Center för säkerhetscertifieringar och efterlevnad

December 2021

Innehåll

Introduktion till Apples säkerhetsförsäkran

Som en del av vårt engagemang för säkerhet samarbetar Apple regelbundet med tredjepartsorganisationer för att certifiera och attestera säkerheten hos Apples maskinvara, programvara och tjänster. Dessa internationellt erkända organisationer tillhandahåller Apple med certifieringar i samband med varje större versionslansering av operativsystem. På det sättet får de ett visst mått av tillförlitlighet, dvs. en säkerhetsförsäkran om att ett systems säkerhetsbehov uppfylls. För tekniska områden som inte accepteras av ömsesidiga avtal om erkännande (MRA:er), eller saknar heltäckande standarder för säkerhetscertifiering, arbetar Apple med att utveckla lämpliga säkerhetsstandarder. Vårt mål är att driva fram globalt accepterade och heltäckande säkerhetscertifieringar för all maskinvara, operativsystem, appar och tjänster från Apple.

Certifieringar är ofta nödvändiga för att uppfylla krav i lagstiftning, regelverk och branschstandarder. Tjänster som Apple School Manager och Apple Business Manager täcks av Apples ISO/IEC 27001- och ISO/IEC 27018-certifieringar. Alla kunder, inklusive myndigheter samt företags- och utbildningsorganisationer som driftsätter Apple-enheter, kan uppvisa kravöverensstämmelse via certifieringarna för maskinvara, operativsystem, programvara och tjänster.

Maskinvarucertifiering

Eftersom säker programvara kräver en stabil inbyggd säkerhetsgrund i maskinvaran har alla Apple-enheter säkerhetsfunktioner som är integrerade i kretsarna vare sig de drivs av iOS, iPadOS, macOS, tvOS eller watchOS. Dessa inkluderar anpassade processorfunktioner som strömförsörjer systemsäkerhetsfunktioner och kretsar som är dedikerade till säkerhetsfunktioner. Den viktigaste komponenten är Secure Enclave-coprocessorn som finns i alla moderna iOS-, iPadOS-, watchOS- och tvOS-enheter samt i alla Mac-datorer med Apple Silicon och Intel-baserade Mac-datorer med Apple T2-säkerhetskrets. Secure Enclave tillhandahåller grunden för kryptering av data vid vila, säker start i macOS och biometri.

Apples engagemang för säkerhetsförsäkran utgår från certifieringen av grundläggande säkerhetskomponenter i kretsar – från maskinvarans betrodda rot till genomdrivning av säker start till Secure Enclave som tillhandahåller säker nyckellagring och säker autentisering med Touch ID och Face ID. De säkerhetsfunktioner som finns i Apple-enheter är möjliga tack vare en kombination av kretsutformning, maskinvara, programvara och tjänster som endast är tillgängliga från Apple. Certifiering av de här komponenterna är en viktig del i verifieringen av den försäkran som Apple tillhandahåller.

Information om publika certifieringar relaterade till maskinvara och tillhörande komponenter för fast programvara finns i:

- Säkerhetscertifieringar för Apples T2-säkerhetskrets
- Säkerhetscertifieringar för Secure Enclave-processorn

Programvaru- och appcertifieringar

Apple upprätthåller oberoende certifieringar och attesteringar för dess operativsystem och appar i överensstämmelse med FIPS 140-2/-3 för kryptografiska moduler och Common Criteria för operativsystem, appar och enhetstjänster. Täckningen av operativsystem omfattar iOS, iPadOS, macOS, sepOS, fast T2-programvara, tvOS och watchOS. För appar omfattar den oberoende certifieringen inledningsvis webbläsaren Safari och Kontakter. Fler appar kommer att ingå i framtiden.

Information om publika certifieringar relaterade till Apples *operativsystem* finns i:

- Säkerhetscertifieringar för iOS
- Säkerhetscertifieringar för iPadOS
- Säkerhetscertifieringar för macOS
- Säkerhetscertifieringar för tvOS
- Säkerhetscertifieringar för watchOS

Information om publika certifieringar relaterade till Apples *appar* finns i:

- Säkerhetscertifieringar för Apple-appar

Tjänstecertifieringar

Apple upprätthåller säkerhetscertifieringar som stöd för våra kunder inom segment från företag till utbildning. Dessa certifieringar gör det möjligt för Apples kunder att efterleva sina skyldigheter enligt föreskrifter och avtal när de använder Apple-tjänster tillsammans med Apples maskinvara och programvara. Dessa certifieringar ger våra kunder tillgång till ett oberoende intyg på Apples praxis gällande informationssäkerhet, miljö och integritet för Apple-system.

Information om publika certifieringar relaterade till Apples *internettjänster* finns i:

- Säkerhetscertifieringar för Apples internettjänster

Om du har frågor om Apples certifieringar för säkerhet och integritet kontaktar du security-certifications@apple.com.

Certifieringar för maskinvarusäkerhet

Säkerhetscertifieringar för Apple-maskinvara i översikt

Apple upprätthåller valideringscertifikat om överensstämmelse med USA:s Federal Information Processing Standard (FIPS) 140-2/-3 för sepOS och fast T2-programvara liksom andra certifieringar. Apple utgår från *certifieringsbyggstenar* som används brett över flera plattformar där det är tillämpligt. En byggsten är valideringen av corecrypto-biblioteket som används vid driftsättning av kryptografiska moduler för program- och maskinvara inom de operativsystem som har utvecklats av Apple. En andra byggsten är certifieringen av Secure Enclave som finns inbyggd i många Apple-enheter. En tredje är certifieringen av Secure Element (SE) som finns i Apple-enheter med Touch ID och enheter med Face ID. Dessa byggstenar för maskinvarucertifiering utgör grunden för bredare säkerhetscertifieringar för plattformar.

Valideringar av kryptografiska algoritmer

Validering av implementeringens riktighet hos många kryptografiska algoritmer och relaterade säkerhetsfunktioner är en förutsättning för FIPS 140-3-validering och ger stöd för andra certifieringar. Valideringen hanteras av NIST (National Institute of Standards and Technology) och dess CAVP (Cryptographic Algorithm Validation Program). Du kan hitta certifikat för validering av Apples implementeringar med hjälp av CAVP-sökning. Mer information finns på webbplatsen för Cryptographic Algorithm Validation Program (CAVP).

Valideringar av kryptografiska moduler: FIPS 140-2/3 (ISO/IEC 19790)

Apples kryptografiska moduler har upprepade gånger validerats och godkänts av Cryptographic Module Validation Program (CMVP) i enlighet med U.S. Federal Information Processing Standard (FIPS 140-2) för kryptografiska moduler efter varje större versionslansering av operativsystem sedan 2012. Efter varje större versionslansering av operativsystem skickar Apple modulerna till CMVP för validering av överensstämmelse med standarden. Utöver att de används av Apples operativsystem och appar tillhandahåller de här modulerna kryptografiska funktioner för tjänster som Apple tillhandahåller och kan även användas av appar från tredje part.

Apple uppnår varje år **Security Level 1** för de programvarubaserade modulerna ”Corecrypto Module for Intel” och ”Corecrypto Kernel Module for Intel” för macOS. För Apple Silicon gäller modulerna ”Corecrypto Module for ARM” och ”Corecrypto Kernel Module for ARM” för iOS, iPadOS, tvOS, watchOS och den fasta programvaran i den inbäddade Apple T2-säkerhetskretsen i Mac-datorer.

2019 erhöll Apple sitt första FIPS 140-2 **Security Level 2** för den inbäddade kryptografiska maskinvarumodulen med namnet ”Apple Corecrypto Module: Secure Key Store” som gjorde det möjligt för myndigheter i USA att använda nycklarna som skapas och hanteras av Secure Enclave. Apple fortsätter att arbeta vidare i sin strävan efter valideringar för den kryptografiska maskinvarumodulen i samband med varje större versionslansering av operativsystem.

FIPS 140-3 godkändes av U.S. Department of Commerce 2019. Den största ändringen i den här versionen av standarden är specifikationen för ISO/IEC-standarder – framförallt ISO/IEC 19790:2015 och den tillhörande teststandarden ISO/IEC 24759:2017. CMVP har initierat ett övergångsprogram och har indikerat att kryptografiska moduler kommer att börja valideras med FIPS 140-3 som grund under 2020. Apple har som mål att Apples kryptografiska moduler ska uppnå och övergå till FIPS 140-3-standarden så fort som det är praktiskt möjligt.

För kryptografiska moduler som för närvarande genomgår testnings- och valideringsprocesser upprätthåller CMVP två separata listor som kan innehålla information om föreslagna valideringar. Kryptografiska moduler som genomgår testning vid ett ackrediterat laboratorium kan finnas med i listan Implementation Under Test List. När laboratoriet har slutfört testning och rekommenderar validering av CMVP visas Apples kryptografiska moduler i Modules in Process List. För närvarande har laboratorietesterna slutförts och validering av testerna av CMVP väntar. Eftersom längden på utvärderingsprocessen kan variera bör du titta i båda processlistorna ovan för att fastställa aktuell status för Apples kryptografiska moduler mellan datumet för en större operativsystemslansering och utfärdandet av valideringscertifikatet av CMVP.

Produktcertifieringar: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) är en standard som många organisationer utgår från vid säkerhetsutvärdering av IT-produkter.

Information om certifieringar som även kan vara internationellt erkända under CCRA (Common Criteria Recognition Arrangement) finns i Common Criteria Portal. Standarden Common Criteria kan också användas utanför CCRA av nationella och privata valideringsscheman. I Europa lyder ömsesidigt erkännande under SOG-IS-avtalet liksom CCRA.

Målet, som det anges av organisationen runt Common Criteria, är att en internationellt godkänd uppsättning säkerhetsstandarder ska tillhandahålla en tydlig och pålitlig utvärdering av säkerhetsfunktionerna i IT-produkter. Genom att tillhandahålla en oberoende utvärdering av en produkts möjlighet att uppnå säkerhetsstandarder ger Common Criteria-certifiering kunderna ökad kunskap om säkerheten för IT-produkter vilket leder till bättre underbyggda beslut.

Via CCRA har medlemsländerna kommit överens om att erkänna certifieringen av IT-produkter med samma nivå av tillförlitlighet. Utvärderingar som krävs inför certifiering är omfattande och inkluderar:

- Skyddsprofiler (Protection Profiles, PPs)
- Säkerhetsmål (Security Targets, STs)
- Säkerhetsfunktionskrav (Security Functional Requirements, SFRs)
- Säkerhetsförsäkranskrav (Security Assurance Requirements, SARs)
- Utvärderingsförsäkranskrav (Evaluation Assurance Levels, EALs)

Skyddsprofiler (Protection Profiles, PPs) är dokument som specificerar säkerhetskraven för en klass av enhetstyper som Mobility och används till att tillhandahålla jämförbarhet mellan utvärderingarna av IT-produkter inom samma klass. Antalet medlemmar i CCRA, tillsammans med en växande lista över godkända PPs, fortsätter att öka varje år. Detta arrangemang gör det möjligt för en produktutvecklare att sträva efter att uppnå en enskild certifiering under valfritt certifikatauktoriseringsschema och få den erkänd av övriga certifikatmottagande undertecknare.

