID-tapahtumat suojatussa istunnossa Apple TV:lle. Siriä tukeva TV-kaukosäädin lähettää äänidataa Apple TV:lle, kun käyttäjä nimenomaisesti aktivoi kaukosäätimen mikrofonin käyttämällä erityistä Siri-painiketta. Kaukosäädin lähettää äänikehykset suoraan Apple TV:lle käyttäen tähän tarkoitukseen varattua yhteyttä lähiverkossa. Lähiverkkoyhteys salataan istuntokohtaisella HKDF-SHA512:lla muodostetulla avainparilla, joka neuvotellaan HomeKit-istunnossa Apple TV:n ja TV-kaukosäätimen välillä. HomeKit purkaa äänikehysten salauksen Apple TV:ssä ja välittää ne Siri-appiin, missä niihin sovelletaan samoja tietosuojatoimia kuin kaikkeen Sirin äänisyötteeseen.

Apple TV -profiilit HomeKit-kodeille

Kun HomeKit-kodin käyttäjä lisää profiilinsa kodin omistajan Apple TV:hen, käyttäjä saa siinä pääsyn TV-ohjelmiinsa, musiikkiinsa ja podcasteihinsa. Kunkin käyttäjän profiilin Apple TV:ssä käyttämistä koskevat asetukset jaetaan omistajan iCloud-tilille käyttäen iCloudin päästä päähän -salausta. Kukin käyttäjä omistaa tietonsa, ja ne jaetaan omistajalle vain luku -muodossa. Kukin kodin käyttäjä voi muuttaa näitä arvoja Koti-apissa, ja omistajan Apple TV käyttää näitä asetuksia.

Kun asetus on päällä, käyttäjän iTunes-tili on saatavilla Apple TV:ssä. Kun asetus laitetaan pois päältä, kyseisen käyttäjän tili ja kaikki hänen tietonsa poistetaan Apple TV:stä. Alussa käyttäjän laite aloittaa CloudKit-jaon, ja suojatun CloudKit-jaon muodostamiseen tarvittava merkki lähetetään käyttäen samaa suojattua kanavaa, jota käytetään tietojen synkronoimiseen käyttäjien ja kodin välillä.

SiriKitin suojaus iOS:lle, iPadOS:lle ja watchOS:lle

Siri käyttää appilaajennusjärjestelmää viestinnässä muiden valmistajien appien kanssa. Laitteessa Siri pääsee käyttäjän yhteystietoihin ja laitteen nykyiseen sijaintiin. Ennen kuin se antaa suojattuja tietoja apille, Siri kuitenkin tarkistaa käyttäjän hallitsemat apin käyttöoikeudet. Siri antaa ainoastaan näiden oikeuksien mukaisen asiaankuuluvan osan käyttäjän alkuperäisestä lausahduksesta appilaajennukselle. Esimerkiksi jos apilla ei ole oikeutta käyttää yhteystietoja, Siri ei ratkaise suhdetta sellaisessa käyttäjän pyynnössä kuten ”Maksa äidilleni 10 euroa käyttäen maksuappia.” Tässä tapauksessa appi näkee vain sanan ”äidilleni” sellaisenaan.

Jos kuitenkin käyttäjä on sallinut apin käyttää yhteystietoja, appi saa ratkaistun tiedon käyttäjän äidistä. Jos suhde nimetään viestin tekstiosassa, kuten ”Kerro äidilleni MessageApissa, että veljeni on huipputyyppi”, Siri ei ratkaise sitä, kuka on ”veljeni”, riippumatta apin oikeuksissa.

SiriKitiä tukevat apit voivat lähettää Sirille appikohtaista tai käyttäjäkohtaista sanastoa kuten käyttäjän yhteystietojen nimet. Tämän tiedon avulla Sirin puheentunnistus ja luonnollisen kielen ymmärtäminen pystyvät tunnistamaan sanastoa kyseistä appia varten, ja se yhdistetään satunnaiseen tunnisteeseen. Nämä yksittäisen apin tiedot ovat saatavilla niin kauan kuin tunniste on käytössä tai kunnes käyttäjä poistaa apin Siri-integraation käytöstä Asetuksissa tai kunnes kyseisen SiriKitiä tukevan apin asennus poistetaan.

Jos käyttäjä esimerkiksi sanoo ”Hanki kyyti äitini kotiin käyttäen RideShareAppia”, pyyntö vaatii sijaintitietoja käyttäjän yhteystiedoista. Siri antaa ainoastaan tätä pyyntöä varten vaadittavat tiedot appilaajennukselle riippumatta käyttäjän apille asettamista oikeuksista sijainti- tai yhteystietojen käyttöön.

DriverKitin suojaus macOS:lle

DriverKit on sovelluskehys, jonka avulla kehittäjät voivat luoda laiteajureita, jotka käyttäjä asentaa Maciin. DriverKitiä käyttäen tehdyt ajurit suoritetaan käyttäjän tilassa eikä kernelin laajennuksina, mikä parantaa järjestelmän vakautta ja suojausta. Tämä helpottaa asentamista ja parantaa macOS:n vakautta ja suojausta.

Käyttäjä yksinkertaisesti lataa apin (asentajia ei tarvita, kun käytetään järjestelmälaajennuksia tai DriverKitiä), ja laajennuksen toiminta sallitaan vain, kun sitä vaaditaan. Nämä korvaavat kernelin laajennukset monissa sellaisissa tapauksissa, joissa vaaditaan ylläpitäjän oikeuksia asentamiselle kansioon /Järjestelmä/Kirjasto tai /Kirjasto.

IT-ylläpitäjille, jotka käyttävät laiteajureita, pilvitallennusratkaisuja, verkkoja ja tietoturva-appeja, jotka vaativat kernelin laajennuksia, suositellaan siirtymistä uudempiin järjestelmälaajennuksille rakentuviin versioihin. Nämä uudemmat versiot pienentävät huomattavasti kernel panic -virheiden mahdollisuutta Macissa ja vähentävät hyökkäyspintaa. Nämä uudet laajennukset suoritetaan käyttäjän tilassa, niiden asentaminen ei vaadi erikoisoikeuksia ja ne poistetaan automaattisesti, kun appi, jolle ne kuuluvat, siirretään roskakoriin.

DriverKit-sovelluskehys tarjoaa C++-luokat I/O-siirtopalveluille, laitteiden yhdistämiselle tietoihin, muistin asiasanoille ja lähetysjonoille. Se myös määrittelee I/O-siirroille sopivat tyypit numeroille, kokoelmille, merkkijonoille ja muille tavallisille tyypeille. Käyttäjä käyttää näitä perhekohtaisten ajurisovelluskehysten kuten USBDriverKitin ja HIDDriverKitin kanssa. Käytä järjestelmälaajennussovelluskehystä ajurin asentamisen ja päivittämiseen.

ReplayKitin suojaus iOS:ssä ja iPadOS:ssä

ReplayKit on sovelluskehys, jota käyttäen kehittäjät voivat lisätä appeihinsa elokuvatallennus- ja livelähetysominaisuuksia. Lisäksi se mahdollistaa käyttäjälle huomautusten tekemisen tallenteisiin ja lähetyksiin käyttäen etukameraa ja mikrofonia.

Elokuvan tallentaminen

Elokuvan tallentamisessa on monikerroksinen suojaus:

- *Oikeusvalintaikkuna:* Ennen kuin tallennus alkaa, ReplayKit näyttää käyttäjälle suostumusta pyytävän ilmoitusviestin, jossa käyttäjän tulee vahvistaa aikovansa tallentaa näytöllä, mikrofonilla ja etukameralla. Tämä ilmoitusviesti näytetään yhden kerran appiprosessia kohden, ja se esitetään uudelleen, jos appi jätetään taustalle yli 8 minuutiksi.
- *Näytön ja äänen tallentaminen:* Näytön ja äänen tallentaminen tapahtuu apin prosessin ulkopuolella ReplayKitin palveluprosessissa nimeltä replayd. Tämä on suunniteltu varmistamaan, että apin prosessi ei koskaan pääse tallennettuun sisältöön.
- *Apin sisäinen näytön ja äänen tallentaminen:* Tämä sallii apin saada video- ja näytepuskureita, joita suojataan oikeusvalintaikkunalla.
- *Elokuvan luominen ja tallennustila:* Elokuvatiedosto kirjoitetaan hakemistoon, johon pääsevät vain ReplayKitin alijärjestelmät eivätkä koskaan mitkään apit. Tämä auttaa estämään kolmansia osapuolia käyttämästä tallenteita ilman käyttäjän suostumusta.
- *Loppukäyttäjän esikatselu ja jakaminen:* Käyttäjä voi esikatsella ja jakaa elokuvaa ReplayKitin myymällä käyttöliittymällä. Käyttöliittymä esitetään prosessin ulkopuolella iOS-laajennusinfrastruktuurin kautta, ja se pääsee luotuun elokuvatiedostoon.

ReplayKit-lähetys

Elokuvan lähettämisessä on monikerroksinen suojaus:

- *Näytön ja äänen tallentaminen:* Näytön ja äänen tallentamismekanismi lähetyksen aikana on samanlainen kuin elokuvaa tallennettaessa, ja se tapahtuu `replayd`-palveluprosessissa.
- *Lähetyslaajennukset:* Osallistuakseen ReplayKit-lähetyksiin kolmannen osapuolen palveluiden täytyy luoda kaksi uutta laajennusta, jotka määritellään käyttäen päätepistettä com.apple.broadcast-services:
  - Käyttöliittymälaajennus, jolla käyttäjä voi määrittää lähetyksen
  - Latauslaajennus, joka käsittelee video- ja äänidatan lataamisen palvelun taustapalvelimille

Arkkitehtuuri auttaa varmistamaan, että isännöivillä apeilla ei ole oikeuksia lähetettävään video- ja äänisisältöön. Vain ReplayKitillä ja muun valmistajan lähetyslaajennuksilla on käyttöoikeus.

- *Lähetysvalitsin:* Lähetysvalitsimen avulla käyttäjä käynnistää järjestelmän lähetyksen suoraan apista käyttäen samaa järjestelmän määrittelemää käyttöliittymää, johon pääsee Ohjauskeskuksesta. Käyttöliittymä toteutetaan käyttäen yksityistä rajapintaa, ja se on ReplayKit-sovelluskehyksessä toimiva laajennus. Se on isännöivän apin prosessin ulkopuolella.

