Senter for sikkerhetssertifiseringer og etterlevelse av regelverk

Desember 2021

Innhold

Introduksjon til Apple og sikkerhet

Som en del av vår forpliktelse til sikkerhet og personvern benytter Apple internasjonale og anerkjente tredjepartsorganisasjoner til å opprettholde uavhengige sertifiseringer og attestasjoner over maskinvare, programvare (inkludert operativsystem og apper) og tjenester, slik at kundene får en uavhengig evaluering av Apples sikkerhets- og personvernpraksis. Disse organisasjonene gir Apple sertifiseringer som sammenfaller med lanseringen av hver store OS-versjon. På denne måten bekrefter de at sikkerhetskravene opprettholdes. De tekniske områder som ikke aksepteres i gjensidige anerkjennelsesavtaler (Mutual Recognition Arrangements, MRA-er), eller som mangler etablerte standarder for sikkerhetssertifiseringer, er Apple med å utvikle sikkerhetsstandarder for. Vår målsetning er å fremme globalt akseptert og omfattende sikkerhetssertifiseringsdekning av maskinvare, operativsystemer, apper og tjenester fra Apple.

Sertifiseringer er ofte nødvendige for å oppfylle kravene til lover, forskrifter og bransjestandarder. Tjenester som Apple School Manager og Apple Business Manager er dekket av Apples ISO/IEC 27001- og ISO/IEC 27018-sertifiseringer. Alle kunder, inkludert offentlige organer og bedrifts- og utdanningsorganisasjoner som ruller ut Apple-enheter, kan bruke sertifisering av maskinvaren, operativsystemene, programvaren og tjenestene for å vise etterlevelse av regelverket.

Maskinvaresertifiseringer

Fordi sikker programvare krever en sikkerhetsgrunnmur som er innebygd i maskinvaren, har alle Apple-enheter med iOS, iPadOS, macOS, tvOS eller watchOS sikkerhetsfunksjoner integrert i chipene. Disse inkluderer spesialutviklede CPU-funksjoner som driver systemsikkerhetsfunksjoner, og chiper for sikkerhetsfunksjoner. Den viktigste komponenten er Secure Enclave-koprosessoren, som finnes på alle moderne iOS-, iPadOS-, watchOS- og tvOS-enheter, alle Macer med Apple-chiper og alle Intel-baserte Macer med Apple T2-sikkerhetschipen. Secure Enclave legger grunnlaget for datakryptering i dvale, sikker oppstart i macOS og biometri.

Apples sikkerhetsgaranti starter med sertifiseringen av grunnleggende sikkerhetskomponenter i chipene fra maskinvarens «root of trust» og omfatter også håndhevingen av sikker oppstart, Secure Enclaves sikre lagring av nøkler til sikker autentisering med Touch ID og Face ID. Sikkerhetsfunksjonene til Apple-enheter muliggjøres av kombinasjonen av chipdesign, maskinvare, programvare og tilgjengelige tjenester fra Apple. Sertifisering av disse komponentene er en viktig del av å verifisere garantien som Apple gir.

Hvis du vil ha informasjon om offentlige sertifiseringer knyttet til maskinvare og tilknyttede firmwarekomponenter, kan du se:

- Sikkerhetssertifiseringer for Apple T2-sikkerhetschip
- Sikkerhetssertifiseringer for Secure Enclave-prosessoren (SEP)

Sertifiseringer for apper og programvare

Apple opprettholder uavhengige sertifiseringer og attesteringer av sine operativsystemer og apper i samsvar med U.S. Federal Information Processing Standards (FIPS) 140-2/-3 for kryptografiske moduler og Common Criteria for operativsystemer, apper og enhetstjenester. Dekningen av operativsystemer inkluderer iOS, iPadOS, macOS, sepOS, T2-firmware, tvOS og watchOS. For apper inkluderer uavhengig sertifisering i første omgang Safari-nettleseren og Kontakter. Flere apper får dekning senere.

Hvis du vil ha informasjon om offentlige sertifiseringer knyttet til Apples *operativsystemer*, kan du se:

- Sikkerhetssertifiseringer for iOS
- Sikkerhetssertifiseringer for iPadOS
- Sikkerhetssertifiseringer for macOS
- Sikkerhetssertifiseringer for tvOS
- Sikkerhetssertifiseringer for watchOS

Hvis du vil ha informasjon om offentlige sertifiseringer knyttet til Apple-*apper*, kan du se:

- Sikkerhetssertifiseringer for Apple-apper

Tjenestesertifiseringer

Apple opprettholder sikkerhetssertifiseringer for å støtte kunder fra næringslivet til utdanningssektoren. Disse sertifiseringene gjør at Apple-kunder kan oppfylle lovpålagte og kontraktsmessige forpliktelser når de bruker Apple-tjenester med Apple-maskinvare og -programvare. Disse sertifiseringene gir kundene våre en uavhengig bekreftelse på Apples informasjonssikkerhets-, miljø- og personvernpraksis for Apple-systemer.

Hvis du vil ha informasjon om offentlige sertifiseringer knyttet til Apples *internettjenester*, kan du se:

- Sikkerhetssertifiseringer for internettjenester fra Apple

Hvis du har spørsmål om sikkerhets- og personvernsertifiseringer fra Apple, kan du kontakte security-certifications@apple.com.

Sertifiseringer for maskinvaresikkerhet

Oversikt over Apples sertifiseringer for maskinvaresikkerhet

Apple opprettholder amerikanske FIPS 140-2/-3-sertifikater for samsvarsvalidering for sepOS og T2-firmware i tillegg til andre sertifiseringer. Apple starter med *byggesteiner for sertifisering* som gjelder på tvers av flere plattformer. Én byggestein er valideringen av corecrypto-biblioteket, som brukes til utrullinger av kryptografiske moduler for programvare og maskinvare i operativsystemer utviklet av Apple. En annen byggestein er sertifiseringen av Secure Enclave, som er innebygd i mange Apple-enheter. En tredje byggestein er sertifiseringen av Secure Element (SE), som finnes i Apple-enheter med Touch ID og enheter med Face ID. Disse byggesteinene for maskinvaresertifisering danner et grunnlag for bredere sertifiseringer av plattformsikkerhet.

Valideringer for kryptografiske algoritmer

Validering av korrekt implementering av mange kryptografiske algoritmer og tilhørende sikkerhetsfunksjoner er et krav for FIPS 140-3-validering, og støtter andre sertifiseringer. Valideringen håndteres av Cryptographic Algorithm Validation Program (CAVP), som er en del av National Institute of Standards and Technology (NIST) Valideringssertifikater for Apple-implementeringer er tilgjengelige via CAVP-søkefunksjonen. Du finner mer informasjon på nettstedet for Cryptographic Algorithm Validation Program (CAVP).

Valideringer for kryptografiske moduler: FIPS 140-2/3 (ISO/IEC 19790)

Siden 2012 har Apples kryptografiske moduler gjentatte ganger blitt validert av Cryptographic Module Validation Program (CMVP) til å være i overensstemmelse med U.S. Federal Information Processing Standards for kryptografiske moduler (FIPS 140-2) etter hver hovedlansering av operativsystemer. Etter hver hovedlansering sender Apple inn modulene til CMVP for overensstemmelsesvalidering med standardene. I tillegg til å brukes i Apples operativsystemer og apper gir disse modulene kryptografisk funksjonalitet for tjenester som leveres av Apple, og de er tilgjengelige for bruk av tredjepartsapper.

Apple har hvert år oppnådd **sikkerhetsnivå 1** for de programvarebaserte modulene «Corecrypto Module for Intel» og «Corecrypto Kernel Module for Intel» til macOS. For Apple-chiper gjelder modulene «CoreCrypto Module on ARM» og «CoreCrypto Kernel Module on ARM» for iOS, iPadOS, tvOS, watchOS og firmwaren i den innebygde Apple T2-sikkerhetschipen i Macer.

Apple oppnådde i 2019 første FIPS 140-2 **sikkerhetsnivå 2** for den integrerte kryptografiske programvaremodulen identifisert som «Apple Corecrypto Module: Secure Key Store», som gjorde at amerikanske myndigheter godkjente bruken av nøkler som har blitt generert og håndtert i Secure Enclave. Apple søker å oppnå valideringer for den kryptografiske maskinvaremodulen for kommende hovedversjoner av operativsystemer.

FIPS 140-3 ble godkjent av det amerikanske handelsdepartementet i 2019. Den største endringen i denne versjonen av standarden er spesifiseringen av ISO/IEC-standardene, særlig ISO/IEC 19790:2015 og den tilhørende teststandarden ISO/IEC 24759:2017. CMVP har iverksatt et overgangsprogram og har indikert at kryptografiske moduler skal valideres etter FIPS 140-3 som standard fra 2020. Apples kryptografiske moduler tar sikte på å oppfylle og gå over til FIPS 140-3-standarden så raskt det er gjennomførbart.

For kryptografiske moduler som for øyeblikket er i testing- og valideringsprosessene, opprettholder CMVP to separate lister som kan inneholde informasjon om foreslåtte valideringer. Kryptografiske moduler som er under testing med et akkreditert laboratorium, kan vises i Implementation Under Test-listen. Når laboratoriet har fullført testingen og anbefalt validering av Apples kryptografiske moduler hos CMVP, vises de i Modules in Process-listen. På dette tidspunktet er laboratorietestingen fullført og avventer validering av testingen av CMVP. Siden varigheten av evalueringsprosessen varierer, kan du sjekke begge disse prosesslistene for å se den gjeldende statusen til Apples kryptografiske moduler mellom datoen for en hovedlansering av operativsystemene og utstedelse av valideringssertifikatet fra CVMP.

Produktsertifiseringer: Common Criteria ISO/IEC 15408

Common Criteria (ISO/IEC 15408) er en standard som brukes av mange organisasjoner som et grunnlag for å utføre sikkerhetsevalueringer av IT-produkter.

Du finner informasjon om sertifiseringer som kan bli gjensidig godkjent under den internasjonale Common Criteria Recognition Arrangement (CCRA), på Common Criteria-portalen. Common Criteria-standarden kan også brukes utenfor CCRA av nasjonale og private valideringssystemer. I Europa styres gjensidig anerkjennelse gjennom SOG-IS-avtalen i tillegg til CCRA.

Målet, slik det framgår av Common Criteria-fellesskapet, er at et internasjonalt godkjent sett med sikkerhetsstandarder skal gi en tydelig og pålitelig evaluering av sikkerhetsfunksjonene til IT-produkter. Common Criteria-sertifiseringen tilbyr en uavhengig vurdering av et produkts evne til å overholde sikkerhetsstandarder, noe som gir kundene mer tillit til sikkerheten til IT-produkter og fører til mer velinformerte avgjørelser.

Gjennom CCRA har medlemslandene blitt enige om å anerkjenne sertifiseringen av IT-produkter med samme nivå av tillit. Evalueringene som kreves før sertifiseringen, er omfattende og inkluderer:

- Protection Profiles (PP-er)
- Security Targets (ST-er)
- Security Functional Requirements (SFR-er)
- Security Assurance Requirements (SAR-er)
- Evaluation Assurance Levels (EAL-er)

Protection Profiles (PP-er) er dokumenter som spesifiserer sikkerhetskrav for en klasse med enhetstyper (for eksempel mobilitet), og brukes til å sammenligne evalueringene av IT-produkter innenfor samme klasse. Medlemskap i CCRA og en økende liste med godkjente PP-er fortsetter å vokse hvert år. Takket være denne avtalen kan en produktutvikler oppnå en enkeltsertifisering under hvilken som helst av autoriseringssystemene og få den anerkjent av en av sertifiseringssignatarene.

