Tietoturvasertifiointi ja vaatimustenmukaisuus

Joulukuu 2021

Sisällysluettelo

Johdanto Applen tietoturvan varmistukseen

Apple on sitoutunut tietoturvan kehittämiseen ja tekee säännöllisesti yhteistyötä kolmansien osapuolien organisaatioiden kanssa, jotta Applen laitteistot, ohjelmistot ja palvelut sertifioidaan ja niiden tietoturva todistetaan. Nämä kansainvälisesti tunnustetut organisaatiot tarjoavat Applelle sertifiointeja, jotka kohdistetaan kaikkiin käyttöjärjestelmien pääversioihin. Tällä tavalla ne tuovat varmuutta (eli suojausvarmuuden), että järjestelmän suojaustarpeet on täytetty. Apple on kehittämässä vastaavia tietoturvastandardeja teknisille alueille, joita ei hyväksytä vastavuoroisen tunnustamisen sopimuksiin tai joista puuttuvat tietoturvasertifiointivaatimukset. Pyrkimyksenämme on saada aikaan maailmanlaajuisesti hyväksytty, kattava tietoturvasertifiointi kaikille Applen laitteistoille, käyttöjärjestelmille, apeille ja palveluille.

Sertifikaatteja tarvitaan usein lakien, säännösten ja alan normien vaatimusten täyttämiseen. Applen ISO/IEC 27001- ja ISO/IEC 27018 -sertifikaatit kattavat palvelut, kuten Apple School Manager ja Apple Business Manager. Kaikki Applen laitteita käyttävät asiakkaat, mukaan lukien viranomaistahot sekä yritys- ja koulutusalan organisaatiot, voivat tukea vaatimustenmukaisuuden täyttämistä käyttämällä laitteiston, käyttöjärjestelmän, ohjelmiston ja palvelujen sertifikaatteja.

Laitteistojen sertifikaatit

Koska tietoturvallinen ohjelmisto vaatii, että tietoturvan perustukset on sisäänrakennettu laitteistoon, kaikissa Applen laitteissa, joissa on iOS, iPadOS, macOS, tvOS tai watchOS, on suojausominaisuuksia aivan laitteistotasolla. Niihin sisältyvät järjestelmän suojauksia mahdollistavat prosessorin ominaisuudet sekä erityinen siru juuri tietoturvatoimintoja varten. Kriittisin osa on Secure Enclave -lisäprosessori, joka on kaikissa uudemmissa iOS-, iPadOS-, watchOS- ja tvOS-laitteissa sekä kaikissa Apple siliconilla varustetuissa Mac-tietokoneissa ja Apple T2 Security -sirulla varustetuissa Intel-pohjaisissa Mac-tietokoneissa. Secure Enclave tarjoaa perustan levossa olevan datan salaamiselle, macOS:n suojatulle käynnistykselle ja biometriselle tunnistamiselle.

Applen sitoomus tietoturvan varmistamiseen alkaa sirun perustavanlaatuisten suojauskomponenttinen sertifioinnista. Siihen lukeutuvat laitteiston luottamuksen perusta, suojattu käynnistys, suojattu avaintallennus Secure Enclavessa ja turvallinen todennus Touch ID:llä ja Face ID:llä. Applen laitteiden tietoturvaominaisuudet tekevät mahdolliseksi sirun suunnittelun, laitteiston, ohjelmiston ja palveluiden yhdistelmän, jonka saa vain Applelta. Näiden osien sertifiointi on tärkeä osa Applen tarjoamaa varmistuksen vahvistamista.

Jos haluat tietoja julkisista sertifioinneista, jotka koskevat laitteistoja ja niihin liittyviä laiteohjelmistokomponentteja, katso:

- Apple T2 Security -sirun suojauksen sertifioinnit
- Tietoturvasertifioinnit Secure Enclave -prosessorille

Ohjelmiston ja appien sertifioinnit

Apple ylläpitää riippumattomia sertifiointeja ja todistuksia käyttöjärjestelmälleen ja apeilleen noudattamalla FIPS (U.S. Federal Information Processing Standards) 140-2/-3 -standardin salausmoduuleja koskevia vaatimuksia sekä käyttöjärjestelmien, appien ja laitepalveluiden Common Criteria -vaatimuksia. Käyttöjärjestelmien sertifiointi kattaa iOS:n, iPadOS:n, macOS:n, sepOS:n, T2-laiteohjelmiston, tvOS:n ja watchOS:n. Itsenäisiin sertifiointeihin sisältyy aluksi Safari-selain- ja Yhteystiedot-apit, ja sertifioitavia appeja lisätään tulevaisuudessa.

Jos haluat tietoja julkisista sertifikaateista, jotka koskevat Applen *käyttöjärjestelmiä*, katso:

- iOS:n tietoturvasertifikaatit
- iPadOS:n tietoturvasertifikaatit
- macOS:n tietoturvasertifikaatit
- tvOS:n tietoturvasertifikaatit
- watchOS:n tietoturvasertifikaatit

Jos haluat tietoja julkisista sertifioinneista, jotka koskevat Applen *appeja*, katso:

- Applen appien tietoturvasertifioinnit

Palveluiden sertifioinnit

Apple ylläpitää tietoturvasertifiointeja tukeakseen yritysmaailman ja koulutusalan asiakkaita. Sertifiointien ansiosta Applen asiakkaat voivat täyttää määräyksiin ja sopimuksiin perustuvat velvoitteensa käyttäessään Applen palveluita Applen laitteistojen ja ohjelmistojen kanssa. Nämä sertifioinnit tarjoavat asiakkaillemme riippumattoman todistuksen Applen sertifioinnin piiriin kuuluvien järjestelmien tietoturva-, ympäristö- ja tietosuojakäytännöistä.

Jos haluat tietoja julkisista sertifikaateista, jotka koskevat Applen *internet-palveluita*, katso:

- Applen internet-palvelujen tietoturvasertifikaatit

Voit lähettää kysymyksiä Applen tietoturva- ja tietosuojasertifioinneista osoitteeseen security-certifications@apple.com.

Laitteistojen tietoturvan sertifioinnit

Applen laitteistojen tietoturvasertifiointien yleiskatsaus

Apple ylläpitää sepOS:lle ja T2-laiteohjelmistolle sekä muille sertifioinneille yhdysvaltalaisen FIPS (Federal Information Processing Standard) -standardin 140-2/-3 mukaisia validointisertifikaatteja. Apple lähtee liikkeelle sellaisista *sertifioinnin osista*, jotka koskevat laajasti eri alustoja. Yksi osa on corecryptokirjaston validointi, jota käytetään laitteistojen ja ohjelmistojen salausmoduuleissa Applen kehittämissä käyttöjärjestelmissä. Toinen osa on moniin Applen laitteisiin sisällytetyn Secure Enclaven sertifiointi. Kolmas on Touch ID:tä tukevissa Apple-laitteissa ja Face ID:tä tukevissa laitteissa olevan Secure Elementin (SE) sertifiointi. Nämä laitteistojen sertifiointien osat muodostavat perustan laajemmille alustojen tietoturvasertifioinneille.

Salausalgoritmien validoinnit

Monien salausalgoritmien ja niihin liittyvien tietoturvatoimintojen oikeanlaisen toteutuksen validointi on edellytys FIPS 140-3 -validoinnille ja samalla se tukee muita sertifiointeja. Validointia hallinnoi Yhdysvaltain standardointielimen NIST:n (National Institute of Standards and Technology) Cryptographic Algorithm Validation Program (CAVP) -ohjelma. Applen toteutusten validointisertifikaatit löytyvät CAVP:n hakupalvelusta. Jos haluat lisätietoja, katso Cryptographic Algorithm Validation Program (CAVP) -ohjelman verkkosivusto.

Salausmoduulien validoinnit: FIPS 140-2/3 (ISO/IEC 19790)

Cryptographic Module Validation Program (CMVP) -ohjelma on toistuvasti validoinut Applen salausmoduulit U.S. Federal Information Processing Standard -standardin (FIPS 140-2) salausmoduuleille asettamien vaatimusten mukaisiksi jokaisen merkittävän käyttöjärjestelmän julkistuksen jälkeen vuodesta 2012 lähtien. Jokaisen merkittävän julkistuksen jälkeen Apple lähettää moduulit CMVP:lle validoitaviksi standardin vaatimusten mukaisesti. Sen lisäksi, että Applen käyttöjärjestelmät ja apit käyttävät näitä moduuleja, ne tarjoavat salaustoimintoja Applen tarjoamille palveluille ja ovat muiden valmistajien appien käytettävissä.

Apple saavuttaa joka vuosi **suojaustason 1** ohjelmistopohjaisille moduuleille ”Corecrypto Module for Intel” ja ”Corecrypto Kernel Module for Intel” macOS:lle. Apple siliconin moduulit "Corecrypto Module for ARM" ja "Corecrypto Kernel Module for ARM" ovat soveltuvia iOS:lle, iPadOS:lle, tvOS:lle, watchOS:lle ja Mac-tietokoneisiin sisällytetyn Apple T2 Security -sirun laiteohjelmistolle.

Vuonna 2019 Apple saavutti ensimmäisen kerran FIPS 140-2 **-suojaustason 2** upotetulle laitteiston salausmoduulille, joka tunnetaan ”Apple Corecrypto Module: Secure Key Store” -salausmoduulina. Tämä mahdollistaa Secure Enclaven generoimien ja hallitsemien avaimien Yhdysvaltain viranomaistahojen hyväksymän käytön. Apple hakee myös jatkossa validointeja laitteiston salausmoduulille jokaisen merkittävän käyttöjärjestelmäjulkaisun myötä.

Yhdysvaltain kauppaministeriö hyväksyi **FIPS 140-3:n** vuonna 2019. Huomattavin muutos tässä standardiversiossa on, että siinä nimetään ISO/IEC-standardit, erityisesti ISO/IEC 19790:2015 ja siihen liittyvä testausstandardi ISO/IEC 24759:2017. CMVP on aloittanut siirtymisohjelman ja ilmoittanut, että vuodesta 2020 lähtien salausmoduulit aletaan validoida FIPS 140-3:n pohjalta. Applen salausmoduuleissa pyritään vastaamaan FIPS 140-3 -standardia ja siirtymään siihen niin pian kuin se on käytännössä mahdollista.

CMVP ylläpitää parhaillaan testattavina ja validoitavina olevista salausmoduuleista kahta eri luetteloa, jotka voivat sisältää tietoja esitetyistä validoinneista. Akkreditoidun laboratorion testattavina olevat moduulit voivat olla Implementation Under Test List -luettelossa. Kun laboratorio on suorittanut testauksen ja suosittelee validointia CMVP:lle, Applen salausmoduulit näkyvät Modules in Process List -luettelossa. Tällä hetkellä laboratoriotestaus on valmis ja odottaa CMVP:n validointia testaukselle. Koska arviointiprosessin kesto voi vaihdella, katso tietoja Applen salausmoduulien validoinnin tilasta kahdesta edellä olevasta luettelosta merkittävän käyttöjärjestelmäjulkaisun ja CMVP:n validointisertifikaatin myöntämisen väliseltä ajalta.

Tuotteiden sertifioinnit: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) on standardi, jota monet organisaatiot käyttävät IT-tuotteiden tietoturva-arviointien perustana.

Jos olet kiinnostunut sertifikaateista, jotka voidaan tunnustaa vastavuoroisesti kansainvälisessä Common Criteria Recognition Arrangement (CCRA) -järjestelyssä, katso tietoja Common Criteria -portaalista. Common Criteria -standardia voidaan myös käyttää CCRA:n ulkopuolella kansallisissa ja yksityisissä validointijärjestelmissä. Euroopassa vastavuoroista tunnustamista ohjaavat SOG-IS-sopimus ja CCRA.

Common Criteria -yhteisön ilmaisema tavoite on kansainvälisesti hyväksytty joukko tietoturvastandardeja IT-tuotteiden suojausominaisuuksien selkeää ja luotettavaa arviointia varten. Tarjoamalla riippumattoman arvion tuotteen edellytyksistä täyttää tietoturvastandardit, Common Criteria -sertifiointi antaa asiakkaille enemmän varmuutta IT-tuotteiden suojauksen suhteen ja auttaa tekemään valistuneempia päätöksiä.

CCRA-järjestelyssä jäsenmaat ovat sopineet, että ne tunnustavat IT-tuotteiden sertifioinnin samalla luottamustasolla. Ennen sertifiointeja tarvittavat arvioinnit ovat laajoja, ja ne sisältävät seuraavat:

- Protection Profiles (PP) -suojausprofiilit
- Security Targets (ST) -dokumentit
- Security Functional Requirements (SFR) -vaatimukset
- Security Assurance Requirements (SAR) -vaatimukset
- Evaluation Assurance Levels (EAL) -tasot

Suojausprofiilit (Protection Profile, PP) ovat dokumentteja, joissa on määritetty mitä suojausvaatimuksia laitetyyppiluokalle (kuten Mobility) vaaditaan, ja niitä käytetään saman luokan IT-tuotteiden vertailemiseksi. CCRA:n jäsenmäärä sekä hyväksyttyjen PP-suojausprofiilien luettelo kasvavat vuosittain. Tämän järjestelyn ansiosta tuotteen kehittäjä voi hakea kertasertifiointia missä tahansa tässä järjestelyssä mukana olevassa sertifikaatteja myöntävässä järjestelmässä ja saada sertifioinnille tunnustuksen kaikilta sen tunnustamiseen sitoutuneilta allekirjoittajajäseniltä.

Security Target -dokumentit määrittävät, *mitä* arvioidaan, kun IT-tuotetta sertifioidaan. Security Target -dokumentit muunnetaan tarkemmiksi *suojauksen toiminnallisiksi vaatimuksiksi (SFR)*, joita käytetään Security Target -dokumenttien yksityiskohtaisempaan arviointiin.

