Center for sikkerhedscertificeringer og compliance

December 2021

Indhold

Introduktion til Apples security assurance

Som led i Apples sikkerhedsforpligtelser er vi regelmæssigt i kontakt med andre organisationer for at få certificeret og godkendt Apples hardware, software og tjenester. Disse internationalt anerkendte organisationer forsyner Apple med certificeringer i takt med hver større udgivelse af operativsystemer. De skaber således tillid – altså security assurance – til, at sikkerhedskravene til et system er opfyldt. Til tekniske områder, som ikke indgår i ordninger om gensidig anerkendelse (MRA'er), eller som mangler standarder for sikkerhedscertificering, arbejder Apple på at udvikle passende sikkerhedsstandarder. Vores mission er at opnå dækning fra globalt accepterede og omfattende sikkerhedscertificeringer til al Apples hardware og alle Apples operativsystemer, programmer, apps og tjenester.

Certificeringer er ofte nødvendige for at opfylde kravene fra lovgivning, myndigheder og branchenormer. Tjenester som Apple School Manager og Apple Business Manager dækkes af Apples ISO/IEC 27001- og ISO/IEC 27018-certificeringer. Alle kunder, herunder myndigheder, store virksomheder og uddannelsesinstitutioner, der bruger Apple-enheder, kan bruge certificeringerne til hardware, operativsystemer, software og tjenester til at vise, at de overholder standarder og krav.

Certificeringer til hardware

Sikker software forudsætter hardware med indbygget sikkerhed, og alle Apple-enheder, hvad enten de bruger iOS, iPadOS, macOS, tvOS eller watchOS, har derfor integrerede sikkerhedsforanstaltninger i chips. Det omfatter specielle CPU-muligheder til at foretage systemsikkerhedsfunktioner og chips, der bruges til sikkerhedsfunktioner. Den mest kritiske komponent er Secure Enclave Coprocessor, som indgår i alle moderne iOS-, iPadOS-, watchOS- og tvOS-enheder og alle Mac-computere med Apple Silicon og Intel-baserede Mac-computere med Apple T2-sikkerhedschippen. Secure Enclave giver mulighed for kryptering af inaktive data, secure boot i macOS og biometri.

Apples security assurance starter med certificering af de fundamentale sikkerhedskomponenter i chips fra hardwaretillidsroden til håndhævelse af sikker start og til Secure Enclave, der giver sikker nøgleopbevaring, og til sikker godkendelse med Touch ID og Face ID. Apple-enheders sikkerhedsfunktioner fungerer gennem en kombination af chipdesign, hardware, software og tjenester, der kun er tilgængelige fra Apple. Certificering af disse komponenter er en vigtig del af underbygningen af den sikkerhed, Apple giver.

Se følgende, hvis du ønsker oplysninger om offentlige certificeringer vedrørende hardware og tilhørende firmwarekomponenter:

- Sikkerhedscertificeringer for Apple T2-sikkerhedschippen
- Sikkerhedscertificeringer til Secure Enclave Processor

Software- og programcertificeringer

Apple har uafhængige certificeringer og attestationer til sine operativsystemer, programmer og apps i overensstemmelse med U.S. Federal Information Processing Standards (FIPS) 140-2/-3 til kryptografimoduler og Common Criteria til operativsystemer, programmer, apps og enhedstjenester. Operativsystemerne omfatter iOS, iPadOS, macOS, sepOS, T2-firmware, tvOS og watchOS. Uafhængig certificering af programmer og apps vil i første omgang omfatte Safari-browseren og Kontakter, mens flere programmer og apps vil blive certificeret senere.

Se følgende, hvis du ønsker oplysninger om offentlige certificeringer vedrørende Apples *operativsystemer*:

- Sikkerhedscertificeringer til iOS
- Sikkerhedscertificeringer til iPadOS
- Sikkerhedscertificeringer til macOS
- Sikkerhedscertificeringer til tvOS
- Sikkerhedscertificeringer til watchOS

Se følgende, hvis du ønsker oplysninger om offentlige certificeringer vedrørende *apps og programmer* fra Apple:

- Sikkerhedscertificeringer til Apple-programmer og -apps

Tjenestecertificeringer

Apple har sikkerhedscertificeringer for at hjælpe vores kunder lige fra virksomheder til uddannelsesinstitutioner. Disse certificeringer giver Apples kunder mulighed for at opfylde deres lovgivnings- og kontraktmæssige forpligtelser, når de bruger Apples tjenester med Apples hardware og software. Disse certificeringer forsyner vores kunder med et uafhængigt vidnesbyrd om Apples praksis med hensyn til informationssikkerhed, miljø og anonymitet for Apples systemer.

Se følgende, hvis du ønsker oplysninger om offentlige certificeringer vedrørende Apples *internettjenester*:

- Sikkerhedscertificeringer til Apples internettjenester

Hvis du har spørgsmål om Apples certificeringer om sikkerhed og anonymitet, kan du kontakte security-certifications@apple.com.

Sikkerhedscertificeringer til hardware

Oversigt over sikkerhedscertificeringer til Apple-hardware

Apple vedligeholder valideringscertifikater for overensstemmelse med FIPS (Federal Information Processing Standard) 140-2/-3 til sepOS og T2-firmware samt andre certificeringer. Apple starter med *certificeringsbyggesten*, der anvendes bredt på flere platforme, hvor det er relevant. En af byggestenene er valideringen af corecrypto-biblioteket, der bruges til implementering af software- og hardwarekryptografimoduler i operativsystemer udviklet af Apple. En anden byggesten er certificeringen af Secure Enclave, som er integreret i mange Apple-enheder. En tredje er certificeringen af Secure Element (SE), der findes i Apple-enheder med Touch ID og enheder med Face ID. Disse byggesten til hardwarecertificeringer danner grundlag for bredere certificeringer af platformsikkerhed.

Valideringer af kryptografiske algoritmer

Validering af korrekt implementering af mange kryptografiske algoritmer og relaterede sikkerhedsfunktioner er en forudsætning for FIPS 140-3-validering og understøtter andre certificeringer. Validering administreres af NIST (National Institute of Standards and Technology) Cryptographic Algorithm Validation Program (CAVP). Valideringscertifikater til Apple-implementeringer kan findes ved hjælp af funktionen til CAVP-søgning. Du kan få flere oplysninger på webstedet om Cryptographic Algorithm Validation Program (CAVP).

Valideringer af kryptografimoduler: FIPS 140-2/3 (ISO/IEC 19790)

Apples kryptografimoduler er flere gange blevet valideret af Cryptographic Module Validation Program (CMVP) i henhold til U.S. Federal Information Processing Standard for kryptografimoduler (FIPS 140-2) i forbindelse med udgivelse af alle større versioner af operativsystemerne siden 2012. Apple sender modulerne til validering hos CMVP i henhold til standarden, hver gang en større version udgives. Disse moduler kan bruges af Apples operativsystemer, programmer og apps og giver kryptografisk funktionalitet til tjenester fra Apple og er tilgængelige til brug i programmer og apps fra tredjeparter.

Apple opnår hvert år **sikkerhedsniveau 1** for de softwarebaserede moduler "Corecrypto Module for Intel" og "Corecrypto Kernel Module for Intel" til macOS. Med Apple Silicon kan "Corecrypto Module on ARM" og "Corecrypto Kernel Module on ARM" bruges til iOS, iPadOS, tvOS, watchOS og firmware på den integrerede Apple T2-sikkerhedschip i Mac-computere.

I 2019 opnåede Apple for første gang **sikkerhedsniveau 2** i henhold til FIPS 140-2 for det integrerede kryptografimodul til hardware "Apple Corecrypto Module: Secure Key Store", hvilket muliggør brug af nøgler, der genereres og administreres i Secure Enclave og er godkendt af myndighederne i USA. Apple vil fortsat arbejde på at opnå valideringer af hardware-kryptografimodulet for kommende store udgivelser af operativsystemer.

FIPS 140-3 blev godkendt af det amerikanske handelsministerium i 2019. Den største ændring i denne version af standarden er specificeringen af ISO/IEC-standarder, især ISO/IEC 19790:2015 og den tilhørende teststandard ISO/IEC 24759:2017. CMVP har iværksat et overgangsprogram og har oplyst, at kryptografimoduler vil blive valideret på grundlag af FIPS 140-3 fra 2020. Apple sigter på, at Apples kryptografimoduler skal overholde og skifte til FIPS 140-3-standarden så hurtigt, det er praktisk muligt.

CMVP vedligeholder to lister, der kan indeholde oplysninger om foreslåede valideringer til de kryptografimoduler, der i øjeblikket er ved at blive testet og valideret. Navnet på de kryptografimoduler, der er ved at blive testet af et anerkendt laboratorie, står muligvis på listen Implementation Under Test. Når laboratoriet har afsluttet sine test og anbefaler validering af CMVP, vises kryptografimodulerne fra Apple på listen Modules in Process (listen med igangværende moduler). På dette tidspunkt er laboratoriets test færdige, og man afventer CMVP-valideringen af testresultaterne. Længden på evalueringsprocessen varierer, men på de to behandlingslister ovenfor kan du se den aktuelle status for Apples kryptografimoduler på et tidspunkt mellem datoen for udgivelse af en større operativsystemversion og udstedelse af certifikatet for validering af CMVP.

Produktcertificeringer: (Common Criteria ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) er en standard, som mange organisationer bruger som grundlag for sikkerhedsevalueringer af IT-produkter.

På Common Criteria Portal kan du se certificeringer, der kan være opnået i kraft af gensidig anerkendelse i henhold til den internationale CCRA-aftale (Common Criteria Recognition Arrangement). Common Criteria-standarden kan også bruges uden for CCRA af nationale og private valideringsordninger. I Europa er gensidig anerkendelse underlagt både SOG-IS-aftalen og CCRA.

Målet er ifølge Common Criteria-fællesskabet at opnå et internationalt godkendt sæt sikkerhedsstandarder, der kan levere en tydelig og pålidelig evaluering af IT-produkters sikkerhedsfunktioner. Common Criteria-certificering er en uafhængig vurdering af et produkts opfyldelse af sikkerhedsstandarder, der giver kunderne større tillid til IT-produkters sikkerhed og danner grundlag for kvalificerede beslutninger.

Medlemslande har via CCRA aftalt at anerkende certificeringen af IT-produkter med samme niveau af tillid. Evalueringer, der er nødvendige inden certificering, er omkostningskrævende og inkluderer:

- Beskyttelsesprofiler (PP'er)
- Sikkerhedsmål (ST'er)
- Funktionelle krav til sikkerhed (SFR'er)
- Security Assurance Requirements (SAR'er)
- Evaluation Assurance Levels (EAL'er)

Beskyttelsesprofiler (PP'er) er dokumenter, som angiver sikkerhedskravene for en bestemt klasse enhedstyper (f.eks. Mobilitet), og de bruges til at skabe et sammenligningsgrundlag for evalueringer af IT-produkter, der tilhører samme klasse. Antallet af medlemmer af CCRA og listen med godkendte PP'er øges hvert år. Denne ordning giver en produktudvikler mulighed for at sigte efter en enkelt certificering i henhold til en af certificeringsgodkendelsesordningerne og få den godkendt af en hvilken som helst forbruger, der har skrevet under på certifikatet.