Security Targets (ST-er) definerer *hva* som evalueres når et IT-produkt blir sertifisert. ST-ene omformes til mer spesifikke *Security Functional Requirements (SFR-er)*, som brukes til å evaluere ST-ene grundigere.

Common Criteria (CC-er) inkluderer også *Security Assurance Requirements (SAR-er)*. Vanlige parametere er *Evaluation Assurance Level (EAL-er)*. EAL-er grupperer sammen hyppige forekomster av sett med SAR-er og kan spesifiseres i PP-er og ST-er for å støtte sammenlignbarhet.

Mange eldre PP-er er arkivert og blir erstattet med målrettede PP-er som utvikles og rettes mot spesifikke løsninger og miljøer. I en felles innsats for å sikre fortsatt gjensidig anerkjennelse på tvers av alle CCRA-medlemmer har ITC (International Technical Community) blitt opprettet for utvikling og oppdateringer av cPP-er (Collaborative Protection Profiles), som utvikles fra starten med medvirkning fra flere CCRA-signatursystemer. PP-er som er rettet mot brukergrupper og avtaler om gjensidig anerkjennelse, med unntak av CCRA, fortsetter å utvikles av egnede interessenter.

Apple begynte å søke om å oppnå sertifiseringer under den oppdaterte CCRA-en med utvalgte cPP-er tidlig i 2015. Siden da har Apple oppnådd Common Criteria-sertifiseringer for hver hovedlansering av iOS og har utvidet dekningen til å inkludere sikkerhetsforsikring gitt av nye PP-er.

Apple tar en aktiv rolle i de tekniske miljøene som fokuserer på å evaluere teknologi for mobilsikkerhet. Disse inkluderer ITC-er som er ansvarlige for å utvikle og oppdatere cPP-er. Apple fortsetter å evaluere og oppnå sertifiseringer mot gjeldende PP-er og cPP-er.

Apples plattformsertifiseringer for det nordamerikanske markedet utføres vanligvis med National Information Assurance Partnership (NIAP), som opprettholder en liste over prosjekter som er under evaluering, men som ikke er sertifisert ennå.

I tillegg til de oppførte generelle plattformsertifikatene er det utstedt andre sertifikater for å demonstrere spesifikke sikkerhetskrav for enkelte markeder.

Sikkerhetssertifiseringer for Secure Enclave-prosessoren (SEP)

Bakgrunn for Secure Enclave-sertifisering

Den kryptografiske maskinvaremodulen – *Apple SEP Secure Key Store Cryptographic Module* – er innebygd i Apple SoC-en som finnes i følgende produkter: Apple A-serien for iPhone og iPad, M-serien for Macer med Apple-chiper, S-serien for Apple Watch og sikkerhetschiper i T-serien i Macer med Intel-chiper fra og med iMac Pro, som ble lansert i 2017.

I 2018 synkroniserte Apple med valideringen av de kryptografiske programvaremodulene med operativsystemer lansert i 2017: iOS 11, macOS 10.13, tvOS 11 og watchOS 4. Den kryptografiske SEP-maskinvaremodulen identifisert som Apple SEP Secure Key Store Cryptographic Module versjon 1.0 ble først validert mot kravene til FIPS 140-2 Security Level 1.

I 2019 validerte Apple maskinvaremodulen opp mot kravene til FIPS 140-2 Security Level 2 og oppdaterte modulversjonidentifikatoren til versjon 9.0 for å synkronisere med versjonene av de tilhørende Corecrypto-bruker- og Corecrypto-kjernemodulvalideringene. I 2019 inkluderte dette iOS 12, macOS 10.14, tvOS 12 og watchOS 5.

I 2020 og 2021 har Apple arbeidet med valideringen av overensstemmelse med FIPS 140-3 og med ekstra sikkerhetsforsikring for sikkerhetsnivå 3 for de fysiske sikkerhetskravene til Apple-chipene: A13, A14, S6 og M1.

Apple tar også aktivt del i valideringen av Corecrypto-bruker- og Corecrypto-kjernemoduler for hver store lansering av et operativsystem. Validering av overensstemmelse kan bare gjøres med en ferdigstilt, lansert versjon.

Valideringsstatus for kryptografiske moduler

Cryptographic Module Validation Program (CMVP) opprettholder valideringsstatus for kryptografiske moduler i tre separate lister, avhengig av deres gjeldende status:

- For å kunne stå på Implementation Under Test-listen til CMVP må laboratoriet ha kontrakt med Apple for å gjennomføre testing.
- Når laboratoriet har gjennomført testingen, laben har anbefalt validering til CMVP og CMVP-avgiftene er betalt, blir modulen lagt til i Modules in Process (MIP)-listen. MIP-listen sporer framgangen til CMVP-valideringen i fire faser:
  - *Gjennomgang venter:* Venter på at CMVP-ressurser skal tilordnes.
  - *Under gjennomgang:* CMVP-ressursene gjennomfører valideringen.
  - *Koordinering:* Laben og CMVP løser eventuelle problemer.
  - *Ferdigstilling:* Aktiviteter og formaliteter omkring utstedelse av sertifikatet.
- Etter CMVP-valideringen blir modulene tildelt et sertifikat for overensstemmelse og legges til i listen over validerte kryptografiske moduler. Dette inkluderer:
  - Validerte moduler som er merket som aktive.
  - Etter fem år merkes modulene som historiske.
  - Hvis modulsertifikatet trekkes tilbake, merkes de som trukket tilbake.

I 2020 tok CMVP i bruk den internasjonale standarden ISO/IEC 19790 som grunnlag for FIPS 140-3.

FIPS 140-3-sertifiseringer

Dagens status

Tabellen under viser de kryptografiske modulene for 2020 og 2021 som nå blir testet av laboratoriet for samsvar med FIPS 140-3.

Secure Key Store (SKS) som er knyttet til operativsystemene lansert i både 2020 og 2021, har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen, og når de er validert, flyttes de til listen over validerte kryptografiske moduler.

Brukerplass, kjerneplass og Secure Key Store i iOS 15 (2021) blir testet av laboratoriet. De ligger i Implementation Under Test-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med 2021-versjonene av iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9–A14, T2, M1, S3–S6) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med 2021-versjonene av iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A13, A14, S6, M1) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med 2020-versjonene av iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9–A14, T2, M1, S3–S6) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med 2020-versjonene av iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A13, A14, S6, M1) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3

FIPS 140-2-sertifiseringer

Tabellen under viser de kryptografiske modulene som har blitt testet av laboratoriet for samsvar med FIPS 140-2.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 05.02.2021	*Sertifikater:* 3811 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 10.0 *Operativsystem:* sepOS for macOS 10.15 Catalina *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3523 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 9.0 *Operativsystem:* sepOS for macOS 10.14 Mojave *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3223 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 1.0 *Operativsystem* sepOS for macOS 10.13 High Sierra *Type:* Maskinvare *Sikkerhetsnivå:* 2

Sertifiseringer for Common Criteria (CC)

Apple tar aktiv del i Common Criteria-evalueringer der egnede Protection Profiles dekker sikkerhetsfunksjonaliteten i Apple-teknologi.

Sertifiseringsstatus for Common Criteria (CC)

Det amerikanske systemet, som drives av NIAP, opprettholder en liste over produkter under evaluering. Denne listen inkluderer produkter som evalueres i USA hos et NIAP-godkjent Common Criteria-testlaboratorium (CCTL), og som har gjennomført et Evaluation Kickoff Meeting (eller liknende), hvor CCEVS-administrasjonen offisielt har akseptert produktet for evaluering.

Etter at produktene har blitt sertifisert, legger NIAP inn gyldige sertifiseringer i listen over overensstemmende produkter. Etter to år blir disse sertifiseringene gjennomgått for overensstemmelse med det gjeldende regelsettet for sikkerhetsvedlikehold. Etter at datoen for regelsettet for sikkerhetsvedlikehold har utløpt, flytter NIAP sertifiseringslisten til listen over arkiverte produkter.

Common Criteria-portalen lister opp sertifiseringer som kan gjensidig anerkjennes under Common Criteria Recognition Arrangement (CCRA). CC-portalen kan beholde produkter på listen over sertifiserte produkter i fem år, og informasjonen ligger i CC-portalen for arkiverte sertifiseringer.

Tabellen under viser sertifiseringer som er under evaluering i en lab, eller som har blitt sertifisert til å være i samsvar med CC.

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: sepOS *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple Secure Enclave [2020] *Protection Profiles (PP-er):* CPP_DSC_V1.0 *Maskinvare:* Secure Enclave for (A9–A14, M1, T2, S3–S6) *Programvare:* sepOS distribuert med iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7

Ytterligere sertifiseringer

Tabellen nedenfor viser sertifiseringer for Secure Enclave som verken bruker Common Criteria eller FIPS 140-3.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* fra 07.12.2019 til 26.12.2022	*Sertifikater:* CFNR201902910002 (P.R. China: Technology Certification of Mobile Financial Service) Kinesisk versjon Engelsk versjon	*Tittel:* Mobile Terminal Trusted Execution Environment *Operativsystem:* iOS 13.5.1 *Spesifikasjon:* JR/T 0156-2017

Sikkerhetssertifiseringer for Apple T2-sikkerhetschip

Valideringsbakgrunn for kryptografiske moduler

Apple tar aktivt del i valideringen av innebygde Apple-moduler for programvare og maskinvare for hver store lansering av et operativsystem. Validering av overensstemmelse kan bare gjøres mot en ferdigstilt lanseringsversjon av en modul.

I 2020 tok CMVP i bruk den internasjonale standarden ISO/IEC 19790 som grunnlag for den amerikanske standarden Federal Information Processing Standard (FIPS) 140-3.

I tillegg til å ha en Intel-prosessor har de fleste Macer siden 2017 også hatt en separat Apple T2-sikkerhetschip, som er en Apple-basert SoC (System on Chip). Disse Macene med T2-chip bruker alle de fem kryptografiske modulene for ulike tjenester på enheten.

- Corecrypto-brukermodul for Intel (brukes av macOS på Intel-baserte Macer)
- Corecrypto-kjernemodul for Intel (brukes av macOS på Intel-baserte Macer)
- Corecrypto-brukermodul for ARM (brukes av T2-chipen)
- Corecrypto-kjernemodul for ARM (brukes av T2-chipen)
- Secure Key Store Cryptographic Module (brukes av den innebygde Secure Enclave-koprosessoren i T2-chipen)

Merk: De Apple-baserte modulene som kjører på T2-chipen, er de samme som de som kjører på andre Apple-chiper, som Apple A-serien, S-serien og M-serien.

