Sicherheitszertifizierungen und Compliance

Dezember 2021

Inhaltsverzeichnis

Einführung in die Sicherheitsstandards von Apple

Im Rahmen seines Engagements für Sicherheit setzt sich Apple regelmäßig in Zusammenarbeit mit anderen Organisationen für die Zertifizierung und Bescheinigung der Sicherheit der Hardware, Software und Dienste von Apple ein. Diese international anerkannten Organisationen stellen Apple Zertifizierungen für jede Hauptversion eines Betriebssystems aus. Somit liefern sie einen Gradmesser für das Vertrauen – also Sicherheitsstandards – und belegen, dass die Sicherheitsanforderungen eines Systems erfüllt sind. Im Falle von technischen Bereichen, die im Rahmen von MRAs (Mutual Recognition Arrangements) nicht anerkannt sind oder für die es keine ausgereiften Standards für die Sicherheitszertifizierung gibt, engagiert sich Apple in der Entwicklung geeigneter Sicherheitsstandards. Unser Ziel ist es, die Abdeckung der gesamten Palette an Hardware, Betriebssystemen, Apps und Diensten von Apple mit international anerkannten, umfassenden Sicherheitszertifizierungen weiter voranzutreiben.

Zertifizierungen sind häufig erforderlich, um gesetzliche, regulatorische und branchenspezifische Vorgaben zu erfüllen. Dienste wie Apple School Manager und Apple Business Manager sind im Rahmen der ISO/IEC 27001- und ISO/IEC 27018-Zertifizierungen von Apple abgedeckt. Alle Kunden, einschließlich Behörden, Unternehmen und Bildungsorganisationen, die Apple-Geräte einsetzen, können die Zertifizierungen für Hardware, Betriebssysteme, Software und Dienste verwenden, um die Einhaltung von Vorgaben (Compliance) zu belegen.

Zertifizierungen für Hardware

Voraussetzung für eine sichere Software ist ein in die Hardware integriertes Sicherheitsfundament. Aus diesem Grund verfügen alle Apple-Geräte – unabhängig davon, ob sie iOS, iPadOS, macOS, tvOS oder watchOS verwenden – über Sicherheitsfunktionen, die in den Siliziumchip integriert sind. Hierzu zählen eine CPU, die die Rechenleistung für die Sicherheitsfunktionen des Systems bereitstellt, sowie dedizierte Chips für Sicherheitsfunktionen. Die wichtigste Komponente ist hierbei der Secure Enclave-Coprozessor, der sich in allen aktuellen iOS-, iPadOS-, watchOS- und tvOS-Geräten sowie in allen Mac-Computern mit Apple Chips und in Intel-basierten Mac-Computern mit Apple T2-Sicherheits-Chip befindet. Die Secure Enclave ist die Basis für die Verschlüsselung von ruhenden Daten (Data-at-Rest), für sicheres Starten (Booten) in macOS und für die biometrischen Funktionen.

Das Engagement von Apple für Sicherheitsstandards beginnt mit der Zertifizierung von grundlegenden Sicherheitskomponenten im Siliziumchip – vom Hardware-Vertrauensanker über die Durchsetzung des sicheren Startens und die Secure Enclave, die den Secure Key Store (SKS) bereitstellt, bis hin zur sicheren Authentifizierung mit Touch ID und Face ID. Die Sicherheitsfunktionen von Apple-Geräten werden durch die Kombination aus Chipdesign, Hardware, Software und Diensten ermöglicht, die ausschließlich von Apple stammen. Die Zertifizierung dieser Komponenten ist ein wichtiger Aspekt, der die von Apple bereitgestellte Vertrauenswürdigkeit belegt.

Weitere Informationen zu öffentlichen Zertifizierungen für Hardware und zugehörige Firmware-Komponenten sind hier zu finden:

- Sicherheitszertifizierungen für den Apple T2-Sicherheits-Chip
- Sicherheitszertifizierungen für den Secure Enclave-Prozessor (SEP)

Zertifizierungen für Software und Apps

Apple hält unabhängige Zertifizierungen und Bescheinigungen für seine Betriebssysteme und Apps, die den Anforderungen der US-Standards für die Informationsverarbeitung für kryptografische Module (FIPS-2/-3; Federal Information Processing Standards) und den CC-Anforderungen (Common Criteria) für Betriebssysteme, Apps und Gerätedienste entsprechen. Zu den abgedeckten Betriebssystemen gehören iOS, iPadOS, macOS, sepOS, T2-Firmware, tvOS und watchOS. Bei den Apps decken die unabhängigen Zertifizierungen zunächst den Webbrowser „Safari“ und die App „Kontakte“ ab, wobei die Zertifizierung weiterer Apps folgen wird.

Weitere Informationen zu öffentlichen Zertifizierungen für *Betriebssysteme* von Apple sind hier zu finden:

- Sicherheitszertifizierungen für iOS
- Sicherheitszertifizierungen für iPadOS
- Sicherheitszertifizierungen für macOS
- Sicherheitszertifizierungen für tvOS
- Sicherheitszertifizierungen für watchOS

Weitere Informationen zu öffentlichen Zertifizierungen für *Apps* von Apple sind hier zu finden:

- Sicherheitszertifizierungen für Apple-Apps

Zertifizierungen für Dienste

Apple hält Sicherheitszertifizierungen, um Kunden aus unterschiedlichen Bereichen zu unterstützen – vom Unternehmensbereich bis hin zum Bildungsbereich. Diese Zertifizierungen ermöglichen es Kunden von Apple, ihre gesetzlichen und vertraglichen Verpflichtungen zu erfüllen, wenn Apple-Dienste in Verbindung mit Hardware und Software von Apple verwendet werden. Diese Zertifizierungen bieten unseren Kunden eine unabhängige Beurteilung der von Apple für die Informationssicherheit sowie für den Umwelt- und Datenschutz in Apple-Systemen eingesetzten Verfahren.

Weitere Informationen zu öffentlichen Zertifizierungen für *Internetdienste* von Apple sind hier zu finden:

- Sicherheitszertifizierungen für Apple-Internetdienste

Fragen zu Apple-Zertifizierungen für Sicherheit und Datenschutz können per E-Mail an security-certifications@apple.com gestellt werden.

Sicherheitszertifizierungen für Hardware

Sicherheitszertifizierungen für Apple-Hardware – Übersicht

Apple hält Validierungszertifikate zur Konformität (Conformance Validation Certificates) mit dem US-Standard Federal Information Processing Standard (FIPS) 140-2/-3 für sepOS und T-Firmware sowie weitere Zertifizierungen. Als Grundlage verwendet Apple *Zertifizierungsbausteine*, die gegebenenfalls für mehrere Plattformen gelten. Ein Baustein ist die Validierung der corecrypto-Bibliothek, die für Implementierungen von kryptografischen Modulen für Software und Hardware in von Apple entwickelten Betriebssystemen verwendet wird. Ein zweiter Baustein ist die Zertifizierung der Secure Enclave, die in viele Apple-Geräte integriert ist. Ein dritter Baustein ist die Zertifizierung des Secure Element (SE), das in Apple-Geräten mit Touch ID und in Geräten mit Face ID vorhanden ist.
Diese Zertifizierungsbausteine für die Hardware bilden das Fundament für weitere Plattform-Sicherheitszertifizierungen.

Validierungen von kryptografischen Algorithmen

Die Validierung der korrekten Implementierung zahlreicher kryptografischer Algorithmen und der zugehörigen Sicherheitsfunktionen ist Voraussetzung für die FIPS 140-3-Validierung und unterstützt andere Zertifizierungen. Die Validierung wird vom Cryptographic Algorithm Validation Program (CAVP) des National Institute of Standards and Technology (NIST) verwaltet. Validierungszertifikate für Apple-Implementierungen können über die CAVP-Suchfunktion abgerufen werden. Weitere Informationen findest du auf der CAVP-Website (Cryptographic Algorithm Validation Program).

Validierungen von kryptografischen Modulen: FIPS 140-2/3 (ISO/IEC 19790)

Die kryptografischen Module von Apple wurden seit 2012 wiederholt nach jeder Hauptversion eines Betriebssystems im Rahmen des Cryptographic Module Validation Program (CMVP) validiert und als mit den U.S. Federal Information Processing Standards für kryptografische Module (FIPS 140-2) konform eingestuft. Nach jeder Hauptversion übermittelt Apple die Module an das CMVP zur Validierung der Konformität mit dem Standard. Diese Module werden nicht nur von den Betriebssystemen und Apps von Apple genutzt, sondern bieten auch die kryptografischen Funktionen für die von Apple bereitgestellten Dienste und stehen den Apps von Drittanbietern zur Verfügung.

Bei den softwarebasierten Modulen „Corecrypto Module for Intel“ und „Corecrypto Kernel Module for Intel“ erreicht Apple jedes Jahr die **Sicherheitsstufe 1** (Security Level 1). Bei Apple Chips sind die Module „CoreCrypto Module for ARM“ und „CoreCrypto Kernel Module for ARM“ für iOS, iPadOS, tvOS, watchOS und die Firmware des integrierten Apple T2-Sicherheits-Chips in Mac-Computern anwendbar.

2019 erreichte Apple zum ersten Mal die **Sicherheitsstufe 2** (Security Level 2) des FIPS 140-2-Standards für das integrierte kryptografische Hardwaremodul mit der Bezeichnung „Apple Corecrypto Module: Secure Key Store“, wodurch eine von der US-Regierung bewilligte Nutzung von Schlüsseln erlaubt wurde, die mittels Secure Enclave generiert und verwaltet werden. Apple wird auch künftig alles dafür tun, bei jeder Hauptversion seiner Betriebssysteme Validierungen für die kryptografischen Hardwaremodule zu erhalten.

FIPS 140-3 wurde 2019 vom US-Handelsministerium (U.S. Department of Commerce) zugelassen. Die wichtigste Änderung in dieser Version des Standards ist die Spezifizierung von ISO/IEC-Standards – insbesondere von ISO/IEC 19790:2015 und dem zugehörigen Teststandard ISO/IEC 24759:2017. Für das CMVP wurde ein Übergangsprogramm initiiert und es wurde angekündigt, dass ab 2020 kryptografische Module auf der Basis von FIPS 140-3 validiert werden. Es ist das Ziel von Apple, dass die kryptografischen Module die Anforderungen des Standards FIPS 140-3 zum frühestmöglichen praktikablen Zeitpunkt erfüllen und zu diesem übergehen.