Common Criteria (CC) -standardi sisältää myös *tietoturvavarmuusvaatimukset (SAR)*. Yksi yleisesti tunnistettu mittaperuste on *varmuustaso (Evaluation Assurance Level, EAL)*. EAL-varmuustasot ryhmittelevät yhteen usein käytettyjä SAR-tietoturvavarmuusvaatimusten joukkoja, ja vertailtavuuden parantamiseksi ne voidaan eritellä PP-suojausprofiilissa ja ST-dokumentissa.

Monet vanhemmat suojausprofiilit (PP) on arkistoitu, ja niitä korvataan kehittämällä kohdennettuja PP-suojausprofiileita, jotka keskittyvät tiettyihin ratkaisuihin ja ympäristöihin. Jotta CCRA:n jäsenet jatkossakin noudattaisivat vastavuoroisen tunnustamisen periaatetta, on muodostettu iTC-yhteisöjä (international Technical Community), jotka kehittävät ja ylläpitävät yhteistyönä laadittuja cPP-profiileja (collaborative Protection Profiles), ja CCRA:n allekirjoittajajäsenet ovat alusta pitäen olleet mukana näiden profiilien kehitystyössä. Muille käyttäjäryhmille ja vastavuoroisen tunnustamisen sopimuksille kuin CCRA:lle kohdennettuja PP-suojausprofiileja kehittävät edelleen niiden kannalta tarkoituksenmukaiset sidosryhmät.

Apple on hakenut tiettyjen cPP-profiilien mukaisia sertifiointeja päivitetyssä CCRA-järjestelyssä alkuvuodesta 2015 alkaen. Siitä lähtien Apple on saavuttanut Common Criteria -sertifioinnit jokaiselle merkittävälle iOS-julkaisulle ja on laajentanut kattavuuden sisältämään uusien PP-suojausprofiilien varmistukset.

Apple toimii aktiivisessa roolissa teknisissä yhteisöissä, jotka keskittyvät mobiililaitteiden suojausteknologioiden arviointiin. Näihin lukeutuvat iTC-yhteisöt, jotka vastaavat cPP-suojausprofiilien kehittämisestä ja päivittämisestä. Apple arvioi ja hakee edelleen sertifiointeja nykyisten PP- ja cPP-suojausprofiilien perusteella.

Apple-alustojen sertifioinnit Pohjois-Amerikan markkinoille suorittaa yleensä National Information Assurance Partnership (NIAP), joka ylläpitää luetteloa parhaillaan arvioitavina olevista projekteista, joita ei ole vielä sertifioitu.

Lueteltujen yleisten alustasertifikaattien lisäksi on myönnetty muita sertifikaatteja joitakin markkinoita koskevien erityisten suojausvaatimusten osoittamiseksi.

Tietoturvasertifioinnit Secure Enclave -prosessorille

Secure Enclave -sertifioinnin tausta

Laitteiston salausmoduuli *Apple SEP Secure Key Store Cryptographic Module* on upotettu Applen järjestelmäpiiriin (SOC), joka on seuraavissa tuotteissa: Applen A-sarja iPhonelle ja iPadille, M-sarja Mac-tietokoneille, joissa on Apple silicon, S-sarja Apple Watchille ja T-sarjan suojauspiiri Intel-pohjaisille Mac-tietokoneille alkaen vuonna 2017 julkaistusta iMac Prosta.

Vuonna 2018 Apple synkronoi vuonna 2017 julkaistujen käyttöjärjestelmäohjelmistoversioiden ohjelmiston salausmoduulien kanssa: iOS 11, macOS 10.13, tvOS 11 ja watchOS 4. SEP:n laitteiston salausmoduuli, josta käytettiin nimeä Apple SEP Secure Key Store Cryptographic Module v1.0, validoitiin aluksi FIPS 140-2 -suojaustason 1 vaatimusten mukaiseksi.

Vuonna 2019 Apple validoi laitteistomoduulin FIPS 140-2 -suojaustason 2 vaatimusten mukaiseksi ja päivitti moduulin versionumeroksi 9.0, jotta se on yhteneväinen vastaavien corecrypto User- ja corecrypto Kernel -moduulien validointiversioiden kanssa. Vuonna 2019 tähän sisältyivät iOS 12, macOS 10.14, tvOS 12 ja watchOS 5.

Vuonna 2020 ja 2021 Apple hakee validointia FIPS 140-3:n vaatimustenmukaisuudelle ja lisävamistuksella Apple siliconin fyysisten suojausvaatimusten suojaustasolle 3: A13-, A14-, S6- ja M1-siruille.

Apple myös hakee aktiivisesti corecrypto User- ja corecrypto Kernel -moduulien validointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä. Vaatimustenmukaisuusvalidointi voidaan tehdä ainoastaan lopullisille julkaistuille versioille.

Salausmoduulien validoinnin tila

Cryptographic Module Validation Program (CMVP) ylläpitää salausmoduulien validoinnin tilasta kolmea eri luetteloa, joilla salausmoduulit voivat olla riippuen validointinsa senhetkisestä tilasta:

- Kun Apple on tehnyt sopimuksen laboratorion kanssa testaamisesta, moduuli voidaan lisätä CMVP:n Implementation Under Test List -luetteloon.
- Kun laboratorio on suorittanut testauksen ja suositellut validointia CMVP:lle ja kun maksut CMVP:lle on suoritettu, moduuli lisätään Modules in Process List -luetteloon. MIP-luettelossa seurataan CMVP:n validoinnin etenemistä neljässä vaiheessa:
  - *Review Pending:* Odottaa, että tehtävä annetaan resurssille CMVP:ssä.
  - *In Review:* CMVP:n resurssit suorittavat validointitoimia.
  - *Coordination:* Laboratorio ja CMVP selvittävät mahdollisesti esiin tulleita ongelmia.
  - *Finalization:* Sertifikaatin antamiseen liittyvät toiminnot ja muodollisuudet.
- Kun CMVP:n validointi on valmis, moduulit saavat sertifikaatin, joka kertoo niiden täyttävän vaatimukset, ja ne lisätään validoitujen salausmoduulien luetteloon. Tähän sisältyy:
  - Validoidut moduulit, jotka on merkitty aktiivisiksi.
  - Viiden vuoden kuluttua moduulit siirretään historical-luetteloon.
  - Jos moduulin sertifikaatti jostakin syystä perutaan, se siirretään revoked-luetteloon.

Vuonna 2020 CMVP otti kansainvälisen ISO/IEC 19790 -standardin FIPS 140-3 -validoinnin perustaksi.

FIPS 140-3 -sertifioinnit

Nykytilanne

Alla olevassa taulukossa näkyvät vuoden 2020 ja 2021 salausmoduulit, joiden FIPS 140-3 -vaatimustenmukaisuutta laboratorio testaa parhaillaan.

Vuoden 2020 ja 2021 käyttöjärjestelmäversioihin liittyvät suojatut avaintallennukset (Secure Key Store, SKS) ovat käyneet läpi laboratoriotestauksen ja saaneet laboratoriolta suosituksen CMVP:n validoinnille. Ne löytyvät Modules in Process -luettelosta ja siirtyvät validoinnin jälkeen validoitujen salausmoduulien luetteloon.

iOS 15:n (2021) käyttäjätila, kerneltila ja avaintallennus ovat laboratoriotestauksessa. Ne löytyvät Implementation Under Test -luettelosta.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan vuoden 2021 iOS-, iPadOS-, macOS-, tvOS- ja watchOS-julkaisujen kanssa *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14, T2, M1, S3-S6) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan vuoden 2021 iOS-, iPadOS-, macOS-, tvOS- ja watchOS-julkaisujen kanssa *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A13, A14, S6, M1) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan vuoden 2020 iOS-, iPadOS-, macOS-, tvOS- ja watchOS-julkaisujen kanssa *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14, T2, M1, S3-S6) *Suojaustaso:* 2

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan vuoden 2020 iOS-, iPadOS-, macOS-, tvOS- ja watchOS-julkaisujen kanssa *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A13, A14, S6, M1) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3

FIPS 140-2 -sertifioinnit

Alla olevassa taulukossa näkyvät salausmoduulit, joiden FIPS 140-2 -vaatimustenmukaisuuden laboratorio on testannut.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 5.2.2021	*Sertifikaatit:* 3811 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v10.0 *Käyttöjärjestelmä:* sepOS macOS 10.15 Catalinalle *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3523 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v9.0 *Käyttöjärjestelmä:* sepOS macOS 10.14 Mojavelle *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3223 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v1.0 *Käyttöjärjestelmä:* sepOS macOS 10.13 High Sierralle *Tyyppi:* Laitteistot *Suojaustaso:* 2

Common Criteria (CC) -sertifioinnit

Apple osallistuu aktiivisesti Common Criteria -arviointeihin, joissa asianmukaiset PP-suojausprofiilit (Protection Profile, PP) kattavat Applen teknologian suojaustoimintoja.

Common Criteria (CC) -sertifioinnin tila

NIAP:n johtamassa Yhdysvaltain arviointijärjestelmässä ylläpidetään Products in Evaluation -luetteloa tuotteista, jotka ovat parhaillaan arvioitavina Yhdysvalloissa NIAP:n hyväksymässä Common Criteria -testauslaboratoriossa (CCTL) ja joille on tehty arvioinnin aloitustapaaminen (tai vastaava), jossa CCEVS:n hallinto on virallisesti hyväksynyt tuotteen arvioitavaksi.

Kun tuotteet on sertifioitu, NIAP lisää parhaillaan voimassa olevat sertifioinnit Product Compliant -luetteloon. Kahden vuoden jälkeen näistä sertifioinneista tarkistetaan, täyttyvätkö senhetkisen käytännön vaatimukset varmistuksen voimassaolon jatkamiselle. Kun varmistuksen voimassaoloaika päättyy, NIAP siirtää sertifioinnin arkistoitujen tuotteiden Archived Products -luetteloon.

Common Criteria -portaalissa luetellaan sertifioinnit, jotka voidaan tunnustaa vastavuoroisesti Common Criteria Recognition Arrangement (CCRA) -järjestelyn puitteissa. Tuotteet voidaan pitää CC-portaalissa sertifioitujen tuotteiden luettelossa viiden vuoden ajan, ja CC-portaalissa säilytetään tiedot myös arkistoiduista sertifioinneista.

Alla olevassa taulukossa näkyvät sertifioinnit, joita laboratorio arvioi parhaillaan tai jotka ovat saaneet Common Criteria -vaatimustenmukaisuuden sertifioinnin.

Käyttöjärjestelmä / sertifiointipäiväys	**Tunniste / dokumentit**	**Nimi / suojausprofiilit**
Käyttöjärjestelmä: sepOS *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple Secure Enclave [2020] *Suojausprofiilit:* CPP_DSC_V1.0 *Laitteisto:* Secure Enclave (A9-A14, M1, T2, S3-S6) *Ohjelmisto:* sepOS, joka toimitetaan iOS 14:n, iPadOS 14:n, macOS 11:n Big Surin, tvOS 14:n ja watchOS 7:n mukana

Muut sertifioinnit

Alla olevassa taulukossa näkyvät sellaiset Secure Enclaven sertifioinnit, jotka eivät perustu Common Criteria -vaatimuksiin tai FIPS 140-3 -standardiin.

Päiväykset	**Sertifikaatit / dokumentit**	**Moduulitiedot**
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* 7.12.2019–26.12.2022	*Sertifikaatit:* CFNR201902910002 (Kiinan kansantasavalta: Technology Certification of Mobile Financial Service) Kiinankielinen versio Englanninkielinen versio	*Nimi:* Mobile Terminal Trusted Execution Environment *Käyttöjärjestelmä:* iOS 13.5.1 *Standardi:* JR/T 0156-2017

Apple T2 Security -sirun suojauksen sertifioinnit

Salausmoduulien validoinnin tausta

Apple hakee aktiivisesti Applen upotettujen ohjelmisto- ja laitteistomoduulien validointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä. Vaatimustenmukaisuusvalidointi voidaan tehdä ainoastaan moduulien lopullisille julkaistuille versioille.

Vuonna 2020 CMVP otti kansainvälisen ISO/IEC 19790 -standardin yhdysvaltalaisen Federal Information Processing Standard (FIPS) 140-3 -validoinnin perustaksi.

Intel-prosessorin lisäksi vuodesta 2017 alkaen useimmissa Mac-tietokoneissa on myös erillinen Apple T2 Security -siru, joka on Apple silicon -pohjainen järjestelmäpiiri (SoC). Nämä T2-sirulla varustetut Mac-tietokoneet käyttävät kaikkia viittä salausmoduulia erilaisiin laitteissa suoritettaviin palveluihin.

- Corecrypto-käyttäjämoduuli Intelille (tätä käyttää macOS Intel-pohjaisissa Mac-tietokoneissa)
- Corecrypto-kernelmoduuli Intelille (tätä käyttää macOS Intel-pohjaisissa Mac-tietokoneissa)
- Corecrypto-käyttäjämoduuli ARM:lle (tätä käyttää T2-siru)
- Corecrypto-kernelmoduuli ARM:lle (tätä käyttää T2-siru)
- Secure Key Store -salausmoduuli (tätä käyttää T2-siruun upotettu Secure Enclave -lisäprosessori)

Huomaa: T2-sirulla toimivat Apple silicon -pohjaiset moduulit ovat samat kuin ne, jotka toimivat muilla Applen silicon-siruilla, kuten Applen A-sarjan, S-sarjan ja M-sarjan siruilla.