- *Latauslaajennus:* Laajennus, jota kolmannen osapuolen lähetyspalvelut käyttävät video- ja äänisisällön käsittelemiseen lähetyksen aikana, käyttää koodaamattomien näytteiden puskureita. Tämän käsittelytavan aikana video- ja äänidata sarjoitetaan ja annetaan kolmannen osapuolen latauslaajennukselle reaaliajassa suoran XPC-yhteyden kautta. Videodata koodataan erottamalla IOSurface-objekti videonäytepuskurista, koodaamalla se suojatusti XPC-objektina, lähettämällä XPC:n kautta kolmannen osapuolen laajennukseen ja dekoodaamalla suojatusti takaisin IOSurface-objektiksi.

ARKitin suojaus iOS:ssä ja iPadOS:ssä

ARKit on sovelluskehys, jolla kehittäjät voivat tuottaa lisätyn todellisuuden kokemuksia apissaan tai pelissään. Kehittäjät voivat lisätä kaksi- tai kolmiulotteisia elementtejä käyttäen iOS- tai iPadOS-laitteen etu- tai takakameraa.

Apple on kiinnittänyt huomiota tietosuojaan kameroita suunnitellessaan, ja muiden valmistajien appien on saatava suostumus käyttäjältä, ennen kuin ne voivat käyttää kameraa. iOS:ssä ja iPadOS:ssä apit, joille käyttäjä sallii kameran käytön, pääsevät reaaliajassa etu- ja takakameroiden kuviin. Appien ei sallita käyttää kameraa, jos ne eivät tee sitä läpinäkyvästi.

Kameralla kuvatut valokuvat ja videot voivat sisältää muita tietoja, kuten kuvausajan ja -paikan, terävyysalueen ja 360 asteen näkymän. Jos käyttäjät eivät halua Kamera-apilla otettujen kuvien ja videoiden sisältävän sijaintia, he voivat milloin tahansa hallita tätä asetusta valitsemalla Asetukset > Tietosuoja > Sijaintipalvelut > Kamera. Jos käyttäjät eivät halua, että kuviin ja videoihin sisältyy sijainti, kun ne jaetaan, he voivat laittaa sijainnin pois päältä jakoikkunan Valinnat-valikossa.

ARKitiä käyttävät apit voivat käyttää ympäristön tai kasvojen seurantatietoja toisesta kamerasta pystyäkseen sijoittamaan käyttäjän lisätyn todellisuuden kokemuksen paremmin. Ympäristön seuranta prosessoi algoritmien avulla käyttäjän laitteessa antureista saatavaa tietoa määrittääkseen niiden sijainnin suhteessa fyysiseen tilaan. Ympäristön seuranta mahdollistaa sellaisia ominaisuuksia kuin optinen suunta Kartoissa.

Suojattu laitehallinta

Suojatun laitehallinnan yleiskatsaus

iOS, iPadOS, macOS ja tvOS tukevat joustavia tietoturvakäytäntöjä ja -määrityksiä, joita on helppo toteuttaa ja hallita. Niiden avulla organisaatiot voivat suojata yritystietoja ja ne auttavat varmistamaan, että työntekijät noudattavat yrityksen vaatimuksia silloinkin, kun he käyttävät omia laitteitaan esimerkiksi osana BYOD-ohjelmaa (”bring your own device”).

Organisaatiot voivat käyttää resursseja, kuten salasanan suojaus, asetusprofiilit, etätyhjennys ja muun valmistajan mobiililaitteiden hallintaratkaisuja (MDM), laitekannan hallitsemiseen ja yritystietojen suojaamiseen myös silloin, kun työntekijät käyttävät näitä tietoja omilla laitteillaan.

iOS 13:n tai uudemman, iPadOS 13.1:n tai uudemman ja macOS 10.15:n tai uudemman myötä Applen laitteet tukevat uutta käyttäjärekisteröinnin vaihtoehtoa, joka on suunniteltu erityisesti BYOD-ohjelmia varten. Käyttäjärekisteröinti tarjoaa omia laitteitaan käytäville työntekijöille enemmän itsenäisyyttä samalla, kun se lisää yritystietojen suojausta tallentamalla ne erilliseen, kryptografisesti salattuun APFS (Apple File System) -taltioon. Näin parannetaan tasapainoa suojauksen, yksityisyyden ja käyttökokemuksen välillä BYOD-ohjelmissa.

Laiteparin muodostamisen mallin suojaus iPhonelle ja iPadille

iOS ja iPadOS käyttävät laiteparin muodostamisen mallia, jolla hallitaan pääsyä laitteelle isäntätietokoneesta. Laiteparin muodostaminen luo laitteen ja siihen yhdistetyn isännän välille luottamussuhteen, joka ilmenee julkisten avainten vaihtona. iOS ja iPadOS käyttävät tätä luottamuksen merkkiä myös ottaakseen käyttöön yhdistetyn isännän lisäominaisuuksia, kuten tietojen synkronointi. iOS 9:ssä tai uudemmissa:

- laiteparin muodostamista vaativia palveluita ei käynnistetä ennen kuin käyttäjä on avannut laitteen lukituksen
- palveluita ei käynnistetä, ellei laitteen lukitusta ole äskettäin avattu
- palvelut (kuten kuvien synkronointi) saattavat vaatia käynnistyäkseen laitteen lukituksen avaamisen.

Laiteparin muodostusprosessi vaatii, että käyttäjä avaa laitteen lukituksen ja hyväksyy isännän pyynnön. iOS 9:ssä ja uudemmissa käyttäjän on myös syötettävä pääsykoodinsa, minkä jälkeen isäntä ja laite vaihtavat ja tallentavat julkiset 2048 bitin RSA-avaimet. Isännälle annetaan 256 bitin avain, jolla voidaan avata laitteessa oleva avainvarastotallenne. Vaihdetuilla avaimilla aloitetaan salattu SSL-istunto, jonka laite vaatii ennen kuin se lähettää suojattua dataa isännälle tai käynnistää palvelun (iTunes- tai Finder-synkronointi, tiedostonsiirrot, Xcode-kehittäminen ja niin edelleen). Jotta laite voi käyttää tätä salattua istuntoa kaikkeen viestintään, se vaatii Wi-Fi-yhteyden isännästä. Laiteparin muodostaminen on täytynyt tapahtua aiemmin USB-yhteyden kautta. Laiteparin muodostaminen mahdollistaa useita vianmääritysominaisuuksia. iOS 9:ssä laitepari raukeaa, jos sitä ei ole käytetty yli kuuteen kuukauteen. iOS 11:ssä ja uudemmissa tämä aika on lyhennetty 30 päivään.

Tietyt vianmääritypalvelut, kuten com.apple.mobile.pcapd, on rajoitettu toimimaan vain USB:n kautta. Lisäksi com.apple.file_relay-palvelu vaatii Applen allekirjoittaman asetusprofiilin asentamisen. iOS 11:ssä tai uudemmissa Apple TV voi käyttää Secure Remote Password -protokollaa laiteparin määrittämiseen langattomasti.

Käyttäjä voi tyhjentää luotettujen isäntien luettelon Nollaa verkkoasetukset- ja Nollaa sijainti ja tietosuoja -valinnoilla.

Mobiililaitteiden hallinta

Mobiililaitteiden hallinnan suojauksen yleiskatsaus

Applen käyttöjärjestelmät tukevat mobiililaitteiden hallintaa (MDM), minkä ansiosta organisaatiot voivat turvallisesti määrittää ja hallita skaalattuja Apple-laitteiden käyttöönottoja.

Miten MDM toimii suojatusti

MDM-ominaisuudet rakentuvat olemassa oleville käyttöjärjestelmäteknologioille, joita ovat esimerkiksi asetusprofiilit, langaton rekisteröinti ja Applen push-ilmoituspalvelu (APNs). Esimerkiksi APNs:ää käytetään laitteen herättämiseksi, jotta se voi viestiä suoraan MDM-ratkaisun kanssa suojatulla yhteydellä. APNs:llä ei lähetetä luottamuksellisia tai omisteisia tietoja.

MDM:n avulla IT-osastot voivat rekisteröidä Applen laitteita yritysympäristössä, määrittää ja päivittää asetuksia langattomasti, valvoa yrityksen käytäntöjen noudattamista, hallita ohjelmistopäivityskäytäntöjä ja jopa tyhjentää tai lukita hallittuja laitteita etänä.

iOS:n, iPadOS:n, macOS:n ja tvOS:n tukemien perinteisten laiterekisteröintien lisäksi iOS 13:ssa ja uudemmissa, iPadOS 13.1:ssä ja uudemmissa ja macOS 10.15:ssä ja uudemmissa on uusi rekisteröintityyppi – käyttäjärekisteröinti. Käyttäjärekisteröinnit ovat erityisesti BYOD-käyttöönotoissa hyödynnettäviä MDM-rekisteröintejä, joissa laite on henkilökohtaisessa omistuksessa, mutta sitä käytetään hallitussa ympäristössä. Käyttäjärekisteröinnit sallivat MDM-ratkaisulle rajoitetummat oikeudet kuin valvomattomien laitteiden rekisteröinnit ja erottavat käyttäjän ja yrityksen tiedot kryptografisesti.

Rekisteröintityypit

- *Automatisoitu laiterekisteröinti:* Automatisoidun laiterekisteröinnin avulla organisaatiot voivat määrittää ja hallita laitteita siitä hetkestä lähtien, kun ne otetaan pakkauksista (prosessissa jota kutsutaan *käyttöönotoksi automaattisilla ennakkomäärityksillä*). Näitä laitteita kutsutaan *valvotuiksi*, ja käyttäjää voidaan estää poistamasta MDM-profiilia niistä. Automatisoitu laiterekisteröinti on suunniteltu käyttäjän organisaation omistamia laitteita varten.
- *Laiterekisteröinti:* Laiterekisteröintiä käytettäessä organisaatiot voivat antaa käyttäjien rekisteröidä laitteita käsin, ja sitten organisaatiot voivat hallita niiden käyttöä monella tapaa, mukaan lukien laitteen tyhjentäminen. Laiterekisteröinti myös tarjoaa käyttöön enemmän tietosisältöjä ja rajoituksia laitteelle. Kun käyttäjä poistaa rekisteröintiprofiilin, kaikki rekisteröintiprofiiliin perustuvat asetusprofiilit, niiden asetukset ja hallitut apit poistetaan sen mukana.
- *Käyttäjärekisteröinti:* Käyttäjärekisteröinti on suunniteltu käyttäjän omistamia laitteita varten ja integroitu hallittujen Apple ID:n kanssa käyttäjän henkilöllisyyden määrittämiseksi. Hallitut Apple ID:t ovat osa käyttäjärekisteröintiprofiilia, ja rekisteröinti edellyttää käyttäjän todennusta. Hallittuja Apple ID:itä voidaan käyttää käyttäjän henkilökohtaisen, sisäänkirjautumiseen käyttämän Apple ID:n rinnalla. Hallitut apit ja tilit käyttävät hallittua Apple ID:tä, ja henkilökohtaiset apit ja tilit käyttävät henkilökohtaista Apple ID:tä.