Für kryptografische Module, die derzeit Test- und Validierungsprozesse durchlaufen, führt das CMVP zwei separate Listen, die Informationen zu vorgeschlagenen Validierungen enthalten können. Kryptografische Module, die derzeit durch eine akkreditierte Prüfstelle getestet werden, werden möglicherweise in der Implementation Under Test List aufgeführt. Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat, werden die kryptografischen Module von Apple in der Modules in Process List angezeigt. Die Tests durch die Prüfstelle sind derzeit abgeschlossen und warten auf ihre Validierung durch das CMVP. Da der Evaluierungsprozess unterschiedlich lange dauern kann, empfiehlt es sich, einen Blick auf die beiden oben genannten Listen zu werfen, um zwischen dem Datum der Veröffentlichung der Hauptversion eines Betriebssystems und der Ausstellung des Validierungszertifikats durch das CMVP den aktuellen Status der kryptografischen Module von Apple in Erfahrung zu bringen.

Produktzertifizierungen: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) ist ein Standard, der von vielen Organisationen als Grundlage für die Sicherheitsevaluierungen von IT-Produkten verwendet wird.

Informationen zu Zertifizierungen, die im Rahmen des internationalen Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können, sind im Common Criteria Portal zu finden. Die Common Criteria-Standards können auch jenseits des CCRA von nationalen und privaten Validierungssystemen verwendet werden. In Europa wird die gegenseitige Anerkennung durch die SOG-IS-Vereinbarung sowie durch das CCRA (Common Criteria Recognition Arrangement) geregelt.

Das von der Common Criteria-Community formulierte Ziel ist eine international anerkannte Sammlung von Sicherheitsstandards, die eine eindeutige und verlässliche Evaluierung der Sicherheitsfunktionen von IT-Produkten ermöglichen. Durch die Bereitstellung einer unabhängigen Bewertung der Fähigkeit eines Produkts, Sicherheitsstandards zu erfüllen, gibt die Common Criteria-Zertifizierung Kunden mehr Vertrauen in die Sicherheit von IT-Produkten und ermöglicht so fundiertere Entscheidungen.

Im Rahmen des CCRA sind die Mitgliedsländer übereingekommen, die Zertifizierung für IT-Produkte mit dem gleichen Maß an Vertrauen anzuerkennen. Die vor der Zertifizierung erforderlichen Evaluierungen sind umfangreich und umfassen:

- Protection Profiles (PPs)
- Security Targets (STs)
- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)
- Evaluation Assurance Levels (EALs)

Protection Profiles (PPs) sind Dokumente, die die Sicherheitsanforderungen für eine Klasse von Gerätetypen (wie Mobilität) definieren, und werden verwendet, um die Evaluierungen von IT-Produkten derselben Klasse miteinander vergleichen zu können. Die Zahl der CCRA-Mitglieder sowie die Liste zugelassener PPs wird jedes Jahr weiterwachsen. Diese Vereinbarung erlaubt es einem Produktentwickler, eine einzelne Zertifizierung unter einem beliebigen Autorisierungsprogramm für Zertifikate durchzuführen und sie durch einen beliebigen autorisierten Zertifikataussteller anerkennen zu lassen.

Security Targets (STs) definieren, *was* bei der Zertifizierung eines IT-Produkts evaluiert wird. Die STs werden in spezifischere *Security Functional Requirements (SFRs)* übertragen, die für die eingehendere Evaluierung der STs eingesetzt werden.

Die Common Criteria (CC) umfassen auch *Security Assurance Requirements (SARs)*. Die am häufigsten verwendeten Kriterien sind dabei die *Evaluation Assurance Levels (EALs)*. EALs gruppieren häufige SARs und können in PPs und STs spezifiziert werden, um die Vergleichbarkeit zu ermöglichen.

Viele ältere PPs wurden archiviert und werden durch zielgerichtete PPs ersetzt, die nun entwickelt werden und sich auf spezifische Lösungen und Umgebungen konzentrieren. Im Rahmen einer gemeinsamen Bemühung, die fortlaufende Anerkennung der Zertifizierung durch alle CCRA-Mitglieder sicherzustellen, wurden International Technical Communities (iTCs) zur Entwicklung und Pflege von Collaborative Protection Profiles (cPPs) eingerichtet, die von Anfang an unter Einbeziehung von CCRA-Zertifizierungsprogrammen entwickelt werden. PPs für andere Benutzergruppen und andere MRAs (Mutual Recognition Agreements) als das CCRA werden weiterhin von den entsprechenden Interessenvertretern entwickelt.

Mit ausgewählten cPPs führt Apple seit Anfang 2015 Zertifizierungen im Rahmen des aktualisierten CCRA durch. Seit dieser Zeit hat Apple Zertifizierungen gemäß Common Criteria für jede iOS-Hauptversion erhalten und den Geltungsbereich auf Sicherheitsstandards ausgeweitet, die von neuen PPs bereitgestellt werden.

Apple übernimmt eine aktive Rolle innerhalb der technischen Communitys, deren Fokus auf der Evaluierung von Sicherheitstechnologien für Mobilgeräte liegt. Hierzu gehören auch die für die Entwicklung und Aktualisierung von cPPs verantwortlichen iTCs. Apple wird auch künftig Zertifizierungen auf Basis von PPs und cPPs evaluieren und durchführen.

Zertifizierungen für Plattformen von Apple für den nordamerikanischen Markt werden allgemein über die National Information Assurance Partnership (NIAP) durchgeführt, die eine Liste von in der Evaluierung befindlichen Projekten (Products in Evaluation) führt, die jedoch noch nicht zertifiziert sind.

Zusätzlich zu den aufgeführten allgemeinen Plattform-Zertifikaten wurden weitere Zertifikate ausgestellt, um spezifische Sicherheitsanforderungen in bestimmten Märkten aufzuzeigen.

Sicherheitszertifizierungen für den Secure Enclave-Prozessor (SEP)

Hintergrundinformationen zu Zertifizierungen der Secure Enclave

Das kryptografische Hardwaremodul – *Apple SEP Secure Key Store Cryptographic Module* – ist in den Apple SoC (System-on-Chip) integriert, der in folgenden Produkten verbaut ist: Apple A Series für iPhone und iPad, M Series für Mac-Computer mit Apple Chips, S Series für die Apple Watch und Sicherheits-Chips der T Series für Intel-basierte Mac-Computer ab dem iMac Pro, der 2017 auf den Markt kam.

Im Jahr 2018 synchronisierte Apple die Validierung der kryptografischen Softwaremodule mit den 2017 veröffentlichten Betriebssystemen iOS 11, macOS 10.13, tvOS 11 und watchOS 4. Das als Apple SEP Secure Key Store Cryptographic Module v1.0 identifizierte kryptografische SEP-Hardwaremodul wurde zuvor auf Erfüllung der Anforderungen gemäß FIPS 140-2 Security Level 1 geprüft.

Im Jahr 2019 hat Apple das Hardwaremodul anhand der Anforderungen von FIPS 140-2 Security Level 2 validiert und die Modulversions-ID auf v9.0 aktualisiert, um es mit den Versionen der entsprechenden Modulvalidierungen von „corecrypto User“ und „corecrypto Kernel“ zu synchronisieren. Im Jahr 2019 umfasste dies iOS 12, macOS 10.14, tvOS 12 und watchOS 5.

2020 und 2021 verfolgt Apple die Validierung der Konformität mit FITS 140-3 und mit der zusätzlichen Sicherheitsstufe 3 der physischen Sicherheitsanforderungen an die Apple Chips: A13, A14, S6 und M1.

Bei jeder Hauptversion eines Betriebssystems beteiligt sich Apple darüber hinaus auch aktiv an der Validierung der „corecrypto User“- und „corecrypto Kernel“-Module. Die Validierung der Konformität kann nur mit einer endgültig freigegebenen Version stattfinden.

Validierung von kryptografischen Modulen – Status

Das Cryptographic Module Validation Program (CMVP) verwaltet den Validierungsstatus kryptografischer Module in Abhängigkeit von ihrem aktuellen Status in drei separaten Listen:

- Damit die Module in der CMVP-Liste Implementation Under Test aufgeführt werden, muss die Prüfstelle von Apple mit dem Testen beauftragt worden sein.
- Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat und sobald die CMVP-Gebühren bezahlt wurden, wird das Modul zur Modules in Process List hinzugefügt. Die „MIP List“ verfolgt den Fortschritt der CMVP-Validierung in vier Phasen:
  - *Review Pending:* Das Modul wartet darauf, dass ihm eine CMVP-Ressource zugewiesen wird.
  - *In Review:* CMVP-Ressourcen führen die erforderlichen Validierungsaktivitäten aus.
  - *Coordination:* Die Prüfstelle und das CMVP beschäftigen sich mit den gefundenen Problemen.
  - *Finalization:* Die Aktivitäten und Formalitäten im Zusammenhang mit der Ausstellung des Zertifikats werden ausgeführt.
- Im Anschluss an die Validierung durch das CMVP erhalten die Module ein Konformitätszertifikat und werden zur Liste Validated Cryptographic Modules hinzugefügt. Hierzu gehören:
  - Validierte Module, die als active markiert wurden.
  - Nach 5 Jahren werden die Module als historical markiert.
  - Wenn das Modulzertifikat aus irgendeinem Grund entzogen wurde, wird es als revoked markiert.

Im Jahr 2020 übernahm das CMVP den internationalen Standard ISO/IEC 19790 als Basis für FIPS 140-3.

FIPS 140-3-Zertifizierungen

Aktueller Status

Die Tabelle unten zeigt die kryptografischen Module aus den Jahren 2020 und 2021, die momentan von der Prüfstelle auf Konformität mit FIPS 140-3 getestet werden.