Sikkerhedsmål (ST'er) definerer, *hvad* der skal evalueres, når et IT-produkt skal certificeres. ST'erne omsættes til mere specifikke *funktionelle krav til sikkerhed (SFR'er)*, der bruges til at evaluere detaljerne i ST'erne.

Common Criteria (CC) inkluderer også *Security Assurance Requirements (SAR'er)*. En fælles måling er *Evaluation Assurance Level (EAL)* – garantimålet for evalueringen. EAL'er grupperer hyppigt anvendte sæt Security Assurance Requirements og kan anføres i PP'er og ST'er for at lette sammenligninger.

Mange af de tidligere PP'er er blevet arkiveret og bliver erstattet af målrettede PP'er, der er ved at blive udviklet og har fokus på bestemte løsninger og miljøer. I en fælles indsats for at sikre, at den gensidige anerkendelse mellem alle CCRA-medlemmer fortsætter, er internationale tekniske fællesskaber (iTC'er) blevet oprettet for at udvikle og vedligeholde samarbejdende beskyttelsesprofiler (cPP'er), som fra starten er udviklet i samarbejde med deltagere, der har underskrevet CCRA-ordninger. PP'er rettet mod brugergrupper og andre ordninger om gensidig anerkendelse end CCRA udvikles fortsat af behørige interessenter.

Apple begyndte at søge om certificeringer i henhold til den opdaterede CCRA med udvalgte cPP'er i starten af 2015. Siden da har Apple opnået Common Criteria-certificeringer for hver større version af iOS og har udvidet dækningen til at omfatte det sikkerhedsniveau, der leveres af nye PP'er.

Apple påtager sig en aktiv rolle i de tekniske fællesskaber med fokus på evaluering af sikkerhedsteknologi til mobile enheder. De omfatter blandt andet de iTC'er, der har ansvaret for at udvikle og opdatere cPP'er. Apple fortsætter med at evaluere og stræbe efter certificeringer for nuværende PP'er og cPP'er.

Certificeringer til Apple-platforme til det nordamerikanske marked foretages normalt sammen med National Information Assurance Partnership (NIAP), som vedligeholder en liste med projekter, der er ved at blive evalueret, men endnu ikke er certificeret.

Ud over de anførte generelle platformcertifikater er der udstedt andre certifikater, der har til formål at påvise opfyldelse af særlige sikkerhedskrav til visse markeder.

Sikkerhedscertificeringer til Secure Enclave Processor

Baggrund for Secure Enclave-certificering

Hardwarekryptografimodulet – *Apple SEP Secure Key Store-kryptografimodulet* – er integreret i den Apple SoC, der findes i følgende produkter: Apple A-serien til iPhone og iPad, M-serien til Mac-computere med Apple Silicon, S-serien til Apple Watch og sikkerhedschippen i T-serien på Intel-baserede Mac-computere fra og med iMac Pro, der blev lanceret i 2017.

I 2018 synkroniserede Apple med valideringen af softwarekryptografimodulerne med operativsystemer, der blev udgivet i 2017: iOS 11, macOS 10.13, tvOS 11 og watchOS 4. SEP hardware-kryptografimodulet, eller Apple SEP Secure Key Store Cryptographic Module v1.0, blev først valideret i henhold til kravene for FIPS 140-2-sikkerhedsniveau 1.

I 2019 godkendte Apple hardwaremodulet i henhold til kravene i FIPS 140-2-sikkerhedsniveau 2 og opdaterede modulversionens identifikator til v9.0 for at synkronisere med versionerne af de tilsvarende godkendte moduler fra corecrypto User og corecrypto Kernel. I 2019 omfattede dette iOS 12, macOS 10.14, tvOS 12 og watchOS 5.

I 2020 og 2021 har Apple fortsat bestræbelserne på at opnå validering af overensstemmelse med FIPS 140-3 og yderligere sikkerhed på niveau 3 af de fysiske sikkerhedskrav til Apple Silicon: A13-, A14-, S6- og M1-chipsene.

Apple deltager også aktivt i valideringen af corecrypto User- og corecrypto Kernel-modulerne til enhver stor udgivelse af et operativsystem. Validering af overensstemmelse kan kun udføres i henhold til en endelig publiceret version.

Valideringsstatus for kryptografimodul

Cryptographic Module Validation Program (CMVP) vedligeholder kryptografimodulers valideringsstatus på tre forskellige lister afhængigt af deres aktuelle status:

- For at komme på CMVP-listen Implementation Under Test skal laboratoriet have en aftale med Apple om at foretage test.
- Når laboratoriet har afsluttet sine test og har anbefalet validering af CMVP, og CMVP-betalingen er foretaget, føjes modulet til listen Modules in Process. MIP-listen følger status for CMVP-valideringen i fire faser:
  - *Gennemgang under behandling:* Afventer at CMVP-ressource tildeles.
  - *Til gennemgang:* CMVP-ressourcerne udfører valideringsaktiviteterne.
  - *Koordinering:* Laboratoriet og CMVP løser eventuelle problemer.
  - *Afslutning:* Aktiviteter og formaliteter i forbindelse med udstedelsen af certifikatet.
- Efter valideringen af CMVP tildeles modulerne et konformitetscertifikat og føjes til listen over validerede kryptografimoduler. Det omfatter:
  - Validerede moduler, der er markeret som aktive.
  - Efter 5 år bliver modulerne markeret som historiske.
  - Hvis modulcertifikatet skulle blive tilbagekaldt, markeres det som tilbagekaldt.

I 2020 indførte CMVP den internationale standard ISO/IEC 19790 som basis for FIPS 140-3.

FIPS 140-3-certificeringer

Aktuel status

Tabellen herunder viser de kryptografimoduler fra 2020 og 2021, der er ved at blive testet af laboratoriet med hensyn til overholdelse af FIPS 140-3.

Secure Key Store (SKS) til både 2020- og 2021-versionerne af operativsystemer har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler), og når de er blevet valideret, flyttes de til listen med validerede kryptografimoduler.

Brugerområde, kerneområde og Secure Key Store i iOS 15 (2021) gennemgår laboratorietest. De er anført på listen Implementation Under Test List.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple corecrypto Module v12 *Operativsystem:* sepOS distribueret med 2021-udgaver af iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14, T2, M1, S3-S6) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med 2021-udgaver af iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware(A13, A14, S6, M1) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med 2020-udgaver af iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14, T2, M1, S3-S6) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med 2020-udgaver af iOS, iPadOS, macOS, tvOS og watchOS *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware(A13, A14, S6, M1) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3

FIPS 140-2-certificeringer

Tabellen herunder viser de kryptografimoduler, der er blevet testet af laboratoriet med hensyn til overholdelse af FIPS 140-2.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 05-02-2021	*Certifikater:* 3811 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS til macOS 10.15 Catalina *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3523 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS til macOS 10.14 Mojave *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3223 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS til macOS 10.13 High Sierra *Type:* Hardware *Sikkerhedsniveau:* 2

Common Criteria-certificeringer (CC)

Apple deltager aktivt i Common Criteria-evalueringer, hvor passende beskyttelsesprofiler dækker sikkerhedsfunktionaliteten i Apples teknologier.

Certificeringsstatus for Common Criteria (CC)

Den amerikanske ordning, der administreres af NIAP, vedligeholder listen Products in Evaluation (Produkter til evaluering). Denne liste omfatter produkter, som i øjeblikket evalueres i USA med et Common Criteria Testing Laboratory (CCTL), der er godkendt af NIAP, og som har afsluttet et evalueringskickoff-møde (eller tilsvarende), hvor CCEVS-ledelsen officielt godkendte produktet til evaluering.

Efter at produkter er blevet certificeret, anbringer NIAP aktuelle godkendte certificeringer på Product Compliant List (liste med produkter, der overholder standarderne). Efter 2 år gennemgås disse certificeringer for at afklare, om de efterlever den aktuelle sikkerhedsvedligeholdelsespolitik. Når datoen for sikkerhedsvedligeholdelsen er udløbet, flytter NIAP certificeringsoptegnelsen til listen Archived Products (arkiverede produkter).

På Common Criteria Portal vises de certificeringer, der kan blive gensidigt anerkendt i henhold til Common Criteria Recognition Arrangement (CCRA). CC-portalen kan vedligeholde produkter på listen med certificerede produkter i 5 år, og fortegnelser om arkiverede certificeringer opbevares på CC-portalen.

Tabellen herunder viser de certificeringer, der er ved at blive evalueret af et laboratorium, og de certificeringer, hvis overholdelse af Common Criteria er færdigbehandlet.

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: sepOS *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple Secure Enclave [2020] *Beskyttelsesprofiler:* CPP_DSC_V1.0 *Hardware:* Secure Enclave for (A9-A14, M1, T2, S3-S6) *Software:* sepOS distribueret med iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14 og watchOS 7

Yderligere certificeringer

Tabellen nedenfor viser certificeringer for Secure Enclave, der hverken bruger Common Criteria eller FIPS 140-3.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* 07.12.2019 til 26.12.2022	*Certifikater:* CFNR201902910002 (P.R. China: Technology Certification of Mobile Financial Service) Kinesisk version Engelsk version	*Titel:* Mobile Terminal Trusted Execution Environment *Operativsystem:* iOS 13.5.1 *Specifikation:* JR/T 0156-2017

Sikkerhedscertificeringer for Apple T2-sikkerhedschippen

Baggrund for validering af kryptografimoduler

Apple deltager aktivt i valideringen af Apple-integrerede software- og hardwaremoduler til enhver stor udgivelse af et operativsystem. Validering af overensstemmelse kan kun udføres i henhold til en endelig moduludgivelsesversion.

I 2020 indførte CMVP den internationale standard ISO/IEC 19790 som basis for U.S. Federal Information Processing Standard (FIPS) 140-3.

Ud over en Intel CPU har de fleste Mac-computere siden 2017 også haft en separat Apple T2-sikkerhedschip, som er en Apple Silicon-baseret SoC (System on Chip). Disse Mac-computere med T2-chip bruger alle fem kryptografimoduler til adskillige tjenester på enheden.

- Corecrypto-brugermodul til Intel (bruges af macOS på Intel-baserede Mac-computere)
- Corecrypto-kernemodul til Intel (bruges af macOS på Intel-baserede Mac-computere)
- Corecrypto-brugermodul til ARM (bruges af T2-chip)
- Corecrypto-kernemodul til ARM (bruges af T2-chip)
- Kryptografimodul til Secure Key Store (bruges af den integrerede Secure Enclave-hjælpeprocessor på T2-chippen)

Bemærk: De Apple Silicon-baserede moduler på T2-chippen er de samme som dem, der findes på andre Apple-chips som f.eks. Apple A-, S- og M-serien.

Valideringsstatus for kryptografimodul

Cryptographic Module Validation Program (CMVP) vedligeholder kryptografimodulers valideringsstatus på tre forskellige lister afhængigt af deres aktuelle status:

- For at komme på CMVP-listen Implementation Under Test skal laboratoriet have en aftale med Apple om at foretage test.
- Når laboratoriet har afsluttet sine test og har anbefalet validering af CMVP, og CMVP-betalingen er foretaget, føjes modulet til listen Modules in Process (MIP). Listen MIP følger CMVP-valideringens fremgang i fire faser:
  - *Gennemgang under behandling:* Afventer at CMVP-ressource tildeles.
  - *Til gennemgang:* CMVP-ressourcerne udfører valideringsaktiviteterne.
  - *Koordinering:* Laboratoriet og CMVP løser eventuelle problemer.
  - *Afslutning:* Aktiviteter og formaliteter i forbindelse med udstedelsen af certifikatet.
- Efter valideringen af CMVP tildeles modulerne et konformitetscertifikat og føjes til listen over validerede kryptografimoduler. Det omfatter:
  - Validerede moduler, der er markeret som aktive.
  - Efter 5 år bliver modulerne markeret som historiske.
  - Hvis modulcertifikatet skulle blive tilbagekaldt, markeres det som tilbagekaldt.