Säkerhetsmål (STs) definierar *vad* som ska utvärderas när en IT-produkt ska certifieras. Dessa STs översätts till specifika *SFRs (Security Functional Requirements)* som används vid mer detaljerad utvärdering av dessa STs.

Common Criteria (CC) innehåller även *säkerhetsförsäkranskrav*. Ett vanligt identifierat mått är *Evaluation Assurance Level (EAL)*. EALs grupperar vanligt förekommande SARs-uppsättningar och kan anges i PPs och STs som stöd vid jämförelser.

Många äldre PPs har arkiverats och ersätts med målriktade PPs som utvecklas och fokuserar på specifika lösningar och miljöer. I en samlad process för att säkerställa ett fortsatt ömsesidigt erkännande från samtliga CCRA-medlemmar har iTCs (International Technical Communities) upprättats i syfte att utveckla och upprätthålla cPPs (Collaborative Protection Profiles) som utvecklas från grunden med användning av CCRA-undertecknings-scheman. PPs som riktar sig till användargrupper och andra ömsesidiga avtal om erkännande än CCRA fortsätter att utvecklas av respektive huvudaktörer.

Apple påbörjade strävan efter certifiering i enlighet med den uppdaterade CCRA:n med valda cPPs i början av 2015. Sedan dess har Apple uppnått Common Criteria-certifieringar för varje större iOS-versionslansering och har utökat täckningen till att inkludera den säkerhetsförsäkran som tillhandahålls av nya PPs.

Apple tar en aktiv roll inom tekniksamhället med fokus på att utvärdera tekniker för mobilsäkerhet. Dessa omfattar de iTCs som ansvarar för utveckling och uppdatering av cPPs. Apple fortsätter att utvärdera och sikta mot certifieringar i enlighet med de PPs och cPPs som finns idag.

Apples plattformscertifieringar för den nordamerikanska marknaden utförs normalt med NIAP (National Information Assurance Partnership) som upprätthåller en lista över projekt som är under utvärdering men ännu inte har certifierats.

Utöver de allmänna plattformscertifikaten som finns i listan har andra certifikat utfärdats för att peka på specifika säkerhetskrav för vissa marknader.

Säkerhetscertifieringar för Secure Enclave-processorn

Bakgrund till certifiering av Secure Enclave

Den kryptografiska modulen för maskinvara – *Apple SEP Secure Key Store Cryptographic Module* – är inbäddad i Apples SoC:er som ingår i följande produkter: Apples A-serie för iPhone och iPad, M-serie för Mac-datorer med Apple Silicon, S-serie för Apple Watch och T-serie för säkerhetskretsar som finns i Intel-baserade Mac-datorer från och med iMac Pro som introducerades 2017.

2018 synkroniserade Apple valideringen av de kryptografiska programvarumodulerna med operativsystemen som släpptes 2017: iOS 11, macOS 10.13, tvOS 11 och watchOS 4. Den kryptografiska SEP-maskinvarumodulen som identifierades som Apple SEP Secure Key Store Cryptographic Module 1.0 validerades ursprungligen mot kraven i FIPS 140-2 Security Level 1.

2019 validerade Apple maskinvarumodulen mot kraven i FIPS 140-2 säkerhetsnivå 2 och uppdaterade modulens versionsidentifierare till 9.0 för att synkronisera med versionerna för motsvarande valideringar av corecrypto-användarmodulen och corecrypto-kärnmodulen. 2019 omfattade detta iOS 12, macOS 10.14, tvOS 12 och watchOS 5.

2020 och 2021 strävar Apple efter validering av överensstämmelse med FIPS 140-3 samt med ytterligare krav gällande säkerhetsnivå 3 för de fysiska säkerhetskraven för följande Apple-kretsar: A13-, A14-, S6- och M1-kretsar.

Apple deltar även aktivt vid validering av corecrypto-användarmodulen och corecrypto-kärnmodulen vid varje större versionslansering av ett operativsystem. Validering av överensstämmelsen kan endast ske med en färdig lanserad version.

Status för kryptografisk modulvalidering

CMVP (Cryptographic Module Validation Program) upprätthåller valideringsstatusen för kryptografiska moduler i tre olika listor beroende på deras aktuella status:

- För att kunna listas i CMVP:s Implementation Under Test List måste laboratoriet ha fått i uppdrag av Apple att tillhandahålla testning.
- När laboratoriet har slutfört testningen, laboratoriet har rekommenderat validering av CMVP och CMVP-arvodet har betalats läggs modulen sedan till i Modules in Process List. MIP-listan spårar statusen för CMVP:s valideringsarbete i fyra faser:
  - *Review Pending:* Väntar på att CMVP-resurser ska tilldelas.
  - *In Review:* CMVP-resurser utför sina valideringsaktiviteter.
  - *Coordination:* Labbet och CMVP löser eventuella problem som har upptäckts.
  - *Finalization:* Aktiviteter och formalia gällande utfärdande av certifikatet.
- Efter validering av CMVP får modulerna ett certifikat för överensstämmelse och läggs till i listan med validerade kryptografiska moduler. Dessa inkluderar:
  - Validerade moduler är markerade som aktiva.
  - Efter 5 år markeras modulerna som historiska.
  - Om modulcertifikatet återkallas av någon anledning markeras det som återkallat.

2020 anammade CMVP den internationella standarden ISO/IEC 19790 som grund för FIPS 140-3.

FIPS 140-3-certifieringar

Aktuell status

Tabellen nedan visar 2020 och 2021 års kryptografiska moduler som för närvarande testas av laboratoriet för överensstämmelse med FIPS 140-3.

Säker nyckellagring (SKS) som är associerad med både 2020 och 2021 års operativsystemslanseringar har slutförda laboratorietestningar och har rekommenderats av laboratoriet till CMVP för validering. De listas på Modules in Process List och flyttas till validated cryptographic modules list när de har validerats.

iOS 15 (2021) användarutrymme, kärnutrymme och säker nyckellagring genomgår laboratorietestning. De listas på Implementation Under Test List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple corecrypto Module v12 *Operativsystem:* sepOS distribuerat med 2021 års versioner av iOS, iPadOS, macOS, tvOS och watchOS *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14, T2, M1, S3-S6) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med 2021 års versioner av iOS, iPadOS, macOS, tvOS och watchOS *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A13, A14, S6, M1) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med 2020 års versioner av iOS, iPadOS, macOS, tvOS och watchOS *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14, T2, M1, S3-S6) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med 2020 års versioner av iOS, iPadOS, macOS, tvOS och watchOS *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A13, A14, S6, M1) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3

FIPS 140-2-certifieringar

Tabellen nedan visar de kryptografiska moduler som har testats av laboratoriet för överensstämmelse med FIPS 140-2.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-02-05	*Certifikat:* 3811 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS för macOS 10.15 Catalina *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3523 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS för macOS 10.14 Mojave *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3223 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS för macOS 10.13 High Sierra *Typ:* Maskinvara *Säkerhetsnivå:* 2

CC-certifieringar (Common Criteria)

Apple deltar aktivt vid CC-utvärderingar där lämpliga skyddsprofiler (PPs) täcker säkerhetsfunktionerna i Apple-teknik.

CC-certifieringsstatus (Common Criteria)

USA-schemat, som drivs av NIAP, upprätthåller listan Products in Evaluation. Denna lista innehåller produkter som för närvarande utvärderas i USA via ett NIAP-godkänt Common Criteria Testing Laboratory (CCTL) och som har slutfört ett Evaluation Kick off Meeting (eller likvärdigt) där CCEVS-ledningen officiellt har accepterat produkten för utvärdering.

När produkter har certifierats placerar NIAP aktuella giltiga certifieringar på Product Compliant List. Efter två år granskas certifieringarna gällande deras överensstämmelse med den aktuella policyn för säkerhetsunderhåll. När datum för säkerhetsunderhåll har passerats flyttar NIAP certifieringslistningen till Archived Products List.

Common Criteria Portal listar certifieringar som kan vara ömsesidigt erkända i enlighet med Common Criteria Recognition Arrangement (CCRA). CC-portalen kan behålla produkter på listan för certifierade produkter under fem år och dessa poster sparas i CC-portalen för arkiverade certifieringar.

Tabellen nedan visar de certifieringar som för närvarande utvärderas av ett laboratorium eller har certifierats som överensstämmande med Common Criteria.

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: sepOS *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple Secure Enclave [2020] *Skyddsprofiler:* CPP_DSC_V1.0 *Maskinvara:* Secure Enclave för (A9–A14, M1, T2, S3–S6) *Programvara:* sepOS distribuerat med iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7

Ytterligare certifieringar

Tabellen nedan visar certifieringar för Secure Enclave som varken använder Common Criteria eller FIPS 140-3.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* 2019-12-07 till 2022-12-26	*Certifikat:* 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

Säkerhetscertifieringar för Apples T2-säkerhetskrets

Bakgrund till kryptografisk modulvalidering

Apple deltar aktivt vid validering av Apples inbäddade programvara och maskinvarumoduler vid varje större versionslansering av ett operativsystem. Validering av överensstämmelsen kan endast ske med en färdig lanseringsversion av modulen.

2020 anammade CMVP den internationella standarden ISO/IEC 19790 som grund för FIPS 140-3.

Utöver Intel-processorn har de flesta Mac-datorerna sedan 2017 även en separat Apple T2-säkerhetskrets som är ett Apple Silicon-baserat SoC (System on Chip). Dessa Mac-datorer med en T2-krets använder alla fem kryptografiska moduler för olika tjänster på enheterna.

- Corecrypto-användarmodul för Intel (används av macOS på Intel-baserade Mac-datorer)
- Corecrypto-kärnmodul för Intel (används av macOS på Intel-baserade Mac-datorer)
- Corecrypto-användarmodul för ARM (används av T2-kretsen)
- Corecrypto-kärnmodul för ARM (används av T2-kretsen)
- Secure Key Store Cryptographic Module (används av den inbäddade Secure Enclave-coprocessorn i T2-kretsen)

Obs! Apple Silicon-baserade moduler som körs på T2-kretsen är likadana som de som körs på andra Apple-kretsar som Apples A-serie, S-serie och M-serie.