Salausmoduulien validoinnin tila

Cryptographic Module Validation Program (CMVP) ylläpitää salausmoduulien validoinnin tilasta kolmea eri luetteloa, joilla salausmoduulit voivat olla riippuen validointinsa senhetkisestä tilasta:

- Kun Apple on tehnyt sopimuksen laboratorion kanssa testaamisesta, moduuli voidaan lisätä CMVP:n Implementation Under Test List -luetteloon.
- Kun laboratorio on suorittanut testauksen ja suositellut validointia CMVP:lle ja kun maksut CMVP:lle on suoritettu, moduuli lisätään Modules in Process List (MIP) -luetteloon. MIP-luettelossa seurataan CMVP:n validoinnin etenemistä neljässä vaiheessa:
  - *Review Pending:* Odottaa, että tehtävä annetaan resurssille CMVP:ssä.
  - *In Review:* CMVP:n resurssit suorittavat validointitoimia.
  - *Coordination:* Laboratorio ja CMVP selvittävät mahdollisesti esiin tulleita ongelmia.
  - *Finalization:* Sertifikaatin antamiseen liittyvät toiminnot ja muodollisuudet.
- Kun CMVP:n validointi on valmis, moduulit saavat sertifikaatin, joka kertoo niiden täyttävän vaatimukset, ja ne lisätään validoitujen salausmoduulien luetteloon. Tähän sisältyy:
  - Validoidut moduulit, jotka on merkitty aktiivisiksi.
  - Viiden vuoden kuluttua moduulit siirretään historical-luetteloon.
  - Jos moduulin sertifikaatti jostakin syystä perutaan, se siirretään revoked-luetteloon.

FIPS 140-3 -sertifioinnit

Nykytilanne

Vuoden 2020 moduulit käyttäjätilalle, kerneltilalle ja avaintallennukselle ovat käyneet läpi laboratoriotestauksen ja saaneet laboratoriolta suosituksen CMVP:n validoinnille. Ne löytyvät luettelosta Modules in Process List.

Vuoden 2021 moduulit käyttäjätilalle, kerneltilalle ja avaintallennukselle ovat laboratoriotestauksessa. Ne löytyvät Implementation Under Test -luettelosta.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* sepOS macOS 12 Montereylle *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* sepOS macOS 12 Montereylle *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* sepOS macOS 12 Montereylle *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (T2) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS macOS 11 Big Surille *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS macOS 11 Big Surille *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS macOS 11 Big Surille (Intel) *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteistot *Suojaustaso:* 2

FIPS 140-2 -sertifioinnit

Alla olevassa taulukossa näkyvät salausmoduulit, joiden FIPS 140-2 -vaatimustenmukaisuuden laboratorio on testannut.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3856 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v10.0 for ARM *Käyttöjärjestelmä:* sepOS macOS 10.15 Catalinalle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3855 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v10.0 for ARM *Käyttöjärjestelmä:* sepOS macOS 10.15 Catalinalle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 5.2.2021	*Sertifikaatit:* 3811 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Käyttöjärjestelmä:* sepOS macOS 10.15 Catalinalle *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 23.4.2019	*Sertifikaatit:* 3438 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v9.0 for ARM *Käyttöjärjestelmä:* sepOS macOS 10.14 Mojavelle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 11.4.2019	*Sertifikaatit:* 3433 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v9.0 for ARM *Käyttöjärjestelmä:* sepOS macOS 10.14 Mojavelle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3523 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v9.0 *Käyttöjärjestelmä:* sepOS macOS 10.14 Mojavelle *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 22.5.2018, 6.7.2018	*Sertifikaatit:* 3148 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v8.0 for ARM *Käyttöjärjestelmä:* sepOS macOS 10.13 High Sierralle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 17.5.2018, 3.7.2018	*Sertifikaatit:* 3147 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v8.0 for ARM *Käyttöjärjestelmä:* sepOS macOS 10.13 High Sierralle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 10.7.2018	*Sertifikaatit:* 3223 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v1.0 *Käyttöjärjestelmä:* sepOS macOS 10.13 High Sierralle *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2016 *Validointipäivät:* 1.2.2017	*Sertifikaatit:* 2828 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple iOS Corecrypto Kernel Module v7.0 *Käyttöjärjestelmä:* sepOS macOS 10.12 Sierralle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2016 *Validointipäivät:* 1.2.2017	*Sertifikaatit:* 2827 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple iOS Corecrypto Kernel Module v7.0 *Käyttöjärjestelmä:* sepOS macOS 10.12 Sierralle *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Käyttöjärjestelmien tietoturvasertifioinnit

Applen käyttöjärjestelmien tietoturvasertifiointien yleiskatsaus

Apple ylläpitää sepOS:lle ja T2-laiteohjelmistolle sekä muille sertifioinneille yhdysvaltalaisen FIPS (Federal Information Processing Standard) -standardin 140-2/-3 mukaisia validointisertifikaatteja. Apple lähtee liikkeelle sellaisista *sertifioinnin osista*, jotka koskevat laajasti eri alustoja. Yksi osa on corecryptokirjaston validointi, jota käytetään laitteistojen ja ohjelmistojen salausmoduuleissa Applen kehittämissä käyttöjärjestelmissä. Toinen osa on moniin Applen laitteisiin sisällytetyn Secure Enclaven sertifiointi. Kolmas on Touch ID:tä tukevissa Apple-laitteissa ja Face ID:tä tukevissa laitteissa olevan Secure Elementin (SE) sertifiointi. Nämä laitteistojen sertifiointien osat muodostavat perustan laajemmille alustojen tietoturvasertifioinneille.

Salausalgoritmien validoinnit

Monien salausalgoritmien ja niihin liittyvien tietoturvatoimintojen oikeanlaisen toteutuksen validointi on edellytys FIPS 140-3 -validoinnille ja samalla se tukee muita sertifiointeja. Validointia hallinnoi Yhdysvaltain standardointielimen NIST:n Cryptographic Algorithm Validation Program (CAVP) -ohjelma. Applen toteutusten validointisertifikaatit löytyvät CAVP:n hakupalvelusta.

Salausmoduulien validoinnit: FIPS 140-2/3 (ISO/IEC 19790)

Cryptographic Module Validation Program (CMVP) -ohjelma on toistuvasti validoinut Applen käyttöjärjestelmien salausmoduulit U.S. Federal Information Processing Standards (FIPS) -standardien 140-2 mukaisiksi jokaisen merkittävän käyttöjärjestelmäjulkistuksen jälkeen vuodesta 2012 lähtien. Jokaisen merkittävän julkistuksen jälkeen Apple lähettää kaikki moduulit CMVP:lle salauksen täyttä validointia varten. Nämä validoidut moduulit tuottavat salaustoimintoja Applen tarjoamille palveluille, ja ne ovat muiden valmistajien appien käytettävissä.

Apple saavuttaa joka vuosi **suojaustason 1** ohjelmistopohjaisille moduuleille ”Corecrypto Module for Intel” ja ”Corecrypto Kernel Module for Intel” macOS:lle. Apple siliconin moduulit "Corecrypto Module for ARM" ja "Corecrypto Kernel Module for ARM" ovat soveltuvia iOS:lle, iPadOS:lle, tvOS:lle, watchOS:lle ja Mac-tietokoneisiin sisällytetyn Apple T2 Security -sirun laiteohjelmistolle.

Vuonna 2019 Apple saavutti ensimmäisen kerran FIPS 140-2 **-suojaustason 2** upotetulle laitteiston salausmoduulille, joka tunnetaan ”Apple Corecrypto Module: Secure Key Store” -salausmoduulina. Tämä mahdollistaa Secure Enclaven generoimien ja hallitsemien avaimien Yhdysvaltain viranomaistahojen hyväksymän käytön. Apple hakee myös jatkossa validointeja laitteiston salausmoduulille jokaisen merkittävän käyttöjärjestelmäjulkaisun myötä.

Yhdysvaltain kauppaministeriö hyväksyi **FIPS 140-3:n** vuonna 2019. Huomattavin muutos tässä standardiversiossa on, että siinä nimetään ISO/IEC-standardit, erityisesti ISO/IEC 19790:2015 ja siihen liittyvä testausstandardi ISO/IEC 24759:2017. CMVP on aloittanut siirtymisohjelman ja ilmoittanut, että vuodesta 2020 lähtien salausmoduulit aletaan validoida FIPS 140-3:n pohjalta. Applen salausmoduuleissa pyritään vastaamaan FIPS 140-3 -standardia ja siirtymään siihen niin pian kuin se on käytännössä mahdollista.

CMVP ylläpitää parhaillaan testattavina ja validoitavina olevista salausmoduuleista kahta eri luetteloa, jotka voivat sisältää tietoja esitetyistä validoinneista. Akkreditoidun laboratorion testattavina olevat moduulit voivat olla Implementation Under Test List -luettelossa. Kun laboratorio on suorittanut testauksen ja suosittelee validointia CMVP:lle, Applen salausmoduulit näkyvät Modules in Process List -luettelossa. Tällä hetkellä laboratoriotestaus on valmis ja odottaa CMVP:n validointia testaukselle. Koska arviointiprosessin kesto voi vaihdella, katso tietoja Applen salausmoduulien validoinnin tilasta kahdesta edellä olevasta luettelosta merkittävän käyttöjärjestelmäjulkaisun ja CMVP:n validointisertifikaatin myöntämisen väliseltä ajalta.

Tuotteiden sertifioinnit: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) on standardi, jota monet organisaatiot käyttävät IT-tuotteiden tietoturva-arviointien perustana.

Jos olet kiinnostunut sertifikaateista, jotka voidaan tunnustaa vastavuoroisesti kansainvälisessä Common Criteria Recognition Arrangement (CCRA) -järjestelyssä, katso tietoja Common Criteria -portaalista. Common Criteria -standardia voidaan myös käyttää CCRA:n ulkopuolella kansallisissa ja yksityisissä validointijärjestelmissä. Euroopassa vastavuoroista tunnustamista ohjaavat SOG-IS-sopimus ja CCRA.

Common Criteria -yhteisön ilmaisema tavoite on kansainvälisesti hyväksytty joukko tietoturvastandardeja IT-tuotteiden suojausominaisuuksien selkeää ja luotettavaa arviointia varten. Tarjoamalla riippumattoman arvion tuotteen edellytyksistä täyttää tietoturvastandardit, Common Criteria -sertifiointi antaa asiakkaille enemmän varmuutt a IT-tuotteiden suojauksen suhteen ja auttaa tekemään valistuneempia päätöksiä.

CCRA-järjestelyssä jäsenmaat ovat sopineet, että ne tunnustavat IT-tuotteiden sertifioinnin samalla luottamustasolla. Ennen sertifiointeja tarvittavat arvioinnit ovat laajoja, ja ne sisältävät seuraavat:

- Protection Profiles (PP) -suojausprofiilit
- Security Targets (ST) -dokumentit
- Security Functional Requirements (SFR) -vaatimukset
- Security Assurance Requirements (SAR) -vaatimukset
- Evaluation Assurance Levels (EAL) -tasot

Suojausprofiilit (Protection Profile, PP) ovat dokumentteja, joissa on määritetty mitä suojausvaatimuksia laitetyyppiluokalle (kuten Mobility) vaaditaan, ja niitä käytetään saman luokan IT-tuotteiden vertailemiseksi. CCRA:n jäsenmäärä sekä hyväksyttyjen PP-suojausprofiilien luettelo kasvavat vuosittain. Tämän järjestelyn ansiosta tuotteen kehittäjä voi hakea kertasertifiointia missä tahansa tässä järjestelyssä mukana olevassa sertifikaatteja myöntävässä järjestelmässä ja saada sertifioinnille tunnustuksen kaikilta sen tunnustamiseen sitoutuneilta allekirjoittajajäseniltä.

Security Target -dokumentit määrittävät, *mitä* arvioidaan, kun IT-tuotetta sertifioidaan. Security Target -dokumentit muunnetaan tarkemmiksi *suojauksen toiminnallisiksi vaatimuksiksi (SFR)*, joita käytetään Security Target -dokumenttien yksityiskohtaisempaan arviointiin.

Common Criteria (CC) -standardi sisältää myös *tietoturvavarmuusvaatimukset (SAR)*. Yksi yleisesti tunnistettu mittaperuste on *varmuustaso (Evaluation Assurance Level, EAL)*. EAL-varmuustasot ryhmittelevät yhteen usein käytettyjä SAR-tietoturvavarmuusvaatimusten joukkoja, ja vertailtavuuden parantamiseksi ne voidaan eritellä PP-suojausprofiilissa ja ST-dokumentissa.

Monet vanhemmat suojausprofiilit (PP) on arkistoitu, ja niitä korvataan kehittämällä kohdennettuja PP-suojausprofiileita, jotka keskittyvät tiettyihin ratkaisuihin ja ympäristöihin. Jotta CCRA:n jäsenet jatkossakin noudattaisivat vastavuoroisen tunnustamisen periaatetta, on muodostettu iTC-yhteisöjä (international Technical Community), jotka kehittävät ja ylläpitävät *yhteistyönä laadittuja cPP-profiileja (collaborative Protection Profiles)*, ja CCRA:n allekirjoittajajäsenet ovat alusta pitäen olleet mukana näiden profiilien kehitystyössä. Muille käyttäjäryhmille ja vastavuoroisen tunnustamisen sopimuksille kuin CCRA:lle kohdennettuja PP-suojausprofiileja kehittävät edelleen niiden kannalta tarkoituksenmukaiset sidosryhmät.

Apple on hakenut tiettyjen cPP-profiilien mukaisia sertifiointeja päivitetyssä CCRA-järjestelyssä alkuvuodesta 2015 alkaen. Siitä lähtien Apple on saavuttanut Common Criteria -sertifioinnit jokaiselle merkittävälle iOS-julkaisulle ja on laajentanut kattavuuden sisältämään uusien PP-suojausprofiilien varmistukset.