FIPS 140-3-certificeringer

Aktuel status

Brugerområde, kerneområde og Secure Key Store i moduler fra 2020 har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Brugerområde, kerneområde og Secure Key Store i modulerne fra 2021 gennemgår laboratorietest. De er anført på listen Implementation Under Test List.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS til macOS 12 Monterey *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS til macOS 12 Monterey *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS til macOS 12 Monterey *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (T2) *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS til macOS 11 Big Sur *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS til macOS 11 Big Sur *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS til ßmacOS 11 Big Sur på Intel *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware *Sikkerhedsniveau:* 2

FIPS 140-2-certificeringer

Tabellen herunder viser de kryptografimoduler, der er blevet testet af laboratoriet med hensyn til overholdelse af FIPS 140-2.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3856 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v10.0 til ARM *Operativsystem:* sepOS til macOS 10.15 Catalina *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3855 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v10.0 til ARM *Operativsystem:* sepOS til macOS 10.15 Catalina *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 05-02-2021	*Certifikater:* 3811 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS til macOS 10.15 Catalina *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 23-04-2019	*Certifikater:* 3438 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v9.0 til ARM *Operativsystem:* sepOS til macOS 10.14 Mojave *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 11-04-2019	*Certifikater:* 3433 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v9.0 til ARM *Operativsystem:* sepOS til macOS 10.14 Mojave *Type:* Software *Sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3523 *Dokumenter:* Certifikat Security Policy Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS til macOS 10.14 Mojave *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Certifikater:* 3148 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v8.0 til ARM *Operativsystem:* sepOS til macOS 10.13 High Sierra *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 17-05-2018, 03-07-2018	*Certifikater:* 3147 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v8.0 til ARM *Operativsystem:* sepOS til macOS 10.13 High Sierra *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 10-07-2018	*Certifikater:* 3223 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS til macOS 10.13 High Sierra *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2016 *Valideringsdatoer:* 01-02-2017	*Certifikater:* 2828 *Dokumenter:* Certifikat Security Policy Vejledning til Crypto Officer	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* sepOS til macOS 10.12 Sierra *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2016 *Valideringsdatoer:* 01-02-2017	*Certifikater:* 2827 *Dokumenter:* Certifikat Security Policy Vejledning til Crypto Officer	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* sepOS til macOS 10.12 Sierra *Type:* Software *Sikkerhedsniveau:* 1

Sikkerhedscertificeringer til operativsystemer

Oversigt over sikkerhedscertificeringer til Apples operativsystemer

Apple vedligeholder valideringscertifikater for overensstemmelse med FIPS (Federal Information Processing Standard) 140-2/-3 til sepOS og T2-firmware samt andre certificeringer. Apple starter med *certificeringsbyggesten*, der anvendes bredt på flere platforme, hvor det er relevant. En af byggestenene er valideringen af corecrypto, der bruges til implementering af software- og hardwarekryptografimoduler i operativsystemer udviklet af Apple. En anden byggesten er certificeringen af Secure Enclave, som er integreret i mange Apple-enheder. En tredje er certificeringen af Secure Element (SE), der findes i Apple-enheder med Touch ID og enheder med Face ID. Disse byggesten til hardwarecertificeringer danner grundlag for bredere certificeringer af platformsikkerhed.

Valideringer af kryptografiske algoritmer

Validering af korrekt implementering af mange kryptografiske algoritmer og relaterede sikkerhedsfunktioner er en forudsætning for FIPS 140-3-validering og understøtter andre certificeringer. Validering administreres af NIST Cryptographic Algorithm Validation Program (CAVP). Valideringscertifikater til Apple-implementeringer kan findes ved hjælp af funktionen til CAVP-søgning.

Valideringer af kryptografimoduler: FIPS 140-2/3 (ISO/IEC 19790)

Kryptografimodulerne i Apples operativsystemer er valideret af Cryptographic Module Validation Program (CMVP) i forbindelse med frigivelsen af alle større versioner af operativsystemerne siden 2012, og det er bekræftet, at modulerne overholder de amerikanske FIPS-standarder (Federal Information Processing Standards) 140-2. Apple sender alle moduler til fuld kryptografisk validering hos CMVP, hver gang en større version udgives. Disse validerede moduler udfører kryptografiske funktioner til tjenester leveret af Apple og kan også bruges til apps og programmer fra tredjeparter.

Apple opnår hvert år **sikkerhedsniveau 1** for de softwarebaserede moduler "Corecrypto Module for Intel" og "Corecrypto Kernel Module for Intel" til macOS. Med Apple Silicon kan "Corecrypto Module on ARM" og "Corecrypto Kernel Module on ARM" bruges til iOS, iPadOS, tvOS, watchOS og firmware på den integrerede Apple T2-sikkerhedschip i Mac-computere.

I 2019 opnåede Apple for første gang **sikkerhedsniveau 2** i henhold til FIPS 140-2 for det integrerede kryptografimodul til hardware "Apple Corecrypto Module: Secure Key Store", hvilket muliggør brug af nøgler, der genereres og administreres i Secure Enclave og er godkendt af myndighederne i USA. Apple vil fortsat arbejde på at opnå valideringer af hardware-kryptografimodulet for kommende store udgivelser af operativsystemer.

FIPS 140-3 blev godkendt af det amerikanske handelsministerium i 2019. Den største ændring i denne version af standarden er specificeringen af ISO/IEC-standarder, især ISO/IEC 19790:2015 og den tilhørende teststandard ISO/IEC 24759:2017. CMVP har iværksat et overgangsprogram og har oplyst, at kryptografimoduler vil blive valideret på grundlag af FIPS 140-3 fra 2020. Apple sigter på, at Apples kryptografimoduler skal overholde og skifte til FIPS 140-3-standarden så hurtigt, det er praktisk muligt.

CMVP vedligeholder to lister, der kan indeholde oplysninger om foreslåede valideringer til de kryptografimoduler, der i øjeblikket er ved at blive testet og valideret. Navnet på de kryptografimoduler, der er ved at blive testet af et anerkendt laboratorie, står muligvis på listen Implementation Under Test. Når laboratoriet har afsluttet sine test og anbefaler validering af CMVP, vises kryptografimodulerne fra Apple på listen Modules in Process (listen med igangværende moduler). På dette tidspunkt er laboratoriets test færdige, og man afventer CMVP-valideringen af testresultaterne. Længden på evalueringsprocessen varierer, men på de to behandlingslister ovenfor kan du se den aktuelle status for Apples kryptografimoduler på et tidspunkt mellem datoen for udgivelse af en større operativsystemversion og udstedelse af certifikatet for validering af CMVP.

Produktcertificeringer: (Common Criteria ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) er en standard, som mange organisationer bruger som grundlag for sikkerhedsevalueringer af IT-produkter.

På Common Criteria Portal kan du se certificeringer, der kan være opnået i kraft af gensidig anerkendelse i henhold til den internationale CCRA-aftale (Common Criteria Recognition Arrangement). Common Criteria-standarden kan også bruges uden for CCRA af nationale og private valideringsordninger. I Europa er gensidig anerkendelse underlagt både SOG-IS-aftalen og CCRA.

Målet er ifølge Common Criteria-fællesskabet at opnå et internationalt godkendt sæt sikkerhedsstandarder, der kan levere en tydelig og pålidelig evaluering af IT-produkters sikkerhedsfunktioner. Common Criteria-certificering er en uafhængig vurdering af et produkts opfyldelse af sikkerhedsstandarder, der giver kunderne større tillid til IT-produkters sikkerhed og danner grundlag for kvalificerede beslutninger.

Medlemslande har via CCRA aftalt at anerkende certificeringen af IT-produkter med samme niveau af tillid. Evalueringer, der er nødvendige inden certificering, er omkostningskrævende og inkluderer:

- Beskyttelsesprofiler (PP'er)
- Sikkerhedsmål (ST'er)
- Funktionelle krav til sikkerhed (SFR'er)
- Security Assurance Requirements (SAR'er)
- Evaluation Assurance Levels (EAL'er)

Beskyttelsesprofiler (PP'er) er dokumenter, som angiver sikkerhedskravene for en bestemt klasse enhedstyper (f.eks. Mobilitet), og de bruges til at skabe et sammenligningsgrundlag for evalueringer af IT-produkter, der tilhører samme klasse. Antallet af medlemmer af CCRA og listen med godkendte PP'er øges hvert år. Denne ordning giver en produktudvikler mulighed for at sigte efter en enkelt certificering i henhold til en af certificeringsgodkendelsesordningerne og få den godkendt af en hvilken som helst forbruger, der har skrevet under på certifikatet.

Sikkerhedsmål (ST'er) definerer, *hvad* der skal evalueres, når et IT-produkt skal certificeres. ST'erne omsættes til mere specifikke *funktionelle krav til sikkerhed (SFR'er)*, der bruges til at evaluere detaljerne i ST'erne.

Common Criteria (CC) inkluderer også *Security Assurance Requirements (SAR'er)*. En fælles måling er *Evaluation Assurance Level (EAL)* – garantimålet for evalueringen. EAL'er grupperer hyppigt anvendte sæt Security Assurance Requirements og kan anføres i PP'er og ST'er for at lette sammenligninger.

Mange af de tidligere PP'er er blevet arkiveret og bliver erstattet af målrettede PP'er, der er ved at blive udviklet og har fokus på bestemte løsninger og miljøer. I en fælles indsats for at sikre, at den gensidige anerkendelse mellem alle CCRA-medlemmer fortsætter, er internationale tekniske fællesskaber (iTC'er) blevet oprettet for at udvikle og vedligeholde *samarbejdende beskyttelsesprofiler (cPP'er)*, som fra starten er udviklet i samarbejde med deltagere, der har underskrevet CCRA-ordninger. PP'er rettet mod brugergrupper og andre ordninger om gensidig anerkendelse end CCRA udvikles fortsat af behørige interessenter.

Apple begyndte at søge om certificeringer i henhold til den opdaterede CCRA med udvalgte cPP'er i starten af 2015. Siden da har Apple opnået Common Criteria-certificeringer for hver større version af iOS og har udvidet dækningen til at omfatte det sikkerhedsniveau, der leveres af nye PP'er.

Apple påtager sig en aktiv rolle i de tekniske fællesskaber med fokus på evaluering af sikkerhedsteknologi til mobile enheder. De omfatter blandt andet de iTC'er, der har ansvaret for at udvikle og opdatere cPP'er. Apple fortsætter med at evaluere og stræbe efter certificeringer for nuværende PP'er og cPP'er.

Certificeringer til Apple-platforme til det nordamerikanske marked foretages normalt sammen med National Information Assurance Partnership (NIAP), som vedligeholder en liste med projekter, der er ved at blive evalueret, men endnu ikke er certificeret.

Ud over de anførte generelle platformcertifikater er der udstedt andre certifikater, der har til formål at påvise opfyldelse af særlige sikkerhedskrav til visse markeder.

