Centro per le certificazioni di sicurezza e la compliance

Dicembre 2021

Indice

Introduzione alla garanzia della sicurezza di Apple 4

Certificazioni per l'hardware 5

Certificazioni per il software e per le app 5

Certificazioni per i servizi 6

Certificazioni di sicurezza per l'hardware 7

Panoramica sulle certificazioni di sicurezza dell'hardware Apple 7

Certificazioni di sicurezza per il processore Secure Enclave 10

Certificazioni di sicurezza per il chip di sicurezza Apple T2 15

Certificazioni di sicurezza dei sistemi operativi 19

Panoramica sulle certificazioni di sicurezza dei sistemi operativi Apple 19

Certificazioni di sicurezza per iOS 23

Certificazioni di sicurezza per iPadOS 30

Certificazioni di sicurezza per macOS 36

Certificazioni di sicurezza per tvOS 44

Certificazioni di sicurezza per watchOS 48

Certificazioni di sicurezza per il software 52

Panoramica sulle certificazioni di sicurezza del software Apple 52

Certificazioni di sicurezza per le app Apple 54

Certificazioni di sicurezza per i servizi internet Apple 57

ISO/IEC 27001 57

ISO/IEC 27018 58

Servizi Apple coperti dagli standard ISO/IEC 27001 e ISO/IEC 27018 58

Certificati 59

macOS Security Compliance Project 60

Cronologia delle revisioni del documento 61

Glossario 62

Introduzione alla garanzia della sicurezza di Apple

Come parte del proprio impegno nei confronti della sicurezza, Apple si rivolge regolarmente a organizzazioni di terze parti per la certificazione e per la verifica della sicurezza dell'hardware, del software e dei servizi Apple. Tali organizzazioni, riconosciute a livello internazionale, forniscono ad Apple certificazioni allineate con ciascuna versione principale dei suoi sistemi operativi. Tali certificazioni offrono una misurazione del livello di affidabilità (ossia della garanzia di sicurezza) del fatto che i requisiti di sicurezza di un sistema siano soddisfatti. Per le aree tecniche che non sono ricomprese nell'ambito di accordi di riconoscimento reciproco o per le quali non esistono standard per la certificazione della sicurezza consolidati, Apple si occupa dello sviluppo degli standard di sicurezza necessari. La nostra missione è raggiungere una copertura completa e accettata a livello globale per le certificazioni di sicurezza relative a tutti i componenti hardware, i sistemi operativi, le app e i servizi di Apple.

Le certificazioni sono spesso necessarie per soddisfare i requisiti legali e regolamentari e le prassi del settore. Servizi come Apple School Manager e Apple Business Manager sono coperti dalla certificazioni Apple ISO/IEC 27001 e ISO/IEC 27018. Tutti i clienti, tra cui le agenzie governative, le organizzazioni aziendali e le organizzazioni didattiche che utilizzano dispositivi Apple, possono utilizzare le certificazioni per l'hardware, per i sistemi operativi, per il software e per i servizi per dimostrare la propria conformità agli standard.

Certificazioni per l'hardware

Dal momento che un software sicuro richiede delle fondamenta di sicurezza integrate nell'hardware, tutti i dispositivi Apple, sia che eseguano iOS, iPadOS, macOS, tvOS o watchOS, presentano funzionalità di sicurezza progettate all'interno dei chip. Queste includono caratteristiche delle CPU personalizzate alla base di funzionalità di sicurezza del sistema e chip dedicati alle operazioni di sicurezza. Il componente più importante è il coprocessore Secure Enclave, presente su tutti i più moderni dispositivi iOS, iPadOS, watchOS e tvOS, su tutti i Mac dotati di chip Apple e sui Mac dotati di processore Intel con chip di sicurezza Apple T2. Secure Enclave è alla base della codifica dei dati a riposo, dell'avvio protetto in macOS e delle misurazioni biometriche.

L'impegno di Apple nel campo della garanzia della sicurezza parte dalle certificazioni dei componenti fisici di sicurezza fondamentali, dalla radice di attendibilità hardware all'implementazione dell'avvio protetto, dall'archiviazione sicura delle chiavi in Secure Enclave all'autenticazione sicura tramite Touch ID e Face ID. Le funzionalità di sicurezza dei dispositivi Apple sono rese possibili dalla combinazione di progettazione dei chip, hardware, software e servizi, un'integrazione che solo Apple è in grado di fornire. La certificazione di tali componenti è una parte importante della verifica della garanzia di sicurezza offerta da Apple.

Per informazioni sulle certificazioni pubbliche relative all'hardware e ai componenti firmware associati, consulta:

- Certificazioni di sicurezza per il chip di sicurezza Apple T2
- Certificazioni di sicurezza per il processore Secure Enclave

Certificazioni per il software e per le app

Apple mantiene certificazioni e attestazioni indipendenti sui propri sistemi operativi e app in conformità con gli standard americani FIPS (Federal Information Processing Standards) 140-2/-3 per i moduli crittografici e Common Criteria per i sistemi operativi, le app e i servizi per i dispositivi. I sistemi operativi coperti dalle certificazioni includono iOS, iPadOS, macOS, sepOS, il firmware del chip T2, tvOS e watchOS. Per quanto riguarda le app, le certificazioni indipendenti includeranno inizialmente il browser Safari e l'app Contatti, con altre app che saranno certificate in futuro.

Per informazioni sulle certificazioni pubbliche relative ai *sistemi operativi* Apple, consulta:

- Certificazioni di sicurezza per iOS
- Certificazioni di sicurezza per iPadOS
- Certificazioni di sicurezza per macOS
- Certificazioni di sicurezza per tvOS
- Certificazioni di sicurezza per watchOS

Per informazioni sulle certificazioni pubbliche relative alle *app* Apple, consulta:

- Certificazioni di sicurezza per le app Apple

Certificazioni per i servizi

Apple mantiene certificazioni di sicurezza per supportare i propri clienti, dagli ambienti aziendali a quelli didattici. Queste certificazioni consentono ai clienti Apple di ottemperare ai propri obblighi normativi e contrattuali quando utilizzano i servizi Apple tramite l'hardware e il software Apple. Esse forniscono inoltre ai nostri clienti un'attestazione indipendente sulle pratiche adottate da Apple in materia di sicurezza delle informazioni, privacy e tutela dell'ambiente per i sistemi Apple.

Per informazioni sulle certificazioni pubbliche relative ai *servizi internet* di Apple, consulta:

- Certificazioni di sicurezza per i servizi internet Apple

Per domande sulle certificazioni per la sicurezza e la privacy di Apple, contatta security-certifications@apple.com.

Certificazioni di sicurezza per l'hardware

Panoramica sulle certificazioni di sicurezza dell'hardware Apple

Apple mantiene certificati di convalida della conformità agli standard FIPS (Federal Information Processing Standard) 140-2/-3 per il firmware sepOS, per il firmware del chip T2 e per altre certificazioni. Apple parte da una serie di *blocchi costituenti delle certificazioni*, applicabili ad ampio raggio a più piattaforme a seconda delle necessità. Uno dei blocchi costituenti è la convalida tramite corecrypto, la libreria utilizzata per l'implementazione dei moduli crittografici software e hardware all'interno dei sistemi operativi sviluppati da Apple. Un secondo blocco costituente è la certificazione di Secure Enclave, un coprocessore integrato in molti dispositivi Apple. Un terzo è la certificazione di Secure Element, presente nei dispositivi Apple dotati di Touch ID e di Face ID. Questi blocchi costituenti delle certificazioni hardware costituiscono le fondamenta per certificazioni di sicurezza delle piattaforme più ampie.

Convalide degli algoritmi crittografici

La convalida della corretta implementazione di molti algoritmi crittografici e delle relative funzionalità di sicurezza è un prerequisito per la convalida FIPS 140-3 e supporta altre certificazioni. La convalida viene gestita tramite il Cryptographic Algorithm Validation Program (CAVP) del National Institute of Standards and Technology (NIST). I certificati di convalida delle implementazioni Apple sono reperibili tramite la pagina di ricerca del CAVP. Per ulteriori informazioni, consulta il sito web del Cryptographic Algorithm Validation Program (CAVP).

Convalide dei moduli crittografici: FIPS 140-2/3 (ISO/IEC 19790)

Il Cryptographic Module Validation Program (CMVP) ha ripetutamente convalidato la conformità dei moduli crittografici di Apple allo standard FIPS (Federal Information Processing Standards) 140-2 degli Stati Uniti dopo l'uscita di ogni versione principale dei sistemi operativi dal 2012. Dopo l'uscita di ogni versione principale, Apple invia i moduli al CMVP per una convalida della conformità allo standard. Oltre a essere utilizzati dai sistemi operativi e dalle app Apple, questi moduli offrono funzionalità crittografiche anche ai servizi forniti da Apple e sono inoltre utilizzabili dalle app di terze parti.

Apple ottiene ogni anno il **livello di sicurezza 1** per i moduli basati sul software "Corecrypto Module for Intel" e "Corecrypto Kernel Module for Intel" per macOS. Per i chip Apple, i moduli "Corecrypto Module for ARM" e "Corecrypto Kernel Module for ARM" sono applicabili ad iOS, iPadOS, tvOS e watchOS e al firmware sul chip di sicurezza Apple T2 integrato nei Mac.

Nel 2019, Apple ha ottenuto il primo **livello di sicurezza 2** FIPS 140-2 per il modulo crittografico hardware integrato conosciuto come "Apple Corecrypto Module: Secure Key Store", che consente l'uso approvato dal governo degli Stati Uniti delle chiavi generate e gestite in Secure Enclave. Apple continua a perseguire le convalide per i moduli crittografici hardware per ogni successiva versione principale dei sistemi operativi.

FIPS 140-3 è stato approvato dal Dipartimento del commercio degli Stati Uniti nel 2019. La modifica più significativa di questa versione dello standard è la specificazione di standard ISO/IEC, in particolare, ISO/IEC 19790:2015 e dei relativi standard di test ISO/IEC 24759:2017. Il CMVP ha avviato un programma di transizione e ha indicato che, all'inizio del 2020, i moduli crittografici inizieranno a essere convalidati usando il FIPS 140-3 come base. I moduli crittografici di Apple puntano a soddisfare lo standard FIPS 140-3 e a passare a esso il prima possibile.

Per i moduli crittografici attualmente in fase di test e di convalida, il CMVP mantiene due elenchi separati che potrebbero contenere informazioni sulle convalide proposte. I moduli crittografici in fase di test da parte di un laboratorio accreditato potrebbero essere presenti nell'elenco dei moduli con implementazione in fase di test. Una volta che il laboratorio ha completato i test e ha richiesto la convalida da parte del CMVP, i moduli crittografici Apple compaiono nell'elenco dei moduli in lavorazione. Attualmente i test di laboratorio sono completi e si attende la convalida degli stessi da parte del CMVP. Dal momento che la durata del processo di valutazione è variabile, consulta entrambi questi elenchi per determinare lo stato attuale dei moduli crittografici Apple tra la data di uscita di una versione principale di un sistema operativo e l'emissione del certificato di convalida da parte del CMVP.

Certificazioni dei prodotti: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) è uno standard utilizzato da molte organizzazioni come base per valutare la sicurezza dei prodotti informatici.

Per le certificazioni che potrebbero essere riconosciute reciprocamente dal Common Criteria Recognition Arrangement (CCRA), vai sul portale di Common Criteria. Lo standard Common Criteria potrebbe essere utilizzato anche al di fuori del CCRA da schemi di convalida nazionali e privati. In Europa, il riconoscimento reciproco è governato dall'accordo SOG-IS e dal CCRA.

L'obiettivo, così come dichiarato dalla comunità di Common Criteria, è quello di ottenere un insieme di standard di sicurezza approvato a livello internazionale, così da poter fornire una valutazione chiara e affidabile delle funzionalità di sicurezza dei prodotti informatici. Fornendo un controllo indipendente della capacità di un prodotto di soddisfare degli standard di sicurezza, la certificazione Common Criteria rafforza la fiducia dei clienti rispetto alla sicurezza dei prodotti informatici, consentendo loro di prendere decisioni più informate.