Valideringsstatus for kryptografiske moduler

Cryptographic Module Validation Program (CMVP) opprettholder valideringsstatus for kryptografiske moduler i tre separate lister, avhengig av deres gjeldende status:

- For å kunne stå på Implementation Under Test-listen til CMVP må laboratoriet ha kontrakt med Apple for å gjennomføre testing.
- Når laboratoriet har gjennomført testingen, laben har anbefalt validering til CMVP og CMVP-avgiftene er betalt, blir modulen lagt til i Modules in Process (MIP)-listen. MIP-listen sporer framgangen til CMVP-valideringen i fire faser:
  - *Gjennomgang venter:* Venter på at CMVP-ressurser skal tilordnes.
  - *Under gjennomgang:* CMVP-ressursene gjennomfører valideringen.
  - *Koordinering:* Laben og CMVP løser eventuelle problemer.
  - *Ferdigstilling:* Aktiviteter og formaliteter omkring utstedelse av sertifikatet.
- Etter CMVP-valideringen blir modulene tildelt et sertifikat for overensstemmelse og legges til i listen over validerte kryptografiske moduler. Dette inkluderer:
  - Validerte moduler som er merket som aktive.
  - Etter fem år merkes modulene som historiske.
  - Hvis modulsertifikatet trekkes tilbake, merkes de som trukket tilbake.

FIPS 140-3-sertifiseringer

Dagens status

2020-moduler for brukerplass, kjerneplass og Secure Key Store har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

2021-moduler for brukerplass, kjerneplass og Secure Key Store blir testet av laboratoriet. De ligger i Implementation Under Test-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS for macOS 12 Monterey *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS for macOS 12 Monterey *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS for macOS 12 Monterey *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (T2) *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS for macOS 11 Big Sur *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS for macOS 11 Big Sur *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS for macOS 11 Big Sur på Intel *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare *Sikkerhetsnivå:* 2

FIPS 140-2-sertifiseringer

Tabellen under viser de kryptografiske modulene som har blitt testet av laboratoriet for samsvar med FIPS 140-2.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3856 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple CoreCrypto User Module versjon 10.0 for ARM *Operativsystem:* sepOS for macOS 10.15 Catalina *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3855 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 10.0 for ARM *Operativsystem:* sepOS for macOS 10.15 Catalina *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 05.02.2021	*Sertifikater:* 3811 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 10.0 *Operativsystem:* sepOS for macOS 10.15 Catalina *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 23.04.2019	*Sertifikater:* 3438 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 9.0 for ARM *Operativsystem:* sepOS for macOS 10.14 Mojave *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 11.04.2019	*Sertifikater:* 3433 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 9.0 for ARM *Operativsystem:* sepOS for macOS 10.14 Mojave *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3523 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 9.0 *Operativsystem:* sepOS for macOS 10.14 Mojave *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikater:* 3148 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 8.0 for ARM *Operativsystem* sepOS for macOS 10.13 High Sierra *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikater:* 3147 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 8.0 for ARM *Operativsystem* sepOS for macOS 10.13 High Sierra *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 10.07.2018	*Sertifikater:* 3223 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 1.0 *Operativsystem* sepOS for macOS 10.13 High Sierra *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2016 *Valideringsdatoer:* 01.02.2017	*Sertifikater:* 2828 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple iOS Corecrypto Kernel Module versjon 7.0 *Operativsystem:* sepOS for macOS 10.12 Sierra *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2016 *Valideringsdatoer:* 01.02.2017	*Sertifikater:* 2827 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple iOS Corecrypto Kernel Module versjon 7.0 *Operativsystem:* sepOS for macOS 10.12 Sierra *Type:* Programvare *Sikkerhetsnivå:* 1

Sertifiseringer for operativsystemsikkerhet

Oversikt over Apples sertifiseringer for operativsystemsikkerhet

Apple opprettholder amerikanske FIPS 140-2/-3-sertifikater for samsvarsvalidering for sepOS og T2-firmware i tillegg til andre sertifiseringer. Apple starter med *byggesteiner for sertifisering* som gjelder på tvers av flere plattformer. Én byggestein er valideringen av corecrypto, som brukes til utrullinger av kryptografiske moduler for programvare og maskinvare i operativsystemer utviklet av Apple. En annen byggestein er sertifiseringen av Secure Enclave, som er innebygd i mange Apple-enheter. En tredje byggestein er sertifiseringen av Secure Element (SE), som finnes i Apple-enheter med Touch ID og enheter med Face ID. Disse byggesteinene for maskinvaresertifisering danner et grunnlag for bredere sertifiseringer av plattformsikkerhet.

Valideringer for kryptografiske algoritmer

Validering av korrekt implementering av mange kryptografiske algoritmer og tilhørende sikkerhetsfunksjoner er et krav for FIPS 140-3-validering, og støtter andre sertifiseringer. Valideringen håndteres av NISTs Cryptographic Algorithm Validation Program (CAVP). Valideringssertifikater for Apple-implementeringer er tilgjengelige via CAVP-søkefunksjonen.

Valideringer for kryptografiske moduler: FIPS 140-2/3 (ISO/IEC 19790)

De kryptografiske modulene i Apples operativsystemer har gjentatte ganger blitt validert av Cryptographic Module Validation Program (CMVP) i samsvar med U.S. Federal Information Processing Standards (FIPS) 140-2 etter hver hovedlansering av operativsystemer siden 2012. Etter hver hovedlansering sender Apple inn alle modulene til CMVP for full kryptografisk validering. Disse validerte modulene leverer kryptografiske operasjoner til tjenester fra Apple og er tilgjengelig for bruk av tredjepartsapper.

Apple har hvert år oppnådd **sikkerhetsnivå 1** for de programvarebaserte modulene «Corecrypto Module for Intel» og «Corecrypto Kernel Module for Intel» til macOS. For Apple-chiper gjelder modulene «CoreCrypto Module on ARM» og «CoreCrypto Kernel Module on ARM» for iOS, iPadOS, tvOS, watchOS og firmwaren i den innebygde Apple T2-sikkerhetschipen i Macer.

Apple oppnådde i 2019 første FIPS 140-2 **sikkerhetsnivå 2** for den integrerte kryptografiske programvaremodulen identifisert som «Apple Corecrypto Module: Secure Key Store», som gjorde at amerikanske myndigheter godkjente bruken av nøkler som har blitt generert og håndtert i Secure Enclave. Apple søker å oppnå valideringer for den kryptografiske maskinvaremodulen for kommende hovedversjoner av operativsystemer.

FIPS 140-3 ble godkjent av det amerikanske handelsdepartementet i 2019. Den største endringen i denne versjonen av standarden er spesifiseringen av ISO/IEC-standardene, særlig ISO/IEC 19790:2015 og den tilhørende teststandarden ISO/IEC 24759:2017. CMVP har iverksatt et overgangsprogram og har indikert at kryptografiske moduler skal valideres etter FIPS 140-3 som standard fra 2020. Apples kryptografiske moduler tar sikte på å oppfylle og gå over til FIPS 140-3-standarden så raskt det er gjennomførbart.

For kryptografiske moduler som for øyeblikket er i testing- og valideringsprosessene, opprettholder CMVP to separate lister som kan inneholde informasjon om foreslåtte valideringer. Kryptografiske moduler som er under testing med et akkreditert laboratorium, kan vises i Implementation Under Test-listen. Når laboratoriet har fullført testingen og anbefalt validering av Apples kryptografiske moduler hos CMVP, vises de i Modules in Process-listen. På dette tidspunktet er laboratorietestingen fullført og avventer validering av testingen av CMVP. Siden varigheten av evalueringsprosessen varierer, kan du sjekke begge disse prosesslistene for å se den gjeldende statusen til Apples kryptografiske moduler mellom datoen for en hovedlansering av operativsystemene og utstedelse av valideringssertifikatet fra CVMP.

Produktsertifiseringer: Common Criteria ISO/IEC 15408

Common Criteria (ISO/IEC 15408) er en standard som brukes av mange organisasjoner som et grunnlag for å utføre sikkerhetsevalueringer av IT-produkter.

Du finner informasjon om sertifiseringer som kan bli gjensidig godkjent under den internasjonale Common Criteria Recognition Arrangement (CCRA), på Common Criteria-portalen. Common Criteria-standarden kan også brukes utenfor CCRA av nasjonale og private valideringssystemer. I Europa styres gjensidig anerkjennelse gjennom SOG-IS-avtalen i tillegg til CCRA.

Målet, slik det framgår av Common Criteria-fellesskapet, er at et internasjonalt godkjent sett med sikkerhetsstandarder skal gi en tydelig og pålitelig evaluering av sikkerhetsfunksjonene til IT-produkter. Common Criteria-sertifiseringen tilbyr en uavhengig vurdering av et produkts evne til å overholde sikkerhetsstandarder, noe som gir kundene mer tillit til sikkerheten til IT-produkter og fører til mer velinformerte avgjørelser.

Gjennom CCRA har medlemslandene blitt enige om å anerkjenne sertifiseringen av IT-produkter med samme nivå av tillit. Evalueringene som kreves før sertifiseringen, er omfattende og inkluderer:

- Protection Profiles (PP-er)
- Security Targets (ST-er)
- Security Functional Requirements (SFR-er)
- Security Assurance Requirements (SAR-er)
- Evaluation Assurance Levels (EAL-er)

Protection Profiles (PP-er) er dokumenter som spesifiserer sikkerhetskrav for en klasse med enhetstyper (for eksempel mobilitet), og brukes til å sammenligne evalueringene av IT-produkter innenfor samme klasse. Medlemskap i CCRA og en økende liste med godkjente PP-er fortsetter å vokse hvert år. Takket være denne avtalen kan en produktutvikler oppnå en enkeltsertifisering under hvilken som helst av autoriseringssystemene og få den anerkjent av en av sertifiseringssignatarene.

Security Targets (ST-er) definerer *hva* som evalueres når et IT-produkt blir sertifisert. ST-ene omformes til mer spesifikke *Security Functional Requirements (SFR-er)*, som brukes til å evaluere ST-ene grundigere.

Common Criteria (CC-er) inkluderer også *Security Assurance Requirements (SAR-er)*. Vanlige parametere er *Evaluation Assurance Level (EAL-er)*. EAL-er grupperer sammen hyppige forekomster av sett med SAR-er og kan spesifiseres i PP-er og ST-er for å støtte sammenlignbarhet.

Mange eldre PP-er er arkivert og blir erstattet med målrettede PP-er som utvikles og rettes mot spesifikke løsninger og miljøer. I en felles innsats for å sikre fortsatt gjensidig anerkjennelse på tvers av alle CCRA-medlemmer har ITC (International Technical Community) blitt opprettet for utvikling og oppdateringer av *cPP-er (Collaborative Protection Profiles)*, som utvikles fra starten med medvirkning fra flere CCRA-signatursystemer. PP-er som er rettet mot brukergrupper og avtaler om gjensidig anerkjennelse, med unntak av CCRA, fortsetter å utvikles av egnede interessenter.

Apple begynte å søke om å oppnå sertifiseringer under den oppdaterte CCRA-en med utvalgte cPP-er tidlig i 2015. Siden da har Apple oppnådd Common Criteria-sertifiseringer for hver hovedlansering av iOS og har utvidet dekningen til å inkludere sikkerhetsforsikring gitt av nye PP-er.

Apple tar en aktiv rolle i de tekniske miljøene som fokuserer på å evaluere teknologi for mobilsikkerhet. Disse inkluderer ITC-er som er ansvarlige for å utvikle og oppdatere cPP-er. Apple fortsetter å evaluere og oppnå sertifiseringer mot gjeldende PP-er og cPP-er.

Apples plattformsertifiseringer for det nordamerikanske markedet utføres vanligvis med National Information Assurance Partnership (NIAP), som opprettholder en liste over prosjekter som er under evaluering, men som ikke er sertifisert ennå.

I tillegg til de oppførte generelle plattformsertifikatene er det utstedt andre sertifikater for å demonstrere spesifikke sikkerhetskrav for enkelte markeder.