Laiterajoitukset

Ylläpitäjät voivat ottaa käyttöön – ja joissakin tapauksissa poistaa käytöstä – rajoituksia, jotka auttavat estämään käyttäjiä käyttämästä tiettyä appia, palvelua tai toimintoa iPhonessa, iPadissa, Macissa tai Apple TV:ssä, joka on rekisteröity MDM-ratkaisuun. Rajoitukset lähetetään laitteeseen rajoitustietosisällössä, joka osa asetusprofiilia. Joitakin iPhonen rajoituksia voidaan peilata pariksi asetetussa Apple Watchissa.

Pääsykoodi- ja salasana-asetusten hallinta

Oletuksena käyttäjän pääsykoodi määritetään numeerisena PIN-koodina. iOS- ja iPadOS-laitteissa, joissa on Face ID tai Touch ID, pääsykoodin minimipituus on neljä numeroa. Pidempiä ja monimutkaisempia pääsykoodeja on vaikeampi arvata ja niihin on vaikeampi kohdistaa hyökkäys, ja siksi niitä suositellaankin.

Ylläpitäjät voivat pakottaa monimutkaisempien pääsykoodien vaatimuksia ja muita käytäntöjä MDM:n tai Microsoft Exchange ActiveSyncin avulla tai edellyttämällä, että käyttäjät asentavat asetusprofiileja käsin. Ylläpitäjän salasana vaaditaan, jotta macOS-pääsykoodikäytäntöjen tietosisältö voidaan asentaa. Jotkin pääsykoodikäytännöt voivat vaatia pääsykoodilta tiettyä pituutta, rakennetta tai muita ominaisuuksia.

Asetusprofiilin käyttäminen

Asetusprofiilit ovat ensisijainen keino, jolla MDM-ratkaisu toimittaa ja hallitsee käytäntöjä ja rajoituksia hallituissa laitteissa. Jos organisaatioiden tarvitsee määrittää suuri joukko laitteita tai antaa runsaasti muokattuja sähköpostiasetuksia, verkkoasetuksia tai varmenteita suurelle joukolle laitteita, asetusprofiilit ovat siihen turvallinen ja varma ratkaisu.

Asetusprofiilit

Asetusprofiili on XML-tiedosto (jonka pääte on .mobileconfig). Se koostuu tietosisällöistä, jotka lataavat Applen laitteisiin asetuksia ja valtuutustietoja. Asetusprofiilit automatisoivat asetusten, tilien, rajoitusten ja tunnistetietojen määrittämisen. Näitä tiedostoja voidaan luoda MDM-ratkaisulla tai Macin Apple Configuratorilla tai käsin. Ennen kuin organisaatiot lähettävät Applen laitteeseen asetusprofiilin, laite on rekisteröitävä MDM-ratkaisuun käyttäen rekisteröintiprofiilia.

Rekisteröintiprofiilit

Rekisteröintiprofiili on MDM-tietosisällön sisältävä asetusprofiili, joka rekisteröi laitteen sille määritettyyn MDM-ratkaisuun. Tällöin MDM-ratkaisu voi lähettää komentoja ja asetusprofiileja laitteelle ja kysellä siltä määrättyjä tietoja. Kun käyttäjä poistaa rekisteröintiprofiilin, kaikki rekisteröintiprofiiliin perustuvat asetusprofiilit, niiden asetukset ja hallitut apit poistetaan sen mukana. Laitteessa voi olla vain yksi rekisteröintiprofiili kerralla.

Asetusprofiilin asetukset

Asetusprofiili sisältää useita asetuksia tietyissä tietosisällöissä, jotka voidaan määrittää, mukaan lukien (mutta niihin rajoittumatta):

- pääsykoodi- ja salasanakäytännöt
- laiteominaisuuksien rajoitukset (esimerkiksi kameran poistaminen käytöstä)
- verkko- ja VPN-asetukset
- Microsoft Exchange -asetukset
- sähköpostiasetukset
- tiliasetukset
- LDAP-hakemistopalveluasetukset
- CalDAV-kalenteripalveluasetukset
- tunnistetiedot ja avaimet
- ohjelmistopäivitykset

Profiilin allekirjoitus ja salaus

Allekirjoittamalla asetusprofiilit voidaan validoida niiden alkuperä ja salaamalla ne voidaan auttaa varmistamaan niiden eheys ja suojaamaan niiden sisältö. iOS:n ja iPadOS:n asetusprofiilit salataan CMS:llä (Cryptographic Message Syntax), joka on määritetty RFC 5652:ssa ja joka tukee 3DES:ää ja AES128:aa.

Profiilien asentaminen

Käyttäjät voivat asentaa asetusprofiileja suoraan laitteisiinsa Macin Apple Configuratorilla. Ne voidaan myös ladata Safarilla, lähettää sähköpostiviestin liitteenä, siirtää AirDropilla tai iOS:n ja iPadOS:n Tiedostot-apilla tai lähettää langattomasti mobiililaitteiden hallintaratkaisulla (MDM). Kun käyttäjä ottaa laitteen käyttöön Apple School Managerissa tai Apple Business Manager, laite lataa ja asentaa profiilin MDM-rekisteröitymistä varten. Jos haluat tietoja siitä, miten profiilit poistetaan, katso Johdatus mobiililaitteiden hallintaan Apple-alustojen käyttöönotossa.

Huomaa: Valvotuissa laitteissa asetusprofiilit voidaan myös lukita laitteeseen. Tämä on suunniteltu estämään niiden poistamista tai sallimaan poistaminen vain pääsykoodilla. Koska monet organisaatiot omistavat iOS- ja iPadOS-laitteensa, laitteen MDM-ratkaisuun sitovat asetusprofiilit voidaan poistaa, mutta silloin myös kaikki hallitut määritystiedot, data ja apit poistetaan.

Automatisoitu laiterekisteröinti

Organisaatiot voivat rekisteröidä iOS-, iPadOS-, macOS- ja tvOS-laitteita automaattisesti mobiililaitteen hallintaan (MDM) ilman, että laitteita täytyy käsitellä tai valmistella fyysisesti ennen kuin ne annetaan käyttäjille. Kun ylläpitäjät ovat rekisteröityneet johonkin palveluista, he kirjautuvat palveluun verkkosivustolle ja linkittävät ohjelman MDM-ratkaisuun. Heidän ostamansa laitteet voidaan sitten määrittää käyttäjille MDM:llä. Laitteen määritysprosessin aikana arkaluontoisten tietojen suojausta voidaan lisätä varmistamalla, että asianmukaiset suojaustoimenpiteet on suoritettu. Esimerkiksi:

- Käyttäjät suorittavat todennuksen Apple-laitteen käyttöönottoapurissa laitetta aktivoidessaan.
- Käyttäjille tarjotaan esimääritykset, jotka rajoittavat pääsyoikeuksia ja vaativat laitteen lisämäärityksiä arkaluontoisiin tietoihin pääsemiseksi.

Kun käyttäjä on määritetty, voidaan MDM:n määrityksiä ja rajoituksia asentaa automaattisesti. Kaikki viestintä laitteiden ja Applen palvelimien välillä salataan liikkeessä HTTPS:llä (TLS).

Käyttöönottoprosessia voidaan entisestään selkeyttää käyttäjille poistamalla tiettyjä käyttöönottoapurin vaiheita laitteille, jolloin käyttäjät voivat ryhtyä nopeasti toimeen. Ylläpitäjät voivat myös hallita sitä, voivatko käyttäjät poistaa MDM-profiilin laitteesta, ja auttaa varmistamaan, että laiterajoitukset ovat voimassa koko laitteen elinkaaren ajan. Kun laite on otettu pakkauksesta ja aktivoitu, se voi rekisteröityä organisaation MDM-ratkaisuun. Kaikki hallinta-asetukset, apit ja kirjat asennetaan MDM-ylläpitäjän määritysten mukaisesti.

Apple School Manager, Apple Business Manager ja Apple Business Essentials

Apple School Manager, Apple Business Manager ja Apple Business Essentials ovat palveluita, joilla IT-ylläpitäjät voivat ottaa käyttöön Applen laitteita, jotka organisaatio on ostanut suoraan Applelta tai ohjelmaan osallistuvalta Applen valtuutetulta jälleenmyyjältä tai operaattorilta.

Kun niitä käytetään yhdessä MDM-ratkaisun kanssa, ylläpitäjät voivat tehdä käyttöönottoprosessin yksinkertaisemmaksi käyttäjille, määrittää laitteiden asetuksia ja jaella näissä kolmessa palvelussa ostettuja appeja ja kirjoja. Apple School Manageriin voi myös integroida oppilastietojärjestelmiä (SIS) joko suoraan tai SFTP:tä käyttäen, ja kaikki kolme palvelua voivat käyttää SCIM-järjestelmää (System for Cross-domain Identity Management) tai Microsoft Azure Active Directoryn (Azure AD) kanssa federoitua todentamista, jotta ylläpitäjät voivat luoda tilit nopeasti.

Apple ylläpitää standardien ISO/IEC 27001 ja 27018 mukaisia sertifiointeja, jotta Applen asiakkaat voivat täyttää määräyksiin ja sopimuksiin perustuvat velvoitteensa. Sertifikaatit tarjoavat asiakkaillemme riippumattoman todistuksen Applen sertifioinnin piiriin kuuluvien järjestelmien tietosuoja- ja tietoturvakäytännöistä. Jos haluat lisätietoja, katso Applen internetpalveluiden tietoturvasertifioinnit Apple-alustojen sertifioinneissa.

Huomaa: Jos haluat tarkistaa, onko Applen ohjelma saatavilla tietyssä maassa tai tietyllä alueella, tutustu Applen tukiartikkeliin Applen oppilaitoksille ja yrityksille suunnattujen ohjelmien ja maksutapojen saatavuus.

Laitteen valvonta

Valvonta merkitsee yleensä, että laite on organisaation omistama, ja se tarjoaa organisaatioille enemmän hallintaa laitteen määritysten ja rajoitusten suhteen. Jos haluat lisätietoja, katso Tietoja Apple-laitteiden valvonnasta Apple-alustojen käyttöönotossa.