Tramite il CCRA, i paesi aderenti hanno concordato di riconoscere la certificazione dei prodotti informatici con lo stesso livello di attendibilità. Le valutazioni richieste prima della certificazione sono ampie e includono:

- Profili di protezione
- Obiettivi di sicurezza
- Requisiti funzionali di sicurezza
- Requisiti di garanzia
- Livelli di garanzia della valutazione

I profili di protezione sono documenti che specificano i requisiti di sicurezza per una classe di dispositivi, come ad esempio la classe Mobility per i dispositivi mobili, e sono utilizzati per consentire il confronto tra le valutazioni dei prodotti informatici all'interno della stessa classe. I membri del CCRA continuano a crescere di anno in anno di pari passo con il numero dei profili di protezione approvati. Questo impianto consente a chi sviluppa un prodotto di conseguire una singola certificazione secondo uno qualsiasi degli schemi di autorizzazione per le certificazioni e di ottenere il riconoscimento da qualsiasi firmatario dei certificati stessi.

Gli obiettivi di sicurezza definiscono *cosa* verrà valutato quando un prodotto informatico è in fase di certificazione. Gli obiettivi di sicurezza vengono tradotti in *requisiti funzionali di sicurezza* più specifici, utilizzati per valutare tali obiettivi più dettagliatamente.

Lo standard Common Criteria (CC) include anche *requisiti per la garanzia di sicurezza*. Uno dei fattori comunemente identificati è il *livello di garanzia della valutazione*. I livelli di garanzia della valutazione, a loro volta, raggruppano i requisiti di garanzia utilizzati comunemente e possono essere specificati in profili di protezione e obiettivi di sicurezza per consentire il confronto.

Molti profili di protezione meno recenti sono stati archiviati e verrano man mano sostituiti da profili di protezione mirati, incentrati su soluzioni e ambienti specifici. In un impegno coordinato mirato a garantire un riconoscimento reciproco tra tutti i membri del CCRA, sono state costituite delle comunità tecniche internazionali (iTC, international Technical Communities) volte a sviluppare e mantenere profili di protezione collaborativi che sono creati fin dall'inizio tenendo conto degli schemi dei firmatari del CCRA. I profili di protezione destinati a gruppi di utenti e accordi di riconoscimento reciproco diversi dal CCRA continuano ad essere sviluppati dalle parti appropriate interessate.

Apple ha iniziato a perseguire certificazioni secondo la versione aggiornata del CCRA con alcuni profili di protezione collaborativi dall'inizio del 2015. Da allora, Apple ha ottenuto certificazioni Common Criteria per ogni versione principale di iOS e ha ampliato la copertura per includere la garanzia di sicurezza fornita dai nuovi profili di protezione.

Apple assume un ruolo attivo all'interno delle comunità tecniche impegnate nella valutazione delle tecnologie di sicurezza dei dispositivi mobili. Queste includono le iTC responsabili dello sviluppo e dell'aggiornamento dei profili di protezione collaborativi. Apple continua a valutare e a perseguire certificazioni per tutti gli attuali profili di protezione e profili di protezione collaborativi.

Le certificazioni delle piattaforme Apple per il mercato del Nord America vengono generalmente effettuate tramite la National Information Assurance Partnership (NIAP), che mantiene un elenco dei progetti attualmente in fase di valutazione, ma non ancora certificati.

Oltre ai certificati generali per le piattaforme elencati, altri certificati sono stati emessi per dimostrare specifici requisiti di sicurezza per alcuni mercati.

Certificazioni di sicurezza per il processore Secure Enclave

Contesto delle certificazioni Secure Enclave

Il modulo crittografico hardware *Apple SEP Secure Key Store Cryptographic Module* è integrato nel system on a chip (SoC) Apple che si trova nei seguenti prodotti: i chip Apple della serie A per iPhone e iPad, i chip Apple della serie M per i computer Mac con chip Apple, i chip della serie S per Apple Watch e i chip di sicurezza della serie T presenti nei computer Mac basati su processore Intel a partire dai modelli di iMac Pro introdotti sul mercato nel 2017.

Nel 2018, Apple ha convalidato i moduli crittografici software sincronizzandoli con i sistemi operativi rilasciati nel 2017: iOS 11, macOS 10.13, tvOS 11 e watchOS 4. Il modulo crittografico hardware SEP identificato come Apple SEP Secure Key Store Cryptographic Module v1.0 è stato inizialmente convalidato secondo i requisiti del livello di sicurezza 1 dello standard FIPS 140-2.

Nel 2019, Apple ha convalidato il modulo hardware secondo i requisiti per il livello di sicurezza 2 dello standard FIPS 140-2 e ha aggiornato l'identificativo della versione del modulo a v9.0 per sincronizzarlo alle versioni delle convalide dei moduli corecrypto User e corecrypto Kernel corrispondenti, che, nel 2019, includevano iOS 12, macOS 10.14, tvOS 12 e watchOS 5.

Nel 2020 e 2021, Apple ha continuato e continua a perseguire le convalide per la conformità con lo standard FIPS 140-3 e con requisiti aggiuntivi per la garanzia di livello 3 della sicurezza fisica per i seguenti chip Apple: chip A13, A14, S6 e M1.

Apple si impegna in maniera attiva anche nella convalida dei moduli corecrypto User e corecrypto Kernel per ogni versione principale dei propri sistemi operativi. La convalida di conformità può essere effettuata solo rispetto a una versione finale già uscita.

Stato delle convalide dei moduli crittografici

Il Cryptographic Module Validation Program (CMVP) riporta lo stato della convalida dei moduli crittografici in tre elenchi separati a seconda del loro stato attuale.

- Per comparire nell'elenco dei moduli con implementazione in fase di test del CMVP, il laboratorio deve aver firmato un contratto con Apple per poter fornire i test.
- Dopo che il laboratorio ha completato i test, richiesto la convalida da parte del CMVP e pagato le tariffe CMVP, il modulo viene aggiunto all'elenco dei moduli in lavorazione. Questo elenco tiene traccia del processo di convalida da parte del CMVP in quattro fasi:
  - *In attesa di revisione:* in attesa dell'assegnazione delle risorse del CMVP.
  - *In fase di revisione:* le risorse del CMVP stanno eseguendo le attività di convalida.
  - *Coordinamento:* il laboratorio e il CMVP stanno risolvendo eventuali problemi riscontrati.
  - *Finalizzazione:* sono in corso le attività e le formalità relative all'emissione del certificato.
- Dopo la convalida da parte del CMVP, i moduli ricevono un certificato di conformità e vengono aggiunti all'elenco dei moduli crittografici convalidati. Questo include:
  - Moduli convalidati contrassegnati come attivi.
  - Dopo 5 anni, i moduli sono contrassegnati come "storici".
  - Se, per qualche ragione, il certificato viene revocato, allora questo viene contrassegnato come revocato.

Nel 2020, il CMVP ha adottato lo standard internazionale ISO/IEC 19790 come base dello standard FIPS 140-3.

Certificazioni FIPS 140-3

Stato attuale

La tabella di seguito mostra i moduli crittografici del 2020 e del 2021 che sono attualmente in fase di test di laboratorio per la conformità allo standard FIPS 140-3.

L'archiviazione sicura delle chiavi (SKS, Secure Key Store) associata alle versioni 2020 e 2021 dei sistemi operativi ha superato i test di laboratorio ed è stato proposto dal laboratorio al CMVP per la convalida. Sono riportati nell'elenco dei moduli in lavorazione e, una volta convalidati, saranno trasferiti nell'elenco dei moduli crittografici convalidati.

Lo spazio utente, lo spazio Kernel e l'archiviazione sicura delle chiavi per iOS 15 (2021) sono attualmente sottoposti a test di laboratorio. Sono riportati nell'elenco dei moduli con implementazione in fase di test.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con le versioni 2021 di iOS, iPadOS, macOS, tvOS e watchOS *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* Hardware (A9-A14, T2, M1, S3-S6) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con le versioni 2021 di iOS, iPadOS, macOS, tvOS e watchOS *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* Hardware(A13, A14, S6, M1) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con le versioni 2020 di iOS, iPadOS, macOS, tvOS e watchOS *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* Hardware (A9-A14, T2, M1, S3-S6) *Livello di sicurezza complessivo:* 2

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con le versioni 2020 di iOS, iPadOS, macOS, tvOS e watchOS *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* Hardware(A13, A14, S6, M1) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3

Certificazioni FIPS 140-2

La tabella di seguito mostra i moduli crittografici che sono stati testati in laboratorio per la conformità allo standard FIPS 140-2.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 05-02-2021	*Certificati:* 3811 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v10.0 *Sistema operativo:* sepOS per macOS 10.15 Catalina *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2018 *Date convalida:* 10-09-2019	*Certificati:* 3523 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v9.0 *Sistema operativo:* sepOS per macOS 10.14 Mojave *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2017 *Date convalida:* 10-09-2019	*Certificati:* 3223 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v1.0 *Sistema operativo:* sepOS per macOS 10.13 High Sierra *Tipo:* hardware *Livello di sicurezza:* 2

Certificazioni Common Criteria (CC)

Apple si impegna in maniera attiva nelle valutazioni di conformità allo standard Common Criteria laddove i profili di protezione idonei sono applicabili alle funzionalità di sicurezza della tecnologia Apple.

Stato delle certificazioni Common Criteria (CC)

Lo schema statunitense, gestito dalla NIAP (National Information Assurance Partnership), mantiene un elenco di prodotti in corso di valutazione, contenente i prodotti che sono attualmente in corso di valutazione negli Stati Uniti presso un laboratorio di test Common Criteria approvato dalla NIAP e che hanno completato un primo incontro di valutazione (o equivalente) in cui il CCEVS (Common Criteria Evaluation and Validation Scheme) ha ufficialmente accettato il prodotto per la valutazione.

Dopo la certificazione, la NIAP inserisce le certificazioni attualmente valide nell'elenco dei prodotti conformi. Dopo 2 anni tali certificazioni vengono ricontrollate per verificare la conformità con le politiche di mantenimento della garanzia di sicurezza attuali. Una volta scaduta la data di mantenimento della garanzia di sicurezza, la NIAP sposta le certificazioni nell'elenco dei prodotti archiviati.

Il portale Common Criteria riporta l'elenco delle certificazioni che possono essere riconosciute reciprocamente in base al Common Criteria Recognition Arrangement (CCRA). Il portale Common Criteria può conservare i prodotti nell'elenco dei prodotti certificati per 5 anni, all'interno delle certificazioni archiviate.

La tabella di seguito mostra le certificazioni attualmente in fase di valutazione da parte di un laboratorio o che sono state certificate come conformi allo standard Common Criteria.

Sistema operativo / Data certificazione	**ID schema / Documenti**	**Nome / Profili di protezione**
Sistema operativo: sepOS *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* Apple Secure Enclave [2020] *Profili di protezione:* CPP_DSC_V1.0 *Hardware:* Secure Enclave per (A9-A14, M1, T2, S3-S6) *Software:* sepOS distribuito con iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14 e watchOS 7

Certificazioni aggiuntive

La tabella di seguito mostra le certificazioni per Secure Enclave che non rientrano negli standard Common Criteria o FIPS 140-3.

Date	**Certificati / Documenti**	**Informazioni modulo**
Data di uscita del sistema operativo: 2020 *Date convalida:* dal 07-12-2019 al 26-12-2022	*Certificati:* CFNR201902910002 (P.R. China: Technology Certification of Mobile Financial Service) Versione cinese Versione inglese	*Nome:* Mobile Terminal Trusted Execution Environment *Sistema operativo:* iOS 13.5.1 *Specifica:* JR/T 0156-2017

Certificazioni di sicurezza per il chip di sicurezza Apple T2

Contesto delle convalide dei moduli crittografici

Apple si impegna in maniera attiva nella convalida dei moduli hardware e software integrati Apple per ogni versione principale dei propri sistemi operativi. La convalida di conformità può essere effettuata solo rispetto a una versione finale del modulo.

Nel 2020, il CMVP ha adottato lo standard internazionale ISO/IEC 19790 come base del FIPS (Federal Information Processing Standard) 140-3 per gli Stati Uniti.

Oltre alla CPU Intel, gran parte dei computer Mac prodotti dal 2017 sono dotati anche di un chip di sicurezza Apple T2 separato, un system on chip (SoC) basato sulla tecnologia Apple. Questi computer Mac con chip T2 utilizzano tutti e cinque i moduli crittografici per vari servizi eseguiti sul dispositivo.

- Corecrypto user module for Intel (utilizzato su macOS su computer con chip Intel)
- Corecrypto kernel module for Intel (utilizzato su macOS su computer con chip Intel)
- Corecrypto user module for ARM (utilizzato dal chip T2)
- Corecrypto kernel module for ARM (utilizzato dal chip T2)
- Secure Key Store Cryptographic Module (utilizzato dal coprocessore Secure Enclave integrato nel chip T2)

Nota: i moduli basati sulla tecnologia Apple in esecuzione sul chip T2 sono gli stessi in esecuzione su altri chip Apple, come i chip delle serie A, S e M.