Sikkerhetssertifiseringer for iOS

Bakgrunn for iOS-sertifisering

Apple tar aktivt del i valideringen av innebygde Apple-moduler for programvare og maskinvare for hver store lansering av et operativsystem. Validering av overensstemmelse kan bare gjøres med en ferdigstilt, lansert versjon.

Valideringsstatus for kryptografiske moduler i iOS

Cryptographic Module Validation Program (CMVP) opprettholder valideringsstatus for kryptografiske moduler i tre separate lister, avhengig av deres gjeldende status:

- For å kunne stå på Implementation Under Test-listen til CMVP må laboratoriet ha kontrakt med Apple for å gjennomføre testing.
- Når laboratoriet har gjennomført testingen, laben har anbefalt validering til CMVP og CMVP-avgiftene er betalt, blir modulen lagt til i Modules in Process (MIP)-listen. MIP-listen sporer framgangen til CMVP-valideringen i fire faser:
  - *Gjennomgang venter:* Venter på at CMVP-ressurser skal tilordnes.
  - *Under gjennomgang:* CMVP-ressursene gjennomfører valideringen.
  - *Koordinering:* Laben og CMVP løser eventuelle problemer.
  - *Ferdigstilling:* Aktiviteter og formaliteter omkring utstedelse av sertifikatet.
- Etter CMVP-valideringen blir modulene tildelt et sertifikat for overensstemmelse og legges til i listen over validerte kryptografiske moduler. Dette inkluderer:
  - Validerte moduler som er merket som aktive.
  - Etter fem år merkes modulene som historiske.
  - Hvis modulsertifikatet trekkes tilbake, merkes de som trukket tilbake.

I 2020 tok CMVP i bruk den internasjonale standarden ISO/IEC 19790 som grunnlag for FIPS 140-3.

FIPS 140-3-sertifiseringer

Dagens status

Brukerplass, kjerneplass og Secure Key Store i iOS 14 (2020) har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

Brukerplass, kjerneplass og Secure Key Store i iOS 15 (2021) blir testet av laboratoriet. De ligger i Implementation Under Test-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* iOS 15 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* iOS 15 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med iOS 15 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9-A14) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med iOS 15 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A13, A14, A15) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* iOS 14 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* iOS 14 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med iOS 14 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9-A14) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med iOS 14 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A13-A14) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3

FIPS 140-2-sertifiseringer

Tabellen under viser de kryptografiske modulene som nå blir testet og har blitt testet av laboratoriet for samsvar med FIPS 140-2.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3856 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple CoreCrypto User Module versjon 10.0 for ARM *Operativsystem:* iOS 13 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3855 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 10.0 for ARM *Operativsystem:* iOS 13 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 05.02.2021	*Sertifikater:* 3811 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 10.0 *Operativsystem:* sepOS distribuert med iOS 13 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 23.04.2019	*Sertifikater:* 3438 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 9.0 for ARM *Operativsystem:* iOS 12 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 11.04.2019	*Sertifikater:* 3433 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 9.0 for ARM *Operativsystem:* iOS 12 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3523 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 9.0 *Operativsystem:* sepOS distribuert med iOS 12 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikater:* 3148 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 8.0 for ARM *Operativsystem:* iOS 11 *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikater:* 3147 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 8.0 for ARM *Operativsystem:* iOS 11 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3223 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 1.0 *Operativsystem:* sepOS distribuert med iOS 11 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2016 *Valideringsdatoer:* 01.02.2017	*Sertifikater:* 2828 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple iOS Corecrypto Kernel Module versjon 7.0 *Operativsystem:* iOS 10 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2016 *Valideringsdatoer:* 01.02.2017	*Sertifikater:* 2827 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple iOS Corecrypto Kernel Module versjon 7.0 *Operativsystem:* iOS 10 *Type:* Programvare *Sikkerhetsnivå:* 1

Tidligere versjoner

Sertifiseringer som er eldre enn fem år, har fått historisk status av CMVP. Disse tidligere iOS-versjonene hadde valideringer for de kryptografiske modulene:

- iOS 9 (corecrypto-moduler versjon 6.0)
- iOS 8 (corecrypto-moduler versjon 5.0)
- iOS 7 (corecrypto-moduler versjon 4.0)
- iOS 6 (corecrypto-moduler versjon 3.0)

Sertifiseringsbakgrunn for Common Criteria (CC)

Apple tar aktivt del i evalueringen av iOS for hver store lansering av operativsystemet. Evalueringen kan kun gjennomføres på en endelig versjon av operativsystemet. Før iPadOS 13.1 ble iPadOS kalt iOS.

Sertifiseringsstatus for Common Criteria (CC)

Det amerikanske systemet, som drives av NIAP, opprettholder en liste over produkter under evaluering. Denne listen inkluderer produkter som evalueres i USA hos et NIAP-godkjent Common Criteria-testlaboratorium (CCTL), og som har gjennomført et Evaluation Kickoff Meeting (eller liknende), hvor CCEVS-administrasjonen offisielt har akseptert produktet for evaluering.

Etter at produktene har blitt sertifisert, legger NIAP inn gyldige sertifiseringer i listen over overensstemmende produkter. Etter to år blir disse sertifiseringene gjennomgått for overensstemmelse med det gjeldende regelsettet for sikkerhetsvedlikehold. Etter at datoen for regelsettet for sikkerhetsvedlikehold har utløpt, flytter NIAP sertifiseringslisten til listen over arkiverte produkter.

Common Criteria-portalen lister opp sertifiseringer som kan gjensidig anerkjennes under Common Criteria Recognition Arrangement (CCRA). CC-portalen kan beholde produkter på listen over sertifiserte produkter i fem år, og informasjonen ligger i CC-portalen for arkiverte sertifiseringer.

Tabellen under viser sertifiseringer som er under evaluering i en lab, eller som har blitt sertifisert til å være i samsvar med CC.

Dagens status

Laboratorietesting med NIAP for iOS 15 er i gang. Se produkter under evaluering (NIAP) og listen over samsvarende produkter for oppdatert informasjon.

Operativsystem/ sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: iOS 15 *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* –	*Tittel:* Apple iOS 15: iPhoner *Protection Profiles (PP-er):* Grunnleggende om mobilenheter (PP-moduler bekreftes senere)
Operativsystem: iOS 14 *Sertifiseringsdato:* 01.09.2021	*System-ID:* 11146 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple iOS 14: iPhoner *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, VPN-klientmodul, WLAN-klienter PP-modul, MDM-agent EP
Operativsystem: iOS 13 *Sertifiseringsdato:* 06.11.2020	*System-ID:* 11036 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple iOS 13 på iPhone *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, VPN-klientmodul, WLAN-klienter EP, MDM-agent EP

Arkiverte CC-sertifiseringer for iOS

Disse tidligere iOS-versjonene hadde Common Criteria-valideringer. De er arkivert av NIAP ifølge NIAPs regler:

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: iOS 12 *Sertifiseringsdato:* 14.03.2019	*System-ID:* 10937 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iPhone med iOS 12 *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, VPN-klientmodul, Trådløs-LAN-klient EP, MDM-agent EP
Operativsystem: iOS 11 *Sertifiseringsdato:* 17.07.2018	*System-ID:* 10851 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* Apple iOS 11 *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, Trådløs-LAN-klient EP, MDM-agent EP
Operativsystem: iOS 10 *Sertifiseringsdato:* 27.07.2017	*System-ID:* 10782 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iOS 10.2 på iPhone og iPad *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, Trådløs-LAN-klient EP, MDM-agent EP
Operativsystem: iOS 10 *Sertifiseringsdato:* 27.07.2017	*System-ID:* 10792 *Dokumenter:* Sikkerhetsmål, Veiledning	*Tittel:* iOS 10.2 VPN-klient på iPhone og iPad *Protection Profiles (PP-er):* VPN Client PP
Operativsystem: iOS 9 *Sertifiseringsdato:* 14.10.2016	*System-ID:* 10725 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iOS 9.3.2 med MDM-agent *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, MDM-agent EP
Operativsystem: iOS 9 *Sertifiseringsdato:* 13.10.2016	*System-ID:* 10714 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* OS VPN-klient på iPhone og iPad *Protection Profiles (PP-er):* VPN Client PP
Operativsystem: iOS 9 *Sertifiseringsdato:* 28.01.2016	*System-ID:* 10695 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iOS 9 *Protection Profiles (PP-er):* Grunnleggende om mobilenheter

Sikkerhetssertifiseringer for iPadOS

Bakgrunn for iPadOS-sertifisering

Apple tar aktivt del i valideringen av Apples operativsystemer for hver store lansering av et operativsystem gjennom å bruke egnede Protection Profiles (PP-er) og FIPS 140-3-sikkerhetsnivåer. Validering av overensstemmelse kan bare gjøres med en ferdigstilt, lansert versjon.

Merk: I 2019 ble operativsystemet for iPad-enheter omdøpt til iPadOS. Før iPadOS 13.1 ble iPadOS kalt iOS.

Valideringsstatus for kryptografiske moduler i iPadOS

Cryptographic Module Validation Program (CMVP) opprettholder valideringsstatus for kryptografiske moduler i tre separate lister, avhengig av deres gjeldende status:

- For å kunne stå på Implementation Under Test-listen til CMVP må laboratoriet ha kontrakt med Apple for å gjennomføre testing.
- Når laboratoriet har gjennomført testingen, laben har anbefalt validering til CMVP og CMVP-avgiftene er betalt, blir modulen lagt til i Modules in Process (MIP)-listen. MIP-listen sporer framgangen til CMVP-valideringen i fire faser:
  - *Gjennomgang venter:* Venter på at CMVP-ressurser skal tilordnes.
  - *Under gjennomgang:* CMVP-ressursene gjennomfører valideringen.
  - *Koordinering:* Laben og CMVP løser eventuelle problemer.
  - *Ferdigstilling:* Aktiviteter og formaliteter omkring utstedelse av sertifikatet.
- Etter CMVP-valideringen blir modulene tildelt et sertifikat for overensstemmelse og legges til i listen over validerte kryptografiske moduler. Dette inkluderer:
  - Validerte moduler som er merket som aktive.
  - Etter fem år merkes modulene som historiske.
  - Hvis modulsertifikatet trekkes tilbake, merkes de som trukket tilbake.

I 2020 tok CMVP i bruk den internasjonale standarden ISO/IEC 19790 som grunnlag for FIPS 140-3.