Aktivointilukitussuojaus

Se, miten Apple toteuttaa aktivointilukituksen, vaihtelee riippuen siitä, onko laite iPhone tai iPad, Apple siliconilla varustettu Mac vai Intel-pohjainen Mac, jossa on Apple T2 Security -siru.

Toiminta iPhonessa ja iPadissa

iPhonessa ja iPadissa aktivointilukitus toteutetaan aktivointiprosessilla Wi-Fi-verkon valintanäytön jälkeen iOS:n ja iPadOS:n käyttöönottoapurissa. Kun laite kertoo, että se aktivoituu, se lähettää pyynnön Applen palvelimelle saadakseen aktivointivarmenteen. Laitteet, jotka on lukittu aktivointilukituksella, pyytävät silloin käyttäjältä sen käyttäjän iCloud-tunnistetietoja, joka on ottanut aktivointilukituksen käyttöön. iOS:n ja iPadOS:n käyttöönottoapuri ei etene, ellei kelvollista varmennetta saada.

Toiminta Apple siliconilla varustetussa Macissa

Apple siliconilla varustetussa Macissa LLB tarkistaa, että laitteelle on olemassa kelvollinen LocalPolicy ja että LocalPolicy-käytännön nonce-arvot vastaavat Secure Storage -komponenttiin tallennettuja arvoja. LLB käynnistää recoveryOS:ään, jos:

- nykyiselle macOS:lle ei ole LocalPolicya
- LocalPolicy ei ole kelvollinen kyseiselle macOS:lle
- LocalPolicyn nonce-tiivistearvot eivät vastaa Secure Storage -komponenttiin tallennettuja arvoja

recoveryOS havaitsee, että Mac-tietokone ei ole aktivoitu ja yhdistää aktivointipalvelimeen aktivointivarmenteen saamista varten. Jos laitteella on aktivointilukitus, recoveryOS pyytää käyttäjältä tässä vaiheessa sen käyttäjän iCloud-tunnistetietoja, joka otti aktivointilukituksen käyttöön. Kun kelvollinen aktivointivarmenne on saatu, kyseisen aktivointivarmenteen avainta käytetään RemotePolicyn varmenteen saamista varten. Mac-tietokone käyttää LocalPolicyn avainta ja RemotePolicyn varmennetta kelvollisen LocalPolicyn tuottamiseen. LLB ei salli macOS:n käynnistämistä, jos kelvollinen LocalPolicy puuttuu.

Toiminta Intel-pohjaisissa Mac-tietokoneissa

Intel-pohjaisessa T2-sirulla varustetussa Macissa T2-sirun laiteohjelmisto tarkistaa, että kelvollinen aktivointivarmenne löytyy, ennen kuin sallii tietokoneelle käynnistyksen macOS:ään. T2-sirun lataama UEFI-laiteohjelmisto vastaa laitteen aktivointitilan kyselystä T2-sirulle sekä käynnistämisestä recoveryOS:ään macOS:n sijasta, jos kelvollinen aktivointivarmenne puuttuu. recoveryOS tunnistaa, että Mac ei ole aktivoitu, ja ottaa yhteyden aktivointipalvelimeen aktivointivarmenteen saamista varten. Jos laitteella on aktivointilukitus, recoveryOS pyytää käyttäjältä tässä vaiheessa sen käyttäjän iCloud-tunnistetietoja, joka otti aktivointilukituksen käyttöön. UEFI-laiteohjelmisto ei salli macOS:n käynnistämistä, jos kelvollinen aktivointivarmenne puuttuu.

Hallittu Kadonnut-tila ja etätyhjennys

Hallittua Kadonnut-tilaa käytetään varastettujen valvottujen laitteiden paikantamiseen. Kun ne on paikannettu, ne voidaan lukita tai tyhjentää etänä.

Hallittu Kadonnut-tila

Jos valvottu iOS- tai iPadOS-laite, jossa on iOS 9 tai uudempi, katoaa tai varastetaan, mobiililaitteiden hallinnan (MDM) ylläpitäjä voi ottaa laitteessa etänä käyttöön Kadonnut-tilan, jota kutsutaan hallituksi Kadonnut-tilaksi. Kun hallittu Kadonnut-tila otetaan käyttöön, käyttäjä kirjataan ulos laitteelta, ja laitteen lukitusta ei voida avata. Näytössä näkyy viesti, jota ylläpitäjä voi muokata. Viesti voi olla esimerkiksi numero, johon laitteen löytäjä voi soittaa. Ylläpitäjä voi pyytää laitetta lähettämään nykyisen sijaintinsa (vaikka Sijaintipalvelut olisi asetettu pois päältä) ja tarvittaessa myös soittamaan äänen. Kun ylläpitäjä laittaa hallitun Kadonnut-tilan pois päältä, mikä on ainoa tapa poistua tilasta, käyttäjälle ilmoitetaan siitä lukitulla näytöllä näkyvällä viestillä tai Koti-valikossa näkyvällä ilmoituksella.

Etätyhjennys

Ylläpitäjä tai käyttäjä voi tyhjentää iOS-, iPadOS- ja macOS-laitteet etänä (välitön etätyhjennys on saatavilla vain, jos Macissa on otettu käyttöön FileVault). Välitön etätyhjennys suoritetaan poistamalla tallennuslaiteavain suojatusti kohteesta Pyyhittävä tallennustila, jolloin kaikista tiedoista tulee lukukelvottomia. Microsoft Exchange ActiveSyncin kautta tapahtuvaa etätyhjennystä varten laite tarkistaa tilanteen Microsoft Exchange Serveriltä ennen kuin suorittaa tyhjennyksen.

Kun MDM tai iCloud käynnistää etätyhjennyskomennon, iPhone-, iPad-, iPod touch- tai Mac-laite lähettää kuittauksen MDM-ratkaisulle ja suorittaa tyhjennyksen.

Etätyhjennystä ei voida tehdä seuraavissa tilanteissa:

- käyttäjärekisteröintiä käytettäessä
- Microsoft Exchange ActiveSyncin avulla, jos tili asennettiin käyttäjärekisteröinnillä
- Microsoft Exchange ActiveSyncin avulla, jos laite on valvottu

Käyttäjät voivat myös tyhjentää käyttämänsä iOS- ja iPadOS-laitteet Asetukset-apilla. Kuten aikaisemmin on mainittu, iOS- ja iPadOS-laitteet voidaan asettaa tyhjentymään automaattisesti useiden epäonnistuneiden pääsykoodin syöttöyritysten jälkeen.

Jaetun iPadin suojaus iPadOS:ssä

Jaettu iPad on usean käyttäjän tila, joka voidaan valita iPadin käyttöönottotavaksi. Sitä käytettäessä käyttäjät voivat jakaa iPadin, mutta kunkin käyttäjän dokumentit ja tiedot pysyvät erillään. Jokaisella käyttäjällä on oma yksityinen, hänelle varattu tallennussijainti, joka toteutetaan APFS (Apple File System) -taltiona ja suojataan käyttäjän tunnisteella. Jaettu iPad vaatii organisaation myöntämän ja omistaman hallitun Apple ID:n käyttöä.

Käytettäessä jaettua iPadia käyttäjä voi kirjautua mihin tahansa organisaation omistamaan laitteeseen, joka on määritetty useiden käyttäjien käytettäväksi. Käyttäjien tiedot osioidaan erillisiin hakemistoihin, joista jokainen on omassa tietojen suojausdomainissaan ja suojattu sekä UNIX-oikeuksilla että eristämällä. iPadOS 13.4:ssä tai uudemmassa käyttäjät voivat myös kirjautua väliaikaiseen istuntoon. Kun käyttäjä kirjautuu ulos väliaikaisesta istunnosta, hänen APFS-taltionsa poistetaan, ja sille varattu tila palautetaan järjestelmälle.

Kirjautuminen jaettuun iPadiin

Sekä natiivit että federoidut hallitut Apple ID:t ovat tuettuja kirjauduttaessa jaettuun iPadiin. Kun federoitua tiliä käytetään ensimmäistä kertaa, käyttäjä uudelleenohjataan tunnistetietojen toimittajan kirjautumisportaaliin. Kun todentautuminen on suoritettu, taustalla toimiville hallituille Apple ID:ille myönnetään lyhytaikainen käyttötunnus, ja sisäänkirjautumisprosessi etenee natiivin hallitun Apple ID:n prosessin kaltaisesti. Kun kirjautuminen on suoritettu, jaetun iPadin käyttöönottoapuri kehottaa käyttäjää asettamaan pääsykoodin (tunnisteen), jolla laitteessa olevat paikalliset tiedot suojataan ja jolla kirjautumisnäytöllä voidaan todentautua jatkossa. Aivan kuten yhden käyttäjän laitteessa, jolla käyttäjä kirjautuu kerran hallittuun Apple ID:hensä käyttämällä federoitua tiliään ja sitten avaa laitteen lukituksen pääsykoodillaan, myös jaetulla iPadilla käyttäjä kirjautuu sisään kerran federoidulla tilillään ja käyttää sen jälkeen asettamaansa pääsykoodia.

Kun käyttäjä kirjautuu sisään ilman federoitua todentautumista, hallittu Apple ID todennetaan Apple Identity Service (IDS) -palvelulla SRP-protokollan avulla. Jos todentaminen onnistuu, laitteelle myönnetään lyhytaikainen käyttötunnus. Jos käyttäjä on käyttänyt samaa laitetta aiemmin, hänellä on jo paikallinen käyttäjätili, jonka lukitus avataan samalla tunnisteella.

Jos käyttäjä ei ole käyttänyt kyseistä laitetta aikaisemmin tai käyttää väliaikaista istuntoa, jaettu iPad provisioi uuden UNIX-käyttäjätunnuksen, APFS-taltion käyttäjän henkilökohtaisten tietojen tallennusta varten ja paikallisen avainnipun. Koska tallennustila kohdennetaan (varataan) käyttäjälle silloin, kun APFS-taltio luodaan, uuden taltion luomiselle ei välttämättä ole riittävästi tilaa. Tällaisessa tapauksessa järjestelmä valitsee olemassa olevan käyttäjän, jonka tiedot ovat ehtineet synkronoitua kokonaan pilveen, ja poistaa kyseisen käyttäjän laitteelta, jotta uusi käyttäjä voi kirjautua sisään. On epätodennäköistä, että kenenkään laitteella jo olevan käyttäjän tiedot eivät olisi ehtineet latautua kokonaan pilveen, mutta jos näin käy, uuden käyttäjän kirjautuminen epäonnistuu. Jotta uusi käyttäjä voi kirjautua sisään, on odotettava, että jonkun käyttäjän tietojen synkronointi saadaan suoritettua loppuun, tai ylläpitäjän on poistettava jokin olemassa oleva tili väkisin, jolloin tietoja saatetaan menettää.