Apple toimii aktiivisessa roolissa teknisissä yhteisöissä, jotka keskittyvät mobiililaitteiden suojausteknologioiden arviointiin. Näihin lukeutuvat iTC-yhteisöt, jotka vastaavat cPP-suojausprofiilien kehittämisestä ja päivittämisestä. Apple arvioi ja hakee edelleen sertifiointeja nykyisten PP- ja cPP-suojausprofiilien perusteella.

Apple-alustojen sertifioinnit Pohjois-Amerikan markkinoille suorittaa yleensä National Information Assurance Partnership (NIAP), joka ylläpitää luetteloa parhaillaan arvioitavina olevista projekteista, joita ei ole vielä sertifioitu.

Lueteltujen yleisten alustasertifikaattien lisäksi on myönnetty muita sertifikaatteja joitakin markkinoita koskevien erityisten suojausvaatimusten osoittamiseksi.

iOS:n tietoturvasertifikaatit

iOS:n sertifioinnin tausta

Apple hakee aktiivisesti Applen upotettujen ohjelmisto- ja laitteistomoduulien validointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä. Vaatimustenmukaisuusvalidointi voidaan tehdä ainoastaan lopullisille julkaistuille versioille.

iOS:n salausmoduulien validoinnin tila

Cryptographic Module Validation Program (CMVP) ylläpitää salausmoduulien validoinnin tilasta kolmea eri luetteloa, joilla salausmoduulit voivat olla riippuen validointinsa senhetkisestä tilasta:

- Kun Apple on tehnyt sopimuksen laboratorion kanssa testaamisesta, moduuli voidaan lisätä CMVP:n Implementation Under Test List -luetteloon.
- Kun laboratorio on suorittanut testauksen ja suositellut validointia CMVP:lle ja kun maksut CMVP:lle on suoritettu, moduuli lisätään Modules in Process List (MIP) -luetteloon. MIP-luettelossa seurataan CMVP:n validoinnin etenemistä neljässä vaiheessa:
  - *Review Pending:* Odottaa, että tehtävä annetaan resurssille CMVP:ssä.
  - *In Review:* CMVP:n resurssit suorittavat validointitoimia.
  - *Coordination:* Laboratorio ja CMVP selvittävät mahdollisesti esiin tulleita ongelmia.
  - *Finalization:* Sertifikaatin antamiseen liittyvät toiminnot ja muodollisuudet.
- Kun CMVP:n validointi on valmis, moduulit saavat sertifikaatin, joka kertoo niiden täyttävän vaatimukset, ja ne lisätään validoitujen salausmoduulien luetteloon. Tähän sisältyy:
  - Validoidut moduulit, jotka on merkitty aktiivisiksi.
  - Viiden vuoden kuluttua moduulit siirretään historical-luetteloon.
  - Jos moduulin sertifikaatti jostakin syystä perutaan, se siirretään revoked-luetteloon.

Vuonna 2020 CMVP otti kansainvälisen ISO/IEC 19790 -standardin FIPS 140-3 -validoinnin perustaksi.

FIPS 140-3 -sertifioinnit

Nykytilanne

iOS 14:n (2020) käyttäjätila, kerneltila ja avaintallennus ovat käyneet läpi laboratoriotestauksen ja saaneet laboratoriolta suosituksen CMVP:n validoinnille. Ne löytyvät luettelosta Modules in Process List.

iOS 15:n (2021) käyttäjätila, kerneltila ja avaintallennus ovat laboratoriotestauksessa. Ne löytyvät Implementation Under Test -luettelosta.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* iOS 15 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* iOS 15 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 15:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 15:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A13, A14, A15) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* iOS 14 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* iOS 14 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 14:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 14:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A13-A14) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3

FIPS 140-2 -sertifioinnit

Alla olevassa taulukossa näkyvät salausmoduulit, joita testataan parhaillaan ja joiden FIPS 140-2 -vaatimustenmukaisuuden laboratorio on testannut.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3856 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v10.0 for ARM *Käyttöjärjestelmä:* iOS 13 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3855 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v10.0 for ARM *Käyttöjärjestelmä:* iOS 13 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 5.2.2021	*Sertifikaatit:* 3811 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v10.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 13:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 23.4.2019	*Sertifikaatit:* 3438 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v9.0 for ARM *Käyttöjärjestelmä:* iOS 12 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 11.4.2019	*Sertifikaatit:* 3433 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v9.0 for ARM *Käyttöjärjestelmä:* iOS 12 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3523 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v9.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 12:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 22.5.2018, 6.7.2018	*Sertifikaatit:* 3148 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v8.0 for ARM *Käyttöjärjestelmä:* iOS 11 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 17.5.2018, 3.7.2018	*Sertifikaatit:* 3147 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v8.0 for ARM *Käyttöjärjestelmä:* iOS 11 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3223 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v1.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 11:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2016 *Validointipäivät:* 1.2.2017	*Sertifikaatit:* 2828 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple iOS Corecrypto Kernel Module v7.0 *Käyttöjärjestelmä:* iOS 10 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2016 *Validointipäivät:* 1.2.2017	*Sertifikaatit:* 2827 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple iOS Corecrypto Kernel Module v7.0 *Käyttöjärjestelmä:* iOS 10 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Aikaisemmat versiot

Yli viisi vuotta vanhat sertifioinnit näkyvät CMVP:n luettelossa historical-tilassa. Näiden aikaisempien iOS-versioiden salausmoduulit on aikanaan validoitu:

- iOS 9 (corecrypto modules v6.0)
- iOS 8 (corecrypto modules v5.0)
- iOS 7 (corecrypto modules v4.0)
- iOS 6 (corecrypto modules v3.0)

Common Criteria (CC) -sertifioinnin tausta

Apple hakee aktiivisesti iOS:n arviointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä. Arviointi voidaan tehdä ainoastaan käyttöjärjestelmän lopulliselle julkaistulle versiolle. Ennen iPadOS 13.1:tä iPadOS:n nimi oli iOS.

Common Criteria (CC) -sertifioinnin tila

NIAP:n johtamassa Yhdysvaltain arviointijärjestelmässä ylläpidetään Products in Evaluation -luetteloa tuotteista, jotka ovat parhaillaan arvioitavina Yhdysvalloissa NIAP:n hyväksymässä Common Criteria -testauslaboratoriossa (CCTL) ja joille on tehty arvioinnin aloitustapaaminen (tai vastaava), jossa CCEVS:n hallinto on virallisesti hyväksynyt tuotteen arvioitavaksi.

Kun tuotteet on sertifioitu, NIAP lisää parhaillaan voimassa olevat sertifioinnit Product Compliant -luetteloon. Kahden vuoden jälkeen näistä sertifioinneista tarkistetaan, täyttyvätkö senhetkisen käytännön vaatimukset varmistuksen voimassaolon jatkamiselle. Kun varmistuksen voimassaoloaika päättyy, NIAP siirtää sertifioinnin arkistoitujen tuotteiden Archived Products -luetteloon.

Common Criteria -portaalissa luetellaan sertifioinnit, jotka voidaan tunnustaa vastavuoroisesti Common Criteria Recognition Arrangement (CCRA) -järjestelyn puitteissa. Tuotteet voidaan pitää CC-portaalissa sertifioitujen tuotteiden luettelossa viiden vuoden ajan, ja CC-portaalissa säilytetään tiedot myös arkistoiduista sertifioinneista.

Alla olevassa taulukossa näkyvät sertifioinnit, joita laboratorio arvioi parhaillaan tai jotka ovat saaneet Common Criteria -vaatimustenmukaisuuden sertifioinnin.

Nykytilanne

NIAP:n arviointien laboratoriotestit iOS 15:lle ovat meneillään. Jos haluat uusimmat tiedot, katso Products in evaluation (NIAP) ja Product Compliant List.

Käyttöjärjestelmä / sertifiointipäiväys	**Tunniste / dokumentit**	**Nimi / suojausprofiilit**
Käyttöjärjestelmä: iOS 15 *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* –	*Nimi:* Apple iOS 15: iPhonet *Suojausprofiilit:* Mobile Device Fundamentals (PP-moduulit vahvistetaan myöhemmin)
Käyttöjärjestelmä: iOS 14 *Sertifiointipäiväys:* 1.9.2021	*Tunniste:* 11146 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple iOS 14: iPhonet *Suojausprofiilit:* Mobile Device Fundamentals, VPN Client module, WLAN Clients PP Module, MDM Agent EP
Käyttöjärjestelmä: iOS 13 *Sertifiointipäiväys:* 6.11.2020	*Tunniste:* 11036 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple iOS 13 on iPhone *Suojausprofiilit:* Mobile Device Fundamentals, VPN Client module, WLAN Clients EP, MDM Agent EP

Arkistoidut iOS:n Common Criteria -sertifioinnit

Näillä aikaisemmilla iOS-versioilla on Common Criteria -validoinnit. NIAP on arkistoinut ne NIAP-käytännön mukaisesti:

Käyttöjärjestelmä / sertifiointipäiväys	**Tunniste / dokumentit**	**Nimi / suojausprofiilit**
Käyttöjärjestelmä: iOS 12 *Sertifiointipäiväys:* 14.3.2019	*Tunniste:* 10937 *Dokumentit:* Security Target -dokumentti Opas	*Nimi:* iPhone with iOS 12 *Suojausprofiilit:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Käyttöjärjestelmä: iOS 11 *Sertifiointipäiväys:* 17.7.2018	*Tunniste:* 10851 *Dokumentit:* Security Target -dokumentti Opas	*Nimi:* Apple iOS 11 *Suojausprofiilit:* Mobile Device Fundamentals, Wireless LAN client EP, MDM Agent EP
Käyttöjärjestelmä: iOS 10 *Sertifiointipäiväys:* 27.7.2017	*Tunniste:* 10782 *Dokumentit:* Security Target -dokumentti, Opas	*Nimi:* iOS 10.2 on iPhone and iPad Devices *Suojausprofiilit:* Mobile Device Fundamentals, Wireless LAN client EP, MDM Agent EP
Käyttöjärjestelmä: iOS 10 *Sertifiointipäiväys:* 27.7.2017	*Tunniste:* 10792 *Dokumentit:* Security Target -dokumentti, Opas	*Nimi:* iOS 10.2 VPN Client on iPhone and iPad *Suojausprofiilit:* VPN Client PP
Käyttöjärjestelmä: iOS 9 *Sertifiointipäiväys:* 14.10.2016	*Tunniste:* 10725 *Dokumentit:* Security Target -dokumentti, Opas	*Nimi:* iOS 9.3.2 with MDM Agent *Suojausprofiilit:* Mobile Device Fundamentals, MDM Agent EP
Käyttöjärjestelmä: iOS 9 *Sertifiointipäiväys:* 13.10.2016	*Tunniste:* 10714 *Dokumentit:* Security Target -dokumentti, Opas	*Nimi:* OS VPN Client on iPhone and iPad *Suojausprofiilit:* VPN Client PP
Käyttöjärjestelmä: iOS 9 *Sertifiointipäiväys:* 28.1.2016	*Tunniste:* 10695 *Dokumentit:* Security Target -dokumentti, Opas	*Nimi:* iOS 9 *Suojausprofiilit:* Mobile Device Fundamentals

iPadOS:n tietoturvasertifikaatit

iPadOS:n sertifioinnin tausta

Apple hakee aktiivisesti Applen käyttöjärjestelmien validointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä käyttäen asianmukaisia PP-suojausprofiileja (Protection Profile, PP) ja FIPS 140-3 -suojaustasoja. Vaatimustenmukaisuusvalidointi voidaan tehdä ainoastaan lopullisille julkaistuille versioille.

Huomaa: Vuonna 2019 iPad-laitteiden käyttöjärjestelmä uudistettiin iPadOS:ksi. Ennen iPadOS 13.1:tä iPadOS:n nimi oli iOS.

iPadOS:n salausmoduulien validoinnin tila

Cryptographic Module Validation Program (CMVP) ylläpitää salausmoduulien validoinnin tilasta kolmea eri luetteloa, joilla salausmoduulit voivat olla riippuen validointinsa senhetkisestä tilasta:

- Kun Apple on tehnyt sopimuksen laboratorion kanssa testaamisesta, moduuli voidaan lisätä CMVP:n Implementation Under Test List -luetteloon.
- Kun laboratorio on suorittanut testauksen ja suositellut validointia CMVP:lle ja kun maksut CMVP:lle on suoritettu, moduuli lisätään Modules in Process List (MIP) -luetteloon. MIP-luettelossa seurataan CMVP:n validoinnin etenemistä neljässä vaiheessa:
  - *Review Pending:* Odottaa, että tehtävä annetaan resurssille CMVP:ssä.
  - *In Review:* CMVP:n resurssit suorittavat validointitoimia.
  - *Coordination:* Laboratorio ja CMVP selvittävät mahdollisesti esiin tulleita ongelmia.
  - *Finalization:* Sertifikaatin antamiseen liittyvät toiminnot ja muodollisuudet.
- Kun CMVP:n validointi on valmis, moduulit saavat sertifikaatin, joka kertoo niiden täyttävän vaatimukset, ja ne lisätään validoitujen salausmoduulien luetteloon. Tähän sisältyy:
  - Validoidut moduulit, jotka on merkitty aktiivisiksi.
  - Viiden vuoden kuluttua moduulit siirretään historical-luetteloon.
  - Jos moduulin sertifikaatti jostakin syystä perutaan, se siirretään revoked-luetteloon.

Vuonna 2020 CMVP otti kansainvälisen ISO/IEC 19790 -standardin FIPS 140-3 -validoinnin perustaksi.