Status för kryptografisk modulvalidering

CMVP (Cryptographic Module Validation Program) upprätthåller valideringsstatusen för kryptografiska moduler i tre olika listor beroende på deras aktuella status:

- För att kunna listas i CMVP:s Implementation Under Test List måste laboratoriet ha fått i uppdrag av Apple att tillhandahålla testning.
- När laboratoriet har slutfört testningen, laboratoriet har rekommenderat validering av CMVP och CMVP-arvodet har betalats läggs modulen sedan till i Modules in Process (MIP) List. MIP-listan spårar statusen för CMVP:s valideringsarbete i fyra faser:
  - *Review Pending:* Väntar på att CMVP-resurser ska tilldelas.
  - *In Review:* CMVP-resurser utför sina valideringsaktiviteter.
  - *Coordination:* Labbet och CMVP löser eventuella problem som har upptäckts.
  - *Finalization:* Aktiviteter och formalia gällande utfärdande av certifikatet.
- Efter validering av CMVP får modulerna ett certifikat för överensstämmelse och läggs till i listan med validerade kryptografiska moduler. Dessa inkluderar:
  - Validerade moduler är markerade som aktiva.
  - Efter 5 år markeras modulerna som historiska.
  - Om modulcertifikatet återkallas av någon anledning markeras det som återkallat.

FIPS 140-3-certifieringar

Aktuell status

watchOS 6 (2019) användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

2021 års moduler för användarutrymme, kärnutrymme och säker nyckellagring genomgår laboratorietestning. De listas på Implementation Under Test List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS för macOS 12 Monterey *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS för macOS 12 Monterey *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS för macOS 12 Monterey *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (T2) *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS för macOS 11 Big Sur *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS för macOS 11 Big Sur *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS för macOS 11 Big Sur *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara *Säkerhetsnivå:* 2

FIPS 140-2-certifieringar

Tabellen nedan visar de kryptografiska moduler som har testats av laboratoriet för överensstämmelse med FIPS 140-2.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3856 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Operativsystem:* sepOS för macOS 10.15 Catalina *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3855 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Operativsystem:* sepOS för macOS 10.15 Catalina *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-02-05	*Certifikat:* 3811 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS för macOS 10.15 Catalina *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-23	*Certifikat:* 3438 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Operativsystem:* sepOS för macOS 10.14 Mojave *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-11	*Certifikat:* 3433 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Operativsystem:* sepOS för macOS 10.14 Mojave *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3523 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS för macOS 10.14 Mojave *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-22, 2018-07-06	*Certifikat:* 3148 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Operativsystem:* sepOS för macOS 10.13 High Sierra *Typ:* Programvara *Säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-17, 2018-07-03	*Certifikat:* 3147 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Operativsystem:* sepOS för macOS 10.13 High Sierra *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-07-10	*Certifikat:* 3223 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS för macOS 10.13 High Sierra *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2016 *Valideringsdatum:* 2017-02-01	*Certifikat:* 2828 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* sepOS för macOS 10.12 Sierra *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2016 *Valideringsdatum:* 2017-02-01	*Certifikat:* 2827 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* sepOS för macOS 10.12 Sierra *Typ:* Programvara *Säkerhetsnivå:* 1

Säkerhetscertifieringar för operativsystem

Säkerhetscertifieringar för Apple-operativsystem i översikt

Apple upprätthåller valideringscertifikat om överensstämmelse med USA:s Federal Information Processing Standard (FIPS) 140-2/-3 för sepOS och fast T2-programvara liksom andra certifieringar. Apple utgår från *certifieringsbyggstenar* som används brett över flera plattformar där det är tillämpligt. En byggsten är valideringen av corecrypto som används vid driftsättning av kryptografiska moduler för program- och maskinvara inom de operativsystem som har utvecklats av Apple. En andra byggsten är certifieringen av Secure Enclave som finns inbyggd i många Apple-enheter. En tredje är certifieringen av Secure Element (SE) som finns i Apple-enheter med Touch ID och enheter med Face ID. Dessa byggstenar för maskinvarucertifiering utgör grunden för bredare säkerhetscertifieringar för plattformar.

Valideringar av kryptografiska algoritmer

Validering av implementeringens riktighet hos många kryptografiska algoritmer och relaterade säkerhetsfunktioner är en förutsättning för FIPS 140-3-validering och ger stöd för andra certifieringar. Valideringen hanteras av NIST:s Cryptographic Algorithm Validation Program (CAVP). Du kan hitta certifikat för validering av Apples implementeringar med hjälp av CAVP-sökning.

Valideringar av kryptografiska moduler: FIPS 140-2/3 (ISO/IEC 19790)

De kryptografiska modulerna i Apples operativsystem har upprepade gånger validerats och godkänts av Cryptographic Module Validation Program (CMVP) i enlighet med U.S. Federal Information Processing Standards (FIPS) 140-2 efter varje större versionslansering av operativsystem sedan 2012. Efter varje större versionslansering skickar Apple alla moduler till CMVP för fullständig kryptografisk validering. Dessa validerade moduler tillhandahåller kryptografiska åtgärder för Apples tjänster och är tillgängliga för användning med appar från tredje part.

Apple uppnår varje år **Security Level 1** för de programvarubaserade modulerna ”Corecrypto Module for Intel” och ”Corecrypto Kernel Module for Intel” för macOS. För Apple Silicon gäller modulerna ”Corecrypto Module for ARM” och ”Corecrypto Kernel Module for ARM” för iOS, iPadOS, tvOS, watchOS och den fasta programvaran i den inbäddade Apple T2-säkerhetskretsen i Mac-datorer.

2019 erhöll Apple sitt första FIPS 140-2 **Security Level 2** för den inbäddade kryptografiska maskinvarumodulen med namnet ”Apple Corecrypto Module: Secure Key Store” som gjorde det möjligt för myndigheter i USA att använda nycklarna som skapas och hanteras av Secure Enclave. Apple fortsätter att arbeta vidare i sin strävan efter valideringar för den kryptografiska maskinvarumodulen i samband med varje större versionslansering av operativsystem.

FIPS 140-3 godkändes av U.S. Department of Commerce 2019. Den största ändringen i den här versionen av standarden är specifikationen för ISO/IEC-standarder – framförallt ISO/IEC 19790:2015 och den tillhörande teststandarden ISO/IEC 24759:2017. CMVP har initierat ett övergångsprogram och har indikerat att kryptografiska moduler kommer att börja valideras med FIPS 140-3 som grund under 2020. Apple har som mål att Apples kryptografiska moduler ska uppnå och övergå till FIPS 140-3-standarden så fort som det är praktiskt möjligt.

För kryptografiska moduler som för närvarande genomgår testnings- och valideringsprocesser upprätthåller CMVP två separata listor som kan innehålla information om föreslagna valideringar. Kryptografiska moduler som genomgår testning vid ett ackrediterat laboratorium kan finnas med i listan Implementation Under Test List. När laboratoriet har slutfört testning och rekommenderar validering av CMVP visas Apples kryptografiska moduler i Modules in Process List. För närvarande har laboratorietesterna slutförts och validering av testerna av CMVP väntar. Eftersom längden på utvärderingsprocessen kan variera bör du titta i båda processlistorna ovan för att fastställa aktuell status för Apples kryptografiska moduler mellan datumet för en större operativsystemslansering och utfärdandet av valideringscertifikatet av CMVP.

Produktcertifieringar: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) är en standard som många organisationer utgår från vid säkerhetsutvärdering av IT-produkter.

Information om certifieringar som även kan vara internationellt erkända under CCRA (Common Criteria Recognition Arrangement) finns i Common Criteria Portal. Standarden Common Criteria kan också användas utanför CCRA av nationella och privata valideringsscheman. I Europa lyder ömsesidigt erkännande under SOG-IS-avtalet liksom CCRA.

Målet, som det anges av organisationen runt Common Criteria, är att en internationellt godkänd uppsättning säkerhetsstandarder ska tillhandahålla en tydlig och pålitlig utvärdering av säkerhetsfunktionerna i IT-produkter. Genom att tillhandahålla en oberoende utvärdering av en produkts möjlighet att uppnå säkerhetsstandarder ger Common Criteria-certifiering kunderna ökad kunskap om säkerheten för IT-produkter vilket leder till bättre underbyggda beslut.

Via CCRA har medlemsländerna kommit överens om att erkänna certifieringen av IT-produkter med samma nivå av tillförlitlighet. Utvärderingar som krävs inför certifiering är omfattande och inkluderar:

- Skyddsprofiler (Protection Profiles, PPs)
- Säkerhetsmål (Security Targets, STs)
- Säkerhetsfunktionskrav (Security Functional Requirements, SFRs)
- Säkerhetsförsäkranskrav (Security Assurance Requirements, SARs)
- Utvärderingsförsäkranskrav (Evaluation Assurance Levels, EALs)

Skyddsprofiler (Protection Profiles, PPs) är dokument som specificerar säkerhetskraven för en klass av enhetstyper som Mobility och används till att tillhandahålla jämförbarhet mellan utvärderingarna av IT-produkter inom samma klass. Antalet medlemmar i CCRA, tillsammans med en växande lista över godkända PPs, fortsätter att öka varje år. Detta arrangemang gör det möjligt för en produktutvecklare att sträva efter att uppnå en enskild certifiering under valfritt certifikatauktoriseringsschema och få den erkänd av övriga certifikatmottagande undertecknare.

Säkerhetsmål (STs) definierar *vad* som ska utvärderas när en IT-produkt ska certifieras. Dessa STs översätts till specifika *SFRs (Security Functional Requirements)* som används vid mer detaljerad utvärdering av dessa STs.

Common Criteria (CC) innehåller även *säkerhetsförsäkranskrav*. Ett vanligt identifierat mått är *Evaluation Assurance Level (EAL)*. EALs grupperar vanligt förekommande SARs-uppsättningar och kan anges i PPs och STs som stöd vid jämförelser.

Många äldre PPs har arkiverats och ersätts med målriktade PPs som utvecklas och fokuserar på specifika lösningar och miljöer. I en samlad process för att säkerställa ett fortsatt ömsesidigt erkännande från samtliga CCRA-medlemmar har iTCs (International Technical Communities) upprättats i syfte att utveckla och upprätthålla *cPPs (Collaborative Protection Profiles)* som utvecklas från grunden med användning av CCRA-undertecknings-scheman. PPs som riktar sig till användargrupper och andra ömsesidiga avtal om erkännande än CCRA fortsätter att utvecklas av respektive huvudaktörer.

Apple påbörjade strävan efter certifiering i enlighet med den uppdaterade CCRA:n med valda cPPs i början av 2015. Sedan dess har Apple uppnått Common Criteria-certifieringar för varje större iOS-versionslansering och har utökat täckningen till att inkludera den säkerhetsförsäkran som tillhandahålls av nya PPs.

Apple tar en aktiv roll inom tekniksamhället med fokus på att utvärdera tekniker för mobilsäkerhet. Dessa omfattar de iTCs som ansvarar för utveckling och uppdatering av cPPs. Apple fortsätter att utvärdera och sikta mot certifieringar i enlighet med de PPs och cPPs som finns idag.