Secure Key Store (SKS) in den Betriebssystemen von 2020 und 2021 wurde von der Prüfstelle getestet und erhielt von der Prüfstelle eine Empfehlung für die Validierung durch das CMVP. Sie werden in der Liste Modules in Process aufgeführt, bis der Validierungsprozess abgeschlossen ist. Im Anschluss werden sie in die Liste der validierten kryptografischen Module verschoben.

iOS 15 (2021): Benutzerbereich (User Space), Kernelbereich und Secure Key Store werden von der Prüfstelle getestet. Die Module befinden sich in der Implementation Under Test List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit den iOS-, iPadOS-, macOS-, tvOS- und watchOS-Versionen von 2021 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14, T2, M1, S3-S6) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit den iOS-, iPadOS-, macOS-, tvOS- und watchOS-Versionen von 2021 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A13, A14, S6, M1) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit den iOS-, iPadOS-, macOS-, tvOS- und watchOS-Versionen von 2020 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14, T2, M1, S3-S6) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit den iOS-, iPadOS-, macOS-, tvOS- und watchOS-Versionen von 2020 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A13, A14, S6, M1) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3

FIPS 140-2-Zertifizierungen

Die Tabelle unten zeigt die kryptografischen Module, die von der Prüfstelle auf Konformität mit FIPS 140-2 getestet wurden.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 05.02.2021	*Zertifikate:* 3811 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Betriebssystem:* sepOS für macOS 10.15 Catalina *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3523 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Betriebssystem:* sepOS für macOS 10.14 Mojave *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3223 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Betriebssystem:* sepOS für macOS 10.13 High Sierra *Typ:* Hardware *Sicherheitsstufe:* 2

CC-Zertifizierungen (Common Criteria)

Apple setzt sich aktiv für CC-Evaluierungen überall dort ein, wo geeignete Protection Profiles die Sicherheitsfunktionalität der Apple-Technologien sicherstellen.

CC-Zertifizierung (Common Criteria) – Status

Das von der National Information Assurance Partnership (NIAP) verwaltete US-Programm führt eine Liste mit in der Evaluierung befindlichen Produkten (Products in Evaluation). Diese Liste enthält Produkte, die momentan in den USA von einer NIAP-autorisierten CCTL-Prüfstelle (Common Criteria Testing Laboratory) evaluiert werden und für die ein Kick-off-Meeting für die Evaluierung oder Ähnliches durchgeführt wurde, bei dem das CCEVS-Management das Produkt offiziell zur Evaluierung zugelassen hat.

Nachdem Produkte zertifiziert wurden, setzt die NIAP die aktuell gültigen Zertifizierungen auf ihre Product Compliant List. Nach 2 Jahren werden diese Zertifizierungen auf Konformität mit der aktuellen Richtlinie zur Aufrechterhaltung der Vertrauenswürdigkeit (Assurance Maintenance Policy) geprüft. Nach Ablauf des für die Aufrechterhaltung der Vertrauenswürdigkeit angegebenen Datums bewegt die NIAP den Eintrag für die Zertifizierung in die Archived Products List.

Im Common Criteria Portal sind Zertifizierungen aufgeführt, die im Rahmen des Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können. Das CC-Portal kann Produkte fünf Jahre lang in der Liste der zertifizierten Produkte führen. Für archivierte Zertifizierungen speichert das CC-Portal entsprechende Einträge.

Die Tabelle unten zeigt die Zertifizierungen, die momentan von einer Prüfstelle evaluiert werden oder als CC-konform zertifiziert wurden.

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssystem: sepOS *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple Secure Enclave [2020] *Protection Profiles (PPs):* CPP_DSC_V1.0 *Hardware:* Secure Enclave für (A9-A14, M1, T2, S3-S6) *Software:* sepOS, vertrieben mit iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7

Zusätzliche Zertifizierungen

Die Tabelle unten zeigt die Zertifizierungen für die Secure Enclave, die weder Common Criteria noch FIPS 140-3 verwenden.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* 07.12.2019 bis 26.12.2022	*Zertifikate:* CFNR201902910002 (P.R. China: Technology Certification of Mobile Financial Service) Chinesische Version Englische Version	*Titel:* Mobile Terminal Trusted Execution Environment *Betriebssystem:* iOS 13.5.1 *Spezifizierung:* JR/T 0156-2017

Sicherheitszertifizierungen für den Apple T2-Sicherheits-Chip

Validierung von kryptografischen Modulen – Hintergrundinformationen

Apple beteiligt sich aktiv an der Validierung der integrierten Software- und Hardwaremodule für jede Hauptversion des Betriebssystems. Die Validierung der Konformität kann nur mit einer endgültigen Modulversion stattfinden.

Im Jahr 2020 übernahm das CMVP den internationalen Standard ISO/IEC 19790 als Basis für den US-Standard Federal Information Processing Standard (FIPS) 140-3.

Neben einer Intel-CPU verfügen die meisten Mac-Computer seit 2017 über einen separaten Apple T2-Sicherheits-Chip, bei dem es sich um ein auf Apple Chips basierendes SoC-Modul (System-on-Chip) handelt. Diese Mac-Computer mit T2-Chip nutzen alle fünf kryptografischen Module für verschiedene auf den Geräten verfügbare Dienste.

- Corecrypto User Module for Intel (wird von macOS auf Intel-basierten Mac-Computern verwendet)
- Corecrypto Kernel Module for Intel (wird von macOS auf Intel-basierten Mac-Computern verwendet)
- Corecrypto User Module for ARM (wird vom T2-Chip verwendet)
- Corecrypto Kernel Module for ARM (wird vom T2-Chip verwendet)
- Secure Key Store Cryptographic Module (wird vom integrierten Secure Enclave-Coprozessor im T2-Chip verwendet)

Hinweis: Die auf Apple Chips basierenden Module, die auf dem T2-Chip ausgeführt werden, sind identisch mit den Modulen, die auf anderen Apple Chips ausgeführt werden wie Apple A Series, S Series und M Series.

Validierung von kryptografischen Modulen – Status

Das Cryptographic Module Validation Program (CMVP) verwaltet den Validierungsstatus kryptografischer Module in Abhängigkeit von ihrem aktuellen Status in drei separaten Listen:

- Damit die Module in der CMVP-Liste Implementation Under Test aufgeführt werden, muss die Prüfstelle von Apple mit dem Testen beauftragt worden sein.
- Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat und sobald die CMVP-Gebühren bezahlt wurden, wird das Modul zur Modules in Process (MIP) List hinzugefügt. Die „MIP List“ verfolgt den Fortschritt der CMVP-Validierung in vier Phasen:
  - *Review Pending:* Das Modul wartet darauf, dass ihm eine CMVP-Ressource zugewiesen wird.
  - *In Review:* CMVP-Ressourcen führen die erforderlichen Validierungsaktivitäten aus.
  - *Coordination:* Die Prüfstelle und das CMVP beschäftigen sich mit den gefundenen Problemen.
  - *Finalization:* Die Aktivitäten und Formalitäten im Zusammenhang mit der Ausstellung des Zertifikats werden ausgeführt.

- Im Anschluss an die Validierung durch das CMVP erhalten die Module ein Konformitätszertifikat und werden zur Liste Validated Cryptographic Modules hinzugefügt. Hierzu gehören:
  - Validierte Module, die als active markiert wurden.
  - Nach 5 Jahren werden die Module als historical markiert.
  - Wenn das Modulzertifikat aus irgendeinem Grund entzogen wurde, wird es als revoked markiert.

FIPS 140-3-Zertifizierungen

Aktueller Status

Module (2020): Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

Module (2021): Benutzerbereich (User Space), Kernelbereich und Secure Key Store werden von der Prüfstelle getestet. Die Module befinden sich in der Implementation Under Test List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* sepOS für macOS 12 Monterey *Umgebung:* Apple Chips, User, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* sepOS für macOS 12 Monterey *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* sepOS für macOS 12 Monterey *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (T2) *Sicherheitsstufe:* 2

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS für macOS 11 Big Sur *Umgebung:* Apple Chips, User, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS für macOS 11 Big Sur *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS für macOS 11 Big Sur auf Intel *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware *Sicherheitsstufe:* 2

FIPS 140-2-Zertifizierungen

Die Tabelle unten zeigt die kryptografischen Module, die von der Prüfstelle auf Konformität mit FIPS 140-2 getestet wurden.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3856 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Betriebssystem:* sepOS für macOS 10.15 Catalina *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3855 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Betriebssystem:* sepOS für macOS 10.15 Catalina *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 05.02.2021	*Zertifikate:* 3811 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Betriebssystem:* sepOS für macOS 10.15 Catalina *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 23.04.2019	*Zertifikate:* 3438 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Betriebssystem:* sepOS für macOS 10.14 Mojave *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 11.04.2019	*Zertifikate:* 3433 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Betriebssystem:* sepOS für macOS 10.14 Mojave *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3523 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Betriebssystem:* sepOS für macOS 10.14 Mojave *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 22.05.2018, 06.07.2018	*Zertifikate:* 3148 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Betriebssystem:* sepOS für macOS 10.13 High Sierra *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 17.05.2018, 03.07.2018	*Zertifikate:* 3147 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Betriebssystem:* sepOS für macOS 10.13 High Sierra *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 10.07.2018	*Zertifikate:* 3223 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Betriebssystem:* sepOS für macOS 10.13 High Sierra *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2016 *Datum der Validierung:* 01.02.2017	*Zertifikate:* 2828 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Betriebssystem:* sepOS für macOS 10.12 Monterey *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2016 *Datum der Validierung:* 01.02.2017	*Zertifikate:* 2827 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Betriebssystem:* sepOS für macOS 10.12 Monterey *Typ:* Software *Sicherheitsstufe:* 1

Sicherheitszertifizierungen für Betriebssysteme

Sicherheitszertifizierungen für Apple-Betriebssysteme – Übersicht

Apple hält Validierungszertifikate zur Konformität (Conformance Validation Certificates) mit dem US-Standard Federal Information Processing Standard (FIPS) 140-2/-3 für sepOS und T-Firmware sowie weitere Zertifizierungen. Als Grundlage verwendet Apple *Zertifizierungsbausteine*, die gegebenenfalls für mehrere Plattformen gelten. Ein Baustein ist die Validierung von corecrypto, das für Implementierungen von kryptografischen Modulen für Software und Hardware in von Apple entwickelten Betriebssystemen verwendet wird. Ein zweiter Baustein ist die Zertifizierung der Secure Enclave, die in viele Apple-Geräte integriert ist. Ein dritter Baustein ist die Zertifizierung des Secure Element (SE), das in Apple-Geräten mit Touch ID und in Geräten mit Face ID vorhanden ist. Diese Zertifizierungsbausteine für die Hardware bilden das Fundament für weitere Plattform-Sicherheitszertifizierungen.