FIPS 140-3 -sertifioinnit

Nykytilanne

iPadOS 14:n (2020) käyttäjätila, kerneltila ja avaintallennus ovat käyneet läpi laboratoriotestauksen ja saaneet laboratoriolta suosituksen CMVP:n validoinnille. Ne löytyvät luettelosta Modules in Process List.

iPadOS 15:n (2021) käyttäjätila, kerneltila ja avaintallennus ovat laboratoriotestauksessa. Ne löytyvät Implementation Under Test -luettelosta.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* iPadOS 15 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* iPadOS 15 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iPadOS 15:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14, M1) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iPadOS 15:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14, M1) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* iPadOS 14 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* iPadOS 14 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iPadOS 14:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14, M1) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iPadOS 14:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A9-A14, M1) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3

FIPS 140-2 -sertifioinnit

Alla olevassa taulukossa näkyvät salausmoduulit, joita testataan parhaillaan ja joiden FIPS 140-2 -vaatimustenmukaisuuden laboratorio on testannut.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3856 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v10.0 for ARM *Käyttöjärjestelmä:* iPadOS 13 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3855 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v10.0 for ARM *Käyttöjärjestelmä:* iPadOS 13 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 5.2.2021	*Sertifikaatit:* 3811 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iPadOS 13:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 23.4.2019	*Sertifikaatit:* 3438 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v9.0 for ARM *Käyttöjärjestelmä:* iOS 12 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 11.4.2019	*Sertifikaatit:* 3433 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v9.0 for ARM *Käyttöjärjestelmä:* iOS 12 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3523 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v9.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 12:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 22.5.2018, 6.7.2018	*Sertifikaatit:* 3148 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v8.0 for ARM *Käyttöjärjestelmä:* iOS 11 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 17.5.2018, 3.7.2018	*Sertifikaatit:* 3147 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v8.0 for ARM *Käyttöjärjestelmä:* iOS 11 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3223 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v1.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan iOS 11:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2016 *Validointipäivät:* 1.2.2017	*Sertifikaatit:* 2828 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple iOS Corecrypto Kernel Module v7.0 *Käyttöjärjestelmä:* iOS 10 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2016 *Validointipäivät:* 1.2.2017	*Sertifikaatit:* 2827 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple iOS Corecrypto Kernel Module v7.0 *Käyttöjärjestelmä:* iOS 10 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Aikaisemmat versiot

Yli viisi vuotta vanhat sertifioinnit näkyvät CMVP:n luettelossa historical-tilassa. Näiden aikaisempien iOS-versioiden salausmoduulit on aikanaan validoitu:

- iOS 9 (corecrypto modules v6.0)
- iOS 8 (corecrypto modules v5.0)
- iOS 7 (corecrypto modules v4.0)
- iOS 6 (corecrypto modules v3.0)

Common Criteria (CC) -sertifioinnin tausta

Apple hakee aktiivisesti iPadOS:n arviointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä. Arviointi voidaan tehdä ainoastaan käyttöjärjestelmän lopulliselle julkaistulle versiolle.

Common Criteria (CC) -sertifioinnin tila

NIAP:n johtamassa Yhdysvaltain arviointijärjestelmässä ylläpidetään Products in Evaluation -luetteloa tuotteista, jotka ovat parhaillaan arvioitavina Yhdysvalloissa NIAP:n hyväksymässä Common Criteria -testauslaboratoriossa (CCTL) ja joille on tehty arvioinnin aloitustapaaminen (tai vastaava), jossa CCEVS:n hallinto on virallisesti hyväksynyt tuotteen arvioitavaksi.

Kun tuotteet on sertifioitu, NIAP lisää parhaillaan voimassa olevat sertifioinnit Product Compliant -luetteloon. Kahden vuoden jälkeen näistä sertifioinneista tarkistetaan, täyttyvätkö senhetkisen käytännön vaatimukset varmistuksen voimassaolon jatkamiselle. Kun varmistuksen voimassaoloaika päättyy, NIAP siirtää sertifioinnin arkistoitujen tuotteiden Archived Products -luetteloon.

Common Criteria -portaalissa luetellaan sertifioinnit, jotka voidaan tunnustaa vastavuoroisesti Common Criteria Recognition Arrangement (CCRA) -järjestelyn puitteissa. Tuotteet voidaan pitää CC-portaalissa sertifioitujen tuotteiden luettelossa viiden vuoden ajan, ja CC-portaalissa säilytetään tiedot myös arkistoiduista sertifioinneista.

Alla olevassa taulukossa näkyvät sertifioinnit, joita laboratorio arvioi parhaillaan tai jotka ovat saaneet Common Criteria -vaatimustenmukaisuuden sertifioinnin.

Nykytilanne

NIAP:n arviointien laboratoriotestit iPadOS 15:lle ovat meneillään. Jos haluat uusimmat tiedot, katso Products in evaluation (NIAP) ja Product Compliant List.

Käyttöjärjestelmä / sertifiointipäiväys	Tunniste / dokumentit	Nimi / suojausprofiilit
Käyttöjärjestelmä: iPadOS 15 *Sertifiointipäiväys:* 14.3.2019	*Tunniste:* – *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* iPad with iOS 12 *Suojausprofiilit:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Käyttöjärjestelmä: iPadOS 14 *Sertifiointipäiväys:* 1.9.2021	*Tunniste:* 11147 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple iPadOS 14: iPads *Suojausprofiilit:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Käyttöjärjestelmä: iPadOS 13 *Sertifiointipäiväys:* 6.11.2020	*Tunniste:* 11036 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* iPadOS 13 on iPad Mobile Devices *Suojausprofiilit:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP

Aikaisemmat versiot

Näillä aikaisemmilla iOS-versioilla on Common Criteria -validoinnit. NIAP on arkistoinut ne NIAP-käytännön mukaisesti:

- iOS 12 (Tunniste: 10937)
- iOS 11 (Tunniste: 10851)
- iOS 10 (Tunniste: 107782, 10792)
- iOS 9 (Tunniste: 10725, 10714, 10695)

macOS:n tietoturvasertifikaatit

macOS:n sertifioinnin tausta

Apple hakee aktiivisesti Applen käyttöjärjestelmien validointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä käyttäen asianmukaisia PP-suojausprofiileja (Protection Profile, PP) ja FIPS 140-3 -suojaustasoja. Vaatimustenmukaisuusvalidointi voidaan tehdä ainoastaan lopullisille julkaistuille versioille.

macOS:n salausmoduulien validoinnin tila

Cryptographic Module Validation Program (CMVP) ylläpitää salausmoduulien validoinnin tilasta kolmea eri luetteloa, joilla salausmoduulit voivat olla riippuen validointinsa senhetkisestä tilasta:

- Kun Apple on tehnyt sopimuksen laboratorion kanssa testaamisesta, moduuli voidaan lisätä CMVP:n Implementation Under Test List -luetteloon.
- Kun laboratorio on suorittanut testauksen ja suositellut validointia CMVP:lle ja kun maksut CMVP:lle on suoritettu, moduuli lisätään Modules in Process List (MIP) -luetteloon. MIP-luettelossa seurataan CMVP:n validoinnin etenemistä neljässä vaiheessa:
  - *Review Pending:* Odottaa, että tehtävä annetaan resurssille CMVP:ssä.
  - *In Review:* CMVP:n resurssit suorittavat validointitoimia.
  - *Coordination:* Laboratorio ja CMVP selvittävät mahdollisesti esiin tulleita ongelmia.
  - *Finalization:* Sertifikaatin antamiseen liittyvät toiminnot ja muodollisuudet.
- Kun CMVP:n validointi on valmis, moduulit saavat sertifikaatin, joka kertoo niiden täyttävän vaatimukset, ja ne lisätään validoitujen salausmoduulien luetteloon. Tähän sisältyy:
  - Validoidut moduulit, jotka on merkitty aktiivisiksi.
  - Viiden vuoden kuluttua moduulit siirretään historical-luetteloon.
  - Jos moduulin sertifikaatti jostakin syystä perutaan, se siirretään revoked-luetteloon.

Vuonna 2020 CMVP otti kansainvälisen ISO/IEC 19790 -standardin FIPS 140-3 -validoinnin perustaksi.

Alla oleva Applen Mac-tietokoneiden taulukko kertoo, mitä salausmoduuleita käytetään kunkin Mac-teknologian kanssa.

Salausmoduuli	Apple siliconilla varustetut Mac-tietokoneet	Mac-tietokoneet, joissa on Apple T2 Security -siru	Intel-pohjaiset Mac-tietokoneet ilman Apple T2 Security -sirua
Apple silicon User Space	✓		
Apple silicon Kernel	✓		
Intel User Space		✓	✓
Intel Kernel		✓	✓
Secure Key Store	✓	✓	

FIPS 140-3 -sertifioinnit

Vuonna 2020 Apple julkaisi Mac-tietokoneet, joiden pohjana on Apple silicon. Salausmoduulien soveltuvuus Apple silicon- tai Intel-pohjaisiin Mac-tietokoneisiin on ilmoitettu Moduulitiedot-sarakkeessa alla olevassa taulukossa.

Huomaa: Apple T2 Security -sirut on sisällytetty moniin Intel-pohjaisiin Mac-tietokoneisiin. Jos haluat lisätietoja T2-sirun sertifioinneista, katso Apple T2 Security -sirun suojauksen sertifioinnit.

macOS:n ssh-asiakas

OpenSSH voidaan määrittää käyttämään FIPS 140-3 -validoituja moduuleja tietyille FIPS 140-3 -algoritmeille. Organisaatiot voivat suorittaa allekirjoitetun ja oikeaksi todistetun asentajan, joka on saatavilla Applelta salasanalla *FIPS140Mode*. Asentaja sijoittaa kaksi tiedostoa Maciin:

- *fips_ssh_config:* Sijoitettu hakemistoon /private/etc/ssh/ssh_config.d/
- *fips_sshd_config:* Sijoitettu hakemistoon /private/etc/ssh/sshd_config.d/

macOS käyttää näitä tiedostoja OpenSSH:n käytettävissä olevien salausten rajoittamiseen NIST:n validoimiin ja varmistaa, että OpenSSH-asiakas käyttää alustan tarjoamaa, validoitua salausmoduulia. Ylläpitäjät voivat myös luoda omia tiedostojaan. Jos haluat lisätietoja, katso `apple_ssh_and_fips` -man-sivu macOS 12.0.1:ssä tai uudemmassa.

Nykytilanne

macOS 11 Big Surin käyttäjätila, kerneltila ja avaintallennus ovat käyneet läpi laboratoriotestauksen ja saaneet laboratoriolta suosituksen CMVP:n validoinnille. Ne löytyvät luettelosta Modules in Process List.

macOS 12 Montereyn käyttäjätila, kerneltila ja avaintallennus ovat laboratoriotestauksessa. Ne löytyvät Implementation Under Test -luettelosta.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* macOS 12 Monterey (Apple silicon) *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* macOS 12 Monterey (Apple silicon) *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* macOS 12 Monterey (Intel) *Ympäristö:* Intel, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* macOS 12 Monterey (Intel) *Ympäristö:* Intel, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan macOS 12 Montereyn mukana (Apple silicon), sepOS, joka toimitetaan macOS 12 Montereyn mukana (Intel, jossa T2) *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (M1 ja T2) *Suojaustaso:* 2

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan macOS 12 Montereyn mukana (Apple silicon) *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (M1) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* macOS 11 Big Sur (Intel) *Ympäristö:* Intel, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* macOS 11 Big Sur (Intel) *Ympäristö:* Intel, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* macOS 11 Big Sur (Apple silicon) *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* macOS 11 Big Sur (Apple silicon) *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan macOS 11 Big Surin mukana (Apple silicon), sepOS, joka toimitetaan macOS 11 Big Surin mukana (Intel) *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (M1) *Suojaustaso:* 2

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan macOS 11 Big Surin mukana (Apple silicon) *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (M1) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3

FIPS 140-2 -sertifioinnit

Alla olevassa taulukossa näkyvät salausmoduulit, joita testataan parhaillaan ja joiden FIPS 140-2 -vaatimustenmukaisuuden laboratorio on testannut.

macOS 10.15 Catalinan käyttäjätilan, kerneltilan ja suojatun avaintallennuksen laboratoriotestaus on suoritettu ja laboratorio on suositellut niiden validointia CMVP:lle. Ne löytyvät luettelosta Modules in Process List.

Huomaa: Apple T2 Security -sirut on sisällytetty moniin Intel-pohjaisiin Mac-tietokoneisiin. Jos haluat lisätietoja T2-sirun sertifioinneista, katso Apple T2 Security -sirun suojauksen sertifioinnit.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 24.3.2021	*Sertifikaatit:* 3859 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Space Module for Intel (ccv10) *Käyttöjärjestelmä:* macOS 10.15 Catalina *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 24.3.2021	*Sertifikaatit:* 3858 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v10.0 for Intel (ccv10) *Käyttöjärjestelmä:* macOS 10.15 Catalina *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 12.4.2019	*Sertifikaatit:* 3402 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v9.0 for Intel *Käyttöjärjestelmä:* macOS 10.14 Mojave *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 12.4.2019	*Sertifikaatit:* 3431 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v9.0 for Intel *Käyttöjärjestelmä:* macOS 10.14 Mojave *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 22.3.2018	*Sertifikaatit:* 3155 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v8.0 for Intel *Käyttöjärjestelmä:* macOS 10.13 High Sierra *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 22.3.2018	*Sertifikaatit:* 3156 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v8.0 for Intel *Käyttöjärjestelmä:* macOS 10.13 High Sierra *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Aikaisemmat versiot

Näiden aikaisempien OS X- ja macOS-versioiden salausmoduulit on aikanaan validoitu. Yli viiden vuoden jälkeen ne näkyvät CMVP:n luettelossa historical-tilassa:

- macOS 10.12 Sierra
- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks
- OS X 10.8 Mountain Lion
- OS X 10.7 Lion
- OS X 10.6 Snow Leopard

Common Criteria (CC) -sertifioinnin tausta

Apple hakee aktiivisesti macOS:n arviointia jokaisen merkittävän käyttöjärjestelmäversion julkaisun yhteydessä. Arviointi voidaan tehdä ainoastaan käyttöjärjestelmän lopulliselle julkaistulle versiolle.