Apples plattformscertifieringar för den nordamerikanska marknaden utförs normalt med NIAP (National Information Assurance Partnership) som upprätthåller en lista över projekt som är under utvärdering men ännu inte har certifierats.

Utöver de allmänna plattformscertifikaten som finns i listan har andra certifikat utfärdats för att peka på specifika säkerhetskrav för vissa marknader.

Säkerhetscertifieringar för iOS

Bakgrund till iOS-certifiering

Apple deltar aktivt vid validering av Apples inbäddade programvara och maskinvarumoduler vid varje större versionslansering av ett operativsystem. Validering av överensstämmelsen kan endast ske med en färdig lanserad version.

Status för kryptografisk modulvalidering i iOS

CMVP (Cryptographic Module Validation Program) upprätthåller valideringsstatusen för kryptografiska moduler i tre olika listor beroende på deras aktuella status:

- För att kunna listas i CMVP:s Implementation Under Test List måste laboratoriet ha fått i uppdrag av Apple att tillhandahålla testning.
- När laboratoriet har slutfört testningen, laboratoriet har rekommenderat validering av CMVP och CMVP-arvodet har betalats läggs modulen sedan till i Modules in Process (MIP) List. MIP-listan spårar statusen för CMVP:s valideringsarbete i fyra faser:
  - *Review Pending:* Väntar på att CMVP-resurser ska tilldelas.
  - *In Review:* CMVP-resurser utför sina valideringsaktiviteter.
  - *Coordination:* Labbet och CMVP löser eventuella problem som har upptäckts.
  - *Finalization:* Aktiviteter och formalia gällande utfärdande av certifikatet.
- Efter validering av CMVP får modulerna ett certifikat för överensstämmelse och läggs till i listan med validerade kryptografiska moduler. Dessa inkluderar:
  - Validerade moduler är markerade som aktiva.
  - Efter 5 år markeras modulerna som historiska.
  - Om modulcertifikatet återkallas av någon anledning markeras det som återkallat.

2020 anammade CMVP den internationella standarden ISO/IEC 19790 som grund för FIPS 140-3.

FIPS 140-3-certifieringar

Aktuell status

iOS 14 (2020) användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

iOS 15 (2021) användarutrymme, kärnutrymme och säker nyckellagring genomgår laboratorietestning. De listas på Implementation Under Test List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iOS 15 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iOS 15 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribuerat med iOS 15 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribuerat med iOS 15 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A13, A14, A15) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iOS 14 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iOS 14 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med iOS 14 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med iOS 14 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A13-A14) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3

FIPS 140-2-certifieringar

Tabellen nedan visar kryptografiska moduler som för närvarande testas och har testats av laboratoriet för överensstämmelse med FIPS 140-2.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3856 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Operativsystem:* iOS 13 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3855 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Operativsystem:* iOS 13 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-02-05	*Certifikat:* 3811 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribuerat med iOS 13 *Typ:* Maskinvara *Säkerhetsnivå:* 2

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-23	*Certifikat:* 3438 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Operativsystem:* iOS 12 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-11	*Certifikat:* 3433 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Operativsystem:* iOS 12 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3523 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribuerat med iOS 12 *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-22, 2018-07-06	*Certifikat:* 3148 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Operativsystem:* iOS 11 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-17, 2018-07-03	*Certifikat:* 3147 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Operativsystem:* iOS 11 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3223 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribuerat med iOS 11 *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2016 *Valideringsdatum:* 2017-02-01	*Certifikat:* 2828 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2016 *Valideringsdatum:* 2017-02-01	*Certifikat:* 2827 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Typ:* Programvara *Säkerhetsnivå:* 1

Föregående versioner

Certifikat som är äldre än 5 år listas av CMVP med historisk status: Dessa föregående iOS-versioner hade kryptografiska modulvalideringar:

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

Bakgrund till CC-certifiering (Common Criteria)

Apple deltar aktivt vid utvärdering av iOS för varje större versionslansering av operativsystemet. Utvärdering kan endast utföras mot en färdig lanseringsversion av operativsystemet. iPadOS hette iOS innan iPadOS 13.1.

CC-certifieringsstatus (Common Criteria)

USA-schemat, som drivs av NIAP, upprätthåller listan Products in Evaluation. Denna lista innehåller produkter som för närvarande utvärderas i USA via ett NIAP-godkänt Common Criteria Testing Laboratory (CCTL) och som har slutfört ett Evaluation Kick off Meeting (eller likvärdigt) där CCEVS-ledningen officiellt har accepterat produkten för utvärdering.

När produkter har certifierats placerar NIAP aktuella giltiga certifieringar på Product Compliant List. Efter två år granskas certifieringarna gällande deras överensstämmelse med den aktuella policyn för säkerhetsunderhåll. När datum för säkerhetsunderhåll har passerats flyttar NIAP certifieringslistningen till Archived Products List.

Common Criteria Portal listar certifieringar som kan vara ömsesidigt erkända i enlighet med Common Criteria Recognition Arrangement (CCRA). CC-portalen kan behålla produkter på listan för certifierade produkter under fem år och dessa poster sparas i CC-portalen för arkiverade certifieringar.

Tabellen nedan visar de certifieringar som för närvarande utvärderas av ett laboratorium eller har certifierats som överensstämmande med Common Criteria.

Aktuell status

Laboratorietestning för utvärderingar med NIAP för iOS 15 pågår. Den senaste informationen finns på Products in evaluation (NIAP) och Product Compliant List.

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: iOS 15 *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* –	*Titel:* Apple iOS 15: iPhones *Skyddsprofiler:* Mobile Device Fundamentals (PP-moduler väntar på bekräftelse)
Operativsystem: iOS 14 *Certifieringsdatum:* 2021-09-01	*Schema-ID:* 11146 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple iOS 14: iPhones *Skyddsprofiler:* Mobile Device Fundamentals, VPN Client module, WLAN Clients PP Module, MDM Agent EP
Operativsystem: iOS 13 *Certifieringsdatum:* 2020-11-06	*Schema-ID:* 11036 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple iOS 13 on iPhone *Skyddsprofiler:* Mobile Device Fundamentals, VPN Client module, WLAN Clients EP, MDM Agent EP

Arkiverade Common Criteria-certifieringar för iOS

Dessa föregående iOS-versioner hade Common Criteria-validering. De har arkiverats av NIAP i enlighet med NIAP-policyn:

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: iOS 12 *Certifieringsdatum:* 2019-03-14	*Schema-ID:* 10937 *Dokument:* Säkerhetsmål Vägledning	*Titel:* iPhone with iOS 12 *Skyddsprofiler:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Operativsystem: iOS 11 *Certifieringsdatum:* 2018-07-17	*Schema-ID:* 10851 *Dokument:* Säkerhetsmål Vägledning	*Titel:* Apple iOS 11 *Skyddsprofiler:* Mobile Device Fundamentals, Wireless LAN client EP, MDM Agent EP
Operativsystem: iOS 10 *Certifieringsdatum:* 2017-07-27	*Schema-ID:* 10782 *Dokument:* Säkerhetsmål, Vägledning	*Titel:* iOS 10.2 on iPhone and iPad Devices *Skyddsprofiler:* Mobile Device Fundamentals, Wireless LAN client EP, MDM Agent EP
Operativsystem: iOS 10 *Certifieringsdatum:* 2017-07-27	*Schema-ID:* 10792 *Dokument:* Säkerhetsmål, Vägledning	*Titel:* iOS 10.2 VPN Client on iPhone and iPad *Skyddsprofiler:* VPN Client PP
Operativsystem: iOS 9 *Certifieringsdatum:* 2016-10-14	*Schema-ID:* 10725 *Dokument:* Säkerhetsmål, Vägledning	*Titel:* iOS 9.3.2 with MDM Agent *Skyddsprofiler:* Mobile Device Fundamentals, MDM Agent EP
Operativsystem: iOS 9 *Certifieringsdatum:* 2016-10-13	*Schema-ID:* 10714 *Dokument:* Säkerhetsmål, Vägledning	*Titel:* OS VPN Client on iPhone and iPad *Skyddsprofiler:* VPN Client PP
Operativsystem: iOS 9 *Certifieringsdatum:* 2016-01-28	*Schema-ID:* 10695 *Dokument:* Säkerhetsmål, Vägledning	*Titel:* iOS 9 *Skyddsprofiler:* Mobile Device Fundamentals

Säkerhetscertifieringar för iPadOS

Bakgrund till iPadOS-certifiering

Apple deltar aktivt vid validering av Apple-operativsystem för alla större versionslanseringar av operativsystem med hjälp av collaborative Protection Profiles och FIPS 140-3-säkerhetsnivåer. Validering av överensstämmelsen kan endast ske med en färdig lanserad version.

Obs! 2019 bytte operativsystemet för iPad-enheter namn till iPadOS. iPadOS hette iOS innan iPadOS 13.1.

Status för kryptografisk modulvalidering i iPadOS

CMVP (Cryptographic Module Validation Program) upprätthåller valideringsstatusen för kryptografiska moduler i tre olika listor beroende på deras aktuella status:

- För att kunna listas i CMVP:s Implementation Under Test List måste laboratoriet ha fått i uppdrag av Apple att tillhandahålla testning.
- När laboratoriet har slutfört testningen, laboratoriet har rekommenderat validering av CMVP och CMVP-arvodet har betalats läggs modulen sedan till i Modules in Process (MIP) List. MIP-listan spårar statusen för CMVP:s valideringsarbete i fyra faser:
  - *Review Pending:* Väntar på att CMVP-resurser ska tilldelas.
  - *In Review:* CMVP-resurser utför sina valideringsaktiviteter.
  - *Coordination:* Labbet och CMVP löser eventuella problem som har upptäckts.
  - *Finalization:* Aktiviteter och formalia gällande utfärdande av certifikatet.
- Efter validering av CMVP får modulerna ett certifikat för överensstämmelse och läggs till i listan med validerade kryptografiska moduler. Dessa inkluderar:
  - Validerade moduler är markerade som aktiva.
  - Efter 5 år markeras modulerna som historiska.
  - Om modulcertifikatet återkallas av någon anledning markeras det som återkallat.

2020 anammade CMVP den internationella standarden ISO/IEC 19790 som grund för FIPS 140-3.