Validierungen von kryptografischen Algorithmen

Die Validierung der korrekten Implementierung zahlreicher kryptografischer Algorithmen und der zugehörigen Sicherheitsfunktionen ist Voraussetzung für die FIPS 140-3-Validierung und unterstützt andere Zertifizierungen. Die Validierung wird vom Cryptographic Algorithm Validation Program (CAVP) des NIST (National Institute of Standards and Technology) verwaltet. Validierungszertifikate für Apple-Implementierungen können über die CAVP-Suchfunktion abgerufen werden.

Validierungen von kryptografischen Modulen: FIPS 140-2/3 (ISO/IEC 19790)

Die kryptografischen Module in den Betriebssystemen von Apple wurden seit 2012 wiederholt nach jeder Hauptversion eines Betriebssystems im Rahmen des Cryptographic Module Validation Program (CMVP) validiert und als mit den U.S. Federal Information Processing Standards (FIPS) 140-2 konform eingestuft. Nach der Veröffentlichung jeder Hauptversion übermittelt Apple alle kryptografischen Module zur vollständigen Validierung an das CMVP. Diese validierten Module ermöglichen kryptografische Operationen für die von Apple bereitgestellten Dienste und stehen Apps von Drittanbietern zur Verfügung.

Bei den softwarebasierten Modulen „Corecrypto Module for Intel“ und „Corecrypto Kernel Module for Intel“ erreicht Apple jedes Jahr die **Sicherheitsstufe 1** (Security Level 1). Bei Apple Chips sind die Module „CoreCrypto Module for ARM“ und „CoreCrypto Kernel Module for ARM“ für iOS, iPadOS, tvOS, watchOS und die Firmware des integrierten Apple T2-Sicherheits-Chips in Mac-Computern anwendbar.

2019 erreichte Apple zum ersten Mal die **Sicherheitsstufe 2** (Security Level 2) des FIPS 140-2-Standards für das integrierte kryptografische Hardwaremodul mit der Bezeichnung „Apple Corecrypto Module: Secure Key Store“, wodurch eine von der US-Regierung bewilligte Nutzung von Schlüsseln erlaubt wurde, die mittels Secure Enclave generiert und verwaltet werden. Apple wird auch künftig alles dafür tun, bei jeder Hauptversion seiner Betriebssysteme Validierungen für die kryptografischen Hardwaremodule zu erhalten.

FIPS 140-3 wurde 2019 vom US-Handelsministerium (U.S. Department of Commerce) zugelassen. Die wichtigste Änderung in dieser Version des Standards ist die Spezifizierung von ISO/IEC-Standards – insbesondere von ISO/IEC 19790:2015 und dem zugehörigen Teststandard ISO/IEC 24759:2017. Für das CMVP wurde ein Übergangsprogramm initiiert und es wurde angekündigt, dass ab 2020 kryptografische Module auf der Basis von FIPS 140-3 validiert werden. Es ist das Ziel von Apple, dass die kryptografischen Module die Anforderungen des Standards FIPS 140-3 zum frühestmöglichen praktikablen Zeitpunkt erfüllen und zu diesem übergehen.

Für kryptografische Module, die derzeit Test- und Validierungsprozesse durchlaufen, führt das CMVP zwei separate Listen, die Informationen zu vorgeschlagenen Validierungen enthalten können. Kryptografische Module, die derzeit durch eine akkreditierte Prüfstelle getestet werden, werden möglicherweise in der Implementation Under Test List aufgeführt. Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat, werden die kryptografischen Module von Apple in der Modules in Process List angezeigt. Die Tests durch die Prüfstelle sind derzeit abgeschlossen und warten auf ihre Validierung durch das CMVP. Da der Evaluierungsprozess unterschiedlich lange dauern kann, empfiehlt es sich, einen Blick auf die beiden oben genannten Listen zu werfen, um zwischen dem Datum der Veröffentlichung der Hauptversion eines Betriebssystems und der Ausstellung des Validierungszertifikats durch das CMVP den aktuellen Status der kryptografischen Module von Apple in Erfahrung zu bringen.

Produktzertifizierungen: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) ist ein Standard, der von vielen Organisationen als Grundlage für die Sicherheitsevaluierungen von IT-Produkten verwendet wird.

Informationen zu Zertifizierungen, die im Rahmen des internationalen Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können, sind im Common Criteria Portal zu finden. Die Common Criteria-Standards können auch jenseits des CCRA von nationalen und privaten Validierungssystemen verwendet werden. In Europa wird die gegenseitige Anerkennung durch die SOG-IS-Vereinbarung sowie durch das CCRA (Common Criteria Recognition Arrangement) geregelt.

Das von der Common Criteria-Community formulierte Ziel ist eine international anerkannte Sammlung von Sicherheitsstandards, die eine eindeutige und verlässliche Evaluierung der Sicherheitsfunktionen von IT-Produkten ermöglichen. Durch die Bereitstellung einer unabhängigen Bewertung der Fähigkeit eines Produkts, Sicherheitsstandards zu erfüllen, gibt die Common Criteria-Zertifizierung Kunden mehr Vertrauen in die Sicherheit von IT-Produkten und ermöglicht so fundiertere Entscheidungen.

Im Rahmen des CCRA sind die Mitgliedsländer übereingekommen, die Zertifizierung für IT-Produkte mit dem gleichen Maß an Vertrauen anzuerkennen. Die vor der Zertifizierung erforderlichen Evaluierungen sind umfangreich und umfassen:

- Protection Profiles (PPs)
- Security Targets (STs)
- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)
- Evaluation Assurance Levels (EALs)

Protection Profiles (PPs) sind Dokumente, die die Sicherheitsanforderungen für eine Klasse von Gerätetypen (wie Mobilität) definieren, und werden verwendet, um die Evaluierungen von IT-Produkten derselben Klasse miteinander vergleichen zu können. Die Zahl der CCRA-Mitglieder sowie die Liste zugelassener PPs wird jedes Jahr weiterwachsen. Diese Vereinbarung erlaubt es einem Produktentwickler, eine einzelne Zertifizierung unter einem beliebigen Autorisierungsprogramm für Zertifikate durchzuführen und sie durch einen beliebigen autorisierten Zertifikataussteller anerkennen zu lassen.

Security Targets (STs) definieren, *was* bei der Zertifizierung eines IT-Produkts evaluiert wird. Die STs werden in spezifischere *Security Functional Requirements (SFRs)* übertragen, die für die eingehendere Evaluierung der STs eingesetzt werden.

Die Common Criteria (CC) umfassen auch *Security Assurance Requirements (SARs)*. Die am häufigsten verwendeten Kriterien sind dabei die *Evaluation Assurance Levels (EALs)*. EALs gruppieren häufige SARs und können in PPs und STs spezifiziert werden, um die Vergleichbarkeit zu ermöglichen.

Viele ältere PPs wurden archiviert und werden durch zielgerichtete PPs ersetzt, die nun entwickelt werden und sich auf spezifische Lösungen und Umgebungen konzentrieren. Im Rahmen einer gemeinsamen Bemühung, die fortlaufende Anerkennung der Zertifizierung durch alle CCRA-Mitglieder sicherzustellen, wurden International Technical Communities (iTCs) zur Entwicklung und Pflege von *Collaborative Protection Profiles (cPPs)* eingerichtet, die von Anfang an unter Einbeziehung von CCRA-Zertifizierungsprogrammen entwickelt werden. PPs für andere Benutzergruppen und andere MRAs (Mutual Recognition Agreements) als das CCRA werden weiterhin von den entsprechenden Interessenvertretern entwickelt.

Mit ausgewählten cPPs führt Apple seit Anfang 2015 Zertifizierungen im Rahmen des aktualisierten CCRA durch. Seit dieser Zeit hat Apple Zertifizierungen gemäß Common Criteria für jede iOS-Hauptversion erhalten und den Geltungsbereich auf Sicherheitsstandards ausgeweitet, die von neuen PPs bereitgestellt werden.

Apple übernimmt eine aktive Rolle innerhalb der technischen Communitys, deren Fokus auf der Evaluierung von Sicherheitstechnologien für Mobilgeräte liegt. Hierzu gehören auch die für die Entwicklung und Aktualisierung von cPPs verantwortlichen iTCs. Apple wird auch künftig Zertifizierungen auf Basis von PPs und cPPs evaluieren und durchführen.

Zertifizierungen für Plattformen von Apple für den nordamerikanischen Markt werden allgemein über die National Information Assurance Partnership (NIAP) durchgeführt, die eine Liste von in der Evaluierung befindlichen Projekten (Products in Evaluation) führt, die jedoch noch nicht zertifiziert sind.

Zusätzlich zu den aufgeführten allgemeinen Plattform-Zertifikaten wurden weitere Zertifikate ausgestellt, um spezifische Sicherheitsanforderungen in bestimmten Märkten aufzuzeigen.

Sicherheitszertifizierungen für iOS

Hintergrundinformationen zu iOS-Zertifizierungen

Apple beteiligt sich aktiv an der Validierung der integrierten Software- und Hardwaremodule für jede Hauptversion des Betriebssystems. Die Validierung der Konformität kann nur mit einer endgültig freigegebenen Version stattfinden.

Validierung von kryptografischen Modulen für iOS – Status

Das Cryptographic Module Validation Program (CMVP) verwaltet den Validierungsstatus kryptografischer Module in Abhängigkeit von ihrem aktuellen Status in drei separaten Listen:

- Damit die Module in der CMVP-Liste Implementation Under Test aufgeführt werden, muss die Prüfstelle von Apple mit dem Testen beauftragt worden sein.
- Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat und sobald die CMVP-Gebühren bezahlt wurden, wird das Modul zur Modules in Process (MIP) List hinzugefügt. Die „MIP List“ verfolgt den Fortschritt der CMVP-Validierung in vier Phasen:
  - *Review Pending:* Das Modul wartet darauf, dass ihm eine CMVP-Ressource zugewiesen wird.
  - *In Review:* CMVP-Ressourcen führen die erforderlichen Validierungsaktivitäten aus.
  - *Coordination:* Die Prüfstelle und das CMVP beschäftigen sich mit den gefundenen Problemen.
  - *Finalization:* Die Aktivitäten und Formalitäten im Zusammenhang mit der Ausstellung des Zertifikats werden ausgeführt.
- Im Anschluss an die Validierung durch das CMVP erhalten die Module ein Konformitätszertifikat und werden zur Liste Validated Cryptographic Modules hinzugefügt. Hierzu gehören:
  - Validierte Module, die als active markiert wurden.
  - Nach 5 Jahren werden die Module als historical markiert.
  - Wenn das Modulzertifikat aus irgendeinem Grund entzogen wurde, wird es als revoked markiert.