Common Criteria (CC) -sertifioinnin tila

NIAP:n johtamassa Yhdysvaltain arviointijärjestelmässä ylläpidetään Products in Evaluation -luetteloa tuotteista, jotka ovat parhaillaan arvioitavina Yhdysvalloissa NIAP:n hyväksymässä Common Criteria -testauslaboratoriossa (CCTL) ja joille on tehty arvioinnin aloitustapaaminen (tai vastaava), jossa CCEVS:n hallinto on virallisesti hyväksynyt tuotteen arvioitavaksi.

Kun tuotteet on sertifioitu, NIAP lisää parhaillaan voimassa olevat sertifioinnit Product Compliant -luetteloon. Kahden vuoden jälkeen näistä sertifioinneista tarkistetaan, täyttyvätkö senhetkisen käytännön vaatimukset varmistuksen voimassaolon jatkamiselle. Kun varmistuksen voimassaoloaika päättyy, NIAP siirtää sertifioinnin arkistoitujen tuotteiden Archived Products -luetteloon.

Common Criteria -portaalissa luetellaan sertifioinnit, jotka voidaan tunnustaa vastavuoroisesti Common Criteria Recognition Arrangement (CCRA) -järjestelyn puitteissa. Tuotteet voidaan pitää CC-portaalissa sertifioitujen tuotteiden luettelossa viiden vuoden ajan, ja CC-portaalissa säilytetään tiedot myös arkistoiduista sertifioinneista.

Alla olevassa taulukossa näkyvät sertifioinnit, joita laboratorio arvioi parhaillaan tai jotka ovat saaneet Common Criteria -vaatimustenmukaisuuden sertifioinnin.

Nykytilanne

Meneillään ovat NIAP:n arvioinnit macOS 11:tä ja macOS 12:ta varten käyttäen yleistä käyttöjärjestelmää ja täyden levyn salauksen (FDE) (AA ja EE) suojausprofiileja.

Jos haluat uusimmat tiedot, katso Products in evaluation (NIAP) ja Product Compliant List.

Käyttöjärjestelmä / sertifiointipäiväys	**Tunniste / dokumentit**	**Nimi / suojausprofiilit**
Käyttöjärjestelmä: macOS 12 Monterey *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* –	*Nimi:* Apple FileVault 2 with macOS 12 Monterey *Suojausprofiilit:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP-suojausprofiilit vahvistetaan myöhemmin)
Käyttöjärjestelmä: macOS 12 Monterey *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* –	*Nimi:* macOS 12 Monterey *Suojausprofiilit:* PP_OS_V4.21 (PP-suojausprofiilit vahvistetaan myöhemmin)
Käyttöjärjestelmä: macOS 11 Big Sur *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple FileVault 2 with macOS 11 Big Sur *Suojausprofiilit:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Käyttöjärjestelmä: macOS 11 Big Sur *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple macOS 11 Big Sur *Suojausprofiilit:* PP_OS_V4.21
Käyttöjärjestelmä: macOS 10.15 Catalina *Sertifiointipäiväys:* 29.4.2021	*Tunniste:* 11078 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple FileVault 2 on T2 computers running macOS 10.15 Catalina *Suojausprofiilit:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E

Käyttöjärjestelmä / sertifiointipäiväys	Tunniste / dokumentit	Nimi / suojausprofiilit
Käyttöjärjestelmä: macOS 10.15 Catalina *Sertifiointipäiväys:* 23.9.2020	*Tunniste:* 11077 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* macOS 10.15 Catalina *Suojausprofiilit:* PP_OS_V4.21

tvOS:n tietoturvasertifikaatit

tvOS:n sertifioinnin tausta

Apple hakee aktiivisesti salausmoduulien validointia jokaisen merkittävän tvOS-version julkaisun yhteydessä. Vaatimustenmukaisuusvalidointi voidaan tehdä ainoastaan lopullisille julkaistuille versioille.

tvOS:n salausmoduulien validoinnin tila

Cryptographic Module Validation Program (CMVP) ylläpitää salausmoduulien validoinnin tilasta kolmea eri luetteloa, joilla salausmoduulit voivat olla riippuen validointinsa senhetkisestä tilasta:

- Kun Apple on tehnyt sopimuksen laboratorion kanssa testaamisesta, moduuli voidaan lisätä CMVP:n Implementation Under Test List -luetteloon.
- Kun laboratorio on suorittanut testauksen ja suositellut validointia CMVP:lle ja kun maksut CMVP:lle on suoritettu, moduuli lisätään Modules in Process List (MIP) -luetteloon. MIP-luettelossa seurataan CMVP:n validoinnin etenemistä neljässä vaiheessa:
  - *Review Pending:* Odottaa, että tehtävä annetaan resurssille CMVP:ssä.
  - *In Review:* CMVP:n resurssit suorittavat validointitoimia.
  - *Coordination:* Laboratorio ja CMVP selvittävät mahdollisesti esiin tulleita ongelmia.
  - *Finalization:* Sertifikaatin antamiseen liittyvät toiminnot ja muodollisuudet.
- Kun CMVP:n validointi on valmis, moduulit saavat sertifikaatin, joka kertoo niiden täyttävän vaatimukset, ja ne lisätään validoitujen salausmoduulien luetteloon. Tähän sisältyy:
  - Validoidut moduulit, jotka on merkitty aktiivisiksi.
  - Viiden vuoden kuluttua moduulit siirretään historical-luetteloon.
  - Jos moduulin sertifikaatti jostakin syystä perutaan, se siirretään revoked-luetteloon.

Vuonna 2020 CMVP otti kansainvälisen ISO/IEC 19790 -standardin FIPS 140-3 -validoinnin perustaksi.

FIPS 140-3 -sertifioinnit

Nykytilanne

tvOS 14:n (2020) käyttäjätilan, kerneltilan ja suojatun avaintallennuksen laboratoriotestaus on suoritettu ja laboratorio on suositellut niiden validointia CMVP:lle. Ne löytyvät luettelosta Modules in Process List.

tvOS 15:n (2021) käyttäjätila, kerneltila ja avaintallennus ovat laboratoriotestauksessa. Ne löytyvät Implementation Under Test -luettelosta.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* tvOS 15 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* tvOS 15 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan tvOS 15:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A10, A12) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* tvOS 14 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* tvOS 14 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan tvOS 14:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (A10, A12) *Suojaustaso:* 2

FIPS 140-2 -sertifioinnit

Alla olevassa taulukossa näkyvät salausmoduulit, joita testataan parhaillaan ja joiden FIPS 140-2 -vaatimustenmukaisuuden laboratorio on testannut.

tvOS 13:n (2019) käyttäjätilan, kerneltilan ja suojatun avaintallennuksen laboratoriotestaus on suoritettu ja laboratorio on suositellut niiden validointia CMVP:lle. Ne löytyvät luettelosta Modules in Process List.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3856 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v10.0 for ARM *Käyttöjärjestelmä:* tvOS 13 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 23.3.2021	*Sertifikaatit:* 3855 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v10.0 for ARM *Käyttöjärjestelmä:* tvOS 13 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 5.2.2021	*Sertifikaatit:* 3811 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v10.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan tvOS 13:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 23.4.2019	*Sertifikaatit:* 3438 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v9.0 for ARM *Käyttöjärjestelmä:* tvOS 12 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 11.4.2019	*Sertifikaatit:* 3433 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v9.0 for ARM *Käyttöjärjestelmä:* tvOS 12 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3523 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v9.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan tvOS 12:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 22.5.2018, 6.7.2018	*Sertifikaatit:* 3148 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v8.0 for ARM *Käyttöjärjestelmä:* tvOS 11 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 17.5.2018, 3.7.2018	*Sertifikaatit:* 3147 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v8.0 for ARM *Käyttöjärjestelmä:* tvOS 11 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3223 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v1.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan tvOS 11:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2

watchOS:n tietoturvasertifikaatit

watchOS:n sertifioinnin tausta

Apple hakee aktiivisesti salausmoduulien validointia jokaisen merkittävän watchOS-version julkaisun yhteydessä. Vaatimustenmukaisuusvalidointi voidaan tehdä ainoastaan lopullisille julkaistuille versioille.

watchOS:n salausmoduulien validoinnin tila

Cryptographic Module Validation Program (CMVP) ylläpitää salausmoduulien validoinnin tilasta kolmea eri luetteloa, joilla salausmoduulit voivat olla riippuen validointinsa senhetkisestä tilasta:

- Kun Apple on tehnyt sopimuksen laboratorion kanssa testaamisesta, moduuli voidaan lisätä CMVP:n Implementation Under Test List -luetteloon.
- Kun laboratorio on suorittanut testauksen ja suositellut validointia CMVP:lle ja kun maksut CMVP:lle on suoritettu, moduuli lisätään Modules in Process List (MIP) -luetteloon. MIP-luettelossa seurataan CMVP:n validoinnin etenemistä neljässä vaiheessa:
  - *Review Pending:* Odottaa, että tehtävä annetaan resurssille CMVP:ssä.
  - *In Review:* CMVP:n resurssit suorittavat validointitoimia.
  - *Coordination:* Laboratorio ja CMVP selvittävät mahdollisesti esiin tulleita ongelmia.
  - *Finalization:* Sertifikaatin antamiseen liittyvät toiminnot ja muodollisuudet.
- Kun CMVP:n validointi on valmis, moduulit saavat sertifikaatin, joka kertoo niiden täyttävän vaatimukset, ja ne lisätään validoitujen salausmoduulien luetteloon. Tähän sisältyy:
  - Validoidut moduulit, jotka on merkitty aktiivisiksi.
  - Viiden vuoden kuluttua moduulit siirretään historical-luetteloon.
  - Jos moduulin sertifikaatti jostakin syystä perutaan, se siirretään revoked-luetteloon.

Vuonna 2020 CMVP otti kansainvälisen ISO/IEC 19790 -standardin FIPS 140-3 -validoinnin perustaksi.

FIPS 140-3 -sertifioinnit

Nykytilanne

watchOS 7:n (2020) käyttäjätila, kerneltila ja avaintallennus ovat käyneet läpi laboratoriotestauksen ja saaneet laboratoriolta suosituksen CMVP:n validoinnille. Ne löytyvät luettelosta Modules in Process List.

watchOS 8:n (2021) käyttäjätila, kerneltila ja avaintallennus ovat laboratoriotestauksessa. Ne löytyvät Implementation Under Test -luettelosta.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* watchOS 8 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* watchOS 8 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan watchOS 8:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (S3, S4, S5, S6) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2021 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v12 *Käyttöjärjestelmä:* sepOS, joka toimitetaan watchOS 8:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (S6) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* watchOS 7 *Ympäristö:* Apple silicon, käyttäjä, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* watchOS 7 *Ympäristö:* Apple silicon, kernel, ohjelmisto *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan watchOS 7:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (S3, S4, S5, S6) *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2020 *Validointipäivät:* –	*Sertifikaatit:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Module v11.1 *Käyttöjärjestelmä:* sepOS, joka toimitetaan watchOS 7:n mukana *Ympäristö:* Apple silicon, suojattu avaintallennus, laitteisto *Tyyppi:* Laitteisto (S6) *Suojaustaso:* 2 *Fyysinen suojaustaso:* 3

FIPS 140-2 -sertifioinnit

Alla olevassa taulukossa näkyvät salausmoduulit, joita testataan parhaillaan ja joiden FIPS 140-2 -vaatimustenmukaisuuden laboratorio on testannut.

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* –	*Sertifikaatit:* 3856 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v10.0 for ARM *Käyttöjärjestelmä:* watchOS 6 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* –	*Sertifikaatit:* 3855 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v10.0 for ARM *Käyttöjärjestelmä:* watchOS 6 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2019 *Validointipäivät:* 5.2.2021	*Sertifikaatit:* 3811 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v10.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan watchOS 6:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2

Päiväykset	Sertifikaatit / dokumentit	Moduulitiedot
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 23.4.2019	*Sertifikaatit:* 3438 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v9.0 for ARM *Käyttöjärjestelmä:* watchOS 5 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 11.4.2019	*Sertifikaatit:* 3433 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v9.0 for ARM *Käyttöjärjestelmä:* watchOS 5 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2018 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3523 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v9.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan watchOS 5:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 22.5.2018, 6.7.2018	*Sertifikaatit:* 3148 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto User Module v8.0 for ARM *Käyttöjärjestelmä:* watchOS 4 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 9.3.2018, 17.5.2018, 3.7.2018	*Sertifikaatit:* 3147 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Corecrypto Kernel Module v8.0 for ARM *Käyttöjärjestelmä:* watchOS 4 *Tyyppi:* Ohjelmistot *Suojaustaso:* 1
Käyttöjärjestelmän julkaisupäivä: 2017 *Validointipäivät:* 10.9.2019	*Sertifikaatit:* 3223 *Dokumentit:* Sertifikaatti Suojauskäytäntö Crypto Officer -ohjeet	*Nimi:* Apple Secure Key Store Cryptographic Module v1.0 *Käyttöjärjestelmä:* sepOS, joka toimitetaan watchOS 4:n mukana *Tyyppi:* Laitteistot *Suojaustaso:* 2

Ohjelmistojen tietoturvasertifioinnit

Applen ohjelmistojen tietoturvasertifiointien yleiskatsaus

Apple ylläpitää sepOS:lle ja T2-laiteohjelmistolle sekä muille sertifioinneille yhdysvaltalaisen FIPS (Federal Information Processing Standard) -standardin 140-2/-3 mukaisia validointisertifikaatteja. Apple lähtee liikkeelle sellaisista *sertifioinnin osista*, jotka koskevat laajasti eri alustoja. Yksi osa on corecryptokirjaston validointi, jota käytetään laitteistojen ja ohjelmistojen salausmoduuleissa Applen kehittämissä käyttöjärjestelmissä. Toinen osa on moniin Applen laitteisiin sisällytetyn Secure Enclaven sertifiointi. Kolmas on Touch ID:tä tukevissa Apple-laitteissa ja Face ID:tä tukevissa laitteissa olevan Secure Elementin (SE) sertifiointi. Nämä laitteistojen sertifiointien osat muodostavat perustan laajemmille alustojen tietoturvasertifioinneille.