Jos laite ei ole yhteydessä internetiin (esimerkiksi jos käyttäjällä ei ole käytettävissään Wi-Fi-tukiasemaa), todentautuminen voi tapahtua paikallisen tilin perusteella vain joidenkin päivien ajan. Siinä tapauksessa vain käyttäjät, joilla on olemassa olevat paikalliset tilit tai väliaikainen istunto, voivat kirjautua sisään. Kun aikaraja on rauennut, käyttäjiä vaaditaan todentautumaan verkossa, vaikka heillä olisi jo paikallinen tili.

Kun käyttäjä on avannut paikallisen tilin lukituksen tai tili on luotu paikallisesti, se yritetään todentaa palvelimella. Jos etätodennus onnistuu, Applen palvelimet antavat lyhytaikaisen käyttötunnuksen, josta saadaan iCloud-tunnus. Sillä laite pääsee kirjautumaan iCloudiin. Seuraavaksi käyttäjän asetukset palautetaan ja hänen dokumenttinsa ja tietonsa synkronoidaan iCloudista.

Kun käyttäjän istunto on aktiivinen ja laite on yhteydessä verkkoon, dokumentit ja tiedot tallennetaan iCloudiin sitä mukaa, kun niitä luodaan tai muokataan. Lisäksi taustalla toimiva synkronointimekanismi auttaa varmistamaan, että muutokset lähetetään iCloudiin tai muihin verkkopalveluihin NSURLSession-taustaistuntojen avulla sen jälkeen, kun käyttäjä kirjautuu ulos. Kun kyseisen käyttäjän tietojen taustasynkronointi on valmis, käyttäjän APFS-taltio poistetaan käytöstä eikä sitä voida ottaa uudelleen käyttöön ilman, että käyttäjä kirjautuu jälleen sisään.

Väliaikaiset istunnot eivät synkronoi tietoja iCloudin kanssa, ja vaikka väliaikainen istunto voi kirjautua muun valmistajan synkronointipalveluun kuten Boxiin tai Google Driveen, tietojen synkronoimista ei voida jatkaa, kun väliaikainen istunto päättyy.

Uloskirjautuminen jaetusta iPadista

Kun käyttäjä kirjautuu ulos jaetusta iPadista, kyseisen käyttäjän avainvarasto lukitaan välittömästi, ja kaikki apit suljetaan. Jotta uusi käyttäjä voi kirjautua nopeasti sisään, iPadOS lykkää joitakin tavallisia uloskirjaamisen toimintoja ja näyttää uudelle käyttäjälle sisäänkirjautumisikkunan. Jos käyttäjä kirjautuu tällöin sisään (noin 30 sekunnin kuluessa), jaettu iPad suorittaa lykätyt toiminnot osana uuden käyttäjän tilille kirjautumista. Jos jaettua iPadia ei käytetä tänä aikana, se suorittaa lykätyt toiminnot. Näiden toimintojen suorittamisen aikana sisäänkirjautumisikkuna käynnistetään uudelleen samaan tapaan kuin jos toinen uloskirjautuminen olisi tapahtunut.

Kun väliaikainen istunto on päättynyt, jaettu iPad suorittaa täysimittaisen uloskirjauksen ja poistaa väliaikaisen istunnon APFS-taltion välittömästi.

Apple Configuratorin suojaus

Macin Apple Configuratorin joustavan ja suojatun laitekeskeisen suunnittelun ansiosta ylläpitäjä voi määrittää sen avulla nopeasti ja helposti yhden tai kymmeniä Maciin USB:n kautta liitettyjä iOS-, iPadOS- ja tvOS-laitteita (tai Bonjourin kautta pariksi asetettuja tvOS-laitteita) ennen niiden antamista käyttäjille. Macin Apple Configuratorilla ylläpitäjä voi muun muassa päivittää ohjelmistoa, asentaa appeja ja asetusprofiileja, nimetä laitteita uudelleen ja vaihtaa niiden taustakuvan sekä viedä laitetietoja ja dokumentteja.

Macin Apple Configurator voi myös elvyttää tai palauttaa Mac-tietokoneita, joissa on Apple silicon tai Apple T2 Security -siru. Kun Mac elvytetään tai palautetaan tällä tavoin, uusimmat käyttöjärjestelmien (macOS, recoveryOS Apple siliconille tai sepOS T2:lle) pienet päivitykset sisältävä tiedosto ladataan suojatusti Applen palvelimilta ja asennetaan suoraan Maciin. Onnistuneen elvytyksen tai palautuksen jälkeen tiedosto poistetaan Macista, joka suorittaa Apple Configuratoria. Käyttäjä ei voi missään vaiheessa tarkastella tai käyttää tätä tiedostoa Apple Configuratorin ulkopuolella.

Ylläpitäjät voivat myös lisätä laitteita Apple School Manageriin, Apple Business Manageriin tai Apple Business Essentialsiin Macin Apple Configuratorilla tai iPhonen Apple Configuratorilla, vaikka laitteita ei olisi ostettu suoraan Applelta, Applen valtuutetulta jälleenmyyjältä tai valtuutetulta operaattorilta. Kun ylläpitäjä ottaa käyttöön laitteen, joka on rekisteröity käsin, se toimii kuten muutkin laitteet näissä palveluissa, eli siinä on pakollinen valvonta ja rekisteröinti MDM:ään. Niille laitteille, joita ei ole ostettu suoraan, käyttäjällä on 30 päivän koeaika, jonka aikana laitteen voi vapauttaa palvelusta, valvonnasta ja MDM:stä.

Organisaatiot voivat myös käyttää Macin Apple Configuratoria aktivoidakseen iOS-, iPadOS- ja tvOS-laitteita, joilla ei ole lainkaan internet-yhteyttä, yhdistämällä ne laitteen käyttöönoton aikana isäntä-Maciin, joka on yhteydessä internetiin. Ylläpitäjät voivat palauttaa, aktivoida ja valmistella laitteita tarvittavilla määrityksillä, jotka sisältävät apit, profiilit ja dokumentit, ilman että laitteita tarvitsee missään vaiheessa liittää Wi-Fi- tai mobiilidataverkkoon. Tämä ominaisuus ei salli ylläpitäjien ohittaa mitään olemassa olevia aktivointilukituksen vaatimuksia, joita vaaditaan normaalisti aktivoinnissa ilman yhdistämistä Maciin.

Ruutuajan suojaus

Ruutuaika on sisäänrakennettu ominaisuus, jolla voidaan katsoa ja hallita, kuinka paljon aikaa aikuiset ja heidän lapsensa käyttävät muun muassa appien ja verkkosivustojen parissa. Käyttäjiä on kahdenlaisia: aikuisia ja (hallittuja) lapsia.

Vaikka Ruutuaika ei ole uusi järjestelmän suojauksen ominaisuus, on tärkeää ymmärtää, miten se pitää yksityisinä ja suojaa tietoja, joita kerätään ja jaetaan laitteiden välillä. Ruutuaika on käytettävissä iOS 12:ssa tai uudemmissa, iPadOS 13.1:ssä tai uudemmissa, macOS 10.15:ssä tai uudemmissa ja joidenkin ominaisuuksien osalta watchOS 6:ssa tai uudemmissa.

Alla olevassa taulukossa kerrotaan Ruutuajan keskeisistä ominaisuuksista.

Ominaisuus	Tuettu käyttöjärjestelmä
käyttötietojen katsominen	iOS iPadOS macOS
lisärajoitusten pakottaminen	iOS iPadOS macOS watchOS
verkkokäytön rajoittaminen	iOS iPadOS macOS
appien rajoittaminen	iOS iPadOS macOS watchOS
käyttötauon määrittäminen	iOS iPadOS macOS watchOS

Oman laitteensa käyttöä hallitseville käyttäjille Ruutuajan säätimet ja käyttötiedot voidaan synkronoida kaikkiin samaan iCloud-tiliin liitettyihin laitteisiin CloudKitillä päästä päähän salattuina. Tähän vaaditaan, että käyttäjän tilille on otettu käyttöön kaksiosainen todennus (synkronointi on oletuksena päällä). Ruutuaika korvaa aiempien iOS- ja iPadOS-versioiden Rajoitukset-ominaisuuden ja aikaisempien macOS-versioiden Käyttörajoitukset-ominaisuuden.

iOS 13:ssa ja uudemmissa, iPadOS 13.1:ssä ja uudemmissa ja macOS 10.15:ssä ja uudemmissa Ruutuaika-käyttäjät ja hallitut lapset jakavat käyttötietonsa automaattisesti laitteiden välillä, jos heidän iCloud-tileilleen on otettu käyttöön kaksiosainen todennus. Kun käyttäjä tyhjentää Safari-historiansa tai poistaa apin, vastaavat käyttötiedot poistetaan laitteesta ja kaikista synkronoiduista laitteista.

Vanhemmat ja Ruutuaika

Vanhemmat voivat myös käyttää Ruutuaikaa iOS-, iPadOS- ja macOS-laitteissa ymmärtääkseen ja hallitakseen lapsiensa laitteiden käyttöä. Jos vanhempi on perheen järjestäjä (iCloudin Perhejaossa), hän voi katsella käyttötietoja ja hallita Ruutuaika-asetuksia lastensa osalta. Lapsille ilmoitetaan, kun heidän vanhempansa laittavat Ruutuajan päälle, ja he voivat myös tarkkailla omaa laitteiden käyttöänsä. Kun vanhemmat laittavat Ruutuajan päälle lapsilleen, he asettavat pääsykoodin, jotta lapset eivät voi tehdä muutoksia. Kun lapset tulevat täysi-ikäisiksi (ikä vaihtelee maasta tai alueesta riippuen), he voivat laittaa tarkkailun pois päältä.

Käyttötietoja ja asetuksia siirretään vanhemman ja lapsen laitteiden välillä käyttäen päästä-päähän-salattua Apple Identity Service (IDS) -protokollaa. Salattuja tietoja voidaan säilyttää lyhytaikaisesti IDS-palvelimilla, kunnes vastaanottava laite lukee ne (esimerkiksi heti, kun aiemmin pois päältä ollut iPhone, iPad tai iPod touch laitetaan päälle). Apple ei voi lukea tietoja.