Sikkerhedscertificeringer til iOS

Baggrund for iOS-certificering

Apple deltager aktivt i valideringen af Apple-integrerede software- og hardwaremoduler til enhver stor udgivelse af et operativsystem. Validering af overensstemmelse kan kun udføres i henhold til en endelig publiceret version.

Status for validering af kryptografimoduler til iOS

Cryptographic Module Validation Program (CMVP) vedligeholder kryptografimodulers valideringsstatus på tre forskellige lister afhængigt af deres aktuelle status:

- For at komme på CMVP-listen Implementation Under Test skal laboratoriet have en aftale med Apple om at foretage test.
- Når laboratoriet har afsluttet sine test og har anbefalet validering af CMVP, og CMVP-betalingen er foretaget, føjes modulet til listen Modules in Process (MIP). Listen MIP følger CMVP-valideringens fremgang i fire faser:
  - *Gennemgang under behandling:* Afventer at CMVP-ressource tildeles.
  - *Til gennemgang:* CMVP-ressourcerne udfører valideringsaktiviteterne.
  - *Koordinering:* Laboratoriet og CMVP løser eventuelle problemer.
  - *Afslutning:* Aktiviteter og formaliteter i forbindelse med udstedelsen af certifikatet.
- Efter valideringen af CMVP tildeles modulerne et konformitetscertifikat og føjes til listen over validerede kryptografimoduler. Det omfatter:
  - Validerede moduler, der er markeret som aktive.
  - Efter 5 år bliver modulerne markeret som historiske.
  - Hvis modulcertifikatet skulle blive tilbagekaldt, markeres det som tilbagekaldt.

I 2020 indførte CMVP den internationale standard ISO/IEC 19790 som basis for FIPS 140-3.

FIPS 140-3-certificeringer

Aktuel status

Brugerområde, kerneområde og Secure Key Store til iOS 14 (2020) har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Brugerområde, kerneområde og Secure Key Store i iOS 15 (2021) gennemgår laboratorietest. De er anført på listen Implementation Under Test List.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iOS 15 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iOS 15 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribueret med iOS 15 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribueret med iOS 15 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A13, A14, A15) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iOS 14 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iOS 14 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med iOS 14 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med iOS 14 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A13-A14) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3

FIPS 140-2-certificeringer

Tabellen herunder viser de kryptografimoduler, der er ved at blive eller er blevet testet af laboratoriet med hensyn til overholdelse af FIPS 140-2.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3856 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v10.0 til ARM *Operativsystem:* iOS 13 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3855 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v10.0 til ARM *Operativsystem:* iOS 13 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 05-02-2021	*Certifikater:* 3811 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribueret med iOS 13 *Type:* Hardware *Sikkerhedsniveau:* 2

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 23-04-2019	*Certifikater:* 3438 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v9.0 til ARM *Operativsystem:* iOS 12 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 11-04-2019	*Certifikater:* 3433 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v9.0 til ARM *Operativsystem:* iOS 12 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3523 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribueret med iOS 12 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Certifikater:* 3148 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v8.0 til ARM *Operativsystem:* iOS 11 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 17-05-2018, 03-07-2018	*Certifikater:* 3147 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v8.0 til ARM *Operativsystem:* iOS 11 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3223 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribueret med iOS 11 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2016 *Valideringsdatoer:* 01-02-2017	*Certifikater:* 2828 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2016 *Valideringsdatoer:* 01-02-2017	*Certifikater:* 2827 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Type:* Software *Sikkerhedsniveau:* 1

Tidligere versioner

Certifikater, der er mere end 5 år gamle, angives at have historisk status af CMVP. Disse tidligere versioner af iOS havde valideringer af kryptografimoduler.

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

Baggrund for Common Criteria-certificeringer (CC)

Apple deltager aktivt i evalueringen af iOS til enhver stor udgivelse af operativsystemet. Evalueringer kan kun foretages i henhold til en offentligt publiceret version af operativsystemet. Forud for iPadOS 13.1 havde iPadOS navnet iOS.

Certificeringsstatus for Common Criteria (CC)

Den amerikanske ordning, der administreres af NIAP, vedligeholder listen Products in Evaluation (Produkter til evaluering). Denne liste omfatter produkter, som i øjeblikket evalueres i USA med et Common Criteria Testing Laboratory (CCTL), der er godkendt af NIAP, og som har afsluttet et evalueringskickoff-møde (eller tilsvarende), hvor CCEVS-ledelsen officielt godkendte produktet til evaluering.

Efter at produkter er blevet certificeret, anbringer NIAP aktuelle godkendte certificeringer på Product Compliant List (liste med produkter, der overholder standarderne). Efter 2 år gennemgås disse certificeringer for at afklare, om de efterlever den aktuelle sikkerhedsvedligeholdelsespolitik. Når datoen for sikkerhedsvedligeholdelsen er udløbet, flytter NIAP certificeringsoptegnelsen til listen Archived Products (arkiverede produkter).

På Common Criteria Portal vises de certificeringer, der kan blive gensidigt anerkendt i henhold til Common Criteria Recognition Arrangement (CCRA). CC-portalen kan vedligeholde produkter på listen med certificerede produkter i 5 år, og fortegnelser om arkiverede certificeringer opbevares på CC-portalen.

Tabellen herunder viser de certificeringer, der er ved at blive evalueret af et laboratorium, og de certificeringer, hvis overholdelse af Common Criteria er færdigbehandlet.

Aktuel status

Laboratorietest af iOS 15 til evaluering af NIAP er undervejs. De nyeste oplysninger kan ses på listen Products in evaluation (NIAP) (produkter under evaluering) og Product Compliant List (liste med produkter, der overholder standarderne).

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: iOS 15 *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* —	*Titel:* Apple iOS 15: iPhone-modeller *Beskyttelsesprofiler:* Grundlæggende om mobile enheder (PP-moduler endnu ikke bekræftet)
Operativsystem: iOS 14 *Certificeringsdato:* 01-09-2021	*Skema-id:* 11146 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple iOS 14: iPhone-modeller *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, modul til VPN-klient, PP-modul til WLAN-klienter, EP til MDM-agent
Operativsystem: iOS 13 *Certificeringsdato:* 06-11-2020	*Skema-id:* 11036 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple iOS 13 på iPhone *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, modul til VPN-klient, EP til WLAN-klienter, EP til MDM-agent

Arkiverede Common Criteria-certificeringer til iOS

Disse tidligere versioner af iOS havde Common Criteria-valideringer. De er arkiveret af NIAP som fastlagt i NIAPs politik:

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: iOS 12 *Certificeringsdato:* 14-03-2019	*Skema-id:* 10937 *Dokumenter:* Sikkerhedsmål Vejledning	*Titel:* iPhone med iOS 12 *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, modul til VPN-klient, EP til trådløs LAN-klient, EP til MDM-agent
Operativsystem: iOS 11 *Certificeringsdato:* 17-07-2018	*Skema-id:* 10851 *Dokumenter:* Sikkerhedsmål Vejledning	*Titel:* Apple iOS 11 *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, EP til trådløs LAN-klient, EP til MDM-agent
Operativsystem: iOS 10 *Certificeringsdato:* 27-07-2017	*Skema-id:* 10782 *Dokumenter:* Sikkerhedsmål, Vejledning	*Titel:* iOS 10.2 på iPhone- og iPad-enheder *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, EP til trådløs LAN-klient, EP til MDM-agent

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: iOS 10 *Certificeringsdato:* 27-07-2017	*Skema-id:* 10792 *Dokumenter:* Sikkerhedsmål, Vejledning	*Titel:* iOS 10.2 VPN-klient på iPhone- og iPad-enheder *Beskyttelsesprofiler:* VPN-klient PP
Operativsystem: iOS 9 *Certificeringsdato:* 14-10-2016	*Skema-id:* 10725 *Dokumenter:* Sikkerhedsmål, Vejledning	*Titel:* iOS 9.3.2 med MDM-agent *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, EP til MDM-agent
Operativsystem: iOS 9 *Certificeringsdato:* 13-10-2016	*Skema-id:* 10714 *Dokumenter:* Sikkerhedsmål, Vejledning	*Titel:* OS VPN-klient på iPhone- og iPad-enheder *Beskyttelsesprofiler:* VPN-klient PP
Operativsystem: iOS 9 *Certificeringsdato:* 28-01-2016	*Skema-id:* 10695 *Dokumenter:* Sikkerhedsmål, Vejledning	*Titel:* iOS 9 *Beskyttelsesprofiler:* Grundlæggende om mobile enheder

Sikkerhedscertificeringer til iPadOS

Baggrund for iPadOS-certificering

Apple deltager aktivt i valideringen af Apple-operativsystemer ved hver store udgivelse af et operativsystem ved hjælp af passende samarbejdende beskyttelsesprofiler og FIPS 140-3-sikkerhedsniveauer. Validering af overensstemmelse kan kun udføres i henhold til en endelig publiceret version.

Bemærk: I 2019 fik operativsystemet til iPad-enheder navnet iPadOS. Forud for iPadOS 13.1 havde iPadOS navnet iOS.

Status for validering af kryptografimoduler til iPadOS

Cryptographic Module Validation Program (CMVP) vedligeholder kryptografimodulers valideringsstatus på tre forskellige lister afhængigt af deres aktuelle status:

- For at komme på CMVP-listen Implementation Under Test skal laboratoriet have en aftale med Apple om at foretage test.
- Når laboratoriet har afsluttet sine test og har anbefalet validering af CMVP, og CMVP-betalingen er foretaget, føjes modulet til listen Modules in Process (MIP). Listen MIP følger CMVP-valideringens fremgang i fire faser:
  - *Gennemgang under behandling:* Afventer at CMVP-ressource tildeles.
  - *Til gennemgang:* CMVP-ressourcerne udfører valideringsaktiviteterne.
  - *Koordinering:* Laboratoriet og CMVP løser eventuelle problemer.
  - *Afslutning:* Aktiviteter og formaliteter i forbindelse med udstedelsen af certifikatet.
- Efter valideringen af CMVP tildeles modulerne et konformitetscertifikat og føjes til listen over validerede kryptografimoduler. Det omfatter:
  - Validerede moduler, der er markeret som aktive.
  - Efter 5 år bliver modulerne markeret som historiske.
  - Hvis modulcertifikatet skulle blive tilbagekaldt, markeres det som tilbagekaldt.

I 2020 indførte CMVP den internationale standard ISO/IEC 19790 som basis for FIPS 140-3.