Tuotteiden sertifioinnit: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) on standardi, jota monet organisaatiot käyttävät IT-tuotteiden tietoturva-arviointien perustana.

Jos olet kiinnostunut sertifikaateista, jotka voidaan tunnustaa vastavuoroisesti kansainvälisessä Common Criteria Recognition Arrangement (CCRA) -järjestelyssä, katso tietoja Common Criteria -portaalista. Common Criteria -standardia voidaan myös käyttää CCRA:n ulkopuolella kansallisissa ja yksityisissä validointijärjestelmissä. Euroopassa vastavuoroista tunnustamista ohjaavat SOG-IS-sopimus ja CCRA.

Common Criteria -yhteisön ilmaisema tavoite on kansainvälisesti hyväksytty joukko tietoturvastandardeja IT-tuotteiden suojausominaisuuksien selkeää ja luotettavaa arviointia varten. Tarjoamalla riippumattoman arvion tuotteen edellytyksistä täyttää tietoturvastandardit, Common Criteria -sertifiointi antaa asiakkaille enemmän varmuutta IT-tuotteiden suojauksen suhteen ja auttaa tekemään valistuneempia päätöksiä.

CCRA-järjestelyssä jäsenmaat ovat sopineet, että ne tunnustavat IT-tuotteiden sertifioinnin samalla luottamustasolla. Ennen sertifiointeja tarvittavat arvioinnit ovat laajoja, ja ne sisältävät seuraavat:

- Protection Profiles (PP) -suojausprofiilit
- Security Targets (ST) -dokumentit
- Security Functional Requirements (SFR) -vaatimukset
- Security Assurance Requirements (SAR) -vaatimukset
- Evaluation Assurance Levels (EAL) -tasot

Suojausprofiilit (Protection Profile, PP) ovat dokumentteja, joissa on määritetty mitä suojausvaatimuksia laitetyyppiluokalle (kuten Mobility) vaaditaan, ja niitä käytetään saman luokan IT-tuotteiden vertailemiseksi. CCRA:n jäsenmäärä sekä hyväksyttyjen PP-suojausprofiilien luettelo kasvavat vuosittain. Tämän järjestelyn ansiosta tuotteen kehittäjä voi hakea kertasertifiointia missä tahansa tässä järjestelyssä mukana olevassa sertifikaatteja myöntävässä järjestelmässä ja saada sertifioinnille tunnustuksen kaikilta sen tunnustamiseen sitoutuneilta allekirjoittajajäseniltä.

Security Target -dokumentit määrittävät, *mitä* arvioidaan, kun IT-tuotetta sertifioidaan. Security Target -dokumentit muunnetaan tarkemmiksi *suojauksen toiminnallisiksi vaatimuksiksi (SFR)*, joita käytetään Security Target -dokumenttien yksityiskohtaisempaan arviointiin.

Common Criteria (CC) -standardi sisältää myös *tietoturvavarmuusvaatimukset (SAR)*. Yksi yleisesti tunnistettu mittaperuste on *varmuustaso (Evaluation Assurance Level, EAL)*. EAL-varmuustasot ryhmittelevät yhteen usein käytettyjä SAR-tietoturvavarmuusvaatimusten joukkoja, ja vertailtavuuden parantamiseksi ne voidaan eritellä PP-suojausprofiilissa ja ST-dokumentissa.

Monet vanhemmat suojausprofiilit (PP) on arkistoitu, ja niitä korvataan kehittämällä kohdennettuja PP-suojausprofiileita, jotka keskittyvät tiettyihin ratkaisuihin ja ympäristöihin. Jotta CCRA:n jäsenet jatkossakin noudattaisivat vastavuoroisen tunnustamisen periaatetta, on muodostettu iTC-yhteisöjä (international Technical Community), jotka kehittävät ja ylläpitävät yhteistyönä laadittuja cPP-profiileja (collaborative Protection Profiles), ja CCRA:n allekirjoittajajäsenet ovat alusta pitäen olleet mukana näiden profiilien kehitystyössä. Muille käyttäjäryhmille ja vastavuoroisen tunnustamisen sopimuksille kuin CCRA:lle kohdennettuja PP-suojausprofiileja kehittävät edelleen niiden kannalta tarkoituksenmukaiset sidosryhmät.

Apple on hakenut tiettyjen cPP-profiilien mukaisia sertifiointeja päivitetyssä CCRA-järjestelyssä alkuvuodesta 2015 alkaen. Siitä lähtien Apple on saavuttanut Common Criteria -sertifioinnit jokaiselle merkittävälle iOS-julkaisulle ja on laajentanut kattavuuden sisältämään uusien PP-suojausprofiilien varmistukset.

Apple toimii aktiivisessa roolissa teknisissä yhteisöissä, jotka keskittyvät mobiililaitteiden suojausteknologioiden arviointiin. Näihin lukeutuvat iTC-yhteisöt, jotka vastaavat cPP-suojausprofiilien kehittämisestä ja päivittämisestä. Apple arvioi ja hakee edelleen sertifiointeja nykyisten PP- ja cPP-suojausprofiilien perusteella.

Apple-alustojen sertifioinnit Pohjois-Amerikan markkinoille suorittaa yleensä National Information Assurance Partnership (NIAP), joka ylläpitää luetteloa parhaillaan arvioitavina olevista projekteista, joita ei ole vielä sertifioitu.

Lueteltujen yleisten alustasertifikaattien lisäksi on myönnetty muita sertifikaatteja joitakin markkinoita koskevien erityisten suojausvaatimusten osoittamiseksi.

Applen appien tietoturvasertifioinnit

Applen appien sertifioinnin tausta

Apple on aktiivinen appiensa suojauksen sertifioinnissa ja käyttää siihen asianmukaisia Common Criteria Protection Profile (PP) -suojausprofiileja. Näiden arviointien taustalla ovat Applen laitteistoille ja käyttöjärjestelmille hankkimat sertifioinnit.

Vuonna 2018 Apple aloitti appien tietoturvallisuuden arvioinnit iOS 11:ssä toimiville keskeisille apeille Safari-selaimen ja Yhteystiedot-apin arvioinnilla. Apple hankki arvioinnit näille apeille myös iOS 12:ssa, iOS 13:ssa ja iPadOS 13.1:ssä. Vuonna 2021 apeille lisätään myös arvioinnit macOS 11:ssä.

Salausmoduulien sertifioinnin tila

Tässä luetellut Applen apit käyttävät kyseessä olevan käyttöjärjestelmän salausmoduuleja. Jos haluat lisätietoja, katso iOS:n tietoturvasertifikaatit, iPadOS:n tietoturvasertifikaatit ja macOS:n tietoturvasertifikaatit.

Common Criteria (CC) -sertifioinnin tila

NIAP:n johtamassa Yhdysvaltain arviointijärjestelmässä ylläpidetään Products in Evaluation -luetteloa tuotteista, jotka ovat parhaillaan arvioitavina Yhdysvalloissa NIAP:n hyväksymässä Common Criteria -testauslaboratoriossa (CCTL) ja joille on tehty arvioinnin aloitustapaaminen (tai vastaava), jossa CCEVS:n hallinto on virallisesti hyväksynyt tuotteen arvioitavaksi.

Kun tuotteet on sertifioitu, NIAP lisää parhaillaan voimassa olevat sertifioinnit Product Compliant -luetteloon. Kahden vuoden jälkeen näistä sertifioinneista tarkistetaan, täyttyvätkö senhetkisen käytännön vaatimukset varmistuksen voimassaolon jatkamiselle. Kun varmistuksen voimassaoloaika päättyy, NIAP siirtää sertifioinnin arkistoitujen tuotteiden Archived Products -luetteloon.

Common Criteria -portaalissa luetellaan sertifioinnit, jotka voidaan tunnustaa vastavuoroisesti Common Criteria Recognition Arrangement (CCRA) -järjestelyn puitteissa. Tuotteet voidaan pitää CC-portaalissa sertifioitujen tuotteiden luettelossa viiden vuoden ajan, ja CC-portaalissa säilytetään tiedot myös arkistoiduista sertifioinneista.

Alla olevassa taulukossa näkyvät sertifioinnit, joita laboratorio arvioi parhaillaan tai jotka ovat saaneet Common Criteria -vaatimustenmukaisuuden sertifioinnin.

Nykytilanne

- NIAP:n arvionnit, jotka on julkaistu käynnissä olevina, on luetteloitu kohdassa Products in evaluation (NIAP).
- NIAP:n valmiit ja validoidut arvioinnit on luetteloitu kohdassa Product Compliant List.

Käyttöjärjestelmä / sertifiointipäiväys	Tunniste / dokumentit	Nimi / suojausprofiilit
Käyttöjärjestelmä: macOS 11 Big Sur *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* macOS 11 Big Sur Yhteystiedot *Suojausprofiilit:* PP for Application SW, EP for Web Browsers
Käyttöjärjestelmä: macOS 11 Big Sur *Sertifiointipäiväys:* –	*Tunniste:* Ei vielä sertifioitu *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* macOS 11 Big Sur Safari *Suojausprofiilit:* PP for Application SW, EP for Web Browsers
Käyttöjärjestelmä: iOS 14, iPadOS 14 *Sertifiointipäiväys:* 20.8.2021	*Tunniste:* 11191 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple iOS 14 and iPadOS 14: Yhteystiedot *Suojausprofiilit:* PP for Application SW, EP for Web Browsers
Käyttöjärjestelmä: iOS 14, iPadOS 14 *Sertifiointipäiväys:* –	*Tunniste:* 11192 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple iOS 14 and iPadOS 14: Safari *Suojausprofiilit:* PP for Application SW, EP for Web Browsers
Käyttöjärjestelmä: iOS 13, iPadOS 13 *Sertifiointipäiväys:* 5.6.2020	*Tunniste:* 11060 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple iOS 13 and iPadOS 13: Safari *Suojausprofiilit:* PP for Application SW, EP for Web Browsers

Käyttöjärjestelmä / sertifiointipäiväys	Tunniste / dokumentit	Nimi / suojausprofiilit
Käyttöjärjestelmä: iOS 13, iPadOS 13 *Sertifiointipäiväys:* 5.6.2020	*Tunniste:* 11050 *Dokumentit:* Sertifikaatti Security Target -dokumentti Opas Validointiraportti Varmistuksen toimintaraportti	*Nimi:* Apple iOS 13 and iPadOS 13: Yhteystiedot *Suojausprofiilit:* PP for Application SW

Applen appien arkistoidut Common Criteria -sertifioinnit

Käyttöjärjestelmä / sertifiointipäiväys	Tunniste / dokumentit	Nimi / suojausprofiilit
Käyttöjärjestelmä: iOS 12 *Sertifiointipäiväys:* 12.6.2019	*Tunniste:* 10960 *Dokumentit:* Security Target -dokumentti Opas	*Nimi:* iOS 12 Safari *Suojausprofiilit:* PP for Application SW, EP for Web Browsers
Käyttöjärjestelmä: iOS 12 *Sertifiointipäiväys:* 28.2.2019	*Tunniste:* 10961 *Dokumentit:* Security Target -dokumentti Opas	*Nimi:* iOS 12 Contacts *Suojausprofiilit:* PP for Application SW
Käyttöjärjestelmä: iOS 11 *Sertifiointipäiväys:* 9.11.2018	*Tunniste:* 10916 *Dokumentit:* Security Target -dokumentti Opas	*Nimi:* iOS 11 Safari *Suojausprofiilit:* PP for Application SW, EP for Web Browsers
Käyttöjärjestelmä: iOS 11 *Sertifiointipäiväys:* 13.9.2018	*Tunniste:* 10915 *Dokumentit:* Security Target -dokumentti Opas	*Nimi:* iOS 11 Contacts *Suojausprofiilit:* PP for Application SW

Applen internet-palvelujen tietoturvasertifikaatit

Apple ylläpitää standardien ISO/IEC 27001 ja ISO/IEC 27018 mukaisia sertifiointeja, jotta Applen asiakkaat voivat täyttää määräyksiin ja sopimuksiin perustuvat velvoitteensa. Sertifikaatit tarjoavat asiakkaillemme riippumattoman todistuksen Applen sertifioinnin piiriin kuuluvien järjestelmien tietoturva- ja tietosuojakäytännöistä.

ISO/IEC 27001 ja ISO/IEC 27018 kuuluvat tietoturvallisuuden hallintajärjestelmien (Information Security Management System, ISMS) standardeihin, jotka on julkaissut kansainvälinen standardoimisjärjestö ISO (International Organization for Standardization). Osana Applen tietoturvallisuuden hallintajärjestelmien standardeja kaikki liitteen A hallintavaatimukset on lisätty soveltuvuusilmoitukseen standardeissa ISO/IEC 27001 ja ISO/IEC 27018 määritetyllä tavalla. Valtuutettu rekisterinpitäjä tekee Applelle vuosittain riippumattoman todistuksen.