FIPS 140-3-sertifiseringer

Dagens status

Brukerplass, kjerneplass og Secure Key Store i iPadOS 14 (2020) har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

Brukerplass, kjerneplass og Secure Key Store i iOS 15 (2021) blir testet av laboratoriet. De ligger i Implementation Under Test-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* iPadOS 15 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* iPadOS 15 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med iPadOS 15 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9–A14, M1) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med iPadOS 15 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9–A14, M1) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* iPadOS 14 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* iPadOS 14 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med iPadOS 14 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9–A14, M1) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med iPadOS 14 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A9–A14, M1) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3

FIPS 140-2-sertifiseringer

Tabellen under viser de kryptografiske modulene som nå blir testet og har blitt testet av laboratoriet for samsvar med FIPS 140-2.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3856 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple CoreCrypto User Module versjon 10.0 for ARM *Operativsystem:* iPadOS 13 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3855 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 10.0 for ARM *Operativsystem:* iPadOS 13 *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 05.02.2021	*Sertifikater:* 3811 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 10.0 *Operativsystem:* sepOS distribuert med iPadOS 13 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 23.04.2019	*Sertifikater:* 3438 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 9.0 for ARM *Operativsystem:* iOS 12 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 11.04.2019	*Sertifikater:* 3433 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 9.0 for ARM *Operativsystem:* iOS 12 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3523 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 9.0 *Operativsystem:* sepOS distribuert med iOS 12 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikater:* 3148 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 8.0 for ARM *Operativsystem:* iOS 11 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikater:* 3147 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 8.0 for ARM *Operativsystem:* iOS 11 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3223 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 1.0 *Operativsystem:* sepOS distribuert med iOS 11 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2016 *Valideringsdatoer:* 01.02.2017	*Sertifikater:* 2828 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple iOS Corecrypto Kernel Module versjon 7.0 *Operativsystem:* iOS 10 *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2016 *Valideringsdatoer:* 01.02.2017	*Sertifikater:* 2827 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple iOS Corecrypto Kernel Module versjon 7.0 *Operativsystem:* iOS 10 *Type:* Programvare *Sikkerhetsnivå:* 1

Tidligere versjoner

Sertifiseringer som er eldre enn fem år, har fått historisk status av CMVP. Disse tidligere iOS-versjonene hadde valideringer for de kryptografiske modulene:

- iOS 9 (corecrypto-moduler versjon 6.0)
- iOS 8 (corecrypto-moduler versjon 5.0)
- iOS 7 (corecrypto-moduler versjon 4.0)
- iOS 6 (corecrypto-moduler versjon 3.0)

Sertifiseringsbakgrunn for Common Criteria (CC)

Apple tar aktivt del i evalueringen av iPadOS for hver store lansering av operativsystemet. Evalueringen kan kun gjennomføres på en endelig versjon av operativsystemet.

Sertifiseringsstatus for Common Criteria (CC)

Det amerikanske systemet, som drives av NIAP, opprettholder en liste over produkter under evaluering. Denne listen inkluderer produkter som evalueres i USA hos et NIAP-godkjent Common Criteria-testlaboratorium (CCTL), og som har gjennomført et Evaluation Kickoff Meeting (eller liknende), hvor CCEVS-administrasjonen offisielt har akseptert produktet for evaluering.

Etter at produktene har blitt sertifisert, legger NIAP inn gyldige sertifiseringer i listen over overensstemmende produkter. Etter to år blir disse sertifiseringene gjennomgått for overensstemmelse med det gjeldende regelsettet for sikkerhetsvedlikehold. Etter at datoen for regelsettet for sikkerhetsvedlikehold har utløpt, flytter NIAP sertifiseringslisten til listen over arkiverte produkter.

Common Criteria-portalen lister opp sertifiseringer som kan gjensidig anerkjennes under Common Criteria Recognition Arrangement (CCRA). CC-portalen kan beholde produkter på listen over sertifiserte produkter i fem år, og informasjonen ligger i CC-portalen for arkiverte sertifiseringer.

Tabellen under viser sertifiseringer som er under evaluering i en lab, eller som har blitt sertifisert til å være i samsvar med CC.

Dagens status

Laboratorietesting med NIAP for iPadOS 15 er i gang. Se produkter under evaluering (NIAP) og listen over samsvarende produkter for oppdatert informasjon.

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: iPadOS 15 *Sertifiseringsdato:* 14.03.2019	*System-ID:* – *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* iPad med iOS 12 *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, VPN-klientmodul, Trådløs-LAN-klient EP, MDM-agent EP
Operativsystem: iPadOS 14 *Sertifiseringsdato:* 01.09.2021	*System-ID:* 11147 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple iPadOS 14: iPader *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, VPN-klientmodul, Trådløs-LAN-klient EP, MDM-agent EP
Operativsystem: iPadOS 13 *Sertifiseringsdato:* 06.11.2020	*System-ID:* 11036 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* iPadOS 13 på den mobile enheten iPad *Protection Profiles (PP-er):* Grunnleggende om mobilenheter, VPN-klientmodul, Trådløs-LAN-klient EP, MDM-agent EP

Tidligere versjoner

Disse tidligere iOS-versjonene hadde Common Criteria-valideringer. De er arkivert av NIAP ifølge NIAPs regler:

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

Sikkerhetssertifiseringer for macOS

Bakgrunn for macOS-sertifisering

Apple tar aktivt del i valideringen av Apples operativsystemer for hver store lansering av et operativsystem gjennom å bruke egnede Protection Profiles (PP-er) og FIPS 140-3-sikkerhetsnivåer. Validering av overensstemmelse kan bare gjøres med en ferdigstilt, lansert versjon.

Valideringsstatus for kryptografiske moduler i macOS

Cryptographic Module Validation Program (CMVP) opprettholder valideringsstatus for kryptografiske moduler i tre separate lister, avhengig av deres gjeldende status:

- For å kunne stå på Implementation Under Test-listen til CMVP må laboratoriet ha kontrakt med Apple for å gjennomføre testing.
- Når laboratoriet har gjennomført testingen, laben har anbefalt validering til CMVP og CMVP-avgiftene er betalt, blir modulen lagt til i Modules in Process (MIP)-listen. MIP-listen sporer framgangen til CMVP-valideringen i fire faser:
  - *Gjennomgang venter:* Venter på at CMVP-ressurser skal tilordnes.
  - *Under gjennomgang:* CMVP-ressursene gjennomfører valideringen.
  - *Koordinering:* Laben og CMVP løser eventuelle problemer.
  - *Ferdigstilling:* Aktiviteter og formaliteter omkring utstedelse av sertifikatet.
- Etter CMVP-valideringen blir modulene tildelt et sertifikat for overensstemmelse og legges til i listen over validerte kryptografiske moduler. Dette inkluderer:
  - Validerte moduler som er merket som aktive.
  - Etter fem år merkes modulene som historiske.
  - Hvis modulsertifikatet trekkes tilbake, merkes de som trukket tilbake.

I 2020 tok CMVP i bruk den internasjonale standarden ISO/IEC 19790 som grunnlag for FIPS 140-3.

For Macer fra Apple viser tabellen nedenfor hvilke kryptografiske moduler som gjelder for hvilken Mac-teknologi.

Kryptografisk modul	Macer med Apple-chip	Macer med Apple T2-sikkerhetschipen	Intel-baserte Macer uten Apple T2-sikkerhetschipen
Apple-chip, brukerplass	✓		
Apple-chip, kjerne	✓		
Intel, brukerplass		✓	✓
Intel, kjerne		✓	✓
Secure Key Store	✓	✓	

FIPS 140-3-sertifiseringer

I 2020 lanserte Apple Macer med Apple-chiper. Brukbarheten av kryptografiske moduler for Macer med enten Apple-chip eller Intel-chip vises i kolonnen Modulinformasjon i tabellen under.

Merk: Apple T2-sikkerhetschiper er inkludert på mange Intel-baserte Macer. Hvis du vil ha mer informasjon om sertifiseringer for T2-chipen, kan du se Sikkerhetssertifiseringer for Apple T2-sikkerhetschip.

ssh-klient i macOS

OpenSSH kan konfigureres til å bruke FIPS 140-3-validerte moduler for utvalgte FIPS 140-3-algoritmer. Organisasjoner kan bruke en signert og notarisert installerer som er tilgjengelig fra Apple med passordet *FIPS140Mode*. Installereren legger til to filer på Macen:

- *fips_ssh_config:* Legges i /private/etc/ssh/ssh_config.d/
- *fips_sshd_config:* Legges i /private/etc/ssh/sshd_config.d/

macOS bruker disse filene for å sikre at kun kodenøkler validert av NIST er tilgjengelige for OpenSSH, og at OpenSSH-klienten bruker platformens validerte kryptografiske modul. Administratorer kan også opprette egne filer. Du finner mer informasjon på `apple_ssh_and_fips`-man-siden i macOS 12.0.1 og nyere.

Dagens status

Brukerplass, kjerneplass og Secure Key Store i macOS 11 Big Sur har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

Brukerplass, kjerneplass og Secure Key Store i macOS 12 Monterey blir testet av laboratoriet. De ligger i Implementation Under Test-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* macOS 12 Monterey på Apple-chiper *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* macOS 12 Monterey på Apple-chiper *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* macOS 12 Monterey på Intel-chiper *Miljø:* Intel, bruker, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* macOS 12 Monterey på Intel-chiper *Miljø:* Intel, kjerne, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med macOS 12 Monterey på Apple-chiper, sepOS distribuert med macOS 12 Monterey på Intel-chiper med T2 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (M1 og T2) *Sikkerhetsnivå:* 2

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med macOS 12 Monterey på Apple-chiper *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (M1) *Sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* macOS 11 Big Sur på Intel-chiper *Miljø:* Intel, bruker, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* macOS 11 Big Sur på Intel-chiper *Miljø:* Intel, kjerne, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* macOS 11 Big Sur på Apple-chiper *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* macOS 11 Big Sur på Apple-chiper *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med macOS 11 Big Sur på Apple-chiper, sepOS distribuert med macOS 11 Big Sur på Intel-chiper *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (M1) *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med macOS 11 Big Sur på Apple-chiper *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (M1) *Sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3

FIPS 140-2-sertifiseringer

Tabellen under viser de kryptografiske modulene som nå blir testet og har blitt testet av laboratoriet for samsvar med FIPS 140-2.

Brukerplass, kjerneplass og Secure Key Store i macOS 10.15 Catalina har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

Merk: Apple T2-sikkerhetschiper er inkludert på mange Intel-baserte Macer. Hvis du vil ha mer informasjon om sertifiseringer for T2-chipen, kan du se Sikkerhetssertifiseringer for Apple T2-sikkerhetschip.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 24.03.2021	*Sertifikater:* 3859 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto-brukerplassmodul for Intel-chiper (ccv10) *Operativsystem:* macOS 10.15 Catalina *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 24.03.2021	*Sertifikater:* 3858 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 10.0 for Intel (ccv10) *Operativsystem:* macOS 10.15 Catalina *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 12.04.2019	*Sertifikater:* 3402 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 9.0 for Intel *Operativsystem:* macOS 10.14 Mojave *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 12.04.2019	*Sertifikater:* 3431 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 9.0 for Intel *Operativsystem:* macOS 10.14 Mojave *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 22.03.2018	*Sertifikater:* 3155 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 8.0 for Intel *Operativsystem:* macOS 10.13 High Sierra *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 22.03.2018	*Sertifikater:* 3156 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 8.0 for Intel *Operativsystem:* macOS 10.13 High Sierra *Type:* Programvare *Sikkerhetsnivå:* 1

Tidligere versjoner

Disse tidligere OS X- og macOS-versjonene hadde valideringer for de kryptografiske modulene. De som er eldre enn fem år, har fått historisk status av CMVP:

- 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

Sertifiseringsbakgrunn for Common Criteria (CC)

Apple tar aktivt del i evalueringen av macOS for hver store lansering av et operativsystem. Evalueringen kan kun gjennomføres på en endelig versjon av operativsystemet.

Sertifiseringsstatus for Common Criteria (CC)

Det amerikanske systemet, som drives av NIAP, opprettholder en liste over produkter under evaluering. Denne listen inkluderer produkter som evalueres i USA hos et NIAP-godkjent Common Criteria-testlaboratorium (CCTL), og som har gjennomført et Evaluation Kickoff Meeting (eller liknende), hvor CCEVS-administrasjonen offisielt har akseptert produktet for evaluering.