FIPS 140-3-certificeringer

Aktuel status

Brugerområde, kerneområde og Secure Key Store til iPadOS 14 (2020) har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Brugerområde, kerneområde og Secure Key Store i iPadOS 15 (2021) gennemgår laboratorietest. De er anført på listen Implementation Under Test List.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iPadOS 15 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iPadOS 15 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribueret med iPadOS 15 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14, M1) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribueret med iPadOS 15 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14, M1) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iPadOS 14 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iPadOS 14 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med iPadOS 14 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14, M1) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med iPadOS 14 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A9-A14, M1) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3

FIPS 140-2-certificeringer

Tabellen herunder viser de kryptografimoduler, der er ved at blive eller er blevet testet af laboratoriet med hensyn til overholdelse af FIPS 140-2.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3856 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v10.0 til ARM *Operativsystem:* iPadOS 13 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3855 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v10.0 til ARM *Operativsystem:* iPadOS 13 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 05-02-2021	*Certifikater:* 3811 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribueret med iPadOS 13 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 23-04-2019	*Certifikater:* 3438 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v9.0 til ARM *Operativsystem:* iOS 12 *Type:* Software *Sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 11-04-2019	*Certifikater:* 3433 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v9.0 til ARM *Operativsystem:* iOS 12 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3523 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribueret med iOS 12 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Certifikater:* 3148 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v8.0 til ARM *Operativsystem:* iOS 11 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 17-05-2018, 03-07-2018	*Certifikater:* 3147 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v8.0 til ARM *Operativsystem:* iOS 11 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3223 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribueret med iOS 11 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2016 *Valideringsdatoer:* 01-02-2017	*Certifikater:* 2828 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2016 *Valideringsdatoer:* 01-02-2017	*Certifikater:* 2827 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Type:* Software *Sikkerhedsniveau:* 1

Tidligere versioner

Certifikater, der er mere end 5 år gamle, angives at have historisk status af CMVP. Disse tidligere versioner af iOS havde valideringer af kryptografimoduler.

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

Baggrund for Common Criteria-certificeringer (CC)

Apple deltager aktivt i evalueringen af iPadOS til enhver stor udgivelse af operativsystemet. Evalueringer kan kun foretages i henhold til en offentligt publiceret version af operativsystemet.

Certificeringsstatus for Common Criteria (CC)

Den amerikanske ordning, der administreres af NIAP, vedligeholder listen Products in Evaluation (Produkter til evaluering). Denne liste omfatter produkter, som i øjeblikket evalueres i USA med et Common Criteria Testing Laboratory (CCTL), der er godkendt af NIAP, og som har afsluttet et evalueringskickoff-møde (eller tilsvarende), hvor CCEVS-ledelsen officielt godkendte produktet til evaluering.

Efter at produkter er blevet certificeret, anbringer NIAP aktuelle godkendte certificeringer på Product Compliant List (liste med produkter, der overholder standarderne). Efter 2 år gennemgås disse certificeringer for at afklare, om de efterlever den aktuelle sikkerhedsvedligeholdelsespolitik. Når datoen for sikkerhedsvedligeholdelsen er udløbet, flytter NIAP certificeringsoptegnelsen til listen Archived Products (arkiverede produkter).

På Common Criteria Portal vises de certificeringer, der kan blive gensidigt godkendt i henhold til Common Criteria Recognition Arrangement (CCRA). CC-portalen kan vedligeholde produkter på listen med certificerede produkter i 5 år, og fortegnelser om arkiverede certificeringer opbevares på CC-portalen.

Tabellen herunder viser de certificeringer, der er ved at blive evalueret af et laboratorium, og de certificeringer, hvis overholdelse af Common Criteria er færdigbehandlet.

Aktuel status

Laboratorietest af iPadOS 15 til evaluering af NIAP er undervejs. De nyeste oplysninger kan ses på listen Products in evaluation (NIAP) (produkter under evaluering) og Product Compliant List (liste med produkter, der overholder standarderne).

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: iPadOS 15 *Certificeringsdato:* 14-03-2019	*Skema-id:* — *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* iPad med iOS 12 *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, modul til VPN-klient, EP til trådløs LAN-klient, EP til MDM-agent
Operativsystem: iPadOS 14 *Certificeringsdato:* 01-09-2021	*Skema-id:* 11147 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple iPadOS 14: iPad-modeller *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, modul til VPN-klient, EP til trådløs LAN-klient, EP til MDM-agent
Operativsystem: iPadOS 13 *Certificeringsdato:* 06-11-2020	*Skema-id:* 11036 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* iPadOS 13 på mobile iPad-enheder *Beskyttelsesprofiler:* Grundlæggende om mobile enheder, modul til VPN-klient, EP til trådløs LAN-klient, EP til MDM-agent

Tidligere versioner

Disse tidligere versioner af iOS havde Common Criteria-valideringer. De er arkiveret af NIAP som fastlagt i NIAPs politik:

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

Sikkerhedscertificeringer til macOS

Baggrund for macOS-certificering

Apple deltager aktivt i valideringen af Apple-operativsystemer ved hver store udgivelse af et operativsystem ved hjælp af passende samarbejdende beskyttelsesprofiler og FIPS 140-3-sikkerhedsniveauer. Validering af overensstemmelse kan kun udføres i henhold til en endelig publiceret version.

Status for validering af kryptografimoduler til macOS

Cryptographic Module Validation Program (CMVP) vedligeholder kryptografimodulers valideringsstatus på tre forskellige lister afhængigt af deres aktuelle status:

- For at komme på CMVP-listen Implementation Under Test skal laboratoriet have en aftale med Apple om at foretage test.
- Når laboratoriet har afsluttet sine test og har anbefalet validering af CMVP, og CMVP-betalingen er foretaget, føjes modulet til listen Modules in Process (MIP). Listen MIP følger CMVP-valideringens fremgang i fire faser:
  - *Gennemgang under behandling:* Afventer at CMVP-ressource tildeles.
  - *Til gennemgang:* CMVP-ressourcerne udfører valideringsaktiviteterne.
  - *Koordinering:* Laboratoriet og CMVP løser eventuelle problemer.
  - *Afslutning:* Aktiviteter og formaliteter i forbindelse med udstedelsen af certifikatet.
- Efter valideringen af CMVP tildeles modulerne et konformitetscertifikat og føjes til listen over validerede kryptografimoduler. Det omfatter:
  - Validerede moduler, der er markeret som aktive.
  - Efter 5 år bliver modulerne markeret som historiske.
  - Hvis modulcertifikatet skulle blive tilbagekaldt, markeres det som tilbagekaldt.

I 2020 indførte CMVP den internationale standard ISO/IEC 19790 som basis for FIPS 140-3.

Tabellen nedenfor viser, hvilke kryptografimoduler der bruges til hvilken Mac-teknologi i Apple Mac-computere.

Kryptografimodul	Mac-computere med Apple Silicon	Mac-computere med Apple T2-sikkerhedschip	Intel-baserede Mac-computere med Apple T2-sikkerhedschip
Apple Silicon-brugerområde	✓		
Apple Silicon-kerne	✓		
Intel-brugerområde		✓	✓
Intel-kerne		✓	✓
Secure Key Store	✓	✓	

FIPS 140-3-certificeringer

I 2020 lancerede Apple Mac-computere baseret på Apple Silicon. Kolonnen Info om modul i tabellen herunder viser, om kryptografimoduler gælder for Mac-computere med Apple Silicon eller Intel-baserede Mac-computere.

Bemærk: Apple T2-sikkerhedschippen findes i mange Intel-baserede Mac-computere. Se Sikkerhedscertificeringer for Apple T2-sikkerhedschippen, hvis du vil læse om certificeringer af T2-chippen.

SSH-klient i macOS

OpenSSH kan konfigureres til brug af FIPS 140-3-validerede moduler med udvalgte FIPS 140-3-algoritmer. Organisationer kan afvikle en signeret og notariseret installeringsapp, som er tilgængelig fra Apple med adgangskoden *FIPS140Mode*. Installeringsappen placerer to arkiver på Mac-computeren:

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

macOS bruger derefter disse arkiver til at begrænse de koder, der er tilgængelige til OpenSSH, til dem, der er godkendt af NIST, og sikrer, at OpenSSH-klienten bruger platformens godkendte kryptografimodul. Administratorer kan også oprette deres egne arkiver. Du kan få flere oplysninger på man-siden `apple_ssh_and_fips` i macOS 12.0.1 eller en nyere version.

Aktuel status

Brugerområde, kerneområde og Secure Key Store til macOS 11 Big Sur har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Brugerområde, kerneområde og Secure Key Store i macOS 12 Monterey gennemgår laboratorietest. De er anført på listen Implementation Under Test List.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Apple Silicon *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Apple Silicon *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Intel *Miljø:* Intel, Bruger, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Intel *Miljø:* Intel, Kerne, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS distribueret med macOS 12 Monterey på Apple Silicon, sepOS distribueret med macOS 12 Monterey på Intel med T2 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (M1 og T2) *Sikkerhedsniveau:* 2

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS distribueret med macOS 12 Monterey på Apple Silicon *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (M1) *Sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Intel *Miljø:* Intel, Bruger, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Intel *Miljø:* Intel, Kerne, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Apple Silicon *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Apple Silicon *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med macOS 11 Big Sur på Apple Silicon, sepOS distribueret med macOS 11 Big Sur på Intel *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (M1) *Sikkerhedsniveau:* 2

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med macOS 11 Big Sur på Apple Silicon *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (M1) *Sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3

FIPS 140-2-certificeringer

Tabellen herunder viser de kryptografimoduler, der er ved at blive eller er blevet testet af laboratoriet med hensyn til overholdelse af FIPS 140-2.

Brugerområde, kerneområde og Secure Key Store til macOS 10.15 Catalina har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Bemærk: Apple T2-sikkerhedschippen findes på mange Intel-baserede Mac-computere. Se Sikkerhedscertificeringer for Apple T2-sikkerhedschippen, hvis du vil læse om certificeringer af T2-chippen.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 24-03-2021	*Certifikater:* 3859 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Space Module til Intel (ccv10) *Operativsystem:* macOS 10.15 Catalina *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 24-03-2021	*Certifikater:* 3858 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v10.0 til Intel (ccv10) *Operativsystem:* macOS 10.15 Catalina *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 12-04-2019	*Certifikater:* 3402 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v9.0 til Intel *Operativsystem:* macOS 10.14 Mojave *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 12-04-2019	*Certifikater:* 3431 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v9.0 til Intel *Operativsystem:* macOS 10.14 Mojave *Type:* Software *Sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 22-03-2018	*Certifikater:* 3155 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v8.0 til Intel *Operativsystem:* macOS 10.13 High Sierra *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 22-03-2018	*Certifikater:* 3156 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v8.0 til Intel *Operativsystem:* macOS 10.13 High Sierra *Type:* Software *Sikkerhedsniveau:* 1

Tidligere versioner

Disse tidligere versioner af OS X og macOS havde valideringer af kryptografimoduler. De, der er ældre end 5 år, angives at have historisk status af 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

Baggrund for Common Criteria-certificeringer (CC)

Apple deltager aktivt i evalueringen af macOS til enhver stor udgivelse af operativsystemet. Evalueringer kan kun foretages i henhold til en offentligt publiceret version af operativsystemet.

Certificeringsstatus for Common Criteria (CC)

Den amerikanske ordning, der administreres af NIAP, vedligeholder listen Products in Evaluation (Produkter til evaluering). Denne liste omfatter produkter, som i øjeblikket evalueres i USA med et Common Criteria Testing Laboratory (CCTL), der er godkendt af NIAP, og som har afsluttet et evalueringskickoff-møde (eller tilsvarende), hvor CCEVS-ledelsen officielt godkendte produktet til evaluering.

Efter at produkter er blevet certificeret, anbringer NIAP aktuelle godkendte certificeringer på Product Compliant List (liste med produkter, der overholder standarderne). Efter 2 år gennemgås disse certificeringer for at afklare, om de efterlever den aktuelle sikkerhedsvedligeholdelsespolitik. Når datoen for sikkerhedsvedligeholdelsen er udløbet, flytter NIAP certificeringsoptegnelsen til listen Archived Products (arkiverede produkter).