ISO/IEC 27001

ISO/IEC 27001 on tietoturvallisuuden hallintajärjestelmien standardi, jossa eritellään vaatimukset organisaation tietoturvallisuuden hallintajärjestelmän luomiselle, toteutukselle, ylläpidolle ja jatkuvalle parantamiselle. ISO/IEC 27001 -standardiin sisältyvät seuraavat Applen ISO/IEC-sertifiointien kattamat tietoturvallisuuden osa-alueet:

- Tietoturvallisuuskäytännöt
- Tietoturvallisuuden organisointi
- Suojattavan omaisuuden hallinta
- Henkilöstöturvallisuus
- Fyysinen turvallisuus ja ympäristön turvallisuus
- Viestintä ja toiminnan hallinta
- Pääsynhallinta
- Tietojärjestelmien hankkiminen, kehittäminen ja ylläpito
- Tietoturvapoikkeamien hallinta
- Liiketoiminnan jatkuvuuden hallinta
- Vaatimustenmukaisuus

ISO/IEC 27018

ISO/IEC 27018 antaa menettelyohjeet henkilötietojen suojaamiseen julkisissa pilvipalveluissa. ISO/IEC 27018 -standardiin sisältyvät seuraavat Applen ISO/IEC-sertifiointien kattamat tietoturvallisuuden osa-alueet:

- Suostumus ja valinnanvapaus
- Tarkoituksen laillisuus ja määrittely
- Tiedonkeruun rajoittaminen
- Tiedonkäsittelyn rajoittaminen
- Käytön, säilytyksen ja luovutuksen rajoittaminen
- Oikeellisuus ja laatu
- Avoimuus, läpinäkyvyys ja ilmoittaminen
- Omien tietojen tarkistusoikeus
- Vastuullisuus
- Tietoturvallisuus
- Tietosuojavaatimusten noudattaminen

Standardien ISO/IEC 27001 ja ISO/IEC 27018 kattamat Applen palvelut

Applen ISO/IEC 27001- ja ISO/IEC 27018 -sertifioinnit kattavat seuraavat palvelut:

- Applen Yrityschat
- Apple Business Manager
- Apple Push Notification service -palvelu (APNs)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork-palvelut
- Hallitut Apple ID:t
- Koulutyöt
- Siri

Sertifikaatit

Osoitukset Applen ISO/IEC 27001- ja 27018-sertifioinneista ovat saatavilla rekisterinpitäjältämme.

Voit katsoa Applen sertifiointeja avaamalla Britannian standardointi-instituutin (BSI) Certificate and Client Directory -haun, kirjoittamalla Company-hakukenttään Apple ja valitsemalla sitten hakutulokset, joilla näet sertifikaatit.

Huomaa: Annettuihin tietoihin tuotteista, jotka eivät ole Applen valmistamia, tai riippumattomista verkkosivustoista, jotka eivät ole Applen hallitsemia tai testaamia, ei sisälly suositusta. Apple ei vastaa muiden tahojen verkkosivustojen tai tuotteiden valikoimasta, toimivuudesta tai käytöstä. Apple ei ota kantaa muiden tahojen verkkosivustojen oikeellisuuteen tai luotettavuuteen. Jos tarvitset lisätietoja, ota yhteys valmistajaan.

macOS Security Compliance Project

macOS Security Compliance Project (mSCP) on avoimen lähdekoodin projekti, jossa hyödynnetään ohjelmallisia keinoja tietoturvaohjeistusten tuottamiseen. Tässä yhteisprojektissa ovat mukana Yhdysvaltain standardointielimen NIST:n operatiivisen tietoturvan asiantuntijat, Yhdysvaltain ilmailu- ja avaruushallintovirasto NASA, Yhdysvaltain puolustusalan tietojärjestelmien virasto DISA sekä Los Alamos National Laboratory (LANL). Projektissa on määritelty vastaavuudet useiden testattujen ja validoitujen macOS:n hallintaominaisuuksien ja projektin tukemissa tietoturvaohjeistuksissa vaadittavien suojausten välillä. Lisäksi projektissa voidaan hyödyntää testattujen ja validoitujen atomisten toimintojen (konfigurointiasetusten) kirjastoa ja luoda sen avulla helposti omiin tarpeisiin muokattuja tietoturvan vertailukohtatiedostoja. Projekti tuottaa käytettävän vertailukohtatiedoston perusteella muokatun dokumentaation, skriptit, asetusprofiilit ja tarkastuslistan.

mSCP voi tuottaa sisältöä, jota voidaan käyttää vaatimustenmukaisuuden täyttämiseksi yhdessä hallinta- ja tietoturvatyökalujen kanssa. Tämän projektin konfigurointiasetuksilla voidaan käyttää vertailukohtana seuraavia ohjeita:

Organisaatio	Tuetut vertailukohdat
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 5	800-53 High, 800-53 Moderate, 800-53 Low
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Rev.2	800-171
Defense Information Systems Agency (DISA) macOS 11 STIG, Apple macOS 11 Security Technical Implementation Guide	STIG
Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems	1253

Lisätietoja:

- Vertailukohtatiedosto kaikkien projektin sääntöjen tarkistamiseksi on täällä.
- Jos haluat lisätietoja projektista ja sen käyttämisestä, tutustu macOS Security Compliance Projectin wikiin.
- Jos haluat ottaa projektin käyttöön, katso: Getting to Know the macOS Security Compliance Project, Part 1 ja Getting to Know the macOS Security Compliance Project, Part 2.
- Jos olet kiinnostunut osallistumaan projektin kehitykseen, katso ohjeet osallistumiseen.

Muutoshistoria

Päiväys	Yhteenveto
27. lokakuuta 2021	Päivitetyt aiheet: • Tietoturvasertifioinnit Secure Enclave -prosessorille • iOS:n tietoturvasertifikaatit • macOS:n tietoturvasertifikaatit
17. elokuuta 2021	Päivitetyt aiheet: • Tietoturvasertifioinnit Secure Enclave -prosessorille • Apple T2 Security -sirun suojauksen sertifioinnit • iOS:n tietoturvasertifikaatit • iPadOS:n tietoturvasertifikaatit • macOS:n tietoturvasertifikaatit • tvOS:n tietoturvasertifikaatit • watchOS:n tietoturvasertifikaatit • Applen appien tietoturvasertifioinnit • Suojaussertifioinnit • macOS Security Compliance Project
26. huhtikuuta 2021	Lisätty aihe: • macOS Security Compliance Project Päivitetyt aiheet: • Apple T2 Security -sirun tietoturvan sertifioinnit: Uusi FIPS 140-2 -sertifikaatti (nro 3811) • Tietoturvasertifioinnit Secure Enclave -prosessorille: Uusi FIPS 140-2 -sertifikaatti (nro 3811) ja uusi muiden sertifiointien taulukko. • iOS:n tietoturvasertifikaatit: Uudet FIPS 140-2 -sertifikaatit (nro 3811), iOS 14 arvioitavana tunnisteella 11146 • iPadOS:n tietoturvasertifikaatit: Uudet FIPS 140-2 -sertifikaatit (nro 3811), iPadOS 14 arvioitavana tunnisteella 11147 • macOS:n tietoturvasertifikaatit: Uusi FIPS 140-2 -sertifikaatti (nro 3811). • tvOS:n tietoturvasertifikaatit: Uudet FIPS 140-2 -sertifikaatit (nro 3811). • watchOS:n tietoturvasertifikaatit: Uudet FIPS 140-2 -sertifikaatit (nro 3811). • Applen appien tietoturvasertifioinnit: Päivityksiä Common Criteria -sertifioinnin tilaan, uusi taulukko arkistoiduille Common Criteria -sertifikaateille.

Sanasto

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 Push Notification service -palvelu (APNs) Applen tarjoama maailmanlaajuinen palvelu, joka toimittaa push-ilmoituksia Apple-laitteille.

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.

Common Criteria (CC) Standardi, jossa määritetään IT-tietoturvan arvioinnin yleiset käsitteet ja periaatteet sekä arvioinnin yleinen malli. Se sisältää tietoturvavaatimusten luettelot standardikielellä.

Common Criteria Recognition Arrangement (CCRA) Vastavuoroisen tunnustamisen sopimus, joka määrittää käytäntöjä ja vaatimuksia ISO/IEC 15408-sarjan tai Common Criteria -standardien mukaisien sertifikaattien kansainväliselle tunnustamiselle.

corecrypto Kirjasto, joka tarjoaa matalan tason salausprimitiivien toteutuksia. Huomaa, että corecrypto ei suoraan tarjoa ohjelmoinnin käyttöliittymiä kehittäjille ja että sitä käytetään kehittäjille tarjottujen API-rajapintojen kautta. Corecrypton lähdekoodi on julkisesti saatavilla, jotta sen tietoturvaominaisuudet ja oikea toiminta voidaan tarkistaa.

cPP-suojausprofiili Suojausprofiili, jonka on kehittänyt iTC-yhteisö, joka on cPP-profiilien luomisesta vastaava asiantuntijoiden joukko.

Cryptographic Algorithm Validation Program (CAVP) NIST:n operoima organisaatio, joka tarjoaa hyväksyttyjen (kuten FIPS-hyväksyttyjen ja NIST-suositeltujen) salausalgoritmien ja niiden yksittäisten osien validointitestausta.

Cryptographic Module Validation Program (CMVP) Yhdysvaltain ja Kanadan viranomaisten järjestämä organisaatio, joka validoi FIPS 140-3 -standardin vaatimuksenmukaisuutta.

FIPS-standardi (Federal Information Processing Standard) NIST:n kehittämät julkaisut, joko sääntöjen edellyttäminä ja/tai kun liittovaltion viranomaisilla on tärkeitä kybersuojaukseen liittyviä tarpeita.

Implementation under Test (IUT) Salausmoduuli, jota testataan laboratoriossa.

IPsec VPN Client Suojausprofiilissa oleva asiakas, joka tarjoaa suojatun IPsec-yhteyden fyysisen tai virtuaalisen isäntäalustan ja etäsijainnin välille.

iTC-yhteisö (international Technical Community) Ryhmä, jonka vastuulla on kehittää suojausprofiileja tai cPP-profiileja Common Criteria Recognition Arrangement (CCRA) -sopimuksen tuella.

järjestelmäpiiri (SoC) Mikropiiri eli integroitu piiri, joka sisältää useita komponentteja yhdessä sirussa.

mobiililaitteiden hallinta (MDM) Palvelu, jolla käyttäjä voi hallita etänä rekisteröityjä laitteita. Kun laite on rekisteröity, käyttäjä voi käyttää verkon kautta MDM-palvelua, joka määrittää asetuksia ja suorittaa muita tehtäviä laitteella ilman käyttäjän toimia.

Modules in Process (MIP) Cryptographic Module Validation Program (CMVP) -ohjelman ylläpitämä luettelo salausmoduuleista, jotka ovat parhaillaan CMVP-validointiprosessissa.

National Information Assurance Partnership (NIAP) Yhdysvaltain viranomaisorganisaatio, jonka vastuulla on Common Criteria -standardin toteutus Yhdysvalloissa ja NIAP:n Common Criteria -arviointi ja -validointijärjestelmä (CCEVS).

National Institute of Standards and Technology (NIST) Yhdysvaltain kauppaministeriön osa, jonka vastuulla on mittaustieteen, standardien ja teknologian edistäminen.

salausmoduuli Laitteisto, ohjelmisto ja/tai laiteohjelmisto, jotka tarjoavat salaustoimintoja ja täyttävät määritetyn salausmoduulistandardin vaatimukset.

Secure Element (SE) Useisiin Apple-laitteisiin upotettu silikonisiru, joka tukee esimerkiksi Apple Payn tapaisia toimintoja.

Secure Enclave -prosessori (SEP) Lisäprosessori, joka on sisäänrakennettu järjestelmäpiiriin (SoC).

Security Target (ST) -dokumentti Dokumentti, jossa määritetään tietyn tuotteen tietoturvaongelma ja tietoturvavaatimukset.

Senior Officials Group Information Systems Security (SOG-IS) Ryhmä, joka hallitsee vastavuoroisen tunnustamisen sopimusta useiden eurooppalaisten valtioiden välillä.

sepOS Secure Enclave -laiteohjelmisto, joka perustuu Applen muokkaamaan versioon L4-mikrokernelistä.

Soveltuvuusilmoitus (Statement of Applicability, SOA) Dokumentti, jossa kuvataan ISMS:n laajuudessa käytettävät suojaukset, jotka on tuotettu ISO/IEC 27001 -sertifioinnin tueksi.

Suojausprofiili (Protection Profile, PP) Dokumentti, jossa määritetään tuotteiden tietyn luokan tietoturvaongelma ja tietoturvavaatimukset.

Suojaustaso (Security Level, SL) ISO/IEC 19790 -standardissa määritetyt neljä yleistä suojaustasoa (1–4), jotka kuvaavat tarvittavien suojausvaatimusten joukkoa. Luokka 4 on tiukin.

T2 Applen suojauspiiri, joka sisältyy tiettyihin Mac-tietokoneisiin vuodesta 2017 alkaen.

Tietoturvallisuuden hallintajärjestelmä (Information Security Management System, ISMS) Joukko tietoturvallisuuskäytäntöjä ja -menetelmiä, jotka määrittävät suojausohjelmaa, joka on suunniteltu suojaamaan tietolaajuutta ja järjestelmiä hallitsemalla järjestelmällisesti tietoturvallisuutta tiedon tai järjestelmän koko elinkaaren ajalta.

Täysi levyn salaus (FDE) Taltion kaiken datan salaaminen.

Apple
One Apple Park Way
Cupertino, CA 95014
Yhdysvallat
apple.com

K028-00499-B