Etter at produktene har blitt sertifisert, legger NIAP inn gyldige sertifiseringer i listen over overensstemmende produkter. Etter to år blir disse sertifiseringene gjennomgått for overensstemmelse med det gjeldende regelsettet for sikkerhetsvedlikehold. Etter at datoen for regelsettet for sikkerhetsvedlikehold har utløpt, flytter NIAP sertifiseringslisten til listen over arkiverte produkter.

Common Criteria-portalen lister opp sertifiseringer som kan gjensidig anerkjennes under Common Criteria Recognition Arrangement (CCRA). CC-portalen kan beholde produkter på listen over sertifiserte produkter i fem år, og informasjonen ligger i CC-portalen for arkiverte sertifiseringer.

Tabellen under viser sertifiseringer som er under evaluering i en lab, eller som har blitt sertifisert til å være i samsvar med CC.

Dagens status

Evalueringer med NIAP for macOS 11 og macOS 12 som bruker General Purpose Operating System og PP-er for Full Disk Encryption (FDE) (AA og EE), er på vei.

Se produkter under evaluering (NIAP) og listen over samsvarende produkter for oppdatert informasjon.

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: macOS 12 Monterey *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* –	*Tittel:* Apple FileVault 2 med macOS 12 Monterey *Protection Profiles (PP-er):* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP-er må bekreftes)
Operativsystem: macOS 12 Monterey *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* –	*Tittel:* macOS 12 Monterey *Protection Profiles (PP-er):* PP_OS_V4.21 (PP-er må bekreftes)
Operativsystem: macOS 11 Big Sur *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple FileVault 2 med macOS 11 Big Sur *Protection Profiles (PP-er):* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: macOS 11 Big Sur *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple macOS 11 Big Sur *Protection Profiles (PP-er):* PP_OS_V4.21
Operativsystem: macOS 10.15 Catalina *Sertifiseringsdato:* 29.04.2021	*System-ID:* 11078 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple FileVault 2 på T2-datamaskiner med macOS 10.15 Catalina *Protection Profiles (PP-er):* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Operativsystem: macOS 10.15 Catalina *Sertifiseringsdato:* 23.09.2020	*System-ID:* 11077 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* macOS 10.15 Catalina *Protection Profiles (PP-er):* PP_OS_V4.21

Sikkerhetssertifiseringer for tvOS

Bakgrunn for tvOS-sertifisering

Apple tar aktivt del i evalueringen av kryptografiske moduler for hver store lansering av tvOS. Validering av overensstemmelse kan bare gjøres med en ferdigstilt, lansert versjon.

Valideringsstatus for kryptografiske moduler i tvOS

Cryptographic Module Validation Program (CMVP) opprettholder valideringsstatus for kryptografiske moduler i tre separate lister, avhengig av deres gjeldende status:

- For å kunne stå på Implementation Under Test-listen til CMVP må laboratoriet ha kontrakt med Apple for å gjennomføre testing.
- Når laboratoriet har gjennomført testingen, laben har anbefalt validering til CMVP og CMVP-avgiftene er betalt, blir modulen lagt til i Modules in Process (MIP)-listen. MIP-listen sporer framgangen til CMVP-valideringen i fire faser:
  - *Gjennomgang venter:* Venter på at CMVP-ressurser skal tilordnes.
  - *Under gjennomgang:* CMVP-ressursene gjennomfører valideringen.
  - *Koordinering:* Laben og CMVP løser eventuelle problemer.
  - *Ferdigstilling:* Aktiviteter og formaliteter omkring utstedelse av sertifikatet.
- Etter CMVP-valideringen blir modulene tildelt et sertifikat for overensstemmelse og legges til i listen over validerte kryptografiske moduler. Dette inkluderer:
  - Validerte moduler som er merket som aktive.
  - Etter fem år merkes modulene som historiske.
  - Hvis modulsertifikatet trekkes tilbake, merkes de som trukket tilbake.

I 2020 tok CMVP i bruk den internasjonale standarden ISO/IEC 19790 som grunnlag for FIPS 140-3.

FIPS 140-3-sertifiseringer

Dagens status

Brukerplass, kjerneplass og Secure Key Store i tvOS 14 (2020) har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

Brukerplass, kjerneplass og Secure Key Store i tvOS 15 (2021) blir testet av laboratoriet. De ligger i Implementation Under Test-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* tvOS 15 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* tvOS 15 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med tvOS 15 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A10, A12) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* tvOS 14 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* tvOS 14 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med tvOS 14 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (A10, A12) *Generelt sikkerhetsnivå:* 2

FIPS 140-2-sertifiseringer

Tabellen under viser de kryptografiske modulene som nå blir testet og har blitt testet av laboratoriet for samsvar med FIPS 140-2.

Brukerplass, kjerneplass og Secure Key Store i tvOS 13 (2019) har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3856 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple CoreCrypto User Module versjon 10.0 for ARM *Operativsystem:* tvOS 13 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 23.03.2021	*Sertifikater:* 3855 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 10.0 for ARM *Operativsystem:* tvOS 13 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 05.02.2021	*Sertifikater:* 3811 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 10.0 *Operativsystem:* sepOS distribuert med tvOS 13 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 23.04.2019	*Sertifikater:* 3438 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 9.0 for ARM *Operativsystem:* tvOS 12 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 11.04.2019	*Sertifikater:* 3433 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 9.0 for ARM *Operativsystem:* tvOS 12 *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3523 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 9.0 *Operativsystem:* sepOS distribuert med tvOS 12 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikater:* 3148 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 8.0 for ARM *Operativsystem:* tvOS 11 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikater:* 3147 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 8.0 for ARM *Operativsystem:* tvOS 11 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3223 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 1.0 *Operativsystem:* sepOS distribuert med tvOS 11 *Type:* Maskinvare *Sikkerhetsnivå:* 2

Sikkerhetssertifiseringer for watchOS

Bakgrunn for watchOS-sertifisering

Apple tar aktivt del i evalueringen av kryptografiske moduler for hver store lansering av watchOS. Validering av overensstemmelse kan bare gjøres med en ferdigstilt, lansert versjon.

Valideringsstatus for kryptografiske moduler i watchOS

Cryptographic Module Validation Program (CMVP) opprettholder valideringsstatus for kryptografiske moduler i tre separate lister, avhengig av deres gjeldende status:

- For å kunne stå på Implementation Under Test-listen til CMVP må laboratoriet ha kontrakt med Apple for å gjennomføre testing.
- Når laboratoriet har gjennomført testingen, laben har anbefalt validering til CMVP og CMVP-avgiftene er betalt, blir modulen lagt til i Modules in Process (MIP)-listen. MIP-listen sporer framgangen til CMVP-valideringen i fire faser:
  - *Gjennomgang venter:* Venter på at CMVP-ressurser skal tilordnes.
  - *Under gjennomgang:* CMVP-ressursene gjennomfører valideringen.
  - *Koordinering:* Laben og CMVP løser eventuelle problemer.
  - *Ferdigstilling:* Aktiviteter og formaliteter omkring utstedelse av sertifikatet.
- Etter CMVP-valideringen blir modulene tildelt et sertifikat for overensstemmelse og legges til i listen over validerte kryptografiske moduler. Dette inkluderer:
  - Validerte moduler som er merket som aktive.
  - Etter fem år merkes modulene som historiske.
  - Hvis modulsertifikatet trekkes tilbake, merkes de som trukket tilbake.

I 2020 tok CMVP i bruk den internasjonale standarden ISO/IEC 19790 som grunnlag for FIPS 140-3.

FIPS 140-3-sertifiseringer

Dagens status

Brukerplass, kjerneplass og Secure Key Store i watchOS 7 (2020) har blitt testet av laboratoriet og blitt anbefalt til CMVP for validering. De ligger i Modules in Process-listen.

Brukerplass, kjerneplass og Secure Key Store i watchOS 8 (2021) blir testet av laboratoriet. De ligger i Implementation Under Test-listen.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* watchOS 8 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* watchOS 8 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med watchOS 8 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (S3, S4, S5, S6) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2021 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 12 *Operativsystem:* sepOS distribuert med watchOS 8 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (S6) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* watchOS 7 *Miljø:* Apple-chip, bruker, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* watchOS 7 *Miljø:* Apple-chip, kjerne, programvare *Type:* Programvare *Generelt sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med watchOS 7 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (S3, S4, S5, S6) *Generelt sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2020 *Valideringsdatoer:* –	*Sertifikater:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Module versjon 11.1 *Operativsystem:* sepOS distribuert med watchOS 7 *Miljø:* Apple-chip, Secure Key Store, maskinvare *Type:* Maskinvare (S6) *Generelt sikkerhetsnivå:* 2 *Fysisk sikkerhetsnivå:* 3

FIPS 140-2-sertifiseringer

Tabellen under viser de kryptografiske modulene som nå blir testet og har blitt testet av laboratoriet for samsvar med FIPS 140-2.

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* –	*Sertifikater:* 3856 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple CoreCrypto User Module versjon 10.0 for ARM *Operativsystem:* watchOS 6 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* –	*Sertifikater:* 3855 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 10.0 for ARM *Operativsystem:* watchOS 6 *Type:* Programvare *Sikkerhetsnivå:* 1

Datoer	Sertifikater/dokumenter	Modulinformasjon
Lanseringsdato for operativsystem: 2019 *Valideringsdatoer:* 05.02.2021	*Sertifikater:* 3811 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 10.0 *Operativsystem:* sepOS distribuert med watchOS 6 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 23.04.2019	*Sertifikater:* 3438 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 9.0 for ARM *Operativsystem:* watchOS 5 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 11.04.2019	*Sertifikater:* 3433 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 9.0 for ARM *Operativsystem:* watchOS 5 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2018 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3523 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 9.0 *Operativsystem:* sepOS distribuert med watchOS 5 *Type:* Maskinvare *Sikkerhetsnivå:* 2
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikater:* 3148 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto User Module versjon 8.0 for ARM *Operativsystem:* watchOS 4 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikater:* 3147 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Corecrypto Kernel Module versjon 8.0 for ARM *Operativsystem:* watchOS 4 *Type:* Programvare *Sikkerhetsnivå:* 1
Lanseringsdato for operativsystem: 2017 *Valideringsdatoer:* 10.09.2019	*Sertifikater:* 3223 *Dokumenter:* Sertifisering Sikkerhetsregelsett Crypto Offer-veiledning	*Tittel:* Apple Secure Key Store Cryptographic Module versjon 1.0 *Operativsystem:* sepOS distribuert med watchOS 4 *Type:* Maskinvare *Sikkerhetsnivå:* 2

Sertifiseringer for programvaresikkerhet

Oversikt over Apples sertifiseringer for programvaresikkerhet

Apple opprettholder amerikanske FIPS 140-2/-3-sertifikater for samsvarsvalidering for sepOS og T2-firmware i tillegg til andre sertifiseringer. Apple starter med *byggesteiner for sertifisering* som gjelder på tvers av flere plattformer. Én byggestein er valideringen av corecrypto, som brukes til utrullinger av kryptografiske moduler for programvare og maskinvare i operativsystemer utviklet av Apple. En annen byggestein er sertifiseringen av Secure Enclave, som er innebygd i mange Apple-enheter. En tredje byggestein er sertifiseringen av Secure Element (SE), som finnes i Apple-enheter med Touch ID og enheter med Face ID. Disse byggesteinene for maskinvaresertifisering danner et grunnlag for bredere sertifiseringer av plattformsikkerhet.