På Common Criteria Portal vises de certificeringer, der kan blive gensidigt godkendt i henhold til Common Criteria Recognition Arrangement (CCRA). CC-portalen kan vedligeholde produkter på listen med certificerede produkter i 5 år, og fortegnelser om arkiverede certificeringer opbevares på CC-portalen.

Tabellen herunder viser de certificeringer, der er ved at blive evalueret af et laboratorium, og de certificeringer, hvis overholdelse af Common Criteria er færdigbehandlet.

Aktuel status

NIAP-evalueringer af macOS 11 og macOS 12 med beskyttelsesprofilerne General Purpose Operating System og Full Disk Encryption (FDE) (AA og EE) er på vej.

De nyeste oplysninger kan ses på listen Products in evaluation (NIAP) (produkter under evaluering) og Product Compliant List (liste med produkter, der overholder standarderne).

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: macOS 12 Monterey *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* —	*Titel:* Apple FileVault 2 med macOS 12 Monterey *Beskyttelsesprofiler:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP'er endnu ikke bekræftet)
Operativsystem: macOS 12 Monterey *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* —	*Titel:* macOS 12 Monterey *Beskyttelsesprofiler:* PP_OS_V4.21 (PP'er endnu ikke bekræftet)
Operativsystem: macOS 11 Big Sur *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple FileVault 2 med macOS 11 Big Sur *Beskyttelsesprofiler:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: macOS 11 Big Sur *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple macOS 11 Big Sur *Beskyttelsesprofiler:* PP_OS_V4.21
Operativsystem: macOS 10.15 Catalina *Certificeringsdato:* 29-04-2021	*Skema-id:* 11078 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple FileVault 2 på T2-computere med macOS 10.15 Catalina *Beskyttelsesprofiler:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Operativsystem: macOS 10.15 Catalina *Certificeringsdato:* 23-09-2020	*Skema-id:* 11077 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* macOS 10.15 Catalina *Beskyttelsesprofiler:* PP_OS_V4.21

Sikkerhedscertificeringer til tvOS

Baggrund for tvOS-certificering

Apple deltager aktivt i valideringen af kryptografimodulerne til enhver stor udgivelse af tvOS. Validering af overensstemmelse kan kun udføres i henhold til en endelig publiceret version.

Status for validering af kryptografimoduler til tvOS

Cryptographic Module Validation Program (CMVP) vedligeholder kryptografimodulers valideringsstatus på tre forskellige lister afhængigt af deres aktuelle status:

- For at komme på CMVP-listen Implementation Under Test skal laboratoriet have en aftale med Apple om at foretage test.
- Når laboratoriet har afsluttet sine test og har anbefalet validering af CMVP, og CMVP-betalingen er foretaget, føjes modulet til listen Modules in Process (MIP). Listen MIP følger CMVP-valideringens fremgang i fire faser:
  - *Gennemgang under behandling:* Afventer at CMVP-ressource tildeles.
  - *Til gennemgang:* CMVP-ressourcerne udfører valideringsaktiviteterne.
  - *Koordinering:* Laboratoriet og CMVP løser eventuelle problemer.
  - *Afslutning:* Aktiviteter og formaliteter i forbindelse med udstedelsen af certifikatet.
- Efter valideringen af CMVP tildeles modulerne et konformitetscertifikat og føjes til listen over validerede kryptografimoduler. Det omfatter:
  - Validerede moduler, der er markeret som aktive.
  - Efter 5 år bliver modulerne markeret som historiske.
  - Hvis modulcertifikatet skulle blive tilbagekaldt, markeres det som tilbagekaldt.

I 2020 indførte CMVP den internationale standard ISO/IEC 19790 som basis for FIPS 140-3.

FIPS 140-3-certificeringer

Aktuel status

Brugerområde, kerneområde og Secure Key Store til tvOS 14 (2020) har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Brugerområde, kerneområde og Secure Key Store i tvOS 15 (2021) gennemgår laboratorietest. De er anført på listen Implementation Under Test List.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* tvOS 15 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* tvOS 15 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribueret med tvOS 15 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A10, A12) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* tvOS 14 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* tvOS 14 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med tvOS 14 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (A10, A12) *Overordnet sikkerhedsniveau:* 2

FIPS 140-2-certificeringer

Tabellen herunder viser de kryptografimoduler, der er ved at blive eller er blevet testet af laboratoriet med hensyn til overholdelse af FIPS 140-2.

Brugerområde, kerneområde og Secure Key Store til tvOS 13 (2019) har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3856 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v10.0 til ARM *Operativsystem:* tvOS 13 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 23-03-2021	*Certifikater:* 3855 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v10.0 til ARM *Operativsystem:* tvOS 13 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 05-02-2021	*Certifikater:* 3811 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribueret med tvOS 13 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 23-04-2019	*Certifikater:* 3438 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v9.0 til ARM *Operativsystem:* tvOS 12 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 11-04-2019	*Certifikater:* 3433 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v9.0 til ARM *Operativsystem:* tvOS 12 *Type:* Software *Sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3523 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribueret med tvOS 12 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Certifikater:* 3148 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v8.0 til ARM *Operativsystem:* tvOS 11 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 17-05-2018, 03-07-2018	*Certifikater:* 3147 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v8.0 til ARM *Operativsystem:* tvOS 11 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3223 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribueret med tvOS 11 *Type:* Hardware *Sikkerhedsniveau:* 2

Sikkerhedscertificeringer til watchOS

Baggrund for watchOS-certificering

Apple deltager aktivt i valideringen af kryptografimodulerne til enhver stor udgivelse af watchOS. Validering af overensstemmelse kan kun udføres i henhold til en endelig publiceret version.

Status for validering af kryptografimoduler til watchOS

Cryptographic Module Validation Program (CMVP) vedligeholder kryptografimodulers valideringsstatus på tre forskellige lister afhængigt af deres aktuelle status:

- For at komme på CMVP-listen Implementation Under Test skal laboratoriet have en aftale med Apple om at foretage test.
- Når laboratoriet har afsluttet sine test og har anbefalet validering af CMVP, og CMVP-betalingen er foretaget, føjes modulet til listen Modules in Process (MIP). Listen MIP følger CMVP-valideringens fremgang i fire faser:
  - *Gennemgang under behandling:* Afventer at CMVP-ressource tildeles.
  - *Til gennemgang:* CMVP-ressourcerne udfører valideringsaktiviteterne.
  - *Koordinering:* Laboratoriet og CMVP løser eventuelle problemer.
  - *Afslutning:* Aktiviteter og formaliteter i forbindelse med udstedelsen af certifikatet.
- Efter valideringen af CMVP tildeles modulerne et konformitetscertifikat og føjes til listen over validerede kryptografimoduler. Det omfatter:
  - Validerede moduler, der er markeret som aktive.
  - Efter 5 år bliver modulerne markeret som historiske.
  - Hvis modulcertifikatet skulle blive tilbagekaldt, markeres det som tilbagekaldt.

I 2020 indførte CMVP den internationale standard ISO/IEC 19790 som basis for FIPS 140-3.

FIPS 140-3-certificeringer

Aktuel status

Brugerområde, kerneområde og Secure Key Store til watchOS 7 (2020) har gennemgået laboratorietest og er blevet anbefalet af laboratoriet til CMVP-validering. De er anført på listen Modules in Process (listen med igangværende moduler).

Brugerområde, kerneområde og Secure Key Store i watchOS 8 (2021) gennemgår laboratorietest. De er anført på listen Implementation Under Test List.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* watchOS 8 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* watchOS 8 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribueret med watchOS 8 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (S3, S4, S5, S6) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2021 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribueret med watchOS 8 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (S6) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* watchOS 7 *Miljø:* Apple Silicon, Bruger, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* watchOS 7 *Miljø:* Apple Silicon, Kerne, Software *Type:* Software *Overordnet sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med watchOS 7 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (S3, S4, S5, S6) *Overordnet sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2020 *Valideringsdatoer:* —	*Certifikater:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribueret med watchOS 7 *Miljø:* Apple Silicon, Secure Key Store, Hardware *Type:* Hardware (S6) *Overordnet sikkerhedsniveau:* 2 *Fysisk sikkerhedsniveau:* 3

FIPS 140-2-certificeringer

Tabellen herunder viser de kryptografimoduler, der er ved at blive eller er blevet testet af laboratoriet med hensyn til overholdelse af FIPS 140-2.

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* —	*Certifikater:* 3856 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v10.0 til ARM *Operativsystem:* watchOS 6 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* —	*Certifikater:* 3855 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v10.0 til ARM *Operativsystem:* watchOS 6 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2019 *Valideringsdatoer:* 05-02-2021	*Certifikater:* 3811 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribueret med watchOS 6 *Type:* Hardware *Sikkerhedsniveau:* 2

Datoer	Certifikater/dokumenter	Info om modul
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 23-04-2019	*Certifikater:* 3438 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v9.0 til ARM *Operativsystem:* watchOS 5 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 11-04-2019	*Certifikater:* 3433 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v9.0 til ARM *Operativsystem:* watchOS 5 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2018 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3523 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribueret med watchOS 5 *Type:* Hardware *Sikkerhedsniveau:* 2
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 22.05.2018, 06.07.2018	*Certifikater:* 3148 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto User Module v8.0 til ARM *Operativsystem:* watchOS 4 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 09.03.2018, 17-05-2018, 03-07-2018	*Certifikater:* 3147 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Corecrypto Kernel Module v8.0 til ARM *Operativsystem:* watchOS 4 *Type:* Software *Sikkerhedsniveau:* 1
Operativsystems udgivelsesdato: 2017 *Valideringsdatoer:* 10-09-2019	*Certifikater:* 3223 *Dokumenter:* Certifikat Sikkerhedspolitik Vejledning til Crypto Officer	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribueret med watchOS 4 *Type:* Hardware *Sikkerhedsniveau:* 2

Sikkerhedscertificeringer til software

Oversigt over sikkerhedscertificeringer til Apple-software

Apple vedligeholder valideringscertifikater for overensstemmelse med FIPS (Federal Information Processing Standard) 140-2/-3 til sepOS og T2-firmware samt andre certificeringer. Apple starter med *certificeringsbyggesten*, der anvendes bredt på flere platforme, hvor det er relevant. En af byggestenene er valideringen af corecrypto, der bruges til implementering af software- og hardwarekryptografimoduler i operativsystemer udviklet af Apple. En anden byggesten er certificeringen af Secure Enclave, som er integreret i mange Apple-enheder. En tredje er certificeringen af Secure Element (SE), der findes i Apple-enheder med Touch ID og enheder med Face ID. Disse byggesten til hardwarecertificeringer danner grundlag for bredere certificeringer af platformsikkerhed.

Produktcertificeringer: (Common Criteria ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) er en standard, som mange organisationer bruger som grundlag for sikkerhedsevalueringer af IT-produkter.

På Common Criteria Portal kan du se certificeringer, der kan være opnået i kraft af gensidig anerkendelse i henhold til den internationale CCRA-aftale (Common Criteria Recognition Arrangement). Common Criteria-standarden kan også bruges uden for CCRA af nationale og private valideringsordninger. I Europa er gensidig anerkendelse underlagt både SOG-IS-aftalen og CCRA.