FIPS 140-3-certifieringar

Aktuell status

iPadOS 14 (2020) användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

iPadOS 15 (2021) användarutrymme, kärnutrymme och säker nyckellagring genomgår laboratorietestning. De listas på Implementation Under Test List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iPadOS 15 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* iPadOS 15 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribuerat med iPadOS 15 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14, M1) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribuerat med iPadOS 15 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14, M1) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iPadOS 14 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* iPadOS 14 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med iPadOS 14 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14, M1) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med iPadOS 14 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A9-A14, M1) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3

FIPS 140-2-certifieringar

Tabellen nedan visar kryptografiska moduler som för närvarande testas och har testats av laboratoriet för överensstämmelse med FIPS 140-2.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3856 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Operativsystem:* iPadOS 13 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3855 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Operativsystem:* iPadOS 13 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-02-05	*Certifikat:* 3811 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribuerat med iPadOS 13 *Typ:* Maskinvara *Säkerhetsnivå:* 2

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-23	*Certifikat:* 3438 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Operativsystem:* iOS 12 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-11	*Certifikat:* 3433 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Operativsystem:* iOS 12 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3523 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribuerat med iOS 12 *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-22, 2018-07-06	*Certifikat:* 3148 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Operativsystem:* iOS 11 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-17, 2018-07-03	*Certifikat:* 3147 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Operativsystem:* iOS 11 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3223 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribuerat med iOS 11 *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2016 *Valideringsdatum:* 2017-02-01	*Certifikat:* 2828 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2016 *Valideringsdatum:* 2017-02-01	*Certifikat:* 2827 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Operativsystem:* iOS 10 *Typ:* Programvara *Säkerhetsnivå:* 1

Föregående versioner

Certifikat som är äldre än 5 år listas av CMVP med historisk status: Dessa föregående iOS-versioner hade kryptografiska modulvalideringar:

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

Bakgrund till CC-certifiering (Common Criteria)

Apple deltar aktivt vid utvärdering av iPadOS för varje större versionslansering av operativsystemet. Utvärdering kan endast utföras mot en färdig lanseringsversion av operativsystemet.

CC-certifieringsstatus (Common Criteria)

USA-schemat, som drivs av NIAP, upprätthåller listan Products in Evaluation. Denna lista innehåller produkter som för närvarande utvärderas i USA via ett NIAP-godkänt Common Criteria Testing Laboratory (CCTL) och som har slutfört ett Evaluation Kick off Meeting (eller likvärdigt) där CCEVS-ledningen officiellt har accepterat produkten för utvärdering.

När produkter har certifierats placerar NIAP aktuella giltiga certifieringar på Product Compliant List. Efter två år granskas certifieringarna gällande deras överensstämmelse med den aktuella policyn för säkerhetsunderhåll. När datum för säkerhetsunderhåll har passerats flyttar NIAP certifieringslistningen till Archived Products List.

Common Criteria Portal listar certifieringar som kan vara ömsesidigt erkända i enlighet med Common Criteria Recognition Arrangement (CCRA). CC-portalen kan behålla produkter på listan för certifierade produkter under fem år och dessa poster sparas i CC-portalen för arkiverade certifieringar.

Tabellen nedan visar de certifieringar som för närvarande utvärderas av ett laboratorium eller har certifierats som överensstämmande med Common Criteria.

Aktuell status

Laboratorietestning för utvärderingar med NIAP för iPadOS 15 pågår. Den senaste informationen finns på Products in evaluation (NIAP) och Product Compliant List.

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: iPadOS 15 *Certifieringsdatum:* 2019-03-14	*Schema-ID:* – *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* iPad with iOS 12 *Skyddsprofiler:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Operativsystem: iPadOS 14 *Certifieringsdatum:* 2021-09-01	*Schema-ID:* 11147 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple iPadOS 14: iPads *Skyddsprofiler:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Operativsystem: iPadOS 13 *Certifieringsdatum:* 2020-11-06	*Schema-ID:* 11036 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* iPadOS 13 on iPad Mobile Devices *Skyddsprofiler:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP

Föregående versioner

Dessa föregående iOS-versioner hade Common Criteria-validering. De har arkiverats av NIAP i enlighet med NIAP-policyn:

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

Säkerhetscertifieringar för macOS

Bakgrund till macOS-certifiering

Apple deltar aktivt vid validering av Apple-operativsystem för alla större versionslanseringar av operativsystem med hjälp av collaborative Protection Profiles och FIPS 140-3-säkerhetsnivåer. Validering av överensstämmelsen kan endast ske med en färdig lanserad version.

Status för kryptografisk modulvalidering i macOS

CMVP (Cryptographic Module Validation Program) upprätthåller valideringsstatusen för kryptografiska moduler i tre olika listor beroende på deras aktuella status:

- För att kunna listas i CMVP:s Implementation Under Test List måste laboratoriet ha fått i uppdrag av Apple att tillhandahålla testning.
- När laboratoriet har slutfört testningen, laboratoriet har rekommenderat validering av CMVP och CMVP-arvodet har betalats läggs modulen sedan till i Modules in Process (MIP) List. MIP-listan spårar statusen för CMVP:s valideringsarbete i fyra faser:
  - *Review Pending:* Väntar på att CMVP-resurser ska tilldelas.
  - *In Review:* CMVP-resurser utför sina valideringsaktiviteter.
  - *Coordination:* Labbet och CMVP löser eventuella problem som har upptäckts.
  - *Finalization:* Aktiviteter och formalia gällande utfärdande av certifikatet.
- Efter validering av CMVP får modulerna ett certifikat för överensstämmelse och läggs till i listan med validerade kryptografiska moduler. Dessa inkluderar:
  - Validerade moduler är markerade som aktiva.
  - Efter 5 år markeras modulerna som historiska.
  - Om modulcertifikatet återkallas av någon anledning markeras det som återkallat.

2020 anammade CMVP den internationella standarden ISO/IEC 19790 som grund för FIPS 140-3.

För Apples Mac-datorer visar tabellen nedan vilka kryptografiska moduler som används för olika Mac-tekniker.

Kryptografisk modul	Mac-datorer med Apple Silicon	Mac-datorer med Apple T2-säkerhetskrets	Intel-baserade Mac-datorer utan Apple T2-säkerhetskrets
Apple Silicon-användarutrymme	✓		
Apple Silicon-kärna	✓		
Intel-användarutrymme		✓	✓
Intel-kärna		✓	✓
Säker nyckellagring	✓	✓	

FIPS 140-3-certifieringar

2020 lanserade Apple Mac-datorer som baseras på Apple Silicon. De kryptografiska modulerna som kan användas i antingen Apple Silicon- eller Intel-baserade Mac-datorer indikeras i kolumnen Modulinformation i tabellen nedan.

Obs! Apple T2-säkerhetskretsen ingår i många Intel-baserade Mac-datorer. Information om certifieringar för T2-kretsen finns i Säkerhetscertifieringar för Apples T2-säkerhetskrets.

ssh-klient för macOS

OpenSSH kan konfigureras för användning av FIPS 140-3-validerade moduler för utvalda FIPS 140-3-algoritmer. Organisationer kan köra en signerad och attesterad installerare som är tillgänglig från Apple med lösenordet *FIPS140Mode*. Installeraren placerar två filer på Mac-datorn:

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

macOS använder sedan dessa filer till att begränsa de koder som är tillgängliga för Open SSH till endast de som har validerats av NIST och säkerställer att OpenSSH-klienten använder den validerade kryptografiska modulen som tillhandahålls för plattformen. Administratörer kan även skapa sina egna filer. Mer information finns på `apple_ssh_and_fips` man-sidan i macOS 12.0.1 eller senare.

Aktuell status

macOS 11 Big Sur användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

macOS 12 Monterey användarutrymme, kärnutrymme och säker nyckellagring genomgår laboratorietestning. De listas på Implementation Under Test List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Apple Silicon *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Apple Silicon *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Intel *Miljö:* Intel, användare, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* macOS 12 Monterey på Intel *Miljö:* Intel, kärna, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS distribuerat med macOS 12 Monterey på Apple Silicon, sepOS distribuerat med macOS 12 Monterey på Intel med T2 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (M1 och T2) *Säkerhetsnivå:* 2

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12.0 *Operativsystem:* sepOS distribuerat med macOS 12 Monterey på Apple Silicon *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (M1) *Säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Intel *Miljö:* Intel, användare, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Intel *Miljö:* Intel, kärna, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Apple Silicon *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* macOS 11 Big Sur på Apple Silicon *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med macOS 11 Big Sur på Apple Silicon, sepOS distribuerat med macOS 11 Big Sur på Intel *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (M1) *Säkerhetsnivå:* 2

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med macOS 11 Big Sur på Apple Silicon *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (M1) *Säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3

FIPS 140-2-certifieringar

Tabellen nedan visar kryptografiska moduler som för närvarande testas och har testats av laboratoriet för överensstämmelse med FIPS 140-2.

macOS 10.15 Catalina användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

Obs! Apple T2-säkerhetskretsen ingår i många Intel-baserade Mac-datorer. Information om certifieringar för T2-kretsen finns i Säkerhetscertifieringar för Apples T2-säkerhetskrets.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-24	*Certifikat:* 3859 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Space Module for Intel (ccv10) *Operativsystem:* macOS 10.15 Catalina *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-24	*Certifikat:* 3858 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v10.0 for Intel (ccv10) *Operativsystem:* macOS 10.15 Catalina *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-12	*Certifikat:* 3402 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v9.0 for Intel *Operativsystem:* macOS 10.14 Mojave *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-12	*Certifikat:* 3431 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v9.0 for Intel *Operativsystem:* macOS 10.14 Mojave *Typ:* Programvara *Säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-22	*Certifikat:* 3155 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v8.0 for Intel *Operativsystem:* macOS 10.13 High Sierra *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-22	*Certifikat:* 3156 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v8.0 for Intel *Operativsystem:* macOS 10.13 High Sierra *Typ:* Programvara *Säkerhetsnivå:* 1

Föregående versioner

Dessa föregående OS X- och macOS-versioner hade kryptografiska modulvalideringar. De som är äldre än fem år listas av CMVP med historisk status:

- 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

Bakgrund till CC-certifiering (Common Criteria)

Apple deltar aktivt vid utvärdering av macOS för varje större versionslansering av operativsystemet. Utvärdering kan endast utföras mot en färdig lanseringsversion av operativsystemet.

CC-certifieringsstatus (Common Criteria)

USA-schemat, som drivs av NIAP, upprätthåller listan Products in Evaluation. Denna lista innehåller produkter som för närvarande utvärderas i USA via ett NIAP-godkänt Common Criteria Testing Laboratory (CCTL) och som har slutfört ett Evaluation Kick off Meeting (eller likvärdigt) där CCEVS-ledningen officiellt har accepterat produkten för utvärdering.

När produkter har certifierats placerar NIAP aktuella giltiga certifieringar på Product Compliant List. Efter två år granskas certifieringarna gällande deras överensstämmelse med den aktuella policyn för säkerhetsunderhåll. När datum för säkerhetsunderhåll har passerats flyttar NIAP certifieringslistningen till Archived Products List.

Common Criteria Portal listar certifieringar som kan vara ömsesidigt erkända i enlighet med Common Criteria Recognition Arrangement (CCRA). CC-portalen kan behålla produkter på listan för certifierade produkter under fem år och dessa poster sparas i CC-portalen för arkiverade certifieringar.