Produktsertifiseringer: Common Criteria ISO/IEC 15408

Common Criteria (ISO/IEC 15408) er en standard som brukes av mange organisasjoner som et grunnlag for å utføre sikkerhetsevalueringer av IT-produkter.

Du finner informasjon om sertifiseringer som kan bli gjensidig godkjent under den internasjonale Common Criteria Recognition Arrangement (CCRA), på Common Criteria-portalen. Common Criteria-standarden kan også brukes utenfor CCRA av nasjonale og private valideringssystemer. I Europa styres gjensidig anerkjennelse gjennom SOG-IS-avtalen i tillegg til CCRA.

Målet, slik det framgår av Common Criteria-fellesskapet, er at et internasjonalt godkjent sett med sikkerhetsstandarder skal gi en tydelig og pålitelig evaluering av sikkerhetsfunksjonene til IT-produkter. Common Criteria-sertifiseringen tilbyr en uavhengig vurdering av et produkts evne til å overholde sikkerhetsstandarder, noe som gir kundene mer tillit til sikkerheten til IT-produkter og fører til mer velinformerte avgjørelser.

Gjennom CCRA har medlemslandene blitt enige om å anerkjenne sertifiseringen av IT-produkter med samme nivå av tillit. Evalueringene som kreves før sertifiseringen, er omfattende og inkluderer:

- Protection Profiles (PP-er)
- Security Targets (ST-er)
- Security Functional Requirements (SFR-er)
- Security Assurance Requirements (SAR-er)
- Evaluation Assurance Levels (EAL-er)

Protection Profiles (PP-er) er dokumenter som spesifiserer sikkerhetskrav for en klasse med enhetstyper (for eksempel mobilitet), og brukes til å sammenligne evalueringene av IT-produkter innenfor samme klasse. Medlemskap i CCRA og en økende liste med godkjente PP-er fortsetter å vokse hvert år. Takket være denne avtalen kan en produktutvikler oppnå en enkeltsertifisering under hvilken som helst av autoriseringssystemene og få den anerkjent av en av sertifiseringssignatarene.

Security Targets (ST-er) definerer *hva* som evalueres når et IT-produkt blir sertifisert. ST-ene omformes til mer spesifikke *Security Functional Requirements (SFR-er)*, som brukes til å evaluere ST-ene grundigere.

Common Criteria (CC-er) inkluderer også *Security Assurance Requirements (SAR-er)*. Vanlige parametere er *Evaluation Assurance Level (EAL-er)*. EAL-er grupperer sammen hyppige forekomster av sett med SAR-er og kan spesifiseres i PP-er og ST-er for å støtte sammenlignbarhet.

Mange eldre PP-er er arkivert og blir erstattet med målrettede PP-er som utvikles og rettes mot spesifikke løsninger og miljøer. I en felles innsats for å sikre fortsatt gjensidig anerkjennelse på tvers av alle CCRA-medlemmer har ITC (International Technical Community) blitt opprettet for utvikling og oppdateringer av cPP-er (Collaborative Protection Profiles), som utvikles fra starten med medvirkning fra flere CCRA-signatursystemer. PP-er som er rettet mot brukergrupper og avtaler om gjensidig anerkjennelse, med unntak av CCRA, fortsetter å utvikles av egnede interessenter.

Apple begynte å søke om å oppnå sertifiseringer under den oppdaterte CCRA-en med utvalgte cPP-er tidlig i 2015. Siden da har Apple oppnådd Common Criteria-sertifiseringer for hver hovedlansering av iOS og har utvidet dekningen til å inkludere sikkerhetsforsikring gitt av nye PP-er.

Apple tar en aktiv rolle i de tekniske miljøene som fokuserer på å evaluere teknologi for mobilsikkerhet. Disse inkluderer ITC-er som er ansvarlige for å utvikle og oppdatere cPP-er. Apple fortsetter å evaluere og oppnå sertifiseringer mot gjeldende PP-er og cPP-er.

Apples plattformsertifiseringer for det nordamerikanske markedet utføres vanligvis med National Information Assurance Partnership (NIAP), som opprettholder en liste over prosjekter som er under evaluering, men som ikke er sertifisert ennå.

I tillegg til de oppførte generelle plattformsertifikatene er det utstedt andre sertifikater for å demonstrere spesifikke sikkerhetskrav for enkelte markeder.

Sikkerhetssertifiseringer for Apple-apper

Bakgrunn for sertifisering av Apple-apper

Apple tar aktivt del i sikkerhetssertifiseringer av Apple-apper gjennom å bruke egnede Common Criteria Protection Profiles (PP-er). Disse evalueringene bygger på maskinvare- og operativsystemsertifiseringer som Apple har oppnådd.

I 2018 iverksatte Apple app-sikkerhetsevalueringer for viktige applikasjoner som kjører på iOS 11 med Safari-nettleseren og Kontakter-appen. Apple fortsatte disse evalueringene på apper som kjører i iOS 12, iOS 13 og iPadOS 13.1. I 2021 legges det til støtte for apper som kjøres i macOS 11.

Sertifiseringsstatus for kryptografiske moduler

Apple-appene som vises her, bruker de kryptografiske modulene for det aktuelle operativsystemet. Hvis du vil ha mer informasjon om dette, kan du se Sikkerhetssertifiseringer for iOS, Sikkerhetssertifiseringer for iPadOS og Sikkerhetssertifiseringer for macOS.

Sertifiseringsstatus for Common Criteria (CC)

Det amerikanske systemet, som drives av NIAP, opprettholder en liste over produkter under evaluering. Denne listen inkluderer produkter som evalueres i USA hos et NIAP-godkjent Common Criteria-testlaboratorium (CCTL), og som har gjennomført et Evaluation Kickoff Meeting (eller liknende), hvor CCEVS-administrasjonen offisielt har akseptert produktet for evaluering.

Etter at produktene har blitt sertifisert, legger NIAP inn gyldige sertifiseringer i listen over overensstemmende produkter. Etter to år blir disse sertifiseringene gjennomgått for overensstemmelse med det gjeldende regelsettet for sikkerhetsvedlikehold. Etter at datoen for regelsettet for sikkerhetsvedlikehold har utløpt, flytter NIAP sertifiseringslisten til listen over arkiverte produkter.

Common Criteria-portalen lister opp sertifiseringer som kan gjensidig anerkjennes under Common Criteria Recognition Arrangement (CCRA). CC-portalen kan beholde produkter på listen over sertifiserte produkter i fem år, og informasjonen ligger i CC-portalen for arkiverte sertifiseringer.

Tabellen under viser sertifiseringer som er under evaluering i en lab, eller som har blitt sertifisert til å være i samsvar med CC.

Dagens status

- Evalueringer hos NIAP som publiseres som påbegynt, vises i listen over produkter under evaluering (NIAP).
- Evalueringer som er fullført og som har blitt validert, vises i listen over overensstemmende produkter (NIAP).

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: macOS 11 Big Sur *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* macOS 11 Big Sur: Kontakter *Protection Profiles (PP-er):* PP for app-programvare, EP for nettlesere
Operativsystem: macOS 11 Big Sur *Sertifiseringsdato:* –	*System-ID:* Ikke sertifisert ennå *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* macOS 11 Big Sur: Safari *Protection Profiles (PP-er):* PP for app-programvare, EP for nettlesere
Operativsystem: iOS 14, iPadOS 14 *Sertifiseringsdato:* 20.08.2021	*System-ID:* 11191 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple iOS 14 og iPadOS 14: Kontakter *Protection Profiles (PP-er):* PP for app-programvare, EP for nettlesere
Operativsystem: iOS 14, iPadOS 14 *Sertifiseringsdato:* –	*System-ID:* 11192 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple iOS 14 og iPadOS 14: Safari *Protection Profiles (PP-er):* PP for app-programvare, EP for nettlesere
Operativsystem: iOS 13, iPadOS 13 *Sertifiseringsdato:* 05.06.2020	*System-ID:* 11060 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple iOS 13 og iPadOS 13: Safari *Protection Profiles (PP-er):* PP for app-programvare, EP for nettlesere

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: iOS 13, iPadOS 13 *Sertifiseringsdato:* 05.06.2020	*System-ID:* 11050 *Dokumenter:* Sertifisering Sikkerhetsmål Veiledning Valideringsrapport Kvalitetssikringsrapport	*Tittel:* Apple iOS 13 og iPadOS 13: Kontakter *Protection Profiles (PP-er):* PP for app-programvare

Arkiverte CC-sertifiseringer for Apple-apper

Operativsystem/sertifiseringsdato	System-ID/dokumenter	Tittel/PP-er
Operativsystem: iOS 12 *Sertifiseringsdato:* 12.06.2019	*System-ID:* 10960 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iOS 12 Safari *Protection Profiles (PP-er):* PP for app-programvare, EP for nettlesere
Operativsystem: iOS 12 *Sertifiseringsdato:* 28.02.2019	*System-ID:* 10961 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iOS 12 Kontakter *Protection Profiles (PP-er):* PP for app-programvare
Operativsystem: iOS 11 *Sertifiseringsdato:* 09.11.2018	*System-ID:* 10916 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iOS 11 Safari *Protection Profiles (PP-er):* PP for app-programvare, EP for nettlesere
Operativsystem: iOS 11 *Sertifiseringsdato:* 13.09.2018	*System-ID:* 10915 *Dokumenter:* Sikkerhetsmål Veiledning	*Tittel:* iOS 11 Kontakter *Protection Profiles (PP-er):* PP for app-programvare

Sikkerhetssertifiseringer for internettjenester fra Apple

Apple opprettholder sertifiseringer i samsvar med standardene ISO/IEC 27001 og ISO/IEC 27018, slik at Apple-kunder kan oppfylle lovpålagte og kontraktsmessige forpliktelser. Disse sertifiseringene gir kundene våre en uavhengig bekreftelse på Apples informasjonssikkerhets- og personvernpraksis for aktuelle systemer.

ISO/IEC 27001 og ISO/IEC 27018 er del av Information Security Management System-standardene (ISMS) som utgis av International Organization for Standardization (ISO). Som en del av Apples ISMS har alle Annex A-kontrollkravene har blitt inkludert i Statement of Applicability, som er beskrevet i ISO/IEC 27001- og ISO/IEC 27018-standardene. Apple gjennomgår en uavhengig attestering utført av en godkjent registrator hvert år.

ISO/IEC 27001

ISO/IEC 27001 er en standard for administreringssystemer for informasjonssikkerhet som angir krav for å opprette, implementere, opprettholde og forbedre en organisasjons administreringssystemer for informasjonssikkerhet. ISO/IEC 27001-standarden inkluderer følgende sikkerhetsområder som dekkes av Apples ISO/IEC-sertifiseringer:

- Regelsett for informasjonssikkerhet
- Organisering av informasjonssikkerhet
- Ressurshåndtering
- Personalsikkerhet
- Fysisk og miljømessig sikkerhet
- Kommunikasjons- og driftsadministrering
- Tilgangskontroll
- Kjøp, utvikling og vedlikehold av informasjonssystemer
- Håndtering av informasjonssikkerhetshendelser
- Håndtering av bedriftskontinuitet
- Etterlevelse av regelverk

ISO/IEC 27018

ISO/IEC 27018 er en praksisstandard for ivaretakelse av sensitive personopplysninger (PII) i offentlige skylagringsmiljøer. ISO/IEC 27018-standarden inkluderer følgende sikkerhetsområder som dekkes av Apples ISO/IEC-sertifiseringer:

- Samtykke og valg
- Formålsbestemthet og spesifisering
- Grenser for innsamling
- Dataminimering
- Grenser for bruk, oppbevaring og framlegging
- Nøyaktighet og kvalitet
- Åpenhet, innsyn og varsling
- Individuell deltakelse og tilgang
- Ansvar
- Informasjonssikkerhet
- Etterlevelse av personvernregelverk

Apple-tjenester dekket av ISO/IEC 27001 og ISO/IEC 27018

Apples sertifiseringer for ISO/IEC 27001 og ISO/IEC 27018 dekker de følgende tjenestene:

- Apple Business Chat
- Apple Business Manager
- Apples pushvarslingstjeneste (APNs)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork-tjenester
- Administrerte Apple-ID-er
- Skolearbeid
- Siri

Sertifiseringer

Bevis på Apples sertifiseringer for ISO/IEC 27001 og ISO/IEC 27018 er tilgjengelige hos registratoren vår.