Målet er ifølge Common Criteria-fællesskabet at opnå et internationalt godkendt sæt sikkerhedsstandarder, der kan levere en tydelig og pålidelig evaluering af IT-produkters sikkerhedsfunktioner. Common Criteria-certificering er en uafhængig vurdering af et produkts opfyldelse af sikkerhedsstandarder, der giver kunderne større tillid til IT-produkters sikkerhed og danner grundlag for kvalificerede beslutninger.

Medlemslande har via CCRA aftalt at anerkende certificeringen af IT-produkter med samme niveau af tillid. Evalueringer, der er nødvendige inden certificering, er omkostningskrævende og inkluderer:

- Beskyttelsesprofiler (PP'er)
- Sikkerhedsmål (ST'er)
- Funktionelle krav til sikkerhed (SFR'er)
- Security Assurance Requirements (SAR'er)
- Evaluation Assurance Levels (EAL'er)

Beskyttelsesprofiler (PP'er) er dokumenter, som angiver sikkerhedskravene for en bestemt klasse enhedstyper (f.eks. Mobilitet), og de bruges til at skabe et sammenligningsgrundlag for evalueringer af IT-produkter, der tilhører samme klasse. Antallet af medlemmer af CCRA og listen med godkendte PP'er øges hvert år. Denne ordning giver en produktudvikler mulighed for at sigte efter en enkelt certificering i henhold til en af certificeringsgodkendelsesordningerne og få den godkendt af en hvilken som helst forbruger, der har skrevet under på certifikatet.

Sikkerhedsmål (ST'er) definerer, *hvad* der skal evalueres, når et IT-produkt skal certificeres. ST'erne omsættes til mere specifikke *funktionelle krav til sikkerhed (SFR'er)*, der bruges til at evaluere detaljerne i ST'erne.

Common Criteria (CC) inkluderer også *Security Assurance Requirements (SAR'er)*. En fælles måling er *Evaluation Assurance Level (EAL)* – garantimålet for evalueringen. EAL'er grupperer hyppigt anvendte sæt Security Assurance Requirements og kan anføres i PP'er og ST'er for at lette sammenligninger.

Mange af de tidligere PP'er er blevet arkiveret og bliver erstattet af målrettede PP'er, der er ved at blive udviklet og har fokus på bestemte løsninger og miljøer. I en fælles indsats for at sikre, at den gensidige anerkendelse mellem alle CCRA-medlemmer fortsætter, er internationale tekniske fællesskaber (iTC'er) blevet oprettet for at udvikle og vedligeholde samarbejdende beskyttelsesprofiler (cPP'er), som fra starten er udviklet i samarbejde med deltagere, der har underskrevet CCRA-ordninger. PP'er rettet mod brugergrupper og andre ordninger om gensidig anerkendelse end CCRA udvikles fortsat af behørige interessenter.

Apple begyndte at søge om certificeringer i henhold til den opdaterede CCRA med udvalgte cPP'er i starten af 2015. Siden da har Apple opnået Common Criteria-certificeringer for hver større version af iOS og har udvidet dækningen til at omfatte det sikkerhedsniveau, der leveres af nye PP'er.

Apple påtager sig en aktiv rolle i de tekniske fællesskaber med fokus på evaluering af sikkerhedsteknologi til mobile enheder. De omfatter blandt andet de iTC'er, der har ansvaret for at udvikle og opdatere cPP'er. Apple fortsætter med at evaluere og stræbe efter certificeringer for nuværende PP'er og cPP'er.

Certificeringer til Apple-platforme til det nordamerikanske marked foretages normalt sammen med National Information Assurance Partnership (NIAP), som vedligeholder en liste med projekter, der er ved at blive evalueret, men endnu ikke er certificeret.

Ud over de anførte generelle platformcertifikater er der udstedt andre certifikater, der har til formål at påvise opfyldelse af særlige sikkerhedskrav til visse markeder.

Sikkerhedscertificeringer til Apple-programmer og -apps

Baggrund for certificering af apps og programmer fra Apple

Apple deltager aktivt i sikkerhedscertificeringer af sine programmer og apps ved hjælp af passende Common Criteria-beskyttelsesprofiler (PP'er). Disse evalueringer bygger på hardware- og operativsystemcertificeringer, som Apple har opnået.

I 2018 igangsatte Apple evalueringer af sikkerheden for nøgleapps i iOS 11 med Safari-browseren og appen Kontakter. Apple fortsatte disse evalueringer af apps i iOS 12, iOS 13 og iPadOS 13.1. I 2021 tilføjes dækning af apps i macOS 11.

Valideringsstatus for kryptografimoduler

Apple bruger kryptografimodulerne vist her til det relevante operativsystem. Du kan få flere oplysninger under Sikkerhedscertificeringer til iOS, Sikkerhedscertificeringer til iPadOS og Sikkerhedscertificeringer til macOS.

Certificeringsstatus for Common Criteria (CC)

Den amerikanske ordning, der administreres af NIAP, vedligeholder listen Products in Evaluation (Produkter til evaluering). Denne liste omfatter produkter, som i øjeblikket evalueres i USA med et Common Criteria Testing Laboratory (CCTL), der er godkendt af NIAP, og som har afsluttet et evalueringskickoff-møde (eller tilsvarende), hvor CCEVS-ledelsen officielt godkendte produktet til evaluering.

Efter at produkter er blevet certificeret, anbringer NIAP aktuelle godkendte certificeringer på Product Compliant List (liste med produkter, der overholder standarderne). Efter 2 år gennemgås disse certificeringer for at afklare, om de efterlever den aktuelle sikkerhedsvedligeholdelsespolitik. Når datoen for sikkerhedsvedligeholdelsen er udløbet, flytter NIAP certificeringsoptegnelsen til listen Archived Products (arkiverede produkter).

På Common Criteria Portal vises de certificeringer, der kan blive gensidigt godkendt i henhold til Common Criteria Recognition Arrangement (CCRA). CC-portalen kan vedligeholde produkter på listen med certificerede produkter i 5 år, og fortegnelser om arkiverede certificeringer opbevares på CC-portalen.

Tabellen herunder viser de certificeringer, der er ved at blive evalueret af et laboratorium, og de certificeringer, hvis overholdelse af Common Criteria er færdigbehandlet.

Aktuel status

- Evalueringer med NIAP, der offentliggøres som undervejs, kan ses på Products in Evaluation (NIAP) (produkter under evaluering).
- Evalueringer, som er blevet gennemført og valideret, vises på NIAP's Product Compliant List (liste med produkter, der overholder standarderne).

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: macOS 11 Big Sur *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* macOS 11 Big Sur: Kontakter *Beskyttelsesprofiler:* Beskyttelsesprofiler til programsoftware, EP til webbrowsere
Operativsystem: macOS 11 Big Sur *Certificeringsdato:* —	*Skema-id:* Endnu ikke certificeret *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* macOS 11 Big Sur: Safari *Beskyttelsesprofiler:* Beskyttelsesprofiler til programsoftware, EP til webbrowsere
Operativsystem: iOS 14, iPadOS 14 *Certificeringsdato:* 20-08-2021	*Skema-id:* 11191 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple iOS 14 og iPadOS 14: Kontakter *Beskyttelsesprofiler:* Beskyttelsesprofiler til programsoftware, EP til webbrowsere
Operativsystem: iOS 14, iPadOS 14 *Certificeringsdato:* —	*Skema-id:* 11192 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple iOS 14 og iPadOS 14: Safari *Beskyttelsesprofiler:* Beskyttelsesprofiler til programsoftware, EP til webbrowsere
Operativsystem: iOS 13, iPadOS 13 *Certificeringsdato:* 05-06-2020	*Skema-id:* 11060 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple iOS 13 og iPadOS 13: Safari *Beskyttelsesprofiler:* Beskyttelsesprofiler til programsoftware, EP til webbrowsere

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: iOS 13, iPadOS 13 *Certificeringsdato:* 05-06-2020	*Skema-id:* 11050 *Dokumenter:* Certifikat Sikkerhedsmål Vejledning Valideringsrapport Rapport om sikkerhedsaktivitet	*Titel:* Apple iOS 13 og iPadOS 13: Kontakter *Beskyttelsesprofiler:* Beskyttelsesprofil til programsoftware

Arkiverede Common Criteria-certificeringer til Apple-programmer og -apps

Operativsystem/certificeringsdato	Skema-id/dokumenter	Titel/beskyttelsesprofiler
Operativsystem: iOS 12 *Certificeringsdato:* 12-06-2019	*Skema-id:* 10960 *Dokumenter:* Sikkerhedsmål Vejledning	*Titel:* iOS 12 Safari *Beskyttelsesprofiler:* Beskyttelsesprofiler til programsoftware, EP til webbrowsere
Operativsystem: iOS 12 *Certificeringsdato:* 28-02-2019	*Skema-id:* 10961 *Dokumenter:* Sikkerhedsmål Vejledning	*Titel:* iOS 12 Kontakter *Beskyttelsesprofiler:* Beskyttelsesprofil til programsoftware
Operativsystem: iOS 11 *Certificeringsdato:* 09-11-2018	*Skema-id:* 10916 *Dokumenter:* Sikkerhedsmål Vejledning	*Titel:* iOS 11 Safari *Beskyttelsesprofiler:* Beskyttelsesprofiler til programsoftware, EP til webbrowsere
Operativsystem: iOS 11 *Certificeringsdato:* 13-09-2018	*Skema-id:* 10915 *Dokumenter:* Sikkerhedsmål Vejledning	*Titel:* iOS 11 Kontakter *Beskyttelsesprofiler:* Beskyttelsesprofil til programsoftware

Sikkerhedscertificeringer til Apples internettjenester

Apple opretholder certificeringer i overensstemmelse med ISO/IEC 27001- og ISO/IEC 27018-standarderne for at give Apples kunder mulighed for at opfylde deres lovgivnings- og kontraktmæssige forpligtelser. Disse certificeringer forsyner vores kunder med et uafhængigt vidnesbyrd om Apples praksis med hensyn til informationssikkerhed og anonymitet for behandlede systemer.

ISO/IEC 27001 og ISO/IEC 27018 er en del af en gruppe standarder til Information Security Management System (ISMS), som offentliggøres af International Organization for Standardization (ISO). Som en del af Apples ISMS er alle kontrolkrav i bilag A inkluderet i Statement of Applicability som defineret i ISO/IEC 27001- og ISO/IEC 27018-standarderne. Apple gennemgår en uafhængig attestering foretaget af en bemyndiget registrator hvert år.

ISO/IEC 27001

ISO/IEC 27001 er en Information Security Management System-standard, som angiver krav for etablering, implementering, vedligeholdelse og vedvarende forbedring af en organisations Information Security Management System. ISO/IEC 27001-standarden omfatter følgende sikkerhedsdomæner, der er dækket af Apples ISO/IEC-certificeringer:

- Politikker for informationssikkerhed
- Organisering af informationssikkerhed
- Aktivadministration
- Human resources-sikkerhed
- Fysisk og miljømæssig sikkerhed
- Kommunikations- og driftsadministration
- Adgangskontrol
- Anskaffelse, udvikling og vedligeholdelse af informationssystemer
- Administration af informationssikkerhedshændelser
- Administration af forretningskontinuitet
- Compliance

ISO/IEC 27018

ISO/IEC 27018 er en fremgangsmåde til beskyttelse af personligt identificerbare informationer (PII) i offentlige skymiljøer. ISO/IEC 27018-standarden omfatter følgende sikkerhedsdomæner, der er dækket af Apples ISO/IEC-certificeringer:

- Samtykke og valg
- Legitimering og specificering af formål
- Indsamlingsbegrænsning
- Dataminimering
- Begrænsninger for brug, bevarelse og offentliggørelse
- Nøjagtighed og kvalitet
- Åbenhed, transparens og opsigelse
- Individuel deltagelse og adgang
- Ansvarlighed
- Informationssikkerhed
- Overholdelse af anonymitet

Apple-tjenester, der er dækket af ISO/IEC 27001 og ISO/IEC 27018

Apples ISO/IEC 27001- og ISO/IEC 27018-certificeringer dækker følgende tjenester:

- Apple Business Chat
- Apple Business Manager
- APNs (Apple Push Notification service)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork-tjenester
- Administrerede Apple-id'er
- Skolearbejde
- Siri

Certificeringer

Beviser for Apples ISO/IEC 27001- og 27018-certificeringer er tilgængelige hos vores registrator.