Stato delle convalide dei moduli crittografici

Il Cryptographic Module Validation Program (CMVP) riporta lo stato della convalida dei moduli crittografici in tre elenchi separati a seconda del loro stato attuale.

- Per comparire nell'elenco dei moduli con implementazione in fase di test del CMVP, il laboratorio deve aver firmato un contratto con Apple per poter fornire i test.
- Dopo che il laboratorio ha completato i test, richiesto la convalida da parte del CMVP e pagato le tariffe CMVP, il modulo viene aggiunto all'elenco dei moduli in lavorazione. Questo elenco tiene traccia del processo di convalida da parte del CMVP in quattro fasi:
  - *In attesa di revisione:* in attesa dell'assegnazione delle risorse del CMVP.
  - *In fase di revisione:* le risorse del CMVP stanno eseguendo le attività di convalida.
  - *Coordinamento:* il laboratorio e il CMVP stanno risolvendo eventuali problemi riscontrati.
  - *Finalizzazione:* sono in corso le attività e le formalità relative all'emissione del certificato.
- Dopo la convalida da parte del CMVP, i moduli ricevono un certificato di conformità e vengono aggiunti all'elenco dei moduli crittografici convalidati. Questo include:
  - Moduli convalidati contrassegnati come attivi.
  - Dopo 5 anni, i moduli sono contrassegnati come "storici".
  - Se, per qualche ragione, il certificato viene revocato, allora questo viene contrassegnato come revocato.

Certificazioni FIPS 140-3

Stato attuale

La tabella di seguito mostra i moduli crittografici del 2020 e del 2021 che sono attualmente in fase di test di laboratorio per la conformità allo standard FIPS 140-3.

I moduli 2020 per lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. La tabella di seguito indica l'elenco dei moduli in lavorazione.

I moduli 2021 per lo spazio utente, lo spazio kernel e l'archiviazione sicura sono attualmente sottoposti a test di laboratorio. Sono riportati nell'elenco dei moduli con implementazione in fase di test.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* sepOS for macOS 12 Monterey *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* sepOS for macOS 12 Monterey *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* sepOS for macOS 12 Monterey *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* Hardware (T2) *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS per macOS 11 Big Sur *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS per macOS 11 Big Sur *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS per macOS 11 Big Sur su processore Intel *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware *Livello di sicurezza:* 2

Certificazioni FIPS 140-2

La tabella di seguito mostra i moduli crittografici che sono stati testati in laboratorio per la conformità allo standard FIPS 140-2.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3856 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v10.0 for ARM *Sistema operativo:* sepOS per macOS 10.15 Catalina *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3855 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v10.0 for ARM *Sistema operativo:* sepOS per macOS 10.15 Catalina *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 05-02-2021	*Certificati:* 3811 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Sistema operativo:* sepOS per macOS 10.15 Catalina *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2018 *Date convalida:* 23-04-2019	*Certificati:* 3438 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v9.0 for ARM *Sistema operativo:* sepOS per macOS 10.14 Mojave *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2018 *Date convalida:* 11-04-2019	*Certificati:* 3433 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v9.0 for ARM *Sistema operativo:* sepOS per macOS 10.14 Mojave *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 10-09-2019	*Certificati:* 3523 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v9.0 *Sistema operativo:* sepOS per macOS 10.14 Mojave *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 22-05-2018, 06-07-2018	*Certificati:* 3148 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v8.0 for ARM *Sistema operativo:* sepOS per macOS 10.13 High Sierra *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 17-05-2018, 03-07-2018	*Certificati:* 3147 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v8.0 for ARM *Sistema operativo:* sepOS per macOS 10.13 High Sierra *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 10-07-2018	*Certificati:* 3223 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v1.0 *Sistema operativo:* sepOS per macOS 10.13 High Sierra *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2016 *Date convalida:* 01-02-2017	*Certificati:* 2828 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple iOS Corecrypto Kernel Module v7.0 *Sistema operativo:* sepOS per macOS 10.12 Sierra *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2016 *Date convalida:* 01-02-2017	*Certificati:* 2827 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple iOS Corecrypto Kernel Module v7.0 *Sistema operativo:* sepOS per macOS 10.12 Sierra *Tipo:* software *Livello di sicurezza:* 1

Certificazioni di sicurezza dei sistemi operativi

Panoramica sulle certificazioni di sicurezza dei sistemi operativi Apple

Apple mantiene certificati di convalida della conformità agli standard FIPS (Federal Information Processing Standard) 140-2/-3 per il firmware sepOS, per il firmware del chip T2 e per altre certificazioni. Apple parte da una serie di *blocchi costituenti delle certificazioni*, applicabili ad ampio raggio a più piattaforme a seconda delle necessità. Uno dei blocchi costituenti è la convalida tramite la libreria corecrypto, che è utilizzata per l'implementazione dei moduli crittografici software e hardware all'interno dei sistemi operativi sviluppati da Apple. Un secondo blocco costituente è la certificazione di Secure Enclave, un coprocessore integrato in molti dispositivi Apple. Un terzo è la certificazione di Secure Element, presente nei dispositivi Apple dotati di Touch ID e di Face ID. Questi blocchi costituenti delle certificazioni hardware costituiscono le fondamenta per certificazioni di sicurezza delle piattaforme più ampie.

Convalide degli algoritmi crittografici

La convalida della corretta implementazione di molti algoritmi crittografici e delle relative funzionalità di sicurezza è un prerequisito per la convalida FIPS 140-3 e supporta altre certificazioni. La convalida viene gestita tramite il programma CAVP (Cryptographic Algorithm Validation Program) del NIST. I certificati di convalida delle implementazioni Apple sono reperibili tramite la pagina di ricerca del CAVP.

Convalide dei moduli crittografici: FIPS 140-2/3 (ISO/IEC 19790)

Il Cryptographic Module Validation Program (CMVP) ha ripetutamente convalidato la conformità dei moduli crittografici di Apple allo standard FIPS (Federal Information Processing Standards) 140-2 degli Stati Uniti dopo il rilascio di ogni versione principale dei sistemi operativi, dal 2012. Dopo ogni versione principale, Apple invia tutti i moduli al CMVP per una convalida completa dei moduli crittografici. Tali moduli convalidati forniscono operazioni crittografiche per i servizi forniti da Apple e sono disponibili per l'utilizzo da parte di app di terze parti.

Apple ottiene ogni anno il **livello di sicurezza 1** per i moduli basati sul software “Corecrypto Module for Intel” e “Corecrypto Kernel Module for Intel” per macOS. Per i chip Apple, i moduli “Corecrypto Module for ARM” e “Corecrypto Kernel Module for ARM” sono applicabili ad iOS, iPadOS, tvOS e watchOS e al firmware sul chip di sicurezza Apple T2 integrato nei Mac.

Nel 2019, Apple ha ottenuto il primo **livello di sicurezza 2** FIPS 140-2 per il modulo crittografico hardware integrato conosciuto come “Apple Corecrypto Module: Secure Key Store”, che consente l'uso approvato dal governo degli Stati Uniti delle chiavi generate e gestite in Secure Enclave. Apple continua a perseguire le convalide per i moduli crittografici hardware per ogni successiva versione principale dei sistemi operativi.

FIPS 140-3 è stato approvato dal Dipartimento del commercio degli Stati Uniti nel 2019. La modifica più significativa di questa versione dello standard è la specificazione di standard ISO/IEC, in particolare, ISO/IEC 19790:2015 e dei relativi standard di test ISO/IEC 24759:2017. Il CMVP ha avviato un programma di transizione e ha indicato che, all'inizio del 2020, i moduli crittografici inizieranno a essere convalidati usando il FIPS 140-3 come base. I moduli crittografici di Apple puntano a soddisfare lo standard FIPS 140-3 e a passare a esso il prima possibile.

Per i moduli crittografici attualmente in fase di test e di convalida, il CMVP mantiene due elenchi separati che potrebbero contenere informazioni sulle convalide proposte. I moduli crittografici in fase di test da parte di un laboratorio accreditato potrebbero essere presenti nell'elenco dei moduli con implementazione in fase di test. Una volta che il laboratorio ha completato i test e ha richiesto la convalida da parte del CMVP, i moduli crittografici Apple compaiono nell'elenco dei moduli in lavorazione. Attualmente i test di laboratorio sono completi e si attende la convalida degli stessi da parte del CMVP. Dal momento che la durata del processo di convalida è variabile, consulta entrambi questi elenchi per determinare lo stato attuale dei moduli crittografici Apple tra la data di uscita di una versione principale di un sistema operativo e l'emissione del certificato di convalida da parte del CMVP.

Certificazioni dei prodotti: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) è uno standard utilizzato da molte organizzazioni come base per valutare la sicurezza dei prodotti informatici.

Per le certificazioni che potrebbero essere riconosciute reciprocamente dal Common Criteria Recognition Arrangement (CCRA), vai sul portale di Common Criteria. Lo standard Common Criteria potrebbe essere utilizzato anche al di fuori del CCRA da schemi di convalida nazionali e privati. In Europa, il riconoscimento reciproco è governato dall'accordo SOG-IS e dal CCRA.

L'obiettivo, così come dichiarato dalla comunità di Common Criteria, è quello di ottenere un insieme di standard di sicurezza approvato a livello internazionale, così da poter fornire una convalida chiara e affidabile delle funzionalità di sicurezza dei prodotti informatici. Fornendo un controllo indipendente della capacità di un prodotto di soddisfare degli standard di sicurezza, la certificazione Common Criteria rafforza la fiducia dei clienti rispetto alla sicurezza dei prodotti informatici, consentendo loro di prendere decisioni più informate.

Tramite il CCRA, i paesi aderenti hanno concordato di riconoscere la certificazione dei prodotti informatici con lo stesso livello di attendibilità. Le valutazioni richieste prima della certificazione sono ampie e includono:

- Profili di protezione
- Obiettivi di sicurezza
- Requisiti funzionali di sicurezza
- Requisiti di garanzia
- Livelli di garanzia della convalida

I profili di protezione sono documenti che specificano i requisiti di sicurezza per una classe di dispositivi, come ad esempio la classe Mobility per i dispositivi mobili, e sono utilizzati per consentire il confronto tra le valutazioni dei prodotti informatici all'interno della stessa classe. I membri del CCRA continuano a crescere di anno in anno di pari passo con il numero dei profili di protezione approvati. Questo impianto consente allo sviluppatore di un prodotto di conseguire una singola certificazione secondo uno qualsiasi degli schemi di autorizzazione per le certificazioni e di ottenere il riconoscimento da qualsiasi firmatario dei certificati stessi.

Gli obiettivi di sicurezza definiscono *cosa* verrà valutato quando un prodotto informatico è in fase di certificazione. Gli obiettivi di sicurezza vengono tradotti in *requisiti funzionali di sicurezza* più specifici, utilizzati per valutare tali obiettivi più dettagliatamente.

Lo standard Common Criteria (CC) include anche *requisiti di garanzia*. Uno dei fattori comunemente identificati è il *livello di garanzia della convalida*. I livelli di garanzia della convalida, a loro volta, raggruppano insiemi i requisiti di garanzia utilizzati comunemente e possono essere specificati in profili di protezione e obiettivi di sicurezza per consentire il confronto.

Molti profili di protezione meno recenti sono stati archiviati e verrano man mano sostituiti da profili di protezione mirati, incentrati su soluzioni e ambienti specifici. In un impegno coordinato mirato a garantire un riconoscimento reciproco tra tutti i membri del CCRA, sono state costituite delle comunità tecniche internazionali (iTC, international Tecnical Community) volte a sviluppare e mantenere *profili di protezione collaborativi* che sono creati fin dall'inizio tenendo conto degli schemi dei firmatari del CCRA. I profili di protezione destinati a gruppi di utenti e accordi di riconoscimento reciproco diversi dal CCRA continuano ad essere sviluppati dalle parti appropriate interessate.

Apple ha iniziato a perseguire certificazioni secondo la versione aggiornata del CCRA con alcuni profili di protezione collaborativi dall'inizio del 2015. Da allora, Apple ha ottenuto certificazioni Common Criteria per ogni versione principale di iOS e ha ampliato la copertura per includere la garanzia di sicurezza fornita dai nuovi profili di protezione.

Apple assume un ruolo attivo all'interno delle comunità tecniche impegnate nella convalida delle tecnologie di sicurezza dei dispositivi mobili. Queste includono le iTC responsabili dello sviluppo e dell'aggiornamento dei profili di protezione collaborativi. Apple continua a valutare e a perseguire certificazioni per tutti gli attuali profili di protezione e profili di protezione collaborativi.