Im Jahr 2020 übernahm das CMVP den internationalen Standard ISO/IEC 19790 als Basis für FIPS 140-3.

FIPS 140-3-Zertifizierungen

Aktueller Status

iOS 14 (2020): Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

iOS 15 (2021): Benutzerbereich (User Space), Kernelbereich und Secure Key Store werden von der Prüfstelle getestet. Die Module befinden sich in der Implementation Under Test List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* iOS 15 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* iOS 15 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit iOS 15 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit iOS 15 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A13, A14, A15) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* iOS 14 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* iOS 14 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit iOS 14 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit iOS 14 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A13-A14) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3

FIPS 140-2-Zertifizierungen

Die Tabelle unten zeigt die kryptografischen Module, die momentan von der Prüfstelle auf Konformität mit FIPS 140-2 getestet werden oder bereits getestet wurden.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3856 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Betriebssystem:* iOS 13 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3855 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Betriebssystem:* iOS 13 *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 05.02.2021	*Zertifikate:* 3811 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Betriebssystem:* sepOS, vertrieben mit iOS 13 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 23.04.2019	*Zertifikate:* 3438 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Betriebssystem:* iOS 12 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 11.04.2019	*Zertifikate:* 3433 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Betriebssystem:* iOS 12 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3523 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Betriebssystem:* sepOS, vertrieben mit iOS 12 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 22.05.2018, 06.07.2018	*Zertifikate:* 3148 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Betriebssystem:* iOS 11 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 17.05.2018, 03.07.2018	*Zertifikate:* 3147 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Betriebssystem:* iOS 11 *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3223 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Betriebssystem:* sepOS, vertrieben mit iOS 11 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2016 *Datum der Validierung:* 01.02.2017	*Zertifikate:* 2828 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Betriebssystem:* iOS 10 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2016 *Datum der Validierung:* 01.02.2017	*Zertifikate:* 2827 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Betriebssystem:* iOS 10 *Typ:* Software *Sicherheitsstufe:* 1

Frühere Versionen

Zertifikate, die älter als fünf Jahre sind, werden vom CMVP mit dem Status historical gelistet. Für die folgenden früheren iOS-Versionen gibt es Validierungen für die kryptografischen Module:

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

CC-Zertifizierung (Common Criteria) – Hintergrundinformationen

Apple beteiligt sich aktiv an der Evaluierung von iOS für jede Hauptversion des Betriebssystems. Die Evaluierung kann nur mit einer endgültigen, veröffentlichten Version des Betriebssystems erfolgen. Bitte beachten: Vor iPadOS 13.1 hieß das Betriebssystem für das iPad iOS.

CC-Zertifizierung (Common Criteria) – Status

Das von der National Information Assurance Partnership (NIAP) verwaltete US-Programm führt eine Liste mit in der Evaluierung befindlichen Produkten (Products in Evaluation). Diese Liste enthält Produkte, die momentan in den USA von einer NIAP-autorisierten CCTL-Prüfstelle (Common Criteria Testing Laboratory) evaluiert werden und für die ein Kick-off-Meeting für die Evaluierung oder Ähnliches durchgeführt wurde, bei dem das CCEVS-Management das Produkt offiziell zur Evaluierung zugelassen hat.

Nachdem Produkte zertifiziert wurden, setzt die NIAP die aktuell gültigen Zertifizierungen auf ihre Product Compliant List. Nach 2 Jahren werden diese Zertifizierungen auf Konformität mit der aktuellen Richtlinie zur Aufrechterhaltung der Vertrauenswürdigkeit (Assurance Maintenance Policy) geprüft. Nach Ablauf des für die Aufrechterhaltung der Vertrauenswürdigkeit angegebenen Datums bewegt die NIAP den Eintrag für die Zertifizierung in die Archived Products List.

Im Common Criteria Portal sind Zertifizierungen aufgeführt, die im Rahmen des Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können. Das CC-Portal kann Produkte fünf Jahre lang in der Liste der zertifizierten Produkte führen. Für archivierte Zertifizierungen speichert das CC-Portal entsprechende Einträge.

Die Tabelle unten zeigt die Zertifizierungen, die momentan von einer Prüfstelle evaluiert werden oder als CC-konform zertifiziert wurden.

Aktueller Status

Tests durch die Prüfstelle zur NIAP-Evaluierung für iOS 15 sind eingeleitet. Aktuelle Informationen sind unter Products in evaluation (NIAP) und Product Compliant List einsehbar.

Betriebssystem / Zertifizierungsdatum	**Programm-ID / Dokumente**	**Titel / Protection Profiles (PPs)**
Betriebssystem: iOS 15 *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* —	*Titel:* Apple iOS 15: iPhones *Protection Profiles (PPs):* Mobile Device Fundamentals (PP-Modules ausstehend)
Betriebssystem: iOS 14 *Zertifizierungsdatum:* 01.09.2021	*Programm-ID:* 11146 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple iOS 14: iPhones *Protection Profiles (PPs):* Mobile Device Fundamentals, VPN Client module, WLAN Clients PP Module, MDM Agent EP
Betriebssystem: iOS 13 *Zertifizierungsdatum:* 06.11.2020	*Programm-ID:* 11036 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple iOS 13 for iPhone *Protection Profiles (PPs):* Mobile Device Fundamentals, VPN Client module, WLAN Clients EP, MDM Agent EP

Archivierte Zertifizierungen gemäß Common Criteria (CC) für iOS

Für die folgenden früheren iOS-Versionen gibt es CC-Validierungen (Common Criteria). Sie wurden gemäß der NIAP-Richtlinie von der NIAP archiviert:

Betriebssystem / Zertifizierungsdatum	**Programm-ID / Dokumente**	**Titel / Protection Profiles (PPs)**
Betriebssystem: iOS 12 *Zertifizierungsdatum:* 14.03.2019	*Programm-ID:* 10937 *Dokumente:* Security Target (Sicherheitsziel) Guidance (Leitfaden)	*Titel:* iPhone with iOS 12 *Protection Profiles (PPs):* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Betriebssystem: iOS 11 *Zertifizierungsdatum:* 17.07.2018	*Programm-ID:* 10851 *Dokumente:* Security Target (Sicherheitsziel) Guidance (Leitfaden)	*Titel:* Apple iOS 11 *Protection Profiles (PPs):* Mobile Device Fundamentals, Wireless LAN client EP, MDM Agent EP
Betriebssystem: iOS 10 *Zertifizierungsdatum:* 27.07.2017	*Programm-ID:* 10782 *Dokumente:* Security Target, Guidance (Leitfaden)	*Titel:* iOS 10.2 on iPhone and iPad Devices *Protection Profiles (PPs):* Mobile Device Fundamentals, Wireless LAN client EP, MDM Agent EP
Betriebssystem: iOS 10 *Zertifizierungsdatum:* 27.07.2017	*Programm-ID:* 10792 *Dokumente:* Security Target, Guidance (Leitfaden)	*Titel:* iOS 10.2 VPN Client on iPhone and iPad *Protection Profiles (PPs):* VPN Client PP
Betriebssystem: iOS 9 *Zertifizierungsdatum:* 14.10.2016	*Programm-ID:* 10725 *Dokumente:* Security Target, Guidance (Leitfaden)	*Titel:* iOS 9.3.2 with MDM Agent *Protection Profiles (PPs):* Mobile Device Fundamentals, MDM Agent EP
Betriebssystem: iOS 9 *Zertifizierungsdatum:* 13.10.2016	*Programm-ID:* 10714 *Dokumente:* Security Target, Guidance (Leitfaden)	*Titel:* OS VPN Client on iPhone and iPad *Protection Profiles (PPs):* VPN Client PP
Betriebssystem: iOS 9 *Zertifizierungsdatum:* 28.01.2016	*Programm-ID:* 10695 *Dokumente:* Security Target, Guidance (Leitfaden)	*Titel:* iOS 9 *Protection Profiles (PPs):* Mobile Device Fundamentals

Sicherheitszertifizierungen für iPadOS

Hintergrundinformationen zu iPadOS-Zertifizierungen

Apple beteiligt sich unter Nutzung geeigneter Collaborative Protection Profiles und Sicherheitsstufen gemäß FIPS 140-3 aktiv an der Evaluierung von Apple-Betriebssystemen für jede Hauptversion des Betriebssystems. Die Validierung der Konformität kann nur mit einer endgültig freigegebenen Version stattfinden.

Hinweis: Im Jahr 2019 wurde das Betriebssystem für iPad-Geräte in iPadOS umbenannt. Bitte beachten: Vor iPadOS 13.1 hieß das Betriebssystem für das iPad iOS.

Validierung von kryptografischen Modulen für iPadOS – Status

Das Cryptographic Module Validation Program (CMVP) verwaltet den Validierungsstatus kryptografischer Module in Abhängigkeit von ihrem aktuellen Status in drei separaten Listen:

- Damit die Module in der CMVP-Liste Implementation Under Test aufgeführt werden, muss die Prüfstelle von Apple mit dem Testen beauftragt worden sein.
- Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat und sobald die CMVP-Gebühren bezahlt wurden, wird das Modul zur Modules in Process (MIP) List hinzugefügt. Die „MIP List“ verfolgt den Fortschritt der CMVP-Validierung in vier Phasen:
  - *Review Pending:* Das Modul wartet darauf, dass ihm eine CMVP-Ressource zugewiesen wird.
  - *In Review:* CMVP-Ressourcen führen die erforderlichen Validierungsaktivitäten aus.
  - *Coordination:* Die Prüfstelle und das CMVP beschäftigen sich mit den gefundenen Problemen.
  - *Finalization:* Die Aktivitäten und Formalitäten im Zusammenhang mit der Ausstellung des Zertifikats werden ausgeführt.
- Im Anschluss an die Validierung durch das CMVP erhalten die Module ein Konformitätszertifikat und werden zur Liste Validated Cryptographic Modules hinzugefügt. Hierzu gehören:
  - Validierte Module, die als active markiert wurden.
  - Nach 5 Jahren werden die Module als historical markiert.
  - Wenn das Modulzertifikat aus irgendeinem Grund entzogen wurde, wird es als revoked markiert.