Hvis du vil se Apples certificeringer, kan du gå til Certificate and Client Directory search på webstedet for British Standards Institution (BSI), skrive Apple i søgefeltet Company, klikke på knappen Search og derefter vælge søgeresultaterne for at se certifikaterne.

Bemærk: Informationer om produkter, der ikke er fremstillet af Apple, eller uafhængige websteder, der ikke kontrolleres eller testes af Apple, leveres uden anbefaling eller godkendelse. Apple påtager sig intet ansvar med hensyn til indsamling, ydeevne eller brug af tredjepartswebsteder eller -produkter. Apple yder ingen garantier med hensyn til tredjepartswebsteders nøjagtighed og pålidelighed. Kontakt leverandøren for at få flere oplysninger.

macOS Security Compliance Project

macOS Security Compliance Project (mSCP) er et open source-forsøg på at levere en programstyret metode til generering af sikkerhedsvejledning. Dette er et fælles projekt, der involverer driftsmedarbejdere inden for it-sikkerhed 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). Projektet bruger et sæt af testede og validerede foranstaltninger til macOS og anvender disse foranstaltninger på sikkerhedsvejledninger, der understøttes af projektet. Dette projekt kan også bruges som en ressource til nemt at oprette tilpasset sikkerhedsgrundlag fra tekniske sikkerhedsforanstaltninger ved at udnytte et bibliotek af testede og validerede atomiske handlinger (konfigurationsindstillinger). Projektet giver et output af tilpasset dokumentation, tilpassede instrukser, konfigurationsprofiler og en testtjekliste baseret på det brugte grundlag.

mSCP kan producere output-indhold, der kan bruges sammen med administrations- og sikkerhedsværktøjer med henblik på at opnå compliance. Konfigurationsindstillinger i dette projekt understøtter følgende vejledningsgrundlag:

Organisation	Understøttede grundlag
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 5	800-53 høj, 800-53 moderat, 800-53 lav
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

Yderligere oplysninger:

- Et grundlag til at gennemgå alle regler i projektet findes her.
- Du kan læse mere om projektet og brug her: macOS Security Compliance Project wiki.
- Læs mere om indstilling af projektet til brug her: Getting to Know the macOS Security Compliance Project, Part 1 og Getting to Know the macOS Security Compliance Project, Part 2.
- Hvis du er interesseret i at bidrage til udvikling af projektet, kan du se flere oplysninger under vejledning til bidragydere.

Revisionshistorik for dokument

Dato	Oversigt
27. oktober 2021	Emner opdateret: • Sikkerhedscertificeringer til Secure Enclave Processor • Sikkerhedscertificeringer til iOS • Sikkerhedscertificeringer til macOS
17. august 2021	Emner opdateret: • Sikkerhedscertificeringer til Secure Enclave Processor • Sikkerhedscertificeringer for Apple T2-sikkerhedschippen • Sikkerhedscertificeringer til iOS • Sikkerhedscertificeringer til iPadOS • Sikkerhedscertificeringer til macOS • Sikkerhedscertificeringer til tvOS • Sikkerhedscertificeringer til watchOS • Sikkerhedscertificeringer til Apple-programmer og -apps • Sikkerhedscertificeringer • macOS Security Compliance Project
26. april 2021	Emne tilføjet: • macOS Security Compliance Project Emner opdateret: • Sikkerhedscertificeringer for Apple T2-sikkerhedschippen: Ny FIPS 140-2-certificering, 3811 • Sikkerhedscertificeringer til Secure Enclave Processor: Ny FIPS 140-2-certificering, 3811 og ny tabel til yderligere certificeringer. • Sikkerhedscertificeringer til iOS: Nye FIPS 140-2-certificeringer, 3811, skema-id 11146 til iOS 14 under evaluering • Sikkerhedscertificeringer til iPadOS: Nye FIPS 140-2-certificeringer, 3811, skema-id 11147 til iPadOS 14 under evaluering • Sikkerhedscertificeringer til macOS: Ny FIPS 140-2-certificering, 3811. • Sikkerhedscertificeringer til tvOS: Nye FIPS 140-2-certificeringer, 3811. • Sikkerhedscertificeringer til watchOS: Nye FIPS 140-2-certificeringer, 3811. • Sikkerhedscertificeringer til Apple-programmer og -apps: Opdateringer til Common Criteria-status og ny tabel til arkiverede Common Criteria-certificeringer.

Ordliste

administration af mobile enheder (MDM) En tjeneste, der giver brugeren mulighed for at administrere tilmeldte enheder eksternt. Når en enhed er tilmeldt, kan brugeren benytte MDM-tjenesten til at konfigurere indstillinger og udføre andre opgaver på enheden via netværket uden selv at gøre noget.

APNs (Apple Push Notification service) En tjeneste, som Apple tilbyder i hele verden, der sørger for push-meddelelser til Apple-enheder.

Apple Business Manager En simpel webbaseret portal til IT-administratorer, der sætter organisationer i stand til på en hurtig og ensartet måde at implementere Apple-enheder, som organisationerne har købt direkte fra Apple eller via autoriserede Apple-forhandlere eller -udbydere, der deltager i programmet. De kan automatisk tilmelde enheder til deres løsning til administration af mobile enheder (MDM) uden at røre eller klargøre enhederne fysisk, før brugerne får dem.

Apple School Manager En simpel webbaseret portal til IT-administratorer, der sætter organisationer i stand til på en hurtig og ensartet måde at implementere Apple-enheder, som organisationerne har købt direkte fra Apple eller via autoriserede Apple-forhandlere eller -udbydere, der deltager i programmet. De kan automatisk tilmelde enheder til deres løsning til administration af mobile enheder (MDM) uden at røre eller klargøre enhederne fysisk, før brugerne får dem.

Beskyttelsesprofil (PP) Et dokument, der beskriver problemer og krav i forbindelse med sikkerheden for en bestemt type produkter.

Common Criteria (CC) En standard, der fastlægger de almindelige begreber og principper inden for evaluering af IT-sikkerhed og beskriver en almindelig evalueringsmetode. Den inkluderer kataloger med sikkerhedskrav på et standardiseret sprog.

Common Criteria Recognition Arrangement (CCRA) En ordning om gensidig anerkendelse, der fastlægger politikkerne og kravene til international anerkendelse af certifikater udstedt i overensstemmelse med ISO/IEC 15408-serien eller Common Criteria-standarder.

corecrypto Et bibliotek, der leverer implementeringer af kryptografiske primitiver på lavt niveau. Bemærk, at corecrypto ikke leverer programmeringsgrænseflader direkte til udviklere, men bruges via API'er, der stilles til rådighed for udviklere. Kildekoden til corecrypto er offentligt tilgængelig, hvilket gør det muligt at kontrollere dens sikkerhedsegenskaber og korrekte virkemåde.

Cryptographic Algorithm Validation Program (CAVP) En organisation, der drives af NIST med henblik på at yde leveringstest af godkendte (f.eks. godkendt af FIPS og anbefalet af NIST) kryptografiske algoritmer og deres enkelte komponenter.

Cryptographic Module Validation Program (CMVP) En organisation, der drives af myndighederne i USA og Canada og har til formål at kontrollere, at FIPS 140-3-standarden overholdes.

Federal Information Processing Standard (FIPS) Publikationer, der udarbejdes af National Institute of Standards and Technology, enten som følge af lovkrav og/eller på grund af myndighedernes uomgængelige krav til cybersikkerhed.

Full Disk Encryption (FDE) Kryptering af alle data på en lagringsenhed.

Implementation under Test (IUT) Et kryptografimodul, der testes af et laboratorium.

Information Security Management System (ISMS) Et sæt sikkerhedspolitikker og -procedurer, der definerer afgrænsningen af et sikkerhedsprogram, der har til formål at beskytte en række oplysninger og systemer, ved at informationssikkerheden administreres systematisk i hele oplysningernes og systemernes levetid.

international Technical Community (iTC) En gruppe, der er underlagt Common Criteria Recognition Arrangement (CCRA) og har ansvaret for at udvikle beskyttelsesprofiler eller samarbejdende beskyttelsesprofiler.

IPsec VPN-klient En klient i en beskyttelsesprofil, der sørger for en sikker IPsec-forbindelse mellem en fysisk eller virtuel værtsplatform og en ekstern lokalitet.

kryptografimodul Den hardware, software og/eller firmware, der stiller kryptografiske funktioner til rådighed og opfylder kravene til en anført kryptografimodulstandard.

Modules in Process (MIP) En liste, der vedligeholdes af CMVP (Cryptographic Module Validation Program) og består af kryptografimoduler, der er ved at blive valideret af CMVP.

National Information Assurance Partnership (NIAP) En organisation etableret af myndighederne i USA, der har ansvaret for at drive implementeringen i USA af Common Criteria-standarden og administrere NIAP Common Criteria Evaluation and Validation Scheme (CCEVS).

National Institute of Standards and Technology (NIST) En del af handelsministeriet i USA, som har ansvaret for at fremme forskning, standarder og teknologi inden for målinger.

samarbejdende beskyttelsesprofil (cPP) En beskyttelsesprofil, der er udviklet af et internationalt teknisk fællesskab bestående af en gruppe eksperter, der har til opgave at oprette cPP'er.

Secure Element (SE) En siliciumchip, der er integreret i mange Apple-enheder, og som understøtter funktioner som Apple Pay.

Secure Enclave Processor (SEP) En hjælpeprocessor, der indgår i en SoC (System on Chip).

Senior Officials Group Information Systems Security (SOG-IS) En gruppe, der administrerer en aftale om gensidig anerkendelse mellem flere europæiske lande.

sepOS Secure Enclave-firmwaren, der er baseret på en Apple-tilpasset version af L4-mikrokernen.

Sikkerhedsmål (ST) Et dokument, der beskriver problemer og krav i forbindelse med sikkerheden for et bestemt produkt.

Sikkerhedsniveau (SL) De fire overordnede sikkerhedsniveauer (1–4), der er defineret i ISO/IEC 19790 og beskriver sæt med relevante sikkerhedskrav. Niveau 4 har de strengeste krav.

SoC (System on Chip) Et integreret kredsløb (IC), der består af flere komponenter på en enkelt chip.

Statement of Applicability (SOA) Et dokument, der beskriver de sikkerhedsforanstaltninger, der er implementeret i et ISMS, og som fremstilles som led i en ISO/IEC 27001-certificering.

T2 En sikkerhedschip fra Apple, der siden 2017 findes i nogle Intel-baserede Mac-computere.

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

DK028-00499-B