Le certificazioni delle piattaforme Apple per il mercato del Nord America vengono generalmente effettuate tramite la National Information Assurance Partnership (NIAP), che mantiene un elenco dei progetti attualmente in fase di convalida, ma non ancora certificati.

Oltre ai certificati generali per le piattaforme elencati, altri certificati sono stati emessi per dimostrare specifici requisiti di sicurezza per alcuni mercati.

Certificazioni di sicurezza per iOS

Contesto delle certificazioni iOS

Apple si impegna in maniera attiva nella convalida dei moduli hardware e software integrati Apple per ogni versione principale dei propri sistemi operativi rispetto a una versione finale del modulo. La convalida di conformità può essere effettuata solo rispetto a una versione finale già uscita.

Stato delle convalide dei moduli crittografici di iOS

Il Cryptographic Module Validation Program (CMVP) riporta lo stato della convalida dei moduli crittografici in tre elenchi separati a seconda del loro stato attuale.

- Per comparire nell'elenco dei moduli con implementazione in fase di test del CMVP, il laboratorio deve aver firmato un contratto con Apple per poter fornire i test.
- Dopo che il laboratorio ha completato i test, richiesto la convalida da parte del CMVP e pagato le tariffe CMVP, il modulo viene aggiunto all'elenco dei moduli in lavorazione. Questo elenco tiene traccia del processo di convalida da parte del CMVP in quattro fasi:
  - *In attesa di revisione:* in attesa dell'assegnazione delle risorse del CMVP.
  - *In fase di revisione:* le risorse del CMVP stanno eseguendo le attività di convalida.
  - *Coordinamento:* il laboratorio e il CMVP stanno risolvendo eventuali problemi riscontrati.
  - *Finalizzazione:* sono in corso le attività e le formalità relative all'emissione del certificato.
- Dopo la convalida da parte del CMVP, i moduli ricevono un certificato di conformità e vengono aggiunti all'elenco dei moduli crittografici convalidati. Questo include:
  - Moduli convalidati contrassegnati come attivi.
  - Dopo 5 anni, i moduli sono contrassegnati come “storici”.
  - Se, per qualche ragione, il certificato viene revocato, allora questo viene contrassegnato come revocato.

Nel 2020, il CMVP ha adottato lo standard internazionale ISO/IEC 19790 come base del FIPS 140-3.

Certificazioni FIPS 140-3

Stato attuale

La tabella di seguito mostra i moduli crittografici del 2020 e del 2021 che sono attualmente in fase di test di laboratorio per la conformità allo standard FIPS 140-3.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per iOS 14 (2020) hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. Sono riportati nell'elenco dei moduli in lavorazione.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per iOS 15 (2021) al momento sono sottoposti a test di laboratorio. Sono riportati nell'elenco dei moduli con implementazione in fase di test.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* iOS 15 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* iOS 15 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con iOS 15 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A9-A14) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con iOS 15 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* Hardware (A13, A14, A15) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* iOS 14 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* iOS 14 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con iOS 14 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A9-A14) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con iOS 14 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A9-A14) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3

Certificazioni FIPS 140-2

La tabella di seguito mostra i moduli crittografici che sono attualmente in fase di test e che sono stati testati in laboratorio per la conformità allo standard FIPS 140-2.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3856 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v10.0 for ARM *Sistema operativo:* iOS 13 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3855 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v10.0 for ARM *Sistema operativo:* iOS 13 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 05-02-2021	*Certificati:* 3811 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v10.0 *Sistema operativo:* sepOS distribuito con iOS 13 *Tipo:* hardware *Livello di sicurezza:* 2

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2018 *Date convalida:* 23-04-2019	*Certificati:* 3438 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v9.0 for ARM *Sistema operativo:* iOS 12 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 11-04-2019	*Certificati:* 3433 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v9.0 for ARM *Sistema operativo:* iOS 12 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 10-09-2019	*Certificati:* 3523 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v9.0 *Sistema operativo:* sepOS distribuito con iOS 12 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 22-05-2018, 06-07-2018	*Certificati:* 3148 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v8.0 for ARM *Sistema operativo:* iOS 11 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 17-05-2018, 03-07-2018	*Certificati:* 3147 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v8.0 for ARM *Sistema operativo:* iOS 11 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 10-09-2019	*Certificati:* 3223 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v1.0 *Sistema operativo:* sepOS distribuito con iOS 11 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2016 *Date convalida:* 01-02-2017	*Certificati:* 2828 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple iOS Corecrypto Kernel Module v7.0 *Sistema operativo:* iOS 10 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2016 *Date convalida:* 01-02-2017	*Certificati:* 2827 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple iOS Corecrypto Kernel Module v7.0 *Sistema operativo:* iOS 10 *Tipo:* software *Livello di sicurezza:* 1

Versioni precedenti

I certificati che risalgono a più di 5 anni fa sono riportati dal CMVP nell'elenco dei moduli "storici". Le versioni di iOS precedenti riportate di seguito sono state sottoposte a convalida dei moduli crittografici:

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

Contesto delle certificazioni Common Criteria (CC)

Apple si impegna in maniera attiva nella convalida di iOS per ogni versione principale del sistema operativo. La convalida può essere eseguita solo rispetto alla versione finale del sistema operativo effettivamente rilasciata pubblicamente. Prima di iPadOS 13.1, iPadOS era conosciuto come iOS.

Stato delle certificazioni Common Criteria (CC)

Lo schema statunitense, gestito dalla NIAP (National Information Assurance Partnership), mantiene un elenco di prodotti in corso di convalida, contenente i prodotti che sono attualmente in corso di convalida negli Stati Uniti presso un laboratorio di test Common Criteria approvato dalla NIAP e che hanno completato un primo incontro di convalida (o equivalente) in cui il CCEVS (Common Criteria Evaluation and Validation Scheme) ha ufficialmente accettato il prodotto per la convalida.

Dopo la certificazione, la NIAP inserisce le certificazioni attualmente valide nell'elenco dei prodotti conformi. Dopo 2 anni tali certificazioni vengono ricontrollate per verificare la conformità con le politiche di mantenimento della garanzia di sicurezza attuali. Una volta scaduta la data di mantenimento della garanzia di sicurezza, la NIAP sposta le certificazioni nell'elenco dei prodotti archiviati.

Il portale Common Criteria riporta l'elenco delle certificazioni che possono essere riconosciute reciprocamente in base al Common Criteria Recognition Arrangement (CCRA). Il portale Common Criteria può conservare i prodotti nell'elenco dei prodotti certificati per 5 anni, all'interno delle certificazioni archiviate.

La tabella di seguito mostra le certificazioni attualmente in fase di convalida da parte di un laboratorio o che sono state certificate come conformi allo standard Common Criteria.

Stato attuale

I test di laboratorio per le valutazioni con NIAP per iOS 15 sono in corso. Per informazioni aggiornate, consulta la sezione Prodotti in corso di convalida (NIAP) e l'elenco dei prodotti conformi.

Sistema operativo / Data certificazione	ID schema / Documenti	Nome / Profili di protezione
Sistema operativo: iOS 15 *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* —	*Nome:* Apple iOS 15: iPhone *Profili di protezione:* Protezioni fondamentali per i dispositivi mobili (moduli PP da confermare)
Sistema operativo: iOS 14 *Data certificazione:* 01-09-2021	*ID schema:* 11146 *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* Apple iOS 14: iPhone *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, modulo del client VPN, pacchetto PP per i client LAN, pacchetto esteso per l'agente MDM
Sistema operativo: iOS 13 *Data certificazione:* 06-11-2020	*ID schema:* 11036 *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* Apple iOS 13 su iPhone *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, modulo del client VPN, pacchetto esteso per i client LAN, pacchetto esteso per l'agente MDM

Certificazioni Common Criteria ottenute per iOS

Le precedenti versioni di iOS elencate di seguito sono state sottoposte a convalide Common Criteria. Sono archiviate dalla NIAP secondo i propri requisiti:

Sistema operativo / Data certificazione	ID schema / Documenti	Nome / Profili di protezione
Sistema operativo: iOS 12 *Data certificazione:* 14-03-2019	*ID schema:* 10937 *Documenti:* Obiettivo di sicurezza Linee guida	*Nome:* iPhone con iOS 12 *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, modulo del client VPN, pacchetto esteso per i client LAN wireless, pacchetto esteso per l'agente MDM
Sistema operativo: iOS 11 *Data certificazione:* 17-07-2018	*ID schema:* 10851 *Documenti:* Obiettivo di sicurezza Linee guida	*Nome:* Apple iOS 11 *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, pacchetto esteso per i client LAN wireless, pacchetto esteso per l'agente MDM
Sistema operativo: iOS 10 *Data certificazione:* 27-07-2017	*ID schema:* 10782 *Documenti:* Obiettivo di sicurezza, Linee guida	*Nome:* iOS 10.2 su iPhone e iPad *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, pacchetto esteso per i client LAN wireless, pacchetto esteso per l'agente MDM
Sistema operativo: iOS 10 *Data certificazione:* 27-07-2017	*ID schema:* 10792 *Documenti:* Obiettivo di sicurezza, Linee guida	*Nome:* Client VPN di iOS 10.2 su iPhone e iPad *Profili di protezione:* profilo di protezione per il client VPN
Sistema operativo: iOS 9 *Data certificazione:* 14-10-2016	*ID schema:* 10725 *Documenti:* Obiettivo di sicurezza, Linee guida	*Nome:* iOS 9.3.2 con agente MDM *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, pacchetto esteso per l'agente MDM
Sistema operativo: iOS 9 *Data certificazione:* 13-10-2016	*ID schema:* 10714 *Documenti:* Obiettivo di sicurezza, Linee guida	*Nome:* Client VPN del sistema operativo su iPhone e iPad *Profili di protezione:* profilo di protezione per il client VPN
Sistema operativo: iOS 9 *Data certificazione:* 28-01-2016	*ID schema:* 10695 *Documenti:* Obiettivo di sicurezza, Linee guida	*Nome:* iOS 9 *Profili di protezione:* protezioni fondamentali per i dispositivi mobili

Certificazioni di sicurezza per iPadOS

Contesto delle certificazioni iPadOS

Apple si impegna in maniera attiva nella convalida dei propri sistemi operativi per ogni versione principale del sistema operativo, utilizzando idonei profili di protezione collaborativa e livelli di sicurezza FIPS 140-3. La convalida di conformità può essere effettuata solo rispetto a una versione finale già uscita.

Nota: nel 2019 il sistema operativo per iPad è stato rinominato iPadOS. Prima di iPadOS 13.1, iPadOS era conosciuto come iOS.

Stato delle convalide dei moduli crittografici di iPadOS

Il Cryptographic Module Validation Program (CMVP) riporta lo stato della convalida dei moduli crittografici in tre elenchi separati a seconda del loro stato attuale.

- Per comparire nell'elenco dei moduli con implementazione in fase di test del CMVP, il laboratorio deve aver firmato un contratto con Apple per poter fornire i test.
- Dopo che il laboratorio ha completato i test, richiesto la convalida da parte del CMVP e pagato le tariffe CMVP, il modulo viene aggiunto all'elenco dei moduli in lavorazione. Questo elenco tiene traccia del processo di convalida da parte del CMVP in quattro fasi:
  - *In attesa di revisione:* in attesa dell'assegnazione delle risorse del CMVP.
  - *In fase di revisione:* le risorse del CMVP stanno eseguendo le attività di convalida.
  - *Coordinamento:* il laboratorio e il CMVP stanno risolvendo eventuali problemi riscontrati.
  - *Finalizzazione:* sono in corso le attività e le formalità relative all'emissione del certificato.
- Dopo la convalida da parte del CMVP, i moduli ricevono un certificato di conformità e vengono aggiunti all'elenco dei moduli crittografici convalidati. Questo include:
  - Moduli convalidati contrassegnati come attivi.
  - Dopo 5 anni, i moduli sono contrassegnati come “storici”.
  - Se, per qualche ragione, il certificato viene revocato, allora questo viene contrassegnato come revocato.

Nel 2020, il CMVP ha adottato lo standard internazionale ISO/IEC 19790 come base del FIPS 140-3.