Ruutuaika-analysointi

Jos käyttäjä laittaa päälle Jaa iPhone- ja Watch-analyysi -toiminnon, vain seuraavia anonymisoituja tietoja kerätään, jotta Apple voi paremmin ymmärtää, miten Ruutuaikaa käytetään:

- laitettiinko Ruutuaika päälle käyttöönottoapurissa vai myöhemmin Asetuksissa
- muutos kategoriakohtaisessa käytössä rajoituksen määrittämisen jälkeen (90 päivän aikana)
- onko Ruutuaika päällä
- onko Käyttötauko otettu käyttöön
- kuinka monta kertaa Pyydä lisää aikaa -toimintoa käytettiin
- appirajoitusten määrä
- kuinka monta kertaa käyttäjät katselivat käyttötietoja Ruutuaika-asetuksissa – käyttäjätyypin mukaan ja katselutyypin mukaan (paikallisesti, etänä, widgetissä)
- kuinka monta kertaa käyttäjät jättävät rajoituksen huomioimatta – käyttäjätyypin mukaan
- kuinka monta kertaa käyttäjät poistavat rajoituksen – käyttäjätyypin mukaan

Apple ei kerää eriteltyjä tietoja appien tai verkon käytöstä. Kun käyttäjä näkee Ruutuaika-käyttötiedoissa appiluettelon, appikuvakkeet noudetaan suoraan App Storesta, joka ei säilytä mitään tietoja näistä pyynnöistä.

Sanasto

Address Space Layout Randomization (ASLR) Käyttöjärjestelmien käyttämä tekniikka, joka vaikeuttaa merkittävästi ohjelmistovirheen haavoittuvuuden hyväksikäyttämistä. Varmistamalla, että muistiosoitteet ja poikkeamat ovat ennalta arvaamattomia, haavoittuvuutta hyödyntävä koodi ei voi kovakoodata näitä arvoja.

AES-salausmoottori Erillinen laitteistokomponentti, joka käyttää AES:ää.

AES-salausstandardi (Advanced Encryption Standard) Suosittu yleinen salausstandardi, jolla pidetään tiedot yksityisinä salaamalla ne.

AES-XTS IEEE 1619-2007:ssä määritetty AES-tila, jonka on tarkoitus salata tallennusväline.

APFS (Apple File System -tiedostojärjestelmä) Oletustiedostojärjestelmä iOS:ssä, iPadOS:ssä, tvOS:ssä, watchOS:ssä ja Mac-tietokoneissa, joissa on macOS 10.13 tai uudempi. APFS tukee vahvaa salausta, tilan jakamista, tilannevedoksia, nopeaa hakemiston koon uudelleenmääritystä ja parannettuja tiedostojärjestelmän perustoimintoja.

Apple Business Manager IT-ylläpitäjille tehty selkeä, verkkopohjainen portaali, joka tarjoaa nopean ja sujuvan keinon organisaatiolle ottaa käyttöön Applen laitteita, jotka se on ostanut suoraan Applelta tai ohjelmaan osallistuvalta Applen valtuutetulta jälleenmyyjältä tai operaattorilta. Laitteita voi rekisteröidä automaattisesti mobiililaitteiden hallintaratkaisuun (MDM) ilman, että niitä täytyy käsitellä tai valmistella fyysisesti ennen kuin ne annetaan käyttäjille.

Apple School Manager IT-ylläpitäjille tehty selkeä, verkkopohjainen portaali, joka tarjoaa nopean ja sujuvan keinon organisaatiolle ottaa käyttöön Applen laitteita, jotka se on ostanut suoraan Applelta tai ohjelmaan osallistuvalta Applen valtuutetulta jälleenmyyjältä tai operaattorilta. Laitteita voi rekisteröidä automaattisesti mobiililaitteiden hallintaratkaisuun (MDM) ilman, että niitä täytyy käsitellä tai valmistella fyysisesti ennen kuin ne annetaan käyttäjille.

Apple Security Bounty -palkkio Applen antama palkkio tutkijoille, jotka raportoivat uusimpiin toimitettaviin käyttöjärjestelmiin ja (tilanteen mukaan) myös uusimpaan laitteistoon vaikuttavan haavoittuvuuden.

Applen identiteettipalvelu (Apple Identity Service, IDS) Applen hakemisto julkisille iMessage-avaimille, APNs-osoitteille sekä puhelinnumeroille ja sähköpostiosoitteille, joita käytetään avainten ja laiteosoitteiden etsimiseen.

Applen push-ilmoituspalvelu (APNs) Applen tarjoama maailmanlaajuinen palvelu, joka toimittaa push-ilmoituksia Apple-laitteille.

avaimen luonti (tangling) Prosessi, jossa käyttäjän pääsykoodi muutetaan salausavaimeksi ja vahvistetaan laitteen UID:llä. Tämä prosessi auttaa varmistamaan, että väsytyshyökkäys on tehtävä kyseisellä laitteella. Hyökkäyksen nopeus on siten rajoitettu eikä sitä voi tehdä rinnakkain. Salasanatiivistealgoritmi on PBKDF2, joka käyttää AES:ää yhdessä laitteen UID:n kanssa näennäissatunnaisfunktiona (PRF) jokaiselle iterointikerralle.

avaimen salaaminen Avaimen salaaminen toisella avaimella. iOS ja iPadOS käyttää RFC 3394:n mukaista NIST AES -avainsalausta.

avainnippu Infrastruktuuri ja API:en sarja, jota Applen käyttöjärjestelmät ja muiden valmistajien apit käyttävät salasanojen ja muiden luottamuksellisten tietojen säilyttämiseen ja hakemiseen.

avainvarasto Tietorakenne luokka-avaimien kokoelman tallentamiseen. Jokaisella tyypillä (käyttäjä, laite, järjestelmä, varmuuskopio, vara-avain tai iCloud-varmuuskopio) on sama muoto.

Otsake, jossa on seuraavat: versio (asetettu neljään iOS 12:ssa ja uudemmissa), tyyppi (järjestelmä, varmuuskopio, tallenne tai iCloud-varmuuskopio), avainvaraston UUID, HMAC, jos avainvarasto on allekirjoitettu, ja luokka-avaimien salausmenetelmä (sidottu UID:llä tai PBKDF2:lla) sekä suola ja iterointimäärä.

Luokka-avaimien luettelo: Avaimen UUID, luokka (mikä tiedoston tai avainnipun tietojen suojausluokka), salaustyyppi (vain UID-johdettu avain; UID-johdettu avain ja pääsykoodijohdettu avain), salattu luokka-avain ja julkinen avain epäsymmetrisille luokille.

Boot Camp Macin lisäappi, joka tukee Microsoft Windowsin asentamista tuettuihin Mac-tietokoneisiin.

Boot ROM Laitteen prosessorin ensimmäinen suoritettava koodi, kun laite käynnistyy. Koska se on kiinteä osa prosessoria, sitä eivät voi muuttaa Apple eikä hyökkääjä.

CKRecord Avainarvoparien sanakirja, joka sisältää CloudKitiin tallennetut tai sieltä haetut tiedot.

DFU-tila (Device Firmware Upgrade) Tila, jossa laitteen Boot ROM -koodi odottaa palautusta USB:llä. Kun laite on DFU-tilassa, sen näyttö on pimeänä, mutta kun se liitetään tietokoneeseen, jossa on iTunes tai Finder, näytetään seuraava kehote: ”iTunes (tai Finder) on havainnut palautustilassa olevan (iPadin, iPhonen tai iPod touchin). (iPadin, iPhonen tai iPod touchin) ohjelmisto on palautettava ennen kuin sitä voidaan käyttää iTunesin (tai Finderin) kanssa.”

ECID-tunniste (Exclusive Chip Identification) 64-bittinen tunniste, joka on ainutlaatuinen jokaisen iOS- ja iPadOS-laitteen prosessorissa. Kun kutsuun vastataan yhdellä laitteella, lähellä olevien iCloudissa pariksi liitettyjen laitteiden kutsuminen lopetetaan mainostamalla lyhyesti Bluetooth Low Energy (BLE) 4.0 -teknologialla. Mainostavut salataan samalla menetelmällä kuin Handoff-mainokset. Käytetään osana yksilöintiprosessia, ei pidetä salaisuutena.

Elliptisen käyrän Diffie-Hellman -avaimenvaihto lyhytaikaisella avaimella (ECDHE) Elliptisiin käyriin perustuva avaimenvaihtomekanismi. ECDHE:llä kaksi osapuolta voi sopia salaisen avaimen tavalla, joka estää kahden osapuolen välisiä viestejä vakoilevaa salakuuntelijaa selvittämästä avainta.

Elliptisen käyrän digitaalinen allekirjoitusalgoritmi (ECDSA) Elliptisen käyrän salaukseen perustuva digitaalinen allekirjoitusalgoritmi.

eSPI (Enhanced Serial Peripheral Interface) Kaikenkattava väylä, joka on suunniteltu synkroniseen sarjaliikenteeseen.

Gatekeeper macOS:n teknologia, jonka tehtävä on auttaa varmistamaan, että käyttäjän Macissa toimii vain luotettu ohjelmisto.

HMAC Tiivisteeseen pohjautuva viestin todennuskoodi, joka perustuu kryptografiseen tiivistefunktioon.

I/O-muistinhallintayksikkö (Input/Output Memory Management Unit, IOMMU) I/O-muistinhallintayksikkö. Integroidun piirin alijärjestelmä, joka hallitsee pääsyä osoiteavaruuteen muista I/O-laitteista ja oheislaitteista.

iBoot Vaiheen 2 käynnistyslataaja kaikille Applen laitteille. Koodi, joka lataa XNU:n osana suojattua käynnistysketjua. Järjestelmäpiirin (SoC) sukupolvesta riippuen iBootin voi ladata LLB (Low Level Bootloader) tai suoraan Boot ROM.

integroitu piiri (integrated circuit, IC) Kutsutaan myös *mikrosiruksi*.

Joint Test Action Group -ryhmä (JTAG) Ohjelmoijien ja piirikehittäjien käyttämä laitteiston vakiovianmääritystyökalu.

järjestelmäohjelmiston valtuutus Prosessi, joka yhdistää laitteiston kiinteät salausavaimet online-palveluun sen tarkistamiseksi, että vain Applen hyväksytty ohjelmisto, joka sopii tuettuihin laitteisiin, toimitetaan ja asennetaan päivitysaikana.

järjestelmäpiiri (SoC) Mikropiiri eli integroitu piiri, joka sisältää useita komponentteja yhdessä sirussa. Appeja suorittava prosessori, Secure Enclave ja muut lisäprosessorit ovat järjestelmäpiirin osia.

kohoumien kulman kuvaus Sormenjäljen osasta peräisin oleva kohoumien suunnan ja leveyden matemaattinen esitys.