Hvis du vil se Apples sertifiseringer, kan du gå til Certificate and Client Directory search på nettstedet til British Standards Institution (BSI), skrive inn Apple i Company-søkefeltet, klikke på Search-knappen, og så velge søkeresultatene for å se sertifikatene.

Merk: Informasjon om produkter som ikke er laget av Apple, samt uavhengige nettsteder som ikke kontrolleres eller testes av Apple, er gitt uten anbefaling eller godkjenning. Apple påtar seg ikke noe ansvar for utvalget av, bruken av eller ytelsen til nettsteder og produkter fra tredjeparter. Apple garanterer ikke for nøyaktigheten eller påliteligheten til tredjeparters nettsteder. Kontakt leverandøren for mer informasjon.

macOS Security Compliance Project

macOS Security Compliance Project (mSCP) er et åpen kildekode-basert samarbeid for å tilby en programmatisk tilnærmelse til generering av sikkerhetsveiledninger. Dette er et fellesprosjekt med føderalt IT-sikkerhetspersonale fra National Institute of Standards and Technology (NIST), National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA) og Los Alamos National Laboratory (LANL). Prosjektet bruker et sett med testede og validerte kontroller for macOS og kartlegger disse kontrollene mot eventuelle sikkerhetsveiledninger som støttes av prosjektet. I tillegg kan dette prosjektet brukes som en ressurs til å opprette tilpassede basiser for sikkerhet med tekniske sikkerhetskontroller på en enkel måte ved å dra nytte av et bibliotek med testede og validerte atomiske operasjoner (konfigurasjonsinnstillinger). Prosjektet produserer tilpasset dokumentasjon, prosedyrer, konfigurasjonsprofiler og en revisjonssjekkliste basert på basiser som benyttes.

mSCP kan produsere utdatainnhold som kan brukes sammen med administrasjons- og sikkerhetsverktøy for å oppnå overensstemmelse. Konfigurasjonsinnstillinger i dette prosjektet støtter følgende veiledende basiser:

Organisasjon	Støttede basiser
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, revisjon 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

Ytterligere informasjon:

- Du finner en basis for å gjennomgå alle reglene i prosjektet her.
- Hvis du vil vite mer om prosjektet og bruk, kan du lese macOS Security Compliance Project wiki.
- Hvis du vil konfigurere prosjektet for bruk, kan du lese: Getting to Know the macOS Security Compliance Project, Part 1 og Getting to Know the macOS Security Compliance Project, Part 2.
- Hvis du er interessert i å støtte utviklingen av prosjektet, kan du lese bidragsveiledningen.

Dokumentrevisjonshistorikk

Dato	Sammendrag
27. oktober 2021	Oppdaterte emner: • Sikkerhetssertifiseringer for Secure Enclave-prosessoren (SEP) • Sikkerhetssertifiseringer for iOS • Sikkerhetssertifiseringer for macOS
17. august 2021	Oppdaterte emner: • Sikkerhetssertifiseringer for Secure Enclave-prosessoren (SEP) • Sikkerhetssertifiseringer for Apple T2-sikkerhetschip • Sikkerhetssertifiseringer for iOS • Sikkerhetssertifiseringer for iPadOS • Sikkerhetssertifiseringer for macOS • Sikkerhetssertifiseringer for tvOS • Sikkerhetssertifiseringer for watchOS • Sikkerhetssertifiseringer for Apple-apper • Sikkerhetssertifiseringer • macOS Security Compliance Project
26. april 2021	Lagt til emne: • macOS Security Compliance Project Oppdaterte emner: • Sikkerhetssertifiseringer for Apple T2-sikkerhetschip: Ny FIPS 140-2-sertifisering, 3811. • Sikkerhetssertifiseringer for Secure Enclave-prosessoren (SEP): Ny FIPS 140-2-sertifisering, 3811, og ny tabell for ytterligere sertifiseringer. • Sikkerhetssertifiseringer for iOS: Nye FIPS 140-2-sertifiseringer, 3811, iOS 14 system-ID 11146 under evaluering. • Sikkerhetssertifiseringer for iPadOS: Nye FIPS 140-2-sertifiseringer, 3811, iPadOS 14 system-ID 11147 under evaluering. • Sikkerhetssertifiseringer for macOS: Ny FIPS 140-2-sertifisering, 3811. • Sikkerhetssertifiseringer for tvOS: Nye FIPS 140-2-sertifiseringer, 3811. • Sikkerhetssertifiseringer for watchOS: Nye FIPS 140-2-sertifiseringer, 3811. • Sikkerhetssertifiseringer for Apple-apper: Oppdateringer av Common Criteria-status, og ny tabell for arkiverte Common Criteria-sertifiseringer.

Ordliste

Apple Business Manager En enkel nettbasert portal for IT-administratorer, som gjør det raskt og effektivt å rulle ut Apple-enheter som organisasjonen har kjøpt direkte fra Apple eller fra en deltakende Apple-autorisert forhandler eller operatør. De kan rulle ut enheter automatisk i MDM-løsningen uten å måtte fysisk berøre eller klargjøre enhetene før brukerne får dem.

Apple School Manager En enkel nettbasert portal for IT-administratorer, som gjør det raskt og effektivt å rulle ut Apple-enheter som organisasjonen har kjøpt direkte fra Apple eller fra en deltakende Apple-autorisert forhandler eller operatør. De kan rulle ut enheter automatisk i MDM-løsningen uten å måtte fysisk berøre eller klargjøre enhetene før brukerne får dem.

Apples pushvarslingstjeneste (APNs) En verdensomspennende tjeneste fra Apple som leverer pushvarslinger til Apple-enheter.

collaborative Protection Profile (cPP-er) En PP utviklet av et ITC, en gruppe eksperter med ansvar for å opprette cPP-er.

Common Criteria (CC) En standard som etablerer de generelle konseptene og prinsippene for evaluering av IT-sikkerhet og som spesifiserer den generelle evalueringsmodellen. Den inkluderer kataloger med sikkerhetskrav på et standardisert språk.

Common Criteria Recognition Arrangement (CCRA) En gjensidig anerkjennelsesavtale som etablerer regelsett og krav for internasjonal anerkjennelse av sertifikater som utstedes i overensstemmelse med ISO/IEC 15408 eller Common Criteria.

corecrypto Et bibliotek som gir implementeringer av kryptografiske grunnelementer på lavt nivå. Merk at corecrypto ikke direkte gir programmeringsgrensesnitt til utviklere, og det brukes gjennom API-er som er tilgjengelige for utviklere. Kildekoden til corecrypto er offentlig tilgjengelig for verifisering av dens sikkerhetskarakteristikk og funksjon.

Cryptographic Algorithm Validation Program (CAVP) En organisasjon som drives av NIAP for å drive valideringstesting av godkjente (for eksempel FIPS-godkjente og NIST-anbefalte) kryptografiske algoritmer og deres individuelle komponenter.

Cryptographic Module Validation Program (CMVP) En organisasjon som drives av amerikanske og canadiske myndigheter og skal validere samsvar med FIPS 140-3-standarden.

Federal Information Processing Standard (FIPS) Utgivelser utviklet av National Institute of Standards and Technology (NIST), enten når det kreves i lovverket eller når det foreligger overbevisende krav fra myndighetene om cybersikkerhet, eller begge.

Full Disk Encryption (FDE) Kryptering av alle data på et lagringsvolum.

Implementation under Test (IUT) En kryptografisk modul som blir testet i en lab.

Information Security Management System (ISMS) Et regelsett for informasjonssikkerhet og prosedyrer som styrer grensene for et sikkerhetsprogram som er designet for å beskytte et utvalg av informasjon og systemer ved å systematisk håndtere informasjonssikkerhet gjennom levetiden til informasjonen og/eller systemet.

international Technical Community (iTC) En gruppe som er ansvarlige for å utvikle PP-er eller cPP-er under beskyttelse av Common Criteria Recognition Arrangement (CCRA).

IPsec VPN Client En klient i en PP som gir en sikker IPsec-tilkobling gjennom en fysisk eller virtuell vertplattform og en fjernposisjon.

Kryptografisk modul Maskinvaren, programvaren og/eller firmwaren som gir kryptografiske funksjoner og oppfyller kravene til en angitt kryptografisk modulstandard.

MDM (Mobile Device Management) En tjeneste som lar brukeren fjernadministrere registrerte enheter. Når en enhet er registrert, kan brukeren bruke MDM-tjenesten over nettverket til å konfigurere innstillinger og utføre andre oppgaver på enheten uten brukermedvirkning.

Modules in Process (MIP) En liste som opprettholdes av Cryptographic Module Validation Program (CMVP) med de kryptografiske modulene som gjennomgår CMVP-valideringsprosessen.

National Information Assurance Partnership (NIAP) En organisasjon i de amerikanske myndighetene som er ansvarlig for driften av implementeringen av CC-standarder i USA og for å administrere NIAP Common Criteria Evaluation and Validation Scheme (CCEVS).

National Institute of Standards and Technology (NIST) En del av et amerikanske handelsdepartementet som har ansvar for å fremme målingsvitenskap, standarder og teknologi.

Protection Profile (PP) Et dokument som spesifiserer sikkerhetsproblemet og sikkerhetskravene for en spesifikk produktklasse.

Secure Element (SE) En silisiumchip som er innebygd i mange Apple-enheter som støtter funksjoner som for eksempel Apple Pay.

Secure Enclave Processor (SEP) En koprosessor på en System on Chip (SoC)

Security Level (SL) De fire generelle sikkerhetsnivåene (1–4) som er definert i ISO/IEC 19790 og beskriver sett med gjeldende sikkerhetskrav. Nivå 4 er det strengeste.

Security Target (ST) Et dokument som spesifiserer sikkerhetsproblemet og sikkerhetskravene for et spesifikt produkt.

Senior Officials Group Information Systems Security (SOG-IS) En gruppe som administrerer en gjensidig anerkjennelsesavtale mellom flere land i Europa.

sepOS Secure Enclave-firmwaren, basert på en Apple-tilpasset versjon av L4-mikrokjernen.

Statement of Applicability (SOA) Et dokument som beskriver sikkerhetskontrollene som er implementert i et ISMS og produsert til støtte for ISO/IEC 27001-sertifisering.

System on Chip (SoC) En integrert krets (IC) der flere komponenter kombineres på én brikke.

T2 En sikkerhetschip fra Apple som har vært innebygd i enkelte Intel-baserte Macer siden 2017.

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

H028-00499-B