Certificazioni FIPS 140-3

Stato attuale

La tabella di seguito mostra i moduli crittografici del 2020 e del 2021 che sono attualmente in fase di test di laboratorio per la conformità allo standard FIPS 140-3.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per iPadOS 14 (2020) hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. Sono riportati nell'elenco dei moduli in lavorazione.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per iPadOS 15 (2021) al momento sono sottoposti a test di laboratorio. Sono riportati nell'elenco dei moduli con implementazione in fase di test.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* iPadOS 15 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* iPadOS 15 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con iPadOS 15 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A9-A14, M1) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con iPadOS 15 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A9-A14, M1) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* iPadOS 14 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* iPadOS 14 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con iPadOS 14 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* Hardware (A9-A14, M1) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con iPadOS 14 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A9-A14, M1) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3

Certificazioni FIPS 140-2

La tabella di seguito mostra i moduli crittografici che sono attualmente in fase di test e che sono stati testati in laboratorio per la conformità allo standard FIPS 140-2.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3856 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v10.0 for ARM *Sistema operativo:* iPadOS 13 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3855 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v10.0 for ARM *Sistema operativo:* iPadOS 13 *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 05-02-2021	*Certificati:* 3811 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Sistema operativo:* sepOS distribuito con iPadOS 13 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2018 *Date convalida:* 23-04-2019	*Certificati:* 3438 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v9.0 for ARM *Sistema operativo:* iOS 12 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 11-04-2019	*Certificati:* 3433 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v9.0 for ARM *Sistema operativo:* iOS 12 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 10-09-2019	*Certificati:* 3523 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v9.0 *Sistema operativo:* sepOS distribuito con iOS 12 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 22-05-2018, 06-07-2018	*Certificati:* 3148 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v8.0 for ARM *Sistema operativo:* iOS 11 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 17-05-2018, 03-07-2018	*Certificati:* 3147 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v8.0 for ARM *Sistema operativo:* iOS 11 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 10-09-2019	*Certificati:* 3223 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v1.0 *Sistema operativo:* sepOS distribuito con iOS 11 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2016 *Date convalida:* 01-02-2017	*Certificati:* 2828 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple iOS Corecrypto Kernel Module v7.0 *Sistema operativo:* iOS 10 *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2016 *Date convalida:* 01-02-2017	*Certificati:* 2827 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple iOS Corecrypto Kernel Module v7.0 *Sistema operativo:* iOS 10 *Tipo:* software *Livello di sicurezza:* 1

Versioni precedenti

I certificati che risalgono a più di 5 anni fa sono riportate dal CMVP nell'elenco dei moduli "storici". Le versioni di iOS precedenti riportate di seguito sono state sottoposte a convalida dei moduli crittografici:

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

Contesto delle certificazioni Common Criteria (CC)

Apple si impegna in maniera attiva nella convalida di iPadOS per ogni versione principale del sistema operativo. La convalida può essere eseguita solo rispetto alla versione finale del sistema operativo effettivamente rilasciata pubblicamente.

Stato delle certificazioni Common Criteria (CC)

Lo schema statunitense, gestito dalla NIAP (National Information Assurance Partnership), mantiene un elenco di prodotti in corso di valutazione, contenente i prodotti che sono attualmente in corso di valutazione negli Stati Uniti presso un laboratorio di test Common Criteria approvato dalla NIAP e che hanno completato un primo incontro di valutazione (o equivalente) in cui il CCEVS (Common Criteria Evaluation and Validation Scheme) ha ufficialmente accettato il prodotto per la valutazione.

Dopo la certificazione, la NIAP inserisce le certificazioni attualmente valide nell'elenco dei prodotti conformi. Dopo 2 anni tali certificazioni vengono ricontrollate per verificare la conformità con le politiche di mantenimento della garanzia di sicurezza attuali. Una volta scaduta la data di mantenimento della garanzia di sicurezza, la NIAP sposta le certificazioni nell'elenco dei prodotti archiviati.

Il portale Common Criteria riporta l'elenco delle certificazioni che possono essere riconosciute reciprocamente in base al Common Criteria Recognition Arrangement (CCRA). Il portale Common Criteria può conservare i prodotti nell'elenco dei prodotti certificati per 5 anni, all'interno delle certificazioni archiviate.

La tabella di seguito mostra le certificazioni attualmente in fase di convalida da parte di un laboratorio o che sono state certificate come conformi allo standard Common Criteria.

Stato attuale

I test di laboratorio per le valutazioni con NIAP per iPadOS 15 sono in corso. Per informazioni aggiornate, consulta la sezione Prodotti in corso di convalida (NIAP) e l'elenco dei prodotti conformi.

Sistema operativo / Data certificazione	ID schema / Documenti	Nome / Profili di protezione
Sistema operativo: iPadOS 15 *Data certificazione:* 14-03-2019	*ID schema:* — *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* iPad con iOS 12 *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, modulo del client VPN, pacchetto esteso per i client LAN wireless, pacchetto esteso per l'agente MDM
Sistema operativo: iPadOS 14 *Data certificazione:* 01-09-2021	*ID schema:* 11147 *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* Apple iPadOS 14: iPad *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, modulo del client VPN, pacchetto esteso per i client LAN wireless, pacchetto esteso per l'agente MDM
Sistema operativo: iPadOS 13 *Data certificazione:* 06-11-2020	*ID schema:* 11036 *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* iPadOS 13 su dispositivi mobili iPad *Profili di protezione:* protezioni fondamentali per i dispositivi mobili, modulo del client VPN, pacchetto esteso per i client LAN wireless, pacchetto esteso per l'agente MDM

Versioni precedenti

Le precedenti versioni di iOS elencate di seguito sono state sottoposte a convalide Common Criteria. Sono archiviate dalla NIAP (National Information Assurance Partnership) secondo i propri requisiti:

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

Certificazioni di sicurezza per macOS

Contesto delle certificazioni macOS

Apple si impegna in maniera attiva nella convalida dei propri sistemi operativi per ogni versione principale del sistema operativo, utilizzando idonei profili di protezione collaborativa e livelli di sicurezza FIPS 140-3. La convalida di conformità può essere effettuata solo rispetto a una versione finale già uscita.

Stato delle convalide dei moduli crittografici di macOS

Il Cryptographic Module Validation Program (CMVP) riporta lo stato della convalida dei moduli crittografici in tre elenchi separati a seconda del loro stato attuale.

- Per comparire nell'elenco dei moduli con implementazione in fase di test del CMVP, il laboratorio deve aver firmato un contratto con Apple per poter fornire i test.
- Dopo che il laboratorio ha completato i test, richiesto la convalida da parte del CMVP e pagato le tariffe CMVP, il modulo viene aggiunto all'elenco dei moduli in lavorazione. Questo elenco tiene traccia del processo di convalida da parte del CMVP in quattro fasi:
  - *In attesa di revisione:* in attesa dell'assegnazione delle risorse del CMVP.
  - *In fase di revisione:* le risorse del CMVP stanno eseguendo le attività di convalida.
  - *Coordinamento:* il laboratorio e il CMVP stanno risolvendo eventuali problemi riscontrati.
  - *Finalizzazione:* sono in corso le attività e le formalità relative all'emissione del certificato.
- Dopo la convalida da parte del CMVP, i moduli ricevono un certificato di conformità e vengono aggiunti all'elenco dei moduli crittografici convalidati. Questo include:
  - Moduli convalidati contrassegnati come attivi.
  - Dopo 5 anni, i moduli sono contrassegnati come "storici".
  - Se, per qualche ragione, il certificato viene revocato, allora questo viene contrassegnato come revocato.

Nel 2020, il CMVP ha adottato lo standard internazionale ISO/IEC 19790 come base del FIPS 140-3.

Per i computer Mac Apple, la tabella di seguito mostra quali moduli crittografici sono applicabili a ciascuna tecnologia Mac.

Modulo crittografico	Computer Mac con chip Apple	Computer Mac con chip di sicurezza Apple T2	Computer Mac con processore Intel privi di chip di sicurezza Apple T2
Spazio utente chip Apple	✓		
Kernel chip Apple	✓		
Spazio utente Intel		✓	✓
Kernel Intel		✓	✓
Archiviazione sicura delle chiavi	✓	✓	

Certificazioni FIPS 140-3

La tabella di seguito mostra i moduli crittografici del 2020 e del 2021 che sono attualmente in fase di test di laboratorio per la conformità allo standard FIPS 140-3.

Nel 2020, Apple ha immesso sul mercato computer Mac dotati di chip Apple. L'applicabilità dei moduli crittografici ai computer Mac con chip Apple o con processore Intel è indicata nella colonna “Informazioni modulo” della tabella di seguito.

Nota: in molti Mac dotati di processore Intel è presente il chip di sicurezza Apple T2. Per informazioni sulle certificazioni del chip T2, consulta Certificazioni di sicurezza per il chip di sicurezza Apple T2.

Client SSH per macOS

OpenSSH può essere configurato per l'utilizzo di moduli convalidati secondo lo standard FIPS 140-3 per una selezione di algoritmi FIPS 140-3. Le organizzazioni possono eseguire programmi di installazione firmati e autenticati disponibili da Apple con la password *FIPS140Mode*. Il programma di installazione introduce due file sul Mac:

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

macOS utilizza tali file per limitare i codici disponibili per OpenSSH unicamente a quelli convalidati tramite NIST (National Institute of Standards and Technology) e assicura che il client OpenSSH utilizzi il modulo crittografico convalidato fornito dalla piattaforma. Gli amministratori possono anche creare i propri file. Per maggiori informazioni, occorre consultare la pagina `apple_ssh_and_fips` in macOS 12.0.1 o versioni successive.

Stato attuale

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per macOS 11 Big Sur hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. Sono riportati nell'elenco dei moduli in lavorazione.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per macOS 12 Monterey al momento sono sottoposti a test di laboratorio. Sono riportati nell'elenco dei moduli con implementazione in fase di test.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* macOS 12 Monterey su chip Apple *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* macOS 12 Monterey su chip Apple *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* macOS 12 Monterey su processore Intel *Ambiente:* Intel, utente, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* macOS 12 Monterey su processore Intel *Ambiente:* Intel, kernel, software *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* sepOS distribuito con macOS 12 Monterey su chip Apple, sepOS distribuito con macOS 12 Monterey su processore Intel con T2 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (M1 e T2) *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12.0 *Sistema operativo:* sepOS distribuito con macOS 12 Monterey su chip Apple *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (M1) *Livello di sicurezza:* 2 *Livello di sicurezza fisica:* 3
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* macOS 11 Big Sur su processore Intel *Ambiente:* Intel, utente, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* macOS 11 Big Sur su processore Intel *Ambiente:* Intel, kernel, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* macOS 11 Big Sur su chip Apple *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* macOS 11 Big Sur su chip Apple *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con macOS 11 Big Sur su chip Apple, sepOS distribuito con macOS 11 Big Sur su processore Intel *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (M1) *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con macOS 11 Big Sur su chip Apple *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (M1) *Livello di sicurezza:* 2 *Livello di sicurezza fisica:* 3

Certificazioni FIPS 140-2

La tabella di seguito mostra i moduli crittografici che sono attualmente in fase di test e che sono stati testati in laboratorio per la conformità allo standard FIPS 140-2.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per macOS 10.15 Catalina hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. Sono riportati nell'elenco dei moduli in lavorazione.

Nota: in molti Mac dotati di processore Intel è presente il chip di sicurezza Apple T2. Per informazioni sulle certificazioni del chip T2, consulta Certificazioni di sicurezza per il chip di sicurezza Apple T2.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 24-03-2021	*Certificati:* 3859 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Space Module for Intel (ccv10) *Sistema operativo:* macOS 10.15 Catalina *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 24-03-2021	*Certificati:* 3858 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v10.0 for Intel (ccv10) *Sistema operativo:* macOS 10.15 Catalina *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 12-04-2019	*Certificati:* 3402 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v9.0 for Intel *Sistema operativo:* macOS 10.14 Mojave *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 12-04-2019	*Certificati:* 3431 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v9.0 for Intel *Sistema operativo:* macOS 10.14 Mojave *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 22-03-2018	*Certificati:* 3155 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v8.0 for Intel *Sistema operativo:* macOS 10.13 High Sierra *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 22-03-2018	*Certificati:* 3156 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v8.0 for Intel *Sistema operativo:* macOS 10.13 High Sierra *Tipo:* software *Livello di sicurezza:* 1

Versioni precedenti

Le versioni di OS X e macOS precedenti sono state sottoposte a convalida dei moduli crittografici. Le seguenti versioni risalgono a più di 5 anni fa e sono riportate dal CMVP nell'elenco dei moduli “storici”:

- 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

Contesto delle certificazioni Common Criteria (CC)

Apple si impegna in maniera attiva nella convalida di macOS per ogni versione principale del sistema operativo. La convalida può essere eseguita solo rispetto alla versione finale del sistema operativo effettivamente rilasciata pubblicamente.