Im Jahr 2020 übernahm das CMVP den internationalen Standard ISO/IEC 19790 als Basis für FIPS 140-3.

FIPS 140-3-Zertifizierungen

Aktueller Status

iPadOS 14 (2020): Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

iPadOS 15 (2021): Benutzerbereich (User Space), Kernelbereich und Secure Key Store werden von der Prüfstelle getestet. Die Module befinden sich in der Implementation Under Test List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* iPadOS 15 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* iPadOS 15 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit iPadOS 15 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14, M1) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit iPadOS 15 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14, M1) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* iPadOS 14 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* iPadOS 14 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit iPadOS 14 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14, M1) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit iPadOS 14 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A9-A14, M1) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3

FIPS 140-2-Zertifizierungen

Die Tabelle unten zeigt die kryptografischen Module, die momentan von der Prüfstelle auf Konformität mit FIPS 140-2 getestet werden oder bereits getestet wurden.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3856 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Betriebssystem:* iPadOS 13 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3855 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Betriebssystem:* iPadOS 13 *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 05.02.2021	*Zertifikate:* 3811 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Secure Key Store Cryptographic Module v10.0 *Betriebssystem:* sepOS, vertrieben mit iPadOS 13 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 23.04.2019	*Zertifikate:* 3438 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Betriebssystem:* iOS 12 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 11.04.2019	*Zertifikate:* 3433 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Betriebssystem:* iOS 12 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3523 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Betriebssystem:* sepOS, vertrieben mit iOS 12 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 22.05.2018, 06.07.2018	*Zertifikate:* 3148 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Betriebssystem:* iOS 11 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 17.05.2018, 03.07.2018	*Zertifikate:* 3147 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Betriebssystem:* iOS 11 *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3223 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Betriebssystem:* sepOS, vertrieben mit iOS 11 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2016 *Datum der Validierung:* 01.02.2017	*Zertifikate:* 2828 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Betriebssystem:* iOS 10 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2016 *Datum der Validierung:* 01.02.2017	*Zertifikate:* 2827 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple iOS Corecrypto Kernel Module v7.0 *Betriebssystem:* iOS 10 *Typ:* Software *Sicherheitsstufe:* 1

Frühere Versionen

Zertifikate, die älter als fünf Jahre sind, werden vom CMVP mit dem Status historical gelistet. Für die folgenden früheren iOS-Versionen gibt es Validierungen für die kryptografischen Module:

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

CC-Zertifizierung (Common Criteria) – Hintergrundinformationen

Apple beteiligt sich aktiv an der Evaluierung von iPadOS für jede Hauptversion des Betriebssystems. Die Evaluierung kann nur mit einer endgültigen, veröffentlichten Version des Betriebssystems erfolgen.

CC-Zertifizierung (Common Criteria) – Status

Das von der National Information Assurance Partnership (NIAP) verwaltete US-Programm führt eine Liste mit in der Evaluierung befindlichen Produkten (Products in Evaluation). Diese Liste enthält Produkte, die momentan in den USA von einer NIAP-autorisierten CCTL-Prüfstelle (Common Criteria Testing Laboratory) evaluiert werden und für die ein Kick-off-Meeting für die Evaluierung oder Ähnliches durchgeführt wurde, bei dem das CCEVS-Management das Produkt offiziell zur Evaluierung zugelassen hat.

Nachdem Produkte zertifiziert wurden, setzt die NIAP die aktuell gültigen Zertifizierungen auf ihre Product Compliant List. Nach 2 Jahren werden diese Zertifizierungen auf Konformität mit der aktuellen Richtlinie zur Aufrechterhaltung der Vertrauenswürdigkeit (Assurance Maintenance Policy) geprüft. Nach Ablauf des für die Aufrechterhaltung der Vertrauenswürdigkeit angegebenen Datums bewegt die NIAP den Eintrag für die Zertifizierung in die Archived Products List.

Im Common Criteria Portal sind Zertifizierungen aufgeführt, die im Rahmen des Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können. Das CC-Portal kann Produkte fünf Jahre lang in der Liste der zertifizierten Produkte führen. Für archivierte Zertifizierungen speichert das CC-Portal entsprechende Einträge.

Die Tabelle unten zeigt die Zertifizierungen, die momentan von einer Prüfstelle evaluiert werden oder als CC-konform zertifiziert wurden.

Aktueller Status

Tests durch die Prüfstelle zur NIAP-Evaluierung für iPadOS 15 sind eingeleitet. Aktuelle Informationen sind unter Products in evaluation (NIAP) und Product Compliant List einsehbar.

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssystem: iPadOS 15 *Zertifizierungsdatum:* 14.03.2019	*Programm-ID:* — *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* iPad with iOS 12 *Protection Profiles (PPs):* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssystem: iPadOS 14 *Zertifizierungsdatum:* 01.09.2021	*Programm-ID:* 11147 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple iPadOS 14: iPads *Protection Profiles (PPs):* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Betriebssystem: iPadOS 13 *Zertifizierungsdatum:* 06.11.2020	*Programm-ID:* 11036 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* iPadOS 13 on iPad Mobile Devices *Protection Profiles (PPs):* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP

Frühere Versionen

Für die folgenden früheren iOS-Versionen gibt es CC-Validierungen (Common Criteria). Sie wurden gemäß der NIAP-Richtlinie von der NIAP archiviert:

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

Sicherheitszertifizierungen für macOS

Hintergrundinformationen zu macOS-Zertifizierungen

Apple beteiligt sich unter Nutzung geeigneter Collaborative Protection Profiles und Sicherheitsstufen gemäß FIPS 140-3 aktiv an der Evaluierung von Apple-Betriebssystemen für jede Hauptversion des Betriebssystems. Die Validierung der Konformität kann nur mit einer endgültig freigegebenen Version stattfinden.

Validierung von kryptografischen Modulen für macOS – Status

Das Cryptographic Module Validation Program (CMVP) verwaltet den Validierungsstatus kryptografischer Module in Abhängigkeit von ihrem aktuellen Status in drei separaten Listen:

- Damit die Module in der CMVP-Liste Implementation Under Test aufgeführt werden, muss die Prüfstelle von Apple mit dem Testen beauftragt worden sein.
- Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat und sobald die CMVP-Gebühren bezahlt wurden, wird das Modul zur Modules in Process (MIP) List hinzugefügt. Die „MIP List“ verfolgt den Fortschritt der CMVP-Validierung in vier Phasen:
  - *Review Pending:* Das Modul wartet darauf, dass ihm eine CMVP-Ressource zugewiesen wird.
  - *In Review:* CMVP-Ressourcen führen die erforderlichen Validierungsaktivitäten aus.
  - *Coordination:* Die Prüfstelle und das CMVP beschäftigen sich mit den gefundenen Problemen.
  - *Finalization:* Die Aktivitäten und Formalitäten im Zusammenhang mit der Ausstellung des Zertifikats werden ausgeführt.
- Im Anschluss an die Validierung durch das CMVP erhalten die Module ein Konformitätszertifikat und werden zur Liste Validated Cryptographic Modules hinzugefügt. Hierzu gehören:
  - Validierte Module, die als active markiert wurden.
  - Nach 5 Jahren werden die Module als historical markiert.
  - Wenn das Modulzertifikat aus irgendeinem Grund entzogen wurde, wird es als revoked markiert.

Im Jahr 2020 übernahm das CMVP den internationalen Standard ISO/IEC 19790 als Basis für FIPS 140-3.

Für Mac-Computer von Apple zeigt die Tabelle unten, welche kryptografischen Module für welche Mac-Technologien zutreffen.

Kryptografisches Modul	Mac-Computer mit Apple Chips	Mac-Computer mit Apple T2-Sicherheits-Chip	Intel-basierte Mac-Computer ohne Apple T2-Sicherheits-Chip
Apple Chips-Benutzerbereich (User Space)	✓		
Apple Chips-Kernel	✓		
Intel-Benutzerbereich (User Space)		✓	✓
Intel-Kernel		✓	✓
Secure Key Store	✓	✓	

FIPS 140-3-Zertifizierungen

Im Jahr 2020 brachte Apple Mac-Computer mit Apple Chips auf den Markt. In der Spalte „Modulinfo“ der Tabelle unten ist angegeben, ob die kryptografischen Module für Mac-Computer mit Apple Chips oder für Intel-basierte Mac-Computer gelten.

Hinweis: Viele Intel-basierte Mac-Computer verfügen über Apple T2-Sicherheits-Chips. Weitere Informationen zu Zertifizierungen für den T2-Chip findest du unter Sicherheitszertifizierungen für den Apple T2-Sicherheits-Chip.

macOS ssh-Client

OpenSSH kann für die Nutzung von FIPS 140-3-validierten Modulen für ausgewählte FIPS 140-3-Algorithmen konfiguriert werden. Organisationen können ein signiertes und beglaubigtes Installationsprogramm ausführen, das bei Apple mit dem Passwort *FIPS140Mode* erhältlich ist. Das Installationsprogramm legt zwei Dateien auf dem Mac ab:

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

macOS verwendet dann diese Dateien, um die für OpenSSH verfügbaren Chiffren auf ausschließlich diejenigen zu begrenzen, die durch NIST validiert wurden, und stellt sicher, dass der OpenSSH-Client das von der Plattform bereitgestellte, validierte, kryptografische Modul nutzt. Administratoren können auch eigene Dateien erstellen. Weitere Informationen findest du auf der man-Seite „`apple_ssh_and_fips`“ in macOS 12.0.1 (oder neuer).