Käynnistymisen edistymisrekisteri (Boot Progress Register, BPR) Järjestelmäpiirin (SoC) laitteistomerkintäsarja, jonka avulla ohjelmisto voi seurata käynnistystiloja, kuten DFU (Device Firmware Update) -tilaa ja palautustilaa, joihin laite on siirtynyt. Kun BPR-merkintä on määritetty, sitä ei voida pyyhkiä. Tämän avulla myöhempi ohjelmisto saa luotettavan merkin järjestelmän tilasta.

laitteiston suojausmoduuli (hardware security module, HSM) Erikoistunut peukalointia kestävä tietokone, joka suojelee ja hallitsee digitaalisia avaimia.

mobiililaitteiden hallinta (MDM) Palvelu, jolla ylläpitäjä voi hallita etänä rekisteröityjä laitteita. Kun laite on rekisteröity, ylläpitäjä voi käyttää verkon kautta MDM-palvelua, joka määrittää asetuksia ja suorittaa muita tehtäviä laitteella ilman käyttäjän toimia.

muistiohjain Järjestelmäpiirin alijärjestelmä, joka hallitsee järjestelmäpiirin ja sen päämuistin välistä liitäntää.

NAND Pysyvä flash-muisti.

nonce Ainutkertainen numero, jota käytetään useissa suojausprotokollissa.

ohjelmiston siemenbitit Secure Enclaven AES-komponentissa olevat tarkoitukseen varatut bitit, jotka lisätään UID:hen, kun avaimia luodaan UID:stä. Jokaisella ohjelmiston siemenbitillä on vastaava lukitusbitti. Secure Enclaven Boot ROM ja käyttöjärjestelmä voivat itsenäisesti muuttaa jokaisen ohjelmistosiemenbitin arvoa, kunhan vastaavaa lukitusbittiä ei ole asetettu. Kun lukitusbitti on asetettu, ohjelmiston siemenbittiä ja lukitusbittiä ei voida muokata. Ohjelmiston siemenbitit ja niiden lukitukset nollataan, kun Secure Enclave käynnistetään uudelleen.

Palautustila Palautustilaa käytetään Apple-laitteiden palauttamiseen, jos se ei tunnista käyttäjän laitetta, jotta käyttäjä voi asentaa käyttöjärjestelmän uudelleen.

Perustason käynnistyslataaja (Low Level Bootloader, LLB) Kaksivaiheisella käynnistysarkkitehtuurilla varustetuissa Mac-tietokoneissa LLB:n sisältämä koodi, jonka Boot ROM käynnistää ja joka puolestaan lataa iBootin osana suojattua käynnistysketjua.

provisiointiprofiili Applen allekirjoittama ominaisuusluettelo (.plist-tiedosto), joka sisältää sarjan entiteettejä ja oikeutuksia, jotka sallivat appien asennuksen ja testauksen iOS- tai iPadOS-laitteessa. Kehitysprovisiointiprofiili luetteloi laitteet, jotka kehittäjä on valinnut ad hoc -jakeluun, ja jakeluprovisiointiprofiili sisältää yrityksessä kehitetyn apin tunnisteen.

Pyyhittävä tallennustila NAND-tallennustilan tarkoitukseen varattu alue, jota käytetään säilyttämään salausavaimia, jotka voidaan osoittaa suoraan ja pyyhkiä turvallisesti. Vaikka pyyhittävä tallennustila ei tarjoa suojaa, jos hyökkääjä pääsee fyysisesti käsiksi laitteeseen, siinä säilytettäviä avaimia voidaan käyttää osana avainhierarkiaa nopean pyyhkimisen helpottamiseksi ja turvallisuuden lisäämiseksi.

pääsykoodijohdettu avain (passcode-derived key, PDK) Salausavain, joka muodostetaan sitomalla käyttäjän salasana pitkäaikaiseen SKP-avaimeen ja Secure Enclaven UID:hen.

ryhmätunnus (group ID, GID) Samanlainen kuin UID, mutta yhteinen jokaiselle luokan prosessorille.

Secure Storage -komponentti Se on siru, jossa on muuttumaton RO-koodi, laitteistosatunnaislukugeneraattori, salausohjelmat ja fyysisen peukaloinnin tunnistin. Tuetuissa laitteissa Secure Enclavesta on muodostettu pari Secure Storage -komponentin kanssa toiston estävän nonce-arvon tallennusta varten. Jotta Secure Enclave ja tallennustilan siru voivat lukea ja päivittää nonce-arvoja, ne käyttävät turvattua protokollaa, joka auttaa varmistamaan vain niille pääsyn nonce-arvoihin. Tästä teknologiasta on useita sukupolvia, joissa on eri suojaustakuut.

sepOS Secure Enclave -laiteohjelmisto, joka perustuu Applen muokkaamaan versioon L4-mikroytimestä.

Sinetöity avaimen suojaus (Sealed Key Protection, SKP) Tietojen suojaukseen sisältyvä teknologia, joka suojaa eli *sinetöi* salausavaimet järjestelmäohjelmiston mittauksilla ja vain laitteistossa saatavissa olevilla avaimilla (kuten Secure Enclaven UID).

SSD-ohjain Laitteiston alijärjestelmä, joka hallitsee tallennusvälinettä (SSD).

suora muistin käyttö (direct memory access, DMA) Ominaisuus, jolla laitteiston alijärjestelmät voivat käyttää päämuistia suoraan ohittaen prosessorin.

System Coprocessor Integrity Protection (SCIP) Applen käyttämä mekanismi, joka on suunniteltu estämään lisäprosessorin laiteohjelmiston muutoksia.

tallennuslaiteavain Osa salaushierarkiaa, joka tarjoaa turvallisen ja välittömän tyhjennyksen. Tallennuslaiteavain salaa iOS:ssä, iPadOS:ssä, tvOS:ssä ja watchOS:ssä datataltion metadatan (ilman sitä mitään tiedostokohtaisia avaimia ei voida käyttää, jolloin tietojen suojauksella suojattuja tiedostoja ei voida käyttää). macOS:ssä tallennuslaiteavain salaa FileVault-suojatun taltion kaikki avaimet sekä kaiken metadatan ja tiedot. Kummassakin tapauksessa tallennuslaiteavaimen tyhjentäminen merkitsee sitä, että salattuja tietoja ei voida käyttää.

tiedostojärjestelmän avain Avain salaa jokaisen tiedoston metatiedot, mukaan lukien sen luokka-avaimen. Sitä säilytetään pyyhittävässä tallennustilassa, mikä helpottaa nopeaa pyyhkimistä pikemminkin kuin luottamuksellisuutta.

tiedostokohtainen avain Avain, jota tietojen suojaus käyttää tiedoston salaamiseen tiedostojärjestelmässä. Tiedostokohtainen avain on salattu luokka-avaimella ja tallennettu tiedoston metatietoihin.

Tietojen suojaus Tiedostojen ja avainnipun suojausmenetelmä tuetuille Apple-laitteille. Se voi viitata myös API-rajapintoihin, joita apit käyttävät tiedostojen ja avainnipun kohteiden suojaamiseen.

Tietosäiliö Kernelin pakottama mekanismi, joka suojaa tietojen luvattomalta käytöltä riippumatta siitä, onko pyytävä appi itse eristetty.

UEFi (Unified Extensible Firmware Interface) -laiteohjelmisto BIOS:n korvaava teknologia, jolla yhdistetään laiteohjelmisto tietokoneen käyttöjärjestelmään.

URI-tunniste (Uniform Resource Identifier, URI) Merkkisarja, joka määrittää verkkopohjaisen resurssin.

xART Lyhenne sanoista eXtended Anti-Replay Technology. Joukko palveluja, jotka tarjoavat Secure Enclavelle salatun, todennetun ja pysyvän tallennustilan toiston estävillä ominaisuuksilla, jotka perustuvat fyysiseen tallennustila-arkkitehtuuriin. Katso Secure Storage -komponentti.

XNU Applen käyttöjärjestelmien ytimessä oleva kernel. Se oletetaan luotettavaksi ja se suorittaa suojaustoimenpiteitä, kuten koodin allekirjoituksen, sandboxaus-eristyksen, oikeutuksien tarkistamisen ja ASLR:n (Address Space Layout Randomization).

XProtect macOS:n virustorjuntateknologia tunnistepohjaista haittaohjelmistojen tunnistusta ja poistamista varten.

yksilöllinen tunnus (Unique ID, UID) 256-bittinen AES-avain, joka poltetaan jokaiseen prosessoriin valmistuksen yhteydessä. Laiteohjelmisto ja ohjelmisto eivät pysty lukemaan sitä, ja sitä käyttää vain prosessorin AES-laitteistokomponentti. Varsinaisen avaimen saamiseksi hyökkääjän täytyisi tehdä erittäin kehittynyt ja kallis fyysinen hyökkäys prosessorin siruun. UID ei liity mihinkään muuhun laitteen tunnisteeseen, mukaan lukien UDID:hen.