Stato delle certificazioni Common Criteria (CC)

Lo schema statunitense, gestito dalla NIAP (National Information Assurance Partnership), mantiene un elenco di prodotti in corso di valutazione, contenente i prodotti che sono attualmente in corso di valutazione negli Stati Uniti presso un laboratorio di test Common Criteria approvato dalla NIAP e che hanno completato un primo incontro di valutazione (o equivalente) in cui il CCEVS (Common Criteria Evaluation and Validation Scheme) ha ufficialmente accettato il prodotto per la valutazione.

Dopo la certificazione, la NIAP inserisce le certificazioni attualmente valide nell'elenco dei prodotti conformi. Dopo 2 anni tali certificazioni vengono ricontrollate per verificare la conformità con le politiche di mantenimento della garanzia di sicurezza attuali. Una volta scaduta la data di mantenimento della garanzia di sicurezza, la NIAP sposta le certificazioni nell'elenco dei prodotti archiviati.

Il portale Common Criteria riporta l'elenco delle certificazioni che possono essere riconosciute reciprocamente in base al Common Criteria Recognition Arrangement (CCRA). Il portale Common Criteria può conservare i prodotti nell'elenco dei prodotti certificati per 5 anni, all'interno delle certificazioni archiviate.

La tabella di seguito mostra le certificazioni attualmente in fase di convalida da parte di un laboratorio o che sono state certificate come conformi allo standard Common Criteria.

Stato attuale

Le valutazioni NIAP per macOS 11 e macOS 12 tramite i profili di protezione per sistemi operativi a scopo generico e per la codifica completa del disco (AA ed EE) sono attualmente in corso.

Per informazioni aggiornate, consulta la sezione Prodotti in corso di convalida (NIAP) e l'elenco dei prodotti conformi.

Sistema operativo / Data certificazione	**ID schema / Documenti**	**Nome / Profili di protezione**
Sistema operativo: macOS 12 Monterey *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* —	*Nome:* Apple FileVault 2 con macOS 12 Monterey *Profili di protezione:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP da confermare)
Sistema operativo: macOS 12 Monterey *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* —	*Nome:* macOS 12 Monterey *Profili di protezione:* PP_OS_V4.21 (PP da confermare)

Sistema operativo / Data certificazione	ID schema / Documenti	Nome / Profili di protezione
Sistema operativo: macOS 11 Big Sur *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* Apple FileVault 2 con macOS 11 Big Sur *Profili di protezione:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Sistema operativo: macOS 11 Big Sur *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* Apple macOS 11 Big Sur *Profili di protezione:* PP_OS_V4.21
Sistema operativo: macOS 10.15 Catalina *Data certificazione:* 29-04-2021	*ID schema:* 11078 *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* Apple FileVault 2 su computer con T2 e macOS 10.15 Catalina *Profili di protezione:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Sistema operativo: macOS 10.15 Catalina *Data certificazione:* 23-09-2020	*ID schema:* 11077 *Documenti:* Certificato Obiettivo di sicurezza Linee guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* macOS 10.15 Catalina *Profili di protezione:* PP_OS_V4.21

Certificazioni di sicurezza per tvOS

Contesto delle certificazioni tvOS

Apple si impegna attivamente nella convalida dei moduli crittografici associati a tutte le versioni principali di tvOS. La convalida di conformità può essere effettuata solo rispetto a una versione finale già uscita.

Stato delle convalide dei moduli crittografici di tvOS

Il Cryptographic Module Validation Program (CMVP) riporta lo stato della convalida dei moduli crittografici in tre elenchi separati a seconda del loro stato attuale.

- Per comparire nell'elenco dei moduli con implementazione in fase di test del CMVP, il laboratorio deve aver firmato un contratto con Apple per poter fornire i test.
- Dopo che il laboratorio ha completato i test, richiesto la convalida da parte del CMVP e pagato le tariffe CMVP, il modulo viene aggiunto all'elenco dei moduli in lavorazione. Questo elenco tiene traccia del processo di convalida da parte del CMVP in quattro fasi:
  - *In attesa di revisione:* in attesa dell'assegnazione delle risorse del CMVP.
  - *In fase di revisione:* le risorse del CMVP stanno eseguendo le attività di convalida.
  - *Coordinamento:* il laboratorio e il CMVP stanno risolvendo eventuali problemi riscontrati.
  - *Finalizzazione:* sono in corso le attività e le formalità relative all'emissione del certificato.
- Dopo la convalida da parte del CMVP, i moduli ricevono un certificato di conformità e vengono aggiunti all'elenco dei moduli crittografici convalidati. Questo include:
  - Moduli convalidati contrassegnati come attivi.
  - Dopo 5 anni, i moduli sono contrassegnati come "storici".
  - Se, per qualche ragione, il certificato viene revocato, allora questo viene contrassegnato come revocato.

Nel 2020, il CMVP ha adottato lo standard internazionale ISO/IEC 19790 come base del FIPS 140-3.

Certificazioni FIPS 140-3

Stato attuale

La tabella di seguito mostra i moduli crittografici del 2020 e del 2021 che sono attualmente in fase di test di laboratorio per la conformità allo standard FIPS 140-3.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per tvOS 14 (2020) hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. Sono riportati nell'elenco dei moduli in lavorazione.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per tvOS 15 (2021) al momento sono sottoposti a test di laboratorio. Sono riportati nell'elenco dei moduli con implementazione in fase di test.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* tvOS 15 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* tvOS 15 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con tvOS 15 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A10, A12) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* tvOS 14 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* tvOS 14 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con tvOS 14 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (A10, A12) *Livello di sicurezza complessivo:* 2

Certificazioni FIPS 140-2

La tabella di seguito mostra i moduli crittografici che sono attualmente in fase di test e che sono stati testati in laboratorio per la conformità allo standard FIPS 140-2.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per tvOS 13 (2019) hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. Sono riportati nell'elenco dei moduli in lavorazione.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3856 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v10.0 for ARM *Sistema operativo:* tvOS 13 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 23-03-2021	*Certificati:* 3855 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v10.0 for ARM *Sistema operativo:* tvOS 13 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 05-02-2021	*Certificati:* 3811 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v10.0 *Sistema operativo:* sepOS distribuito con tvOS 13 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2018 *Date convalida:* 23-04-2019	*Certificati:* 3438 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v9.0 for ARM *Sistema operativo:* tvOS 12 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 11-04-2019	*Certificati:* 3433 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v9.0 for ARM *Sistema operativo:* tvOS 12 *Tipo:* software *Livello di sicurezza:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2018 *Date convalida:* 10-09-2019	*Certificati:* 3523 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v9.0 *Sistema operativo:* sepOS distribuito con tvOS 12 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 22-05-2018, 06-07-2018	*Certificati:* 3148 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v8.0 for ARM *Sistema operativo:* tvOS 11 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 17-05-2018, 03-07-2018	*Certificati:* 3147 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v8.0 for ARM *Sistema operativo:* tvOS 11 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 10-09-2019	*Certificati:* 3223 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v1.0 *Sistema operativo:* sepOS distribuito con tvOS 11 *Tipo:* hardware *Livello di sicurezza:* 2

Certificazioni di sicurezza per watchOS

Contesto delle certificazioni watchOS

Apple si impegna attivamente nella convalida dei moduli crittografici associati a tutte le versioni principali di watchOS. La convalida di conformità può essere effettuata solo rispetto a una versione finale già uscita.

Stato delle convalide dei moduli crittografici di watchOS

Il Cryptographic Module Validation Program (CMVP) riporta lo stato della convalida dei moduli crittografici in tre elenchi separati a seconda del loro stato attuale.

- Per comparire nell'elenco dei moduli con implementazione in fase di test del CMVP, il laboratorio deve aver firmato un contratto con Apple per poter fornire i test.
- Dopo che il laboratorio ha completato i test, richiesto la convalida da parte del CMVP e pagato le tariffe CMVP, il modulo viene aggiunto all'elenco dei moduli in lavorazione. Questo elenco tiene traccia del processo di convalida da parte del CMVP in quattro fasi:
  - *In attesa di revisione:* in attesa dell'assegnazione delle risorse del CMVP.
  - *In fase di revisione:* le risorse del CMVP stanno eseguendo le attività di convalida.
  - *Coordinamento:* il laboratorio e il CMVP stanno risolvendo eventuali problemi riscontrati.
  - *Finalizzazione:* sono in corso le attività e le formalità relative all'emissione del certificato.
- Dopo la convalida da parte del CMVP, i moduli ricevono un certificato di conformità e vengono aggiunti all'elenco dei moduli crittografici convalidati. Questo include:
  - Moduli convalidati contrassegnati come attivi.
  - Dopo 5 anni, i moduli sono contrassegnati come "storici".
  - Se, per qualche ragione, il certificato viene revocato, allora questo viene contrassegnato come revocato.

Nel 2020, il CMVP ha adottato lo standard internazionale ISO/IEC 19790 come base del FIPS 140-3.

Certificazioni FIPS 140-3

Stato attuale

La tabella di seguito mostra i moduli crittografici del 2020 e del 2021 che sono attualmente in fase di test di laboratorio per la conformità allo standard FIPS 140-3.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per watchOS 7 (2020) hanno superato i test di laboratorio e il laboratorio ne ha raccomandato la convalida da parte del CMVP. Sono riportati nell'elenco dei moduli in lavorazione.

Lo spazio utente, lo spazio kernel e l'archiviazione sicura delle chiavi per watchOS 8 (2021) al momento sono sottoposti a test di laboratorio. Sono riportati nell'elenco dei moduli con implementazione in fase di test.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* watchOS 8 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* watchOS 8 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con watchOS 8 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (S3, S4, S5, S6) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2021 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v12 *Sistema operativo:* sepOS distribuito con watchOS 8 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (S6) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* watchOS 7 *Ambiente:* chip Apple, utente, software *Tipo:* software *Livello di sicurezza complessivo:* 1

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* watchOS 7 *Ambiente:* chip Apple, kernel, software *Tipo:* software *Livello di sicurezza complessivo:* 1
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con watchOS 7 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (S3, S4, S5, S6) *Livello di sicurezza complessivo:* 2
Data di uscita del sistema operativo: 2020 *Date convalida:* —	*Certificati:* non ancora certificato *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Module v11.1 *Sistema operativo:* sepOS distribuito con watchOS 7 *Ambiente:* chip Apple, archiviazione sicura delle chiavi, hardware *Tipo:* hardware (S6) *Livello di sicurezza complessivo:* 2 *Livello di sicurezza fisica:* 3

Certificazioni FIPS 140-2

La tabella di seguito mostra i moduli crittografici che sono attualmente in fase di test e che sono stati testati in laboratorio per la conformità allo standard FIPS 140-2.

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2019 *Date convalida:* —	*Certificati:* 3856 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v10.0 for ARM *Sistema operativo:* watchOS 6 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* —	*Certificati:* 3855 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v10.0 for ARM *Sistema operativo:* watchOS 6 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2019 *Date convalida:* 05-02-2021	*Certificati:* 3811 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v10.0 *Sistema operativo:* sepOS distribuito con watchOS 6 *Tipo:* hardware *Livello di sicurezza:* 2

Date	Certificati / Documenti	Informazioni modulo
Data di uscita del sistema operativo: 2018 *Date convalida:* 23-04-2019	*Certificati:* 3438 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v9.0 for ARM *Sistema operativo:* watchOS 5 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 11-04-2019	*Certificati:* 3433 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v9.0 for ARM *Sistema operativo:* watchOS 5 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2018 *Date convalida:* 10-09-2019	*Certificati:* 3523 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v9.0 *Sistema operativo:* sepOS distribuito con watchOS 5 *Tipo:* hardware *Livello di sicurezza:* 2
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 22-05-2018, 06-07-2018	*Certificati:* 3148 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto User Module v8.0 for ARM *Sistema operativo:* watchOS 4 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 09-03-2018, 17-05-2018, 03-07-2018	*Certificati:* 3147 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Corecrypto Kernel Module v8.0 for ARM *Sistema operativo:* watchOS 4 *Tipo:* software *Livello di sicurezza:* 1
Data di uscita del sistema operativo: 2017 *Date convalida:* 10-09-2019	*Certificati:* 3223 *Documenti:* Certificato Politica di sicurezza Linee guida Crypto Officer	*Nome:* Apple Secure Key Store Cryptographic Module v1.0 *Sistema operativo:* sepOS distribuito con watchOS 4 *Tipo:* hardware *Livello di sicurezza:* 2

Certificazioni di sicurezza per il software

Panoramica sulle certificazioni di sicurezza del software Apple

Apple mantiene certificati di convalida della conformità agli standard FIPS (Federal Information Processing Standard) 140-2/-3 per il firmware sepOS, per il firmware del chip T2 e per altre certificazioni. Apple parte da una serie di *blocchi costituenti delle certificazioni*, applicabili ad ampio raggio a più piattaforme a seconda delle necessità. Uno dei blocchi costituenti è la convalida tramite la libreria corecrypto, che è utilizzata per l'implementazione dei moduli crittografici software e hardware all'interno dei sistemi operativi sviluppati da Apple. Un secondo blocco costituente è la certificazione di Secure Enclave, un coprocessore integrato in molti dispositivi Apple. Un terzo è la certificazione di Secure Element, presente nei dispositivi Apple dotati di Touch ID e di Face ID. Questi blocchi costituenti delle certificazioni hardware costituiscono le fondamenta per certificazioni di sicurezza delle piattaforme più ampie.