Aktueller Status

macOS 11 Big Sur: Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

macOS 12 Monterey: Benutzerbereich (User Space), Kernelbereich und Secure Key Store werden von der Prüfstelle getestet. Die Module befinden sich in der Implementation Under Test List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* macOS 12 Monterey für Apple Chips *Umgebung:* Apple Chips, User, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* macOS 12 Monterey für Apple Chips *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* macOS 12 Monterey für Intel *Umgebung:* Intel, Benutzer, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* macOS 12 Monterey für Intel *Umgebung:* Intel, Kernel, Software *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* sepOS, vertrieben mit macOS 12 Monterey für Apple Chips, sepOS, vertrieben mit macOS 12 Monterey für Intel mit T2 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (M1 und T2) *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12.0 *Betriebssystem:* sepOS, vertrieben mit macOS 12 Monterey für Apple Chips *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (M1) *Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* macOS 11 Big Sur für Intel *Umgebung:* Intel, Benutzer, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* macOS 11 Big Sur für Intel *Umgebung:* Intel, Kernel, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* macOS 11 Big Sur für Apple Chips *Umgebung:* Apple Chips, User, Software *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* macOS 11 Big Sur für Apple Chips *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit macOS 11 Big Sur für Apple Chips, sepOS, vertrieben mit macOS 11 Big Sur für Intel *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (M1) *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit macOS 11 Big Sur für Apple Chips *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (M1) *Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3

FIPS 140-2-Zertifizierungen

Die Tabelle unten zeigt die kryptografischen Module, die momentan von der Prüfstelle auf Konformität mit FIPS 140-2 getestet werden oder bereits getestet wurden.

macOS 10.15 Catalina: Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

Hinweis: Viele Intel-basierte Mac-Computer verfügen über Apple T2-Sicherheits-Chips. Weitere Informationen zu Zertifizierungen für den T2-Chip findest du unter Sicherheitszertifizierungen für den Apple T2-Sicherheits-Chip.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 24.03.2021	*Zertifikate:* 3859 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Space Module for Intel (ccv10) *Betriebssystem:* macOS 10.15 Catalina *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 24.03.2021	*Zertifikate:* 3858 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v10.0 for Intel (ccv10) *Betriebssystem:* macOS 10.15 Catalina *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 12.04.2019	*Zertifikate:* 3402 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v9.0 for Intel *Betriebssystem:* macOS 10.14 Mojave *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 12.04.2019	*Zertifikate:* 3431 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v9.0 for Intel *Betriebssystem:* macOS 10.14 Mojave *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 22.03.2018	*Zertifikate:* 3155 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v8.0 for Intel *Betriebssystem:* macOS 10.13 High Sierra *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 22.03.2018	*Zertifikate:* 3156 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v8.0 for Intel *Betriebssystem:* macOS 10.13 High Sierra *Typ:* Software *Sicherheitsstufe:* 1

Frühere Versionen

Für die folgenden OS X- und macOS-Versionen gibt es Validierungen für die kryptografischen Module. Alle, die älter als fünf Jahre sind, werden vom CMVP mit dem Status Historical gelistet:

- 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

CC-Zertifizierung (Common Criteria) – Hintergrundinformationen

Apple beteiligt sich aktiv an der Evaluierung von macOS für jede Hauptversion des Betriebssystems. Die Evaluierung kann nur mit einer endgültigen, veröffentlichten Version des Betriebssystems erfolgen.

CC-Zertifizierung (Common Criteria) – Status

Das von der National Information Assurance Partnership (NIAP) verwaltete US-Programm führt eine Liste mit in der Evaluierung befindlichen Produkten (Products in Evaluation). Diese Liste enthält Produkte, die momentan in den USA von einer NIAP-autorisierten CCTL-Prüfstelle (Common Criteria Testing Laboratory) evaluiert werden und für die ein Kick-off-Meeting für die Evaluierung oder Ähnliches durchgeführt wurde, bei dem das CCEVS-Management das Produkt offiziell zur Evaluierung zugelassen hat.

Nachdem Produkte zertifiziert wurden, setzt die NIAP die aktuell gültigen Zertifizierungen auf ihre Product Compliant List. Nach 2 Jahren werden diese Zertifizierungen auf Konformität mit der aktuellen Richtlinie zur Aufrechterhaltung der Vertrauenswürdigkeit (Assurance Maintenance Policy) geprüft. Nach Ablauf des für die Aufrechterhaltung der Vertrauenswürdigkeit angegebenen Datums bewegt die NIAP den Eintrag für die Zertifizierung in die Archived Products List.

Im Common Criteria Portal sind Zertifizierungen aufgeführt, die im Rahmen des Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können. Das CC-Portal kann Produkte fünf Jahre lang in der Liste der zertifizierten Produkte führen. Für archivierte Zertifizierungen speichert das CC-Portal entsprechende Einträge.

Die Tabelle unten zeigt die Zertifizierungen, die momentan von einer Prüfstelle evaluiert werden oder als CC-konform zertifiziert wurden.

Aktueller Status

NIAP-Evaluierungen für macOS 11 und macOS 12, die die Protection Profiles „General Purpose Operating System“ und „Full Disk Encryption (FDE)“ (AA und EE) nutzen, sind eingeleitet.

Aktuelle Informationen sind unter Products in evaluation (NIAP) und Product Compliant List einsehbar.

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssystem: macOS 12 Monterey *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* —	*Titel:* Apple FileVault 2 with macOS 12 Monterey *Protection Profiles (PPs):* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PPs ausstehend)
Betriebssystem: macOS 12 Monterey *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* —	*Titel:* macOS 12 Monterey *Protection Profiles (PPs):* PP_OS_V4.21 (PPs PPs ausstehend)

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssystem: macOS 11 Big Sur *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple FileVault 2 with macOS 11 Big Sur *Protection Profiles (PPs):* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Betriebssystem: macOS 11 Big Sur *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple macOS 11 Big Sur *Protection Profiles (PPs):* PP_OS_V4.21
Betriebssystem: macOS 10.15 Catalina *Zertifizierungsdatum:* 29.04.2021	*Programm-ID:* 11078 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple FileVault 2 on T2 computers running macOS 10.15 Catalina *Protection Profiles (PPs):* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Betriebssystem: macOS 10.15 Catalina *Zertifizierungsdatum:* 23.09.2020	*Programm-ID:* 11077 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* macOS 10.15 Catalina *Protection Profiles (PPs):* PP_OS_V4.21

Sicherheitszertifizierungen für tvOS

Hintergrundinformationen zu tvOS-Zertifizierungen

Apple beteiligt sich bei jeder Hauptversion von tvOS aktiv an der Validierung der zugehörigen kryptografischen Module. Die Validierung der Konformität kann nur mit einer endgültig freigegebenen Version stattfinden.

Validierung von kryptografischen Modulen für tvOS – Status

Das Cryptographic Module Validation Program (CMVP) verwaltet den Validierungsstatus kryptografischer Module in Abhängigkeit von ihrem aktuellen Status in drei separaten Listen:

- Damit die Module in der CMVP-Liste Implementation Under Test aufgeführt werden, muss die Prüfstelle von Apple mit dem Testen beauftragt worden sein.
- Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat und sobald die CMVP-Gebühren bezahlt wurden, wird das Modul zur Modules in Process (MIP) List hinzugefügt. Die „MIP List“ verfolgt den Fortschritt der CMVP-Validierung in vier Phasen:
  - *Review Pending:* Das Modul wartet darauf, dass ihm eine CMVP-Ressource zugewiesen wird.
  - *In Review:* CMVP-Ressourcen führen die erforderlichen Validierungsaktivitäten aus.
  - *Coordination:* Die Prüfstelle und das CMVP beschäftigen sich mit den gefundenen Problemen.
  - *Finalization:* Die Aktivitäten und Formalitäten im Zusammenhang mit der Ausstellung des Zertifikats werden ausgeführt.
- Im Anschluss an die Validierung durch das CMVP erhalten die Module ein Konformitätszertifikat und werden zur Liste Validated Cryptographic Modules hinzugefügt. Hierzu gehören:
  - Validierte Module, die als active markiert wurden.
  - Nach 5 Jahren werden die Module als historical markiert.
  - Wenn das Modulzertifikat aus irgendeinem Grund entzogen wurde, wird es als revoked markiert.

Im Jahr 2020 übernahm das CMVP den internationalen Standard ISO/IEC 19790 als Basis für FIPS 140-3.

FIPS 140-3-Zertifizierungen

Aktueller Status

tvOS 14 (2020): Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

tvOS 15 (2021): Benutzerbereich (User Space), Kernelbereich und Secure Key Store werden von der Prüfstelle getestet. Die Module befinden sich in der Implementation Under Test List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* tvOS 15 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* tvOS 15 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit tvOS 15 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A10, A12) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* tvOS 14 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* tvOS 14 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit tvOS 14 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (A10, A12) *Generelle Sicherheitsstufe:* 2

FIPS 140-2-Zertifizierungen

Die Tabelle unten zeigt die kryptografischen Module, die momentan von der Prüfstelle auf Konformität mit FIPS 140-2 getestet werden oder bereits getestet wurden.

tvOS 13 (2019): Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3856 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Betriebssystem:* tvOS 13 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 23.03.2021	*Zertifikate:* 3855 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Betriebssystem:* tvOS 13 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 05.02.2021	*Zertifikate:* 3811 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Betriebssystem:* sepOS, vertrieben mit tvOS 13 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 23.04.2019	*Zertifikate:* 3438 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Betriebssystem:* tvOS 12 *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 11.04.2019	*Zertifikate:* 3433 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Betriebssystem:* tvOS 12 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3523 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Betriebssystem:* sepOS, vertrieben mit tvOS 12 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 22.05.2018, 06.07.2018	*Zertifikate:* 3148 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Betriebssystem:* tvOS 11 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 17.05.2018, 03.07.2018	*Zertifikate:* 3147 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Betriebssystem:* tvOS 11 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3223 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Betriebssystem:* sepOS, vertrieben mit tvOS 11 *Typ:* Hardware *Sicherheitsstufe:* 2

Sicherheitszertifizierungen für watchOS

Hintergrundinformationen zu watchOS-Zertifizierungen

Apple beteiligt sich bei jeder Hauptversion von watchOS aktiv an der Validierung der zugehörigen kryptografischen Module. Die Validierung der Konformität kann nur mit einer endgültig freigegebenen Version stattfinden.