Tabellen nedan visar de certifieringar som för närvarande utvärderas av ett laboratorium eller har certifierats som överensstämmande med Common Criteria.

Aktuell status

Utvärderingar av NIAP för macOS 11 och macOS 12 med hjälp av General Purpose Operating System och Full Disk Encryption (FDE) (AA och EE) Protection Profiles pågår.

Den senaste informationen finns på Products in evaluation (NIAP) och Product Compliant List.

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: macOS 12 Monterey *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* –	*Titel:* Apple FileVault 2 with macOS 12 Monterey *Skyddsprofiler:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP-moduler väntar på bekräftelse)
Operativsystem: macOS 12 Monterey *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* –	*Titel:* macOS 12 Monterey *Skyddsprofiler:* PP_OS_V4.21 (PP-moduler väntar på bekräftelse)
Operativsystem: macOS 11 Big Sur *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple FileVault 2 with macOS 11 Big Sur *Skyddsprofiler:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Operativsystem: macOS 11 Big Sur *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple macOS 11 Big Sur *Skyddsprofiler:* PP_OS_V4.21

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: macOS 10.15 Catalina *Certifieringsdatum:* 2021-04-29	*Schema-ID:* 11078 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple FileVault 2 on T2 computers running macOS 10.15 Catalina *Skyddsprofiler:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Operativsystem: macOS 10.15 Catalina *Certifieringsdatum:* 2020-09-23	*Schema-ID:* 11077 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* macOS 10.15 Catalina *Skyddsprofiler:* PP_OS_V4.21

Säkerhetscertifieringar för tvOS

Bakgrund till tvOS-certifiering

Apple deltar aktivt vid validering av kryptografiska moduler som associeras med varje större versionslansering av tvOS. Validering av överensstämmelsen kan endast ske med en färdig lanserad version.

Status för kryptografisk modulvalidering i tvOS

CMVP (Cryptographic Module Validation Program) upprätthåller valideringsstatusen för kryptografiska moduler i tre olika listor beroende på deras aktuella status:

- För att kunna listas i CMVP:s Implementation Under Test List måste laboratoriet ha fått i uppdrag av Apple att tillhandahålla testning.
- När laboratoriet har slutfört testningen, laboratoriet har rekommenderat validering av CMVP och CMVP-arvodet har betalats läggs modulen sedan till i Modules in Process (MIP) List. MIP-listan spårar statusen för CMVP:s valideringsarbete i fyra faser:
  - *Review Pending:* Väntar på att CMVP-resurser ska tilldelas.
  - *In Review:* CMVP-resurser utför sina valideringsaktiviteter.
  - *Coordination:* Labbet och CMVP löser eventuella problem som har upptäckts.
  - *Finalization:* Aktiviteter och formalia gällande utfärdande av certifikatet.
- Efter validering av CMVP får modulerna ett certifikat för överensstämmelse och läggs till i listan med validerade kryptografiska moduler. Dessa inkluderar:
  - Validerade moduler är markerade som aktiva.
  - Efter 5 år markeras modulerna som historiska.
  - Om modulcertifikatet återkallas av någon anledning markeras det som återkallat.

2020 anammade CMVP den internationella standarden ISO/IEC 19790 som grund för FIPS 140-3.

FIPS 140-3-certifieringar

Aktuell status

tvOS 14 (2020) användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

tvOS 15 (2021) användarutrymme, kärnutrymme och säker nyckellagring genomgår laboratorietestning. De listas på Implementation Under Test List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* tvOS 15 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* tvOS 15 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribuerat med tvOS 15 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A10, A12) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* tvOS 14 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* tvOS 14 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med tvOS 14 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (A10, A12) *Övergripande säkerhetsnivå:* 2

FIPS 140-2-certifieringar

Tabellen nedan visar kryptografiska moduler som för närvarande testas och har testats av laboratoriet för överensstämmelse med FIPS 140-2.

tvOS 13 (2019) användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3856 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Operativsystem:* tvOS 13 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-03-23	*Certifikat:* 3855 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Operativsystem:* tvOS 13 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-02-05	*Certifikat:* 3811 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribuerat med tvOS 13 *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-23	*Certifikat:* 3438 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Operativsystem:* tvOS 12 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-11	*Certifikat:* 3433 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Operativsystem:* tvOS 12 *Typ:* Programvara *Säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3523 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribuerat med tvOS 12 *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-22, 2018-07-06	*Certifikat:* 3148 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Operativsystem:* tvOS 11 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-17, 2018-07-03	*Certifikat:* 3147 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Operativsystem:* tvOS 11 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3223 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribuerat med tvOS 11 *Typ:* Maskinvara *Säkerhetsnivå:* 2

Säkerhetscertifieringar för watchOS

Bakgrund till watchOS-certifiering

Apple deltar aktivt vid validering av kryptografiska moduler som associeras med varje större versionslansering av watchOS. Validering av överensstämmelsen kan endast ske med en färdig lanserad version.

Status för kryptografisk modulvalidering i watchOS

CMVP (Cryptographic Module Validation Program) upprätthåller valideringsstatusen för kryptografiska moduler i tre olika listor beroende på deras aktuella status:

- För att kunna listas i CMVP:s Implementation Under Test List måste laboratoriet ha fått i uppdrag av Apple att tillhandahålla testning.
- När laboratoriet har slutfört testningen, laboratoriet har rekommenderat validering av CMVP och CMVP-arvodet har betalats läggs modulen sedan till i Modules in Process (MIP) List. MIP-listan spårar statusen för CMVP:s valideringsarbete i fyra faser:
  - *Review Pending:* Väntar på att CMVP-resurser ska tilldelas.
  - *In Review:* CMVP-resurser utför sina valideringsaktiviteter.
  - *Coordination:* Labbet och CMVP löser eventuella problem som har upptäckts.
  - *Finalization:* Aktiviteter och formalia gällande utfärdande av certifikatet.
- Efter validering av CMVP får modulerna ett certifikat för överensstämmelse och läggs till i listan med validerade kryptografiska moduler. Dessa inkluderar:
  - Validerade moduler är markerade som aktiva.
  - Efter 5 år markeras modulerna som historiska.
  - Om modulcertifikatet återkallas av någon anledning markeras det som återkallat.

2020 anammade CMVP den internationella standarden ISO/IEC 19790 som grund för FIPS 140-3.

FIPS 140-3-certifieringar

Aktuell status

watchOS 7 (2020) användarutrymme, kärnutrymme och säker nyckellagring har testats av laboratoriet och laboratoriet har rekommenderat validering av CMVP. De listas i Modules in Process List.

watchOS 8 (2021) användarutrymme, kärnutrymme och säker nyckellagring genomgår laboratorietestning. De listas på Implementation Under Test List.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* watchOS 8 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* watchOS 8 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribuerat med watchOS 8 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (S3, S4, S5, S6) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2021 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v12 *Operativsystem:* sepOS distribuerat med watchOS 8 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (S6) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* watchOS 7 *Miljö:* Apple Silicon, användare, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* watchOS 7 *Miljö:* Apple-krets, kärna, programvara *Typ:* Programvara *Övergripande säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med watchOS 7 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (S3, S4, S5, S6) *Övergripande säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2020 *Valideringsdatum:* –	*Certifikat:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Module v11.1 *Operativsystem:* sepOS distribuerat med watchOS 7 *Miljö:* Apple-kretsar, säker nyckellagring, maskinvara *Typ:* Maskinvara (S6) *Övergripande säkerhetsnivå:* 2 *Fysisk säkerhetsnivå:* 3

FIPS 140-2-certifieringar

Tabellen nedan visar kryptografiska moduler som för närvarande testas och har testats av laboratoriet för överensstämmelse med FIPS 140-2.

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* –	*Certifikat:* 3856 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Operativsystem:* watchOS 6 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* –	*Certifikat:* 3855 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Operativsystem:* watchOS 6 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2019 *Valideringsdatum:* 2021-02-05	*Certifikat:* 3811 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Operativsystem:* sepOS distribuerat med watchOS 6 *Typ:* Maskinvara *Säkerhetsnivå:* 2

Datum	Certifikat/dokument	Modulinformation
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-23	*Certifikat:* 3438 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Operativsystem:* watchOS 5 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-04-11	*Certifikat:* 3433 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Operativsystem:* watchOS 5 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2018 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3523 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Operativsystem:* sepOS distribuerat med watchOS 5 *Typ:* Maskinvara *Säkerhetsnivå:* 2
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-22, 2018-07-06	*Certifikat:* 3148 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Operativsystem:* watchOS 4 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2018-03-09, 2018-05-17, 2018-07-03	*Certifikat:* 3147 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Operativsystem:* watchOS 4 *Typ:* Programvara *Säkerhetsnivå:* 1
Operativsystemets lanseringsdatum: 2017 *Valideringsdatum:* 2019-09-10	*Certifikat:* 3223 *Dokument:* Certifikat Säkerhetspolicy Vägledning för krypteringsansvarig	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Operativsystem:* sepOS distribuerat med watchOS 4 *Typ:* Maskinvara *Säkerhetsnivå:* 2

Säkerhetscertifieringar för programvara

Säkerhetscertifieringar för Apple-programvara i översikt

Apple upprätthåller valideringscertifikat om överensstämmelse med USA:s Federal Information Processing Standard (FIPS) 140-2/-3 för sepOS och fast T2-programvara liksom andra certifieringar. Apple utgår från *certifieringsbyggstenar* som används brett över flera plattformar där det är tillämpligt. En byggsten är valideringen av corecrypto som används vid driftsättning av kryptografiska moduler för program- och maskinvara inom de operativsystem som har utvecklats av Apple. En andra byggsten är certifieringen av Secure Enclave som finns inbyggd i många Apple-enheter. En tredje är certifieringen av Secure Element (SE) som finns i Apple-enheter med Touch ID och enheter med Face ID. Dessa byggstenar för maskinvarucertifiering utgör grunden för bredare säkerhetscertifieringar för plattformar.

Produktcertifieringar: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) är en standard som många organisationer utgår från vid säkerhetsutvärdering av IT-produkter.

Information om certifieringar som även kan vara internationellt erkända under CCRA (Common Criteria Recognition Arrangement) finns i Common Criteria Portal. Standarden Common Criteria kan också användas utanför CCRA av nationella och privata valideringsscheman. I Europa lyder ömsesidigt erkännande under SOG-IS-avtalet liksom CCRA.

Målet, som det anges av organisationen runt Common Criteria, är att en internationellt godkänd uppsättning säkerhetsstandarder ska tillhandahålla en tydlig och pålitlig utvärdering av säkerhetsfunktionerna i IT-produkter. Genom att tillhandahålla en oberoende utvärdering av en produkts möjlighet att uppnå säkerhetsstandarder ger Common Criteria-certifiering kunderna ökad kunskap om säkerheten för IT-produkter vilket leder till bättre underbyggda beslut.