Certificazioni dei prodotti: Common Criteria (ISO/IEC 15408)

Lo standard Common Criteria (ISO/IEC 15408) è utilizzato da molte organizzazioni come base per valutare la sicurezza dei prodotti informatici.

Per le certificazioni che potrebbero essere riconosciute reciprocamente dal Common Criteria Recognition Arrangement (CCRA), vai sul portale di Common Criteria. Lo standard Common Criteria potrebbe essere utilizzato anche al di fuori del CCRA da schemi di convalida nazionali e privati. In Europa, il riconoscimento reciproco è governato dall'accordo SOG-IS e dal CCRA.

L'obiettivo, così come dichiarato dalla comunità di Common Criteria, è quello di ottenere un insieme di standard di sicurezza approvato a livello internazionale, così da poter fornire una valutazione chiara e affidabile delle funzionalità di sicurezza dei prodotti informatici. Fornendo un controllo indipendente della capacità di un prodotto di soddisfare determinati standard di sicurezza, la certificazione Common Criteria rafforza la fiducia dei clienti in merito alla sicurezza dei prodotti informatici, consentendo loro di prendere decisioni più informate.

Tramite il CCRA, i paesi aderenti hanno concordato di riconoscere la certificazione dei prodotti informatici con lo stesso livello di attendibilità. Le valutazioni richieste prima della certificazione sono ampie e includono:

- Profili di protezione
- Obiettivi di sicurezza
- Requisiti funzionali di sicurezza
- Requisiti di garanzia
- Livelli di garanzia della valutazione

I profili di protezione sono documenti che specificano i requisiti di sicurezza per una classe di dispositivi, come, ad esempio, la classe Mobility per i dispositivi mobili, e sono utilizzati per consentire il confronto tra le valutazioni dei prodotti informatici all'interno della stessa classe. I membri del CCRA continuano a crescere di anno in anno di pari passo con il numero dei profili di protezione approvati. Questo impianto consente a chi sviluppa un prodotto di conseguire una singola certificazione secondo uno qualsiasi degli schemi di autorizzazione per le certificazioni e di ottenere il riconoscimento da qualsiasi firmatario dei certificati stessi.

Gli obiettivi di sicurezza definiscono *cosa* verrà valutato quando un prodotto informatico è in fase di certificazione. Gli obiettivi di sicurezza vengono tradotti in *requisiti funzionali di sicurezza* più specifici, utilizzati per valutare tali obiettivi più dettagliatamente.

Lo standard Common Criteria (CC) include anche *requisiti di garanzia*. Uno dei fattori comunemente identificati è il *livello di garanzia della valutazione*. I livelli di garanzia della valutazione, a loro volta, raggruppano insiemi i requisiti di garanzia utilizzati comunemente e possono essere specificati in profili di protezione e obiettivi di sicurezza per consentire il confronto.

Molti profili di protezione meno recenti sono stati archiviati e verrano man mano sostituiti da profili di protezione mirati, incentrati su soluzioni e ambienti specifici. In un impegno coordinato mirato a garantire un riconoscimento reciproco tra tutti i membri del CCRA, sono state costituite delle comunità tecniche internazionali (iTC, international Tecnical Community) volte a sviluppare e mantenere profili di protezione collaborativi che sono creati fin dall'inizio tenendo conto degli schemi dei firmatari del CCRA. I profili di protezione destinati a gruppi di utenti e accordi di riconoscimento reciproco diversi dal CCRA continuano ad essere sviluppati dalle parti appropriate interessate.

Apple ha iniziato a perseguire certificazioni secondo la versione aggiornata del CCRA con alcuni profili di protezione collaborativi dall'inizio del 2015. Da allora, Apple ha ottenuto certificazioni Common Criteria per ogni versione principale di iOS e ha ampliato la copertura per includere la garanzia di sicurezza fornita dai nuovi profili di protezione.

Apple assume un ruolo attivo all'interno delle comunità tecniche impegnate nella valutazione delle tecnologie di sicurezza dei dispositivi mobili. Queste includono le iTC responsabili dello sviluppo e dell'aggiornamento dei profili di protezione collaborativi. Apple continua a valutare e a perseguire certificazioni per tutti gli attuali profili di protezione e profili di protezione collaborativi.

Le certificazioni delle piattaforme Apple per il mercato del Nord America vengono generalmente effettuate tramite la National Information Assurance Partnership (NIAP), che mantiene un elenco dei progetti attualmente in fase di valutazione, ma non ancora certificati.

Oltre ai certificati generali per le piattaforme elencati, altri certificati sono stati emessi per dimostrare specifici requisiti di sicurezza per alcuni mercati.

Certificazioni di sicurezza per le app Apple

Contesto delle certificazioni per app Apple

Apple si impegna in maniera attiva nelle certificazioni di sicurezza delle proprie app tramite adeguati profili di protezione di Common Criteria. Tali valutazioni hanno come punto di partenza le certificazioni per l'hardware e per i sistemi operativi che Apple ha già ottenuto.

Nel 2018, Apple ha avviato le valutazioni di sicurezza partendo dalle principali app per iOS 11, il browser Safari e l'app Contatti. Ha poi proseguito le valutazioni per le app su iOS 12, iOS 13 e iPadOS 13.1. Nel 2021, verrà aggiunta la copertura per le app eseguite su macOS 11.

Stato delle certificazioni dei moduli crittografici

Le app Apple elencate nel presente documento utilizzano i moduli crittografici per i relativi sistemi operativi. Per ulteriori informazioni, consulta Certificazioni di sicurezza per iOS, Certificazioni di sicurezza per iPadOS e Certificazioni di sicurezza per macOS.

Stato delle certificazioni Common Criteria (CC)

Lo schema statunitense, gestito dalla NIAP (National Information Assurance Partnership), mantiene un elenco di prodotti in corso di valutazione, contenente i prodotti che sono attualmente in corso di valutazione negli Stati Uniti presso un laboratorio di test Common Criteria approvato dalla NIAP e che hanno completato un primo incontro di valutazione (o equivalente) in cui il CCEVS (Common Criteria Evaluation and Validation Scheme) ha ufficialmente accettato il prodotto per la valutazione.

Dopo la certificazione, la NIAP inserisce le certificazioni attualmente valide nell'elenco dei prodotti conformi. Dopo 2 anni tali certificazioni vengono ricontrollate per verificare la conformità con le politiche di mantenimento della garanzia di sicurezza attuali. Una volta scaduta la data di mantenimento della garanzia di sicurezza, la NIAP sposta le certificazioni nell'elenco dei prodotti archiviati.

Il portale Common Criteria riporta l'elenco delle certificazioni che possono essere riconosciute reciprocamente in base al Common Criteria Recognition Arrangement (CCRA). Il portale Common Criteria può conservare i prodotti nell'elenco dei prodotti certificati per 5 anni, all'interno delle certificazioni archiviate.

La tabella di seguito mostra le certificazioni attualmente in fase di valutazione da parte di un laboratorio o che sono state certificate come conformi allo standard Common Criteria.

Stato attuale

- Le valutazioni NIAP pubblicate come attualmente in corso sono elencate in Prodotti in corso di valutazione (NIAP).
- Le valutazioni che sono state completate e convalidate sono elencate nell'elenco dei prodotti conformi NIAP.

Sistema operativo / Data certificazione	ID schema / Documenti	Nome / Profili di protezione
Sistema operativo: macOS 11 Big Sur *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* Certificato Obiettivo di sicurezza Guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* macOS 11 Big Sur: Contatti *Profili di protezione:* profilo di protezione per software applicativo, pacchetto esteso per i browser web
Sistema operativo: macOS 11 Big Sur *Data certificazione:* —	*ID schema:* non ancora certificato *Documenti:* Certificato Obiettivo di sicurezza Guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* macOS 11 Big Sur: Safari *Profili di protezione:* profilo di protezione per software applicativo, pacchetto esteso per i browser web
Sistema operativo: iOS 14, iPadOS 14 *Data certificazione:* 20-08-2021	*ID schema:* 11191 *Documenti:* Certificato Obiettivo di sicurezza Guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* iOS 14 e iPadOS 14 Apple: Contatti *Profili di protezione:* profilo di protezione per software applicativo, pacchetto esteso per i browser web
Sistema operativo: iOS 14, iPadOS 14 *Data certificazione:* —	*ID schema:* 11192 *Documenti:* Certificato Obiettivo di sicurezza Guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* iOS 14 e iPadOS 14 Apple: Safari *Profili di protezione:* profilo di protezione per software applicativo, pacchetto esteso per i browser web

Sistema operativo / Data certificazione	ID schema / Documenti	Nome / Profili di protezione
Sistema operativo: iOS 13, iPadOS 13 *Data certificazione:* 05-06-2020	*ID schema:* 11060 *Documenti:* Certificato Obiettivo di sicurezza Guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* iOS 13 e iPadOS 13 Apple: Safari *Profili di protezione:* profilo di protezione per software applicativo, pacchetto esteso per i browser web
Sistema operativo: iOS 13, iPadOS 13 *Data certificazione:* 05-06-2020	*ID schema:* 11050 *Documenti:* Certificato Obiettivo di sicurezza Guida Relazione di convalida Relazione delle attività di garanzia	*Nome:* iOS 13 e iPadOS 13 Apple: Contatti *Profili di protezione:* profilo di protezione per software applicativo

Certificazioni Common Criteria archiviate per le app Apple

Sistema operativo / Data certificazione	ID schema / Documenti	Nome / Profili di protezione
Sistema operativo: iOS 12 *Data certificazione:* 12-06-2019	*ID schema:* 10960 *Documenti:* Obiettivo di sicurezza Guida	*Nome:* iOS 12 Safari *Profili di protezione:* profilo di protezione per software applicativo, pacchetto esteso per i browser web
Sistema operativo: iOS 12 *Data certificazione:* 28-02-2019	*ID schema:* 10961 *Documenti:* Obiettivo di sicurezza Linee guida	*Nome:* iOS 12 Contatti *Profili di protezione:* profilo di protezione per software applicativo
Sistema operativo: iOS 11 *Data certificazione:* 09-11-2018	*ID schema:* 10916 *Documenti:* Obiettivo di sicurezza Linee guida	*Nome:* iOS 11 Safari *Profili di protezione:* profilo di protezione per software applicativo, pacchetto esteso per i browser web
Sistema operativo: iOS 11 *Data certificazione:* 13-09-2018	*ID schema:* 10915 *Documenti:* Obiettivo di sicurezza Linee guida	*Nome:* iOS 11 Contatti *Profili di protezione:* profilo di protezione per software applicativo

Certificazioni di sicurezza per i servizi internet Apple

Apple mantiene certificazioni che soddisfano gli standard ISO/IEC 27001 e ISO/IEC 27018, per consentire ai clienti Apple di adempiere ai propri obblighi legali e contrattuali. Tali certificazioni forniscono ai nostri clienti un'attestazione indipendente sulle pratiche adottate da Apple in materia di sicurezza delle informazioni e privacy per i sistemi Apple.

ISO/IEC 27001 e ISO/IEC 27018 fanno parte di una famiglia di standard per sistemi di gestione della sicurezza delle informazioni pubblicati dall'Organizzazione internazionale per la normazione (ISO, International Organization for Standardization). Come parte del sistema di gestione della sicurezza delle informazioni, tutti i requisiti di controllo dell'Allegato A sono stati inclusi nella dichiarazione di applicabilità secondo quanto definito dagli standard ISO/IEC 27001 e ISO/IEC 27018. Apple viene sottoposta a verifiche indipendenti da parte di registrar accreditati su base annuale.

ISO/IEC 27001

ISO/IEC 27001 è uno standard che specifica i requisiti per stabilire, implementare, mantenere e migliorare costantemente il sistema di gestione della sicurezza delle informazioni di un'organizzazione. Lo standard ISO/IEC 27001 include i seguenti domini di sicurezza, coperti dalle certificazioni ISO/IEC di Apple.