Validierung von kryptografischen Modulen für watchOS – Status

Das Cryptographic Module Validation Program (CMVP) verwaltet den Validierungsstatus kryptografischer Module in Abhängigkeit von ihrem aktuellen Status in drei separaten Listen:

- Damit die Module in der CMVP-Liste Implementation Under Test aufgeführt werden, muss die Prüfstelle von Apple mit dem Testen beauftragt worden sein.
- Nachdem die Prüfstelle die Tests abgeschlossen und die Validierung durch das CMVP empfohlen hat und sobald die CMVP-Gebühren bezahlt wurden, wird das Modul zur Modules in Process (MIP) List hinzugefügt. Die „MIP List“ verfolgt den Fortschritt der CMVP-Validierung in vier Phasen:
  - *Review Pending:* Das Modul wartet darauf, dass ihm eine CMVP-Ressource zugewiesen wird.
  - *In Review:* CMVP-Ressourcen führen die erforderlichen Validierungsaktivitäten aus.
  - *Coordination:* Die Prüfstelle und das CMVP beschäftigen sich mit den gefundenen Problemen.
  - *Finalization:* Die Aktivitäten und Formalitäten im Zusammenhang mit der Ausstellung des Zertifikats werden ausgeführt.
- Im Anschluss an die Validierung durch das CMVP erhalten die Module ein Konformitätszertifikat und werden zur Liste Validated Cryptographic Modules hinzugefügt. Hierzu gehören:
  - Validierte Module, die als active markiert wurden.
  - Nach 5 Jahren werden die Module als historical markiert.
  - Wenn das Modulzertifikat aus irgendeinem Grund entzogen wurde, wird es als revoked markiert.

Im Jahr 2020 übernahm das CMVP den internationalen Standard ISO/IEC 19790 als Basis für FIPS 140-3.

FIPS 140-3-Zertifizierungen

Aktueller Status

watchOS 7 (2020): Benutzerbereich (User Space), Kernelbereich und Secure Key Store wurden von der Prüfstelle getestet und erhielten eine Empfehlung für die Validierung durch das CMVP. Die Module befinden sich in der Modules in Process List.

watchOS 8 (2021): Benutzerbereich (User Space), Kernelbereich und Secure Key Store werden von der Prüfstelle getestet. Die Module befinden sich in der Implementation Under Test List.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* watchOS 8 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* watchOS 8 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit watchOS 8 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (S3, S4, S5, S6) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2021 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v12 *Betriebssystem:* sepOS, vertrieben mit watchOS 8 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (S6) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* watchOS 7 *Umgebung:* Apple Chips, User, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* watchOS 7 *Umgebung:* Apple Chips, Kernel, Software *Typ:* Software *Generelle Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit watchOS 7 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (S3, S4, S5, S6) *Generelle Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2020 *Datum der Validierung:* —	*Zertifikate:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Module v11.1 *Betriebssystem:* sepOS, vertrieben mit watchOS 7 *Umgebung:* Apple Chips, Secure Key Store, Hardware *Typ:* Hardware (S6) *Generelle Sicherheitsstufe:* 2 *Physische Sicherheitsstufe:* 3

FIPS 140-2-Zertifizierungen

Die Tabelle unten zeigt die kryptografischen Module, die momentan von der Prüfstelle auf Konformität mit FIPS 140-2 getestet werden oder bereits getestet wurden.

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* —	*Zertifikate:* 3856 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v10.0 for ARM *Betriebssystem:* watchOS 6 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* —	*Zertifikate:* 3855 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v10.0 for ARM *Betriebssystem:* watchOS 6 *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2019 *Datum der Validierung:* 05.02.2021	*Zertifikate:* 3811 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v10.0 *Betriebssystem:* sepOS, vertrieben mit watchOS 6 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 23.04.2019	*Zertifikate:* 3438 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v9.0 for ARM *Betriebssystem:* watchOS 5 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 11.04.2019	*Zertifikate:* 3433 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v9.0 for ARM *Betriebssystem:* watchOS 5 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2018 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3523 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v9.0 *Betriebssystem:* sepOS, vertrieben mit watchOS 5 *Typ:* Hardware *Sicherheitsstufe:* 2
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 22.05.2018, 06.07.2018	*Zertifikate:* 3148 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto User Module v8.0 for ARM *Betriebssystem:* watchOS 4 *Typ:* Software *Sicherheitsstufe:* 1
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 09.03.2018, 17.05.2018, 03.07.2018	*Zertifikate:* 3147 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Corecrypto Kernel Module v8.0 for ARM *Betriebssystem:* watchOS 4 *Typ:* Software *Sicherheitsstufe:* 1

Daten	Zertifikate / Dokumente	Modulinfo
Erscheinungsdatum des Betriebssystems: 2017 *Datum der Validierung:* 10.09.2019	*Zertifikate:* 3223 *Dokumente:* Certificate (Zertifikat) Security Policy (Sicherheitsrichtlinie) Crypto Officer Guidance (Leitfaden für Kryptoverantwortliche)	*Titel:* Apple Secure Key Store Cryptographic Module v1.0 *Betriebssystem:* sepOS, vertrieben mit watchOS 4 *Typ:* Hardware *Sicherheitsstufe:* 2

Sicherheitszertifizierungen für Software

Sicherheitszertifizierungen für Apple-Software – Übersicht

Apple hält Validierungszertifikate zur Konformität (Conformance Validation Certificates) mit dem US-Standard Federal Information Processing Standard (FIPS) 140-2/-3 für sepOS und T-Firmware sowie weitere Zertifizierungen. Als Grundlage verwendet Apple *Zertifizierungsbausteine*, die gegebenenfalls für mehrere Plattformen gelten. Ein Baustein ist die Validierung von corecrypto, das für Implementierungen von kryptografischen Modulen für Software und Hardware in von Apple entwickelten Betriebssystemen verwendet wird. Ein zweiter Baustein ist die Zertifizierung der Secure Enclave, die in viele Apple-Geräte integriert ist. Ein dritter Baustein ist die Zertifizierung des Secure Element (SE), das in Apple-Geräten mit Touch ID und in Geräten mit Face ID vorhanden ist. Diese Zertifizierungsbausteine für die Hardware bilden das Fundament für weitere Plattform-Sicherheitszertifizierungen.

Produktzertifizierungen: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) ist ein Standard, der von vielen Organisationen als Grundlage für die Sicherheitsevaluierungen von IT-Produkten verwendet wird.

Informationen zu Zertifizierungen, die im Rahmen des internationalen Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können, sind im Common Criteria Portal zu finden. Die Common Criteria-Standards können auch jenseits des CCRA von nationalen und privaten Validierungssystemen verwendet werden. In Europa wird die gegenseitige Anerkennung durch die SOG-IS-Vereinbarung sowie durch das CCRA (Common Criteria Recognition Arrangement) geregelt.

Das von der Common Criteria-Community formulierte Ziel ist eine international anerkannte Sammlung von Sicherheitsstandards, die eine eindeutige und verlässliche Evaluierung der Sicherheitsfunktionen von IT-Produkten ermöglichen. Durch die Bereitstellung einer unabhängigen Bewertung der Fähigkeit eines Produkts, Sicherheitsstandards zu erfüllen, gibt die Common Criteria-Zertifizierung Kunden mehr Vertrauen in die Sicherheit von IT-Produkten und ermöglicht so fundiertere Entscheidungen.

Im Rahmen des CCRA sind die Mitgliedsländer übereingekommen, die Zertifizierung für IT-Produkte mit dem gleichen Maß an Vertrauen anzuerkennen. Die vor der Zertifizierung erforderlichen Evaluierungen sind umfangreich und umfassen:

- Protection Profiles (PPs)
- Security Targets (STs)
- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)
- Evaluation Assurance Levels (EALs)

Protection Profiles (PPs) sind Dokumente, die die Sicherheitsanforderungen für eine Klasse von Gerätetypen (wie Mobilität) definieren, und werden verwendet, um die Evaluierungen von IT-Produkten derselben Klasse miteinander vergleichen zu können. Die Zahl der CCRA-Mitglieder sowie die Liste zugelassener PPs wird jedes Jahr weiterwachsen. Diese Vereinbarung erlaubt es einem Produktentwickler, eine einzelne Zertifizierung unter einem beliebigen Autorisierungsprogramm für Zertifikate durchzuführen und sie durch einen beliebigen autorisierten Zertifikataussteller anerkennen zu lassen.

Security Targets (STs) definieren, *was* bei der Zertifizierung eines IT-Produkts evaluiert wird. Die STs werden in spezifischere *Security Functional Requirements (SFRs)* übertragen, die für die eingehendere Evaluierung der STs eingesetzt werden.

Die Common Criteria (CC) umfassen auch *Security Assurance Requirements (SARs)*. Die am häufigsten verwendeten Kriterien sind dabei die *Evaluation Assurance Levels (EALs)*. EALs gruppieren häufige SARs und können in PPs und STs spezifiziert werden, um die Vergleichbarkeit zu ermöglichen.

Viele ältere PPs wurden archiviert und werden durch zielgerichtete PPs ersetzt, die nun entwickelt werden und sich auf spezifische Lösungen und Umgebungen konzentrieren. Im Rahmen einer gemeinsamen Bemühung, die fortlaufende Anerkennung der Zertifizierung durch alle CCRA-Mitglieder sicherzustellen, wurden International Technical Communities (iTCs) zur Entwicklung und Pflege von Collaborative Protection Profiles (cPPs) eingerichtet, die von Anfang an unter Einbeziehung von CCRA-Zertifizierungsprogrammen entwickelt werden. PPs für andere Benutzergruppen und andere MRAs (Mutual Recognition Agreements) als das CCRA werden weiterhin von den entsprechenden Interessenvertretern entwickelt.

Mit ausgewählten cPPs führt Apple seit Anfang 2015 Zertifizierungen im Rahmen des aktualisierten CCRA durch. Seit dieser Zeit hat Apple Zertifizierungen gemäß Common Criteria für jede iOS-Hauptversion erhalten und den Geltungsbereich auf Sicherheitsstandards ausgeweitet, die von neuen PPs bereitgestellt werden.

Apple übernimmt eine aktive Rolle innerhalb der technischen Communitys, deren Fokus