Via CCRA har medlemsländerna kommit överens om att erkänna certifieringen av IT-produkter med samma nivå av tillförlitlighet. Utvärderingar som krävs inför certifiering är omfattande och inkluderar:

- Skyddsprofiler (Protection Profiles, PPs)
- Säkerhetsmål (Security Targets, STs)
- Säkerhetsfunktionskrav (Security Functional Requirements, SFRs)
- Säkerhetsförsäkranskrav (Security Assurance Requirements, SARs)
- Utvärderingsförsäkranskrav (Evaluation Assurance Levels, EALs)

Skyddsprofiler (Protection Profiles, PPs) är dokument som specificerar säkerhetskraven för en klass av enhetstyper som Mobility och används till att tillhandahålla jämförbarhet mellan utvärderingarna av IT-produkter inom samma klass. Antalet medlemmar i CCRA, tillsammans med en växande lista över godkända PPs, fortsätter att öka varje år. Detta arrangemang gör det möjligt för en produktutvecklare att sträva efter att uppnå en enskild certifiering under valfritt certifikatauktoriseringsschema och få den erkänd av övriga certifikatmottagande undertecknare.

Säkerhetsmål (STs) definierar *vad* som ska utvärderas när en IT-produkt ska certifieras. Dessa STs översätts till specifika *SFRs (Security Functional Requirements)* som används vid mer detaljerad utvärdering av dessa STs.

Common Criteria (CC) innehåller även *säkerhetsförsäkranskrav*. Ett vanligt identifierat mått är *Evaluation Assurance Level (EAL)*. EALs grupperar vanligt förekommande SARs-uppsättningar och kan anges i PPs och STs som stöd vid jämförelser.

Många äldre PPs har arkiverats och ersätts med målriktade PPs som utvecklas och fokuserar på specifika lösningar och miljöer. I en samlad process för att säkerställa ett fortsatt ömsesidigt erkännande från samtliga CCRA-medlemmar har iTCs (International Technical Communities) upprättats i syfte att utveckla och upprätthålla cPPs (Collaborative Protection Profiles) som utvecklas från grunden med användning av CCRA-undertecknings-scheman. PPs som riktar sig till användargrupper och andra ömsesidiga avtal om erkännande än CCRA fortsätter att utvecklas av respektive huvudaktörer.

Apple påbörjade strävan efter certifiering i enlighet med den uppdaterade CCRA:n med valda cPPs i början av 2015. Sedan dess har Apple uppnått Common Criteria-certifieringar för varje större iOS-versionslansering och har utökat täckningen till att inkludera den säkerhetsförsäkran som tillhandahålls av nya PPs.

Apple tar en aktiv roll inom tekniksamhället med fokus på att utvärdera tekniker för mobilsäkerhet. Dessa omfattar de iTCs som ansvarar för utveckling och uppdatering av cPPs. Apple fortsätter att utvärdera och sikta mot certifieringar i enlighet med de PPs och cPPs som finns idag.

Apples plattformscertifieringar för den nordamerikanska marknaden utförs normalt med NIAP (National Information Assurance Partnership) som upprätthåller en lista över projekt som är under utvärdering men ännu inte har certifierats.

Utöver de allmänna plattformscertifikaten som finns i listan har andra certifikat utfärdats för att peka på specifika säkerhetskrav för vissa marknader.

Säkerhetscertifieringar för Apple-appar

Bakgrund till certifiering av Apple-appar

Apple deltar aktivt vid säkerhetscertifieringar av Apple-appar med hjälp av tillämpliga Common Criteria-skyddsprofiler (PPs). Dessa utvärderingar bygger på de maskinvaru- och operativsystemscertifieringar som Apple har erhållit.

2018 tog Apple initiativ till appsäkerhetsutvärderingar för viktiga appar som körs i iOS 11 med webbläsaren Safari och appen Kontakter. Apple fortsatte dessa utvärderingar av appar som körs i iOS 12, iOS 13 och iPadOS 13.1. Under 2021 blir täckning för appar som körs i macOS 11 tillagd.

Status för kryptografisk modulcertifiering

Apple-appar som listas här använder de kryptografiska modulerna för tillämpligt operativsystem. Mer information finns i Säkerhetscertifieringar för iOS, Säkerhetscertifieringar för iPadOS och Säkerhetscertifieringar för macOS.

CC-certifieringsstatus (Common Criteria)

USA-schemat, som drivs av NIAP, upprätthåller listan Products in Evaluation. Denna lista innehåller produkter som för närvarande utvärderas i USA via ett NIAP-godkänt Common Criteria Testing Laboratory (CCTL) och som har slutfört ett Evaluation Kick off Meeting (eller likvärdigt) där CCEVS-ledningen officiellt har accepterat produkten för utvärdering.

När produkter har certifierats placerar NIAP aktuella giltiga certifieringar på Product Compliant List. Efter två år granskas certifieringarna gällande deras överensstämmelse med den aktuella policyn för säkerhetsunderhåll. När datum för säkerhetsunderhåll har passerats flyttar NIAP certifieringslistningen till Archived Products List.

Common Criteria Portal listar certifieringar som kan vara ömsesidigt erkända i enlighet med Common Criteria Recognition Arrangement (CCRA). CC-portalen kan behålla produkter på listan för certifierade produkter under fem år och dessa poster sparas i CC-portalen för arkiverade certifieringar.

Tabellen nedan visar de certifieringar som för närvarande utvärderas av ett laboratorium eller har certifierats som överensstämmande med Common Criteria.

Aktuell status

- Utvärderingar via NIAP som publiceras som pågående listas på Products in evaluation (NIAP).
- Utvärderingar som har slutförts och har validerats listas på NIAP:s Product Compliant List.

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: macOS 11 Big Sur *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* macOS 11 Big Sur: Contacts *Skyddsprofiler:* PP för applikationsprogramvara, EP för webbläsare
Operativsystem: macOS 11 Big Sur *Certifieringsdatum:* –	*Schema-ID:* Inte certifierat ännu *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* macOS 11 Big Sur: Safari *Skyddsprofiler:* PP för applikationsprogramvara, EP för webbläsare
Operativsystem: iOS 14, iPadOS 14 *Certifieringsdatum:* 2021-08-20	*Schema-ID:* 11191 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple iOS 14 and iPadOS 14: Contacts *Skyddsprofiler:* PP för applikationsprogramvara, EP för webbläsare
Operativsystem: iOS 14, iPadOS 14 *Certifieringsdatum:* –	*Schema-ID:* 11192 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple iOS 14 and iPadOS 14: Safari *Skyddsprofiler:* PP för applikationsprogramvara, EP för webbläsare
Operativsystem: iOS 13, iPadOS 13 *Certifieringsdatum:* 2020-06-05	*Schema-ID:* 11060 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple iOS 13 and iPadOS 13: Safari *Skyddsprofiler:* PP för applikationsprogramvara, EP för webbläsare

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: iOS 13, iPadOS 13 *Certifieringsdatum:* 2020-06-05	*Schema-ID:* 11050 *Dokument:* Certifikat Säkerhetsmål Vägledning Valideringsrapport Revisionsverksamhetsrapport	*Titel:* Apple iOS 13 and iPadOS 13: Contacts *Skyddsprofiler:* PP för programvara

Arkiverade Common Criteria-certifieringar för Apple-appar

Operativsystem/certifieringsdatum	Schema-ID/dokument	Titel/skyddsprofiler
Operativsystem: iOS 12 *Certifieringsdatum:* 2019-06-12	*Schema-ID:* 10960 *Dokument:* Säkerhetsmål Vägledning	*Titel:* iOS 12 Safari *Skyddsprofiler:* PP för programvara, EP för webbläsare
Operativsystem: iOS 12 *Certifieringsdatum:* 2019-02-28	*Schema-ID:* 10961 *Dokument:* Säkerhetsmål Vägledning	*Titel:* iOS 12 Contacts *Skyddsprofiler:* PP för programvara
Operativsystem: iOS 11 *Certifieringsdatum:* 2018-11-09	*Schema-ID:* 10916 *Dokument:* Säkerhetsmål Vägledning	*Titel:* iOS 11 Safari *Skyddsprofiler:* PP för programvara, EP för webbläsare
Operativsystem: iOS 11 *Certifieringsdatum:* 2018-09-13	*Schema-ID:* 10915 *Dokument:* Säkerhetsmål Vägledning	*Titel:* iOS 11 Contacts *Skyddsprofiler:* PP för programvara

Säkerhetscertifieringar för Apples internettjänster

Apple upprätthåller certifieringar i enlighet med standarderna ISO/IEC 27001 och ISO/IEC 27018 för att göra det möjligt för Apples kunder att efterleva sina skyldigheter enligt föreskrifter och avtal. Dessa certifieringar ger våra kunder tillgång till ett oberoende intyg på Apples praxis vad gäller informationssäkerhet och integritet för de system som omfattas av certifieringarna.

ISO/IEC 27001 och ISO/IEC 27018 ingår i en uppsättning standarder gällande säkerhetshantering för informationssystem (Information Security Management System, ISMS) som publiceras av ISO (International Organization for Standardization). Som en del av Apples ISMS har alla kontrollkrav i bilaga A inkluderats i Statement of Applicability (uttalande om tillämplighet) enligt definitionerna i standarderna ISO/IEC 27001 och ISO/IEC 27018. Apple genomgår årligen en oberoende attestering av en godkänd registrator.

ISO/IEC 27001

ISO/IEC 27001 är en standard gällande hanteringssystem för informationssäkerhet som anger krav för att upprätta, implementera, underhålla och kontinuerligt förbättra en organisations hanteringssystem för informationssäkerhet. Standarden ISO/IEC 27001 omfattar följande säkerhetsdomäner som omfattas av Apples ISO/IEC-certifieringar:

- Informationssäkerhetspolicyer
- Organisering av informationssäkerhet
- Resurshantering
- Mänsklig resurssäkerhet
- Fysisk och miljömässig säkerhet
- Kommunikations- och drifthantering
- Åtkomststyrning
- Förvärv av informationssystem, utveckling och underhåll
- Hantering av informationssäkerhetsincidenter
- Hantering av företagskontinuitet
- Överensstämmelse

ISO/IEC 27018

ISO/IEC 27018 är en förfarandekod för skydd av personligt identifierbar information (PII) i offentliga molnmiljöer. Standarden ISO/IEC 27018 omfattar följande säkerhetsdomäner som omfattas av Apples ISO/IEC-certifieringar:

- Samtycke och val
- Legitimitet och specifikation av syfte
- Begränsning av insamling
- Dataminimering
- Begränsning av användning, lagring och underrättelse
- Riktighet och kvalitet
- Öppenhet, insyn och meddelande
- Individuellt deltagande och åtkomst
- Ansvarsskyldighet
- Informationssäkerhet
- Integritetsöverenstämmelse

Apple-tjänster omfattas av ISO/IEC 27001 och ISO/IEC 27018

Apples ISO/IEC 27001- och ISO/IEC 27018-certifieringar omfattar följande tjänster:

- Kundchatt
- Apple Business Manager
- APNs (Apples tjänst för pushnotiser)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork-tjänster
- Hanterade Apple-ID:n
- Skolarbete
- Siri

Certifieringar

Bevis för Apples ISO/IEC 27001- och 27018-certifieringar finns hos vår registrator.