- Politiche di sicurezza delle informazioni
- Organizzazione della sicurezza delle informazioni
- Gestione delle risorse
- Sicurezza delle risorse umane
- Sicurezza fisica e ambientale
- Gestione delle comunicazioni e delle operazioni
- Controllo degli accessi
- Acquisizione, sviluppo e mantenimento dei sistemi informativi
- Gestione degli incidenti informatici
- Gestione della continuità aziendale
- Conformità

ISO/IEC 27018

ISO/IEC 27018 è un codice di condotta per la protezione delle informazioni a carattere personale (PII, Personally Identifiable information) negli ambienti cloud pubblici. Lo standard ISO/IEC 27018 include i seguenti domini di sicurezza, coperti dalle certificazioni ISO/IEC di Apple.

- Consenso e scelta
- Legittimità e specificazione dello scopo
- Limitazione della raccolta
- Minimizzazione dei dati
- Uso, conservazione e limiti alla divulgazione
- Accuratezza e qualità
- Apertura, trasparenza e informativa
- Partecipazione e accesso da parte degli individui
- Responsabilità
- Sicurezza delle informazioni
- Conformità privacy

Servizi Apple coperti dagli standard ISO/IEC 27001 e ISO/IEC 27018

Le certificazioni Apple ISO/IEC 27001 e ISO/IEC 27018 coprono i seguenti servizi:

- Apple Business Chat
- Apple Business Manager
- Servizio di notifiche push di Apple (APN, Apple Push Notification)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- Servizi iWork
- ID Apple gestiti
- Schoolwork
- Siri

Certificati

I documenti che provano le certificazioni Apple per gli standard ISO/IEC 27001 e 27018 sono disponibili presso il nostro registro.

Per visualizzare le certificazioni Apple, consulta la pagina di ricerca dei certificati e delle organizzazioni del sito web della British Standards Institution (BSI), inserisci Apple nel campo di ricerca delle aziende, fai clic sul pulsante Cerca, quindi seleziona i risultati di ricerca per visualizzare i certificati.

Nota: le informazioni sui prodotti non fabbricati da Apple o sui siti indipendenti non controllati o testati da Apple vengono fornite solo a scopo informativo e non costituiscono raccomandazioni o approvazioni da parte di Apple. Apple declina ogni responsabilità per quanto riguarda la selezione, le prestazioni e l'uso di siti web o prodotti di terze parti. Apple non rilascia alcuna dichiarazione in merito all'accuratezza o all'affidabilità dei siti web di terze parti. Contatta il fornitore per ulteriori informazioni.

macOS Security Compliance Project

Il macOS Security Compliance Project (Progetto per la conformità della sicurezza di macOS, mSCP) è un'iniziativa open source che mira a di fornire un approccio programmatico per la creazione di linee guida per la sicurezza. Si tratta di un progetto congiunto che coinvolge il personale operativo federale per la sicurezza informatica del National Institute of Standards and Technology (NIST), della National Aeronautics and Space Administration (NASA), della Defense Information Systems Agency (DISA) e del Los Alamos National Laboratory (LANL). Il progetto utilizza un insieme di controlli testati e convalidati per macOS e li sottopone a qualsiasi standard di sicurezza supportato dall'iniziativa. Inoltre, il progetto può essere utilizzato come risorsa per creare agevolmente delle linee guida personalizzate per i controlli di sicurezza tecnici sfruttando una libreria di operazioni atomiche (impostazioni di configurazione) testate e convalidate. Il progetto produce risorse personalizzate, tra cui materiale di documentazione, script, profili di configurazione e un elenco di controllo per la verifica basato sui riferimenti adottati.

L'mSCP è in grado di produrre contenuti che possono essere utilizzati insieme a strumenti per la gestione e per la sicurezza per raggiungere la conformità agli standard. Le impostazioni di configurazione del progetto supportano le seguenti linee guida di base.

Organizzazione	Linee guida supportate
Pubblicazione speciale 800-53 del NIST, Recommended Security Controls for Federal Information Systems and Organizations, Revision 5	800-53 High, 800-53 Moderate, 800-53 Low
Pubblicazione speciale 800-171 del NIST, 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

Informazioni aggiuntive:

- Le risorse per la consultazione delle regole del progetto sono disponibili qui.
- Per ulteriori informazioni sul progetto e sul suo utilizzo, consulta la pagina wiki del macOS Security Compliance Project.
- Per la configurazione del progetto per il suo utilizzo, consulta: Getting to Know the macOS Security Compliance Project, Part 1 e Getting to Know the macOS Security Compliance Project, Part 2.
- Per supportare lo sviluppo del progetto, consulta le linee guida per la collaborazione.

Cronologia delle revisioni del documento

Data	Riepilogo
27 ottobre 2021	Argomenti aggiornati: • Certificazioni di sicurezza per il processore Secure Enclave • Certificazioni di sicurezza per iOS • Certificazioni di sicurezza per macOS
17 agosto 2021	Argomenti aggiornati: • Certificazioni di sicurezza per il processore Secure Enclave • Certificazioni di sicurezza per il chip di sicurezza Apple T2 • Certificazioni di sicurezza per iOS • Certificazioni di sicurezza per iPadOS • Certificazioni di sicurezza per macOS • Certificazioni di sicurezza per tvOS • Certificazioni di sicurezza per watchOS • Certificazioni di sicurezza per le app Apple • Certificazioni di sicurezza • macOS Security Compliance Project
26 aprile 2021	Argomento aggiunto: • macOS Security Compliance Project Argomenti aggiornati: • Certificazioni di sicurezza per il chip di sicurezza Apple T2: nuova certificazione FIPS 140-2, 3811. • Certificazioni di sicurezza per il processore Secure Enclave: nuova certificazione FIPS 140-2, 3811 e nuova tabella per le certificazioni aggiuntive. • Certificazioni di sicurezza per iOS: nuova certificazione FIPS 140-2, 3811, ID schema 11146 in valutazione per iOS 14. • Certificazioni di sicurezza per iPadOS: nuova certificazione FIPS 140-2, 3811, ID schema 11147 in valutazione per iPadOS 14. • Certificazioni di sicurezza per macOS: nuova certificazione FIPS 140-2, 3811. • Certificazioni di sicurezza per tvOS: nuove certificazioni FIPS 140-2, 3811. • Certificazioni di sicurezza per watchOS: nuove certificazioni FIPS 140-2, 3811. • Certificazioni di sicurezza per le app Apple: aggiornamenti relativi al Common Criteria e nuova tabella per le certificazioni Common Criteria ottenute.

Glossario

Apple Business Manager Portale web di facile utilizzo pensato per gli amministratori IT. Offre un metodo rapido ed efficiente per la distribuzione dei dispositivi che l'organizzazione ha acquistato direttamente da Apple o da un rivenditore o gestore autorizzato. Le organizzazioni possono registrare automaticamente i dispositivi in una soluzione di gestione dei dispositivi mobili (MDM) senza doverli toccare o preparare materialmente prima di consegnarli agli utenti.

Apple School Manager Portale web di facile utilizzo pensato per gli amministratori IT. Offre un metodo rapido ed efficiente per la distribuzione dei dispositivi che l'organizzazione ha acquistato direttamente da Apple o da un rivenditore o gestore autorizzato. Le organizzazioni possono registrare automaticamente i dispositivi in una soluzione di gestione dei dispositivi mobili (MDM) senza doverli toccare o preparare materialmente prima di consegnarli agli utenti.

client VPN IPsec In un profilo di protezione, un client che fornisce una connessione IPsec sicura tra una piattaforma host fisica o virtuale e una posizione remota.

codifica completa del disco Codifica di tutti i dati su un volume di archiviazione.

Common Criteria (CC) Standard che stabilisce i concetti e i principi generali della valutazione della sicurezza informatica e specifica un modello di valutazione generale. Include cataloghi di requisiti di sicurezza redatti in un linguaggio standardizzato.

Common Criteria Recognition Arrangement (CCRA) Accordo di riconoscimento reciproco che stabilisce le politiche e i requisisti per il riconoscimento internazionale dei certificati emessi secondo gli standard ISO/IEC 15408 o Common Criteria.

comunità tecnica internazionale (iTC, international Tecnical Community) Gruppo responsabile dello sviluppo dei profili di protezione o dei profili di protezione collaborativi secondo le direttive dell'accordo Common Criteria Recognition Arrangement (CCRA).

corecrypto Libreria che fornisce implementazioni di livello base dei primitivi crittografici. La libreria corecrypto non offre direttamente interfacce di programmazione per gli sviluppatori, ma viene utilizzata attraverso delle API fornite agli sviluppatori. Il codice di corecrypto è disponibile pubblicamente per consentire la verifica delle sue caratteristiche di sicurezza e del suo corretto funzionamento.

Cryptographic Algorithm Validation Program (CAVP) Organizzazione gestita dal NIST per fornire test di convalida degli algoritmi crittografici approvati (ad esempio, approvati dagli standard FIPS e consigliati dal NIST) e dei relativi componenti individuali.

Cryptographic Module Validation Program (CMVP) Organizzazione gestita dal governo americano e dal governo canadese per convalidare la conformità allo standard FIPS 140-3.

Dichiarazione di applicabilità Documento che descrive i controlli di sicurezza implementati nell'ambito di un sistema di gestione della sicurezza delle informazioni, prodotto a supporto di una certificazione ISO/IEC 27001.

FIPS (Federal Information Processing Standard) Pubblicazioni sviluppate dal National Institute of Standards and Technology (NIST) quando richieste dallo statuto, in caso di importanti requisiti governativi federali per la sicurezza informatica o in entrambi i casi.

Gestione dei dispositivi mobili (MDM) Servizio che consente all'utente di gestire da remoto i dispositivi registrati. Dopo che un dispositivo è registrato, l'utente può utilizzare il servizio MDM sulla rete per configurare le impostazioni ed eseguire altre attività sul dispositivo senza l'interazione dell'utente.

Implementazione in fase di test Modulo crittografico attualmente in fase di test presso un laboratorio.

Livello di sicurezza Uno dei quattro livelli di sicurezza (1-4) definiti dallo standard ISO/IEC 19790 per descrivere insiemi di requisiti di sicurezza applicabili. Il livello 4 è quello più rigido.

Moduli in lavorazione Elenco redatto dal CMVP (Cryptographic Module Validation Program) contenente i moduli crittografici attualmente in lavorazione.

modulo crittografico Componente hardware, software e/o firmware che fornisce funzioni crittografiche ed è conforme ai requisiti stabiliti da uno standard per moduli crittografici dichiarato.

National Information Assurance Partnership (NIAP) Organizzazione del governo americano responsabile dell'implementazione negli Stati Uniti dello standard Common Criteria e della gestione dello schema CCEVS (Common Criteria Evaluation and Validation Scheme).

National Institute of Standards and Technology (NIST) Parte del Dipartimento del commercio degli Stati Uniti responsabile dell'avanzamento nel campo delle misurazioni scientifiche, degli standard e della tecnologia.

Obiettivo di sicurezza Documento che specifica le problematiche e i requisiti di sicurezza di un particolare prodotto.

Processore Secure Enclave Coprocessore fabbricato all'interno di un system on chip (SoC).

Profilo di protezione Documento che specifica le problematiche e i requisiti di sicurezza di una particolare classe di prodotti.

profilo di protezione collaborativo Profilo di protezione sviluppato da una comunità tecnica internazionale, un gruppo di esperti che ha il compito di creare profili di protezione collaborativi.

Secure Element Chip integrato in molti prodotti Apple che supporta funzionalità come Apple Pay.

Senior Officials Group Information Systems Security (SOG-IS) Gruppo che gestisce un accordo di riconoscimento reciproco tra varie nazioni europee.

sepOS Il firmware di Secure Enclave, basato su una versione personalizzata da Apple del microkernel L4.

Servizio di notifiche push di Apple (APN, Apple Push Notification) Servizio fornito da Apple che trasmette notifiche push ai dispositivi Apple in tutto il mondo.

sistema di gestione della sicurezza delle informazioni Insieme di politiche e procedure per la sicurezza delle informazioni che delimitano un programma di sicurezza destinato a proteggere informazioni e sistemi, gestendo in modo sistematico la sicurezza dei dati e dei sistemi in tutto il loro ciclo di vita.

system on chip (SoC) Circuito integrato che comprende più componenti in un unico chip.

T2 Chip di sicurezza Apple incluso in alcuni Mac dotati di processore Intel a partire dal 2017.

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

T028-00499-B