Muutoshistoria

Muutoshistoria

Päiväys	Yhteenveto
Joulukuu 2022	Lisätyt aiheet: • iCloudin edistyksellinen tietosuojaus Päivitetyt aiheet: • iCloudin suojauksen yleiskatsaus • iCloudin salaus • iCloud-varmuuskopioinnin suojaus • Tilin palautuksen yhteyshenkilön suojaus • Tilin perijän suojaus

Päiväys	Yhteenveto
Toukokuu 2022	Päivitetty seuraaville: • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 Lisätyt aiheet: • Parina olevan recoveryOS:n rajoitukset • Paikallinen käyttöjärjestelmäversio (love) • Terveystietojen jako • Tilin palautuksen yhteyshenkilön suojaus • Tilin perijän suojaus • Tap to Pay on iPhone -ominaisuuden suojaus • Pääsy Applen Lompakkoa käyttäen • Pääsytunnistetietojen tyypit • Henkilökortit Applen Lompakossa • Siriä tukevat HomeKit-lisälaitteet Päivitetyt aiheet: • Touch ID:llä varustettu Magic Keyboard • Face ID, Touch ID, pääsykoodit ja salasanat • Kasvojen tunnistuksen suojaus • ExpressCard-kortit virransäästöllä • Apple siliconilla varustetun Macin käynnistystilat • Apple siliconilla varustetun Macin LocalPolicy-tiedoston sisältö • Allekirjoitetun järjestelmätaltion suojaus iOS:ssä, iPadOS:ssä ja macOS:ssä • watchOS-järjestelmän suojaus • Applen tietoturvatutkimuslaite • Apple File Systemin rooli • Appien pääsyoikeuden estäminen käyttäjätietoihin • Johdanto appien suojaukseen macOS:ssä • Suojaaminen haittaohjelmistoilta macOS:ssä • iCloudin suojauksen yleiskatsaus • Suojattu salasanan synkronointi • iCloud-avainnipun suojattu palautus • Maksaminen korteilla Apple Payta käyttäen • Lähiluettavat kortit Apple Payssa • Korttien Apple Pay -käytön estäminen • Apple Card -hakemus • Apple Cashin suojaus • Matka- ja eMoney-korttien lisääminen Applen Lompakkoon • Suojatut Apple Messages for Business -viestit • FaceTimen suojaus • Auton avaimen suojaus iOS:ssä • Apple Configuratorin suojaus Poistetut aiheet: • HomeKit-lisälaitteet ja iCloud

Päiväys	Yhteenveto
Toukokuu 2021	Päivitetty seuraaville: • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 Lisätyt aiheet: • Touch ID:llä varustettu Magic Keyboard. • Aikomus muodostaa pari luotettavasti ja yhteydet Secure Enclaveen. • Automaattinen lukituksen avaaminen ja Apple Watch. • CustomOS:n Image4-vaatimustiedoston tiiviste (coih). Muokatut aiheet: • Kaksi uutta pikatilatoimintoa lisätty osioon ExpressCard-kortit virransäästöllä. • Muokkauksia osioon Secure Enclaven ominaisuuksien yhteenveto. • Ohjelmistopäivityssisältöä lisätty osioon Suojattu monikäynnistys (smb3). • Sisältöä lisätty osioon Sinetöity avaimen suojaus (Sealed Key Protection, SKP).

Päiväys	Yhteenveto
Helmikuu 2021	Päivitetty seuraaville: • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 Lisätyt aiheet: • Muistiturvallinen iBoot • Apple siliconilla varustetun Macin käynnistysprosessi • Apple siliconilla varustetun Macin käynnistystilat • Käynnistyslevyn suojauskäytännön hallinta Apple siliconilla varustetussa Macissa • LocalPolicyn allekirjoitusavaimen luominen ja hallinta • Apple siliconilla varustetun Macin LocalPolicy-tiedoston sisältö • Allekirjoitetun järjestelmätaltion suojaus iOS:ssä, iPadOS:ssä ja macOS:ssä • Applen tietoturvatutkimuslaite • Salasanojen valvonta • IPv6:n suojaus • Auton avaimen suojaus iOS:ssä Päivitetyt aiheet: • Secure Enclave -alue • Mikrofonin laitteistopohjainen poiskytkentä • recoveryOS ja vianmääritysympäristöt Intel-pohjaiselle Macille • DMA-suojaukset Mac-tietokoneilla • Kernelin laajennukset macOS:ssä • Järjestelmän eheyden suojaus • watchOS-järjestelmän suojaus • FileVaultin hallinta macOS:ssä • Appien pääsy tallennettuihin salasanoihin • Salasanojen turvallisuutta koskevat suositukset • Apple Cashin suojaus • Suojatut Apple Messages for Business -viestit • Wi-Fin yksityisyys • Aktivointilukitussuojaus • Apple Configuratorin suojaus
Huhtikuu 2020	Päivitetty seuraaville: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Päivitykset: • iPadin mikrofonin poistaminen käytöstä lisätty osioon Mikrofonin laitteistopohjainen poiskytkentä. • Tietosäiliöt lisätty osioon Appien pääsyoikeuden estäminen käyttäjätietoihin. • Päivityksiä osioihin FileVaultin hallinta macOS:ssä ja Komentorivityökalut. • Haittaohjelmiston poistotyökalua koskevia lisäyksiä osioon Suojaaminen haittaohjelmistoilta macOS:ssä. • Päivityksiä osioon Jaetun iPadin suojaus iPadOS:ssä.

Päiväys	Yhteenveto
Joulukuu 2019	Yhdistetty iOS-tietoturvaopas, macOS:n tietoturvan yleiskatsaus ja Apple T2 Security -sirun yleiskatsaus Päivitetty seuraaville: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Tietosuojan säätimet, Siri ja Siri-ehdotukset sekä Safarin älykäs seurannan esto on poistettu. Näiden ominaisuuksien uusimmat tiedot löytyvät osoitteesta https://www.apple.com/privacy/.
Toukokuu 2019	Päivitetty iOS 12.3:lle • Tuki TLS 1.3:lle • AirDropin suojauksen muokattu kuvaus • DFU-tila ja palautustila • Pääsykoodivaatimukset lisälaitteiden yhteyksille
Marraskuu 2018	Päivitetty iOS 12.1:lle • Ryhmä-FaceTime
Syyskuu 2018	Päivitetty iOS 12:lle • Secure Enclave -alue • Käyttöjärjestelmän eheyden suojaus • ExpressCard virransäästöllä • DFU-tila ja palautustila • HomeKit-TV-kaukosäädinlisälaitteet • Lähiluettavat kortit • Opiskelijakortit • Siri-ehdotukset • Sirin pikakomennot • Pikakomennot-appi • Käyttäjän salasanojen hallinta • Ruutuaika • Suojaussertifioinnit ja -ohjelmat
Heinäkuu 2018	Päivitetty iOS 11.4:lle • Biometriset käytännöt • HomeKit • Apple Pay • Yrityschat • iCloud-viestit • Apple Business Manager
Joulukuu 2017	Päivitetty iOS 11.2:lle • Apple Pay Cash

Päiväys	Yhteenveto
Lokakuu 2017	Päivitetty iOS 11.1:lle • Suojaussertifioinnit ja -ohjelmat • Touch ID/Face ID • Jaetut muistiinpanot • CloudKitin päästä päähän -salaus • TLS-päivitys • Apple Pay, verkossa maksaminen Apple Paylla • Siri-ehdotukset • Jaettu iPad
Heinäkuu 2017	Päivitetty iOS 10.3:lle • Secure Enclave -alue • Tiedostojen tietojen suojaus • Avainvarastot • Suojaussertifioinnit ja -ohjelmat • SiriKit • HealthKit • Verkon suojaus • Bluetooth • Jaettu iPad • Kadonnut-tila • Aktivointilukitus • Tietosuojan säätimet
Maaliskuu 2017	Päivitetty iOS 10:lle • Järjestelmän tietoturva • Tietojen suojausluokat • Suojaussertifioinnit ja -ohjelmat • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Kertakirjautuminen • Apple Pay, verkossa maksaminen Apple Paylla • Luotto-, pankki- ja prepaid-korttien valmistelu • Safarin ehdotukset
Toukokuu 2016	Päivitetty iOS 9.3:lle • Hallittu Apple ID • Kaksiosainen todennus Apple ID:lle • Avainvarastot • Suojaussertifioinnit • Kadonnut-tila, aktivointilukitus • Suojatut muistiinpanot • Apple School Manager • Jaettu iPad

Päiväys	Yhteenveto
Syyskuu 2015	Päivitetty iOS 9:lle • Apple Watchin aktivointilukitus • Pääsykoodikäytännöt • Touch ID:n API-tuki • Tietojen suojaus A8:lla käyttää AES-XTS:ää • Avainvarastot valvomattomille ohjelmistopäivityksille • Sertifiointipäivitykset • Yritysappien luottamusmalli • Safari-kirjanmerkkien tietojen suojaus • ATS (App Transport Security) • VPN-tiedot • HomeKitin iCloud-etäkäyttö • Apple Pay -etukortit, Apple Pay -kortinmyöntäjän appi • Spotlightin laitteessa tapahtuva indeksointi • iOS:n laiteparin muodostamisen malli • Apple Configurator 2 • Rajoitukset

”Näppäimistön” Apple-logon (optio-vaihto-K) käyttö kaupallisiin tarkoituksiin ilman Applen etukäteissuostumusta voi olla tavaramerkkirikkomus ja vilpillistä kilpailua, joka rikkoo liitto- ja osavaltion lakeja.

Apple, Apple-logo, AirDrop, AirPlay, Apple Books, Apple Card, Apple Music, Apple Pay, Apple TV, Apple Wallet, Apple Watch, AppleScript, ARKit, Bonjour, Boot Camp, CarPlay, Face ID, FaceTime, FileVault, Finder, FireWire, Handoff, HealthKit, HomeKit, HomePod, HomePod mini, iMac, iMac Pro, iMessage, iPad, iPadOS, iPad Air, iPad Pro, iPhone, iPod touch, iTunes, Keychain, Lightning, Mac, Mac Catalyst, Mac mini, Mac Pro, MacBook, MacBook Air, MacBook Pro, macOS, Magic Keyboard, Objective-C, OS X, QuickType, Retina, Rosetta, Safari, Siri, Siri Remote, SiriKit, Swift, Spotlight, Touch ID, TrueDepth, tvOS, watchOS ja Xcode ovat Apple Inc:n Yhdysvalloissa ja muissa maissa ja muilla alueilla rekisteröityjä tavaramerkkejä.

App Clips, Find My ja Touch Bar ovat Apple Inc:n tavaramerkkejä.

App Store, AppleCare, CloudKit, iCloud, iCloud Drive, iCloud Keychain ja iTunes Store ovat Apple Inc:n Yhdysvalloissa ja muissa maissa ja muilla alueilla rekisteröityjä palvelumerkkejä.

Apple Messages for Business on Apple Inc:n palvelumerkki.

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

IOS on Ciscon tavaramerkki tai rekisteröity tavaramerkki Yhdysvalloissa ja muissa maissa, ja sitä käytetään lisenssillä.

Bluetooth®-merkki ja -logo ovat Bluetooth SIG Inc:n omistamia rekisteröityjä tavaramerkkejä, ja Apple käyttää kaikkia sellaisia merkkejä lisenssillä.

Java on Oraclen ja/tai sen konserniyhtiöiden rekisteröimä tavaramerkki.

UNIX® on The Open Groupin rekisteröimä tavaramerkki.

Muut mainitut yritys- ja tuotenimet saattavat olla omistajiensa tavaramerkkejä.

Tämän käyttöoppaan tietojen oikeellisuus on pyritty varmistamaan kaikin mahdollisin tavoin. Apple ei ole vastuussa paino- tai kirjoitusvirheistä.

Jotkin apit eivät ole saatavilla kaikilla alueilla. Appien saatavuus voi muuttua.

K028-00625