Du kan granska Apples certifieringar genom att besöka Certificate and Client Directory search på webbplatsen för British Standards Institution (BSI), ange Apple i sökfältet Company, klicka på knappen Search och sedan välja sökträffar för att granska certifikaten.

Obs! Information om produkter som inte tillverkas av Apple, eller fristående webbplatser som inte administreras eller testas av Apple, tillhandahålls utan att utgöra en rekommendation. Apple lämnar inga som helst garantier gällande urval, prestanda eller användning av webbplatser eller produkter från tredje part. Apple lämnar inga som helst utsagor gällande riktighet eller tillförlitlighet hos webbplatser från tredje part. Kontakta leverantören för ytterligare information.

macOS Security Compliance Project

macOS Security Compliance Project (mSCP) är ett öppet projekt som arbetar med att generera säkerhetsvägledning genom ett programmatiskt tillvägagångssätt. Det är ett gemensamt projekt mellan federal driftpersonal inom IT-säkerhet från National Institute of Standards and Technology (NIST), National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA) och Los Alamos National Laboratory (LANL). Projektet använder en uppsättning testade och validerade kontroller för macOS och kopplar dessa kontroller till eventuella säkerhetsvägledningar som stöds av projektet. Dessutom kan projektet användas som en resurs för att enkelt skapa anpassade säkerhetsbaslinjer med tekniska säkerhetskontroller genom att dra nytta av ett bibliotek med testade och validerade atomåtgärder (konfigurationsinställningar). Projektet skapar anpassad dokumentation, skript, konfigurationsprofiler och en granskningschecklista som baseras på den använda baslinjen.

mSCP kan skapa innehåll för användning i kombination med hanterings- och säkerhetsverktyg för att åstadkomma överensstämmelse. Konfigurationsinställningarna i projektet stöder följande vägledningsbaslinjer:

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

Ytterligare information:

- En baslinje för granskning av alla regler i projektet finns här.
- Du kan läsa mer om projektet och dess användning på wiki-sidan om macOS Security Compliance Project.
- Förbered projektet för användning genom att läsa följande: Getting to Know the macOS Security Compliance Project, Part 1 och Getting to Know the macOS Security Compliance Project, Part 2.
- Om du vill bidra till det vidare arbetet på projektet kan du läsa riktlinjerna för deltagande.

Dokumentets versionshistorik

Datum	Sammanfattning
27 oktober 2021	Uppdaterade ämnen: • Säkerhetscertifieringar för Secure Enclave-processorn • Säkerhetscertifieringar för iOS • Säkerhetscertifieringar för macOS
17 augusti 2021	Uppdaterade ämnen: • Säkerhetscertifieringar för Secure Enclave-processorn • Säkerhetscertifieringar för Apples T2-säkerhetskrets • Säkerhetscertifieringar för iOS • Säkerhetscertifieringar för iPadOS • Säkerhetscertifieringar för macOS • Säkerhetscertifieringar för tvOS • Säkerhetscertifieringar för watchOS • Säkerhetscertifieringar för Apple-appar • Säkerhetscertifieringar • macOS Security Compliance Project
26 april 2021	Tillagt ämne: • macOS Security Compliance Project Uppdaterade ämnen: • Säkerhetscertifieringar för Apples T2-säkerhetskrets: Ny FIPS 140-2-certifiering, 3811 • Säkerhetscertifieringar för Secure Enclave-processorn: Ny FIPS 140-2-certifiering, 3811 och ny tabell för ytterligare certifieringar. • Säkerhetscertifieringar för iOS: Nya FIPS 140-2-certifieringar, 3811, Schema-ID 11146 för iOS 14 under utvärdering • Säkerhetscertifieringar för iPadOS: Nya FIPS 140-2-certifieringar, 3811, Schema-ID 11147 för iPadOS 14 under utvärdering • Säkerhetscertifieringar för macOS: Ny FIPS 140-2-certifiering, 3811. • Säkerhetscertifieringar för tvOS: Nya FIPS 140-2-certifieringar, 3811. • Säkerhetscertifieringar för watchOS: Nya FIPS 140-2-certifieringar, 3811. • Säkerhetscertifieringar för Apple-appar: Uppdateringar av Common Criteria-status och ny tabell för arkiverade Common Criteria-certifieringar.

Ordlista

APNs (Apples tjänst för pushnotiser) En världsomspännande tjänst från Apple som levererar pushnotiser till Apple-enheter.

Apple Business Manager En enkel, webbaserad portal för IT-administratörer som gör att organisationer snabbt och smidigt kan driftsätta Apple-enheter som organisationen har köpt direkt av Apple eller via auktoriserade Apple-återförsäljare och operatörer som deltar. De kan automatiskt registrera enheter i sin MDM-lösning utan att behöva förbereda eller ens röra vid själva enheterna innan användarna får dem.

Apple School Manager En enkel, webbaserad portal för IT-administratörer som gör att organisationer snabbt och smidigt kan driftsätta Apple-enheter som organisationen har köpt direkt av Apple eller via auktoriserade Apple-återförsäljare och operatörer som deltar. De kan automatiskt registrera enheter i sin MDM-lösning utan att behöva förbereda eller ens röra vid själva enheterna innan användarna får dem.

CAVP (Cryptographic Algorithm Validation Program) En organisation som drivs av NIST i syfte att tillhandahålla valideringstestning av godkända (exempelvis FIPS-godkända och NIST-rekommenderade) kryptografiska algoritmer och deras enskilda komponenter.

CC (Common Criteria) En standard som upprättar de generella koncepten och principerna för utvärdering av IT-säkerhet och specificerar en allmän utvärderingsmodell. Den omfattar kataloger med säkerhetskrav på ett standardiserat språk.

CCRA (Common Criteria Recognition Arrangement) Ett ömsesidigt avtal om erkännande som fastställer de policyer och krav som gäller för internationellt erkännande av certifikat som har utfärdats i enlighet med ISO/IEC 15408-serien eller Common Criteria-standarderna.

CMVP (Cryptographic Module Validation Program) En organisation som drivs av myndigheter i USA och Kanada i syfte att validera överensstämmelse med standarden FIPS 140-3.

corecrypto Ett bibliotek som tillhandahåller implementeringar av kryptografiska primitiv på låg nivå. Observera att corecrypto inte direkt tillhandahåller programmeringsgränssnitt för utvecklare utan används via API:er som utvecklare får tillgång till. Källkoden till corecrypto är offentligt tillgänglig så att dess säkerhetsegenskaper och funktionalitet kan verifieras.

cPP (collaborative Protection Profile) En skyddsprofil (Protection Profile) som är utvecklad av en internationell teknisk kommitté bestående av experter som har till uppgift att skapa cPP:er.

Federal Information Processing Standard (FIPS) Publikationer som utvecklas av National Institute of Standards and Technology i USA, antingen enligt regelverk eller när det finns övertygande myndighetskrav gällande cybersäkerhet eller både och.

Full Disk Encryption (FDE) Kryptering av alla data på en lagringsvolym

Implementation under Test (IUT) En kryptografisk modul som testas av ett laboratorium.

Information Security Management System (ISMS) En uppsättning informationssäkerhetspolicyer och processer som styr gränserna hos ett säkerhetsprogram som är utformat för att skydda en mängd information och system genom att systematiskt hantera informationssäkerhet under hela informations- och/eller systemlivscykeln.

international Technical Community (iTC) En grupp som ansvarar för utveckling av Protection Profiles eller collaborative Protection Profiles i enlighet med Common Criteria Recognition Arrangement (CCRA).

IPsec VPN-klient I en Protection Profile är det här en klient som tillhandahåller en säker IPsec-anslutning mellan en fysisk eller virtuell värdplattform och en fjärrplats.

kryptografisk modul Den maskinvara, programvara och/eller fasta programvara som tillhandahåller kryptografiska funktioner och uppfyller kraven hos en angiven kryptografisk modulstandard.

MDM (Mobile Device Management) En tjänst som användaren kan använda till att fjärrhantera registrerade enheter. När en enhet är registrerad kan användaren använda MDM-tjänsten via nätverket till att konfigurera inställningar och utföra andra åtgärder på enheten utan att enhetsanvändaren behöver göra något.

MIP (Modules in Process) En lista som upprätthålls av Cryptographic Module Validation Program (CMVP) och innehåller kryptografiska moduler som för närvarande genomgår CMVP-valideringsprocessen.

NIAP (National Information Assurance Partnership) En myndighetsorganisation i USA som ansvarar för att driva USA:s implementering av Common Criteria-standarden och hantering av NIAP:s CCEVS (Common Criteria Evaluation and Validation Scheme).

NIST (National Institute of Standards and Technology) En del av USA:s handelsdepartement som ansvarar för att främja mätvetenskap, -standarder och -teknik.

Secure Element (SE) En kiselkrets som är inbäddad i många Apple-enheter som ger stöd för funktioner som Apple Pay.

Secure Enclave Processor (SEP) En coprocessor som ingår inuti en SoC (System on Chip).

Senior Officials Group Information Systems Security (SOG-IS) En grupp som hanterar ett ömsesidigt avtal om erkännande mellan flera europeiska länder.

sepOS Den fasta maskinvaran för Secure Enclave, baserad på en Apple-anpassad version av L4-mikrokärnan.

Skyddsprofil (Protection Profile, PP) Ett dokument som specificerar säkerhetsproblem och säkerhetskrav för en viss klass av produkter.

SOA (Statement of Applicability) Ett dokument som beskriver de säkerhetskontroller som implementerats inom tillämpningen av en ISM som tagits fram som stöd för en ISO/IEC 27001-certifiering.

SoC (System on Chip) En integrerad krets (IC) där flera komponenter är samlade på en krets.

Säkerhetsmål (Security Target, ST) Ett dokument som specificerar säkerhetsproblem och säkerhetskrav för en viss produkt.

Säkerhetsnivå (Security Level, SL) De fyra övergripnde säkerhetsnivåer (1-4) som definieras i ISO/IEC 19790 för att beskriva uppsättningar av tillämpliga säkerhetskrav. Nivå 4 är den striktaste.

T2 En Apple-säkerhetskrets som ingår i en del Intel-baserade Mac-datorer från och med 2017.

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

S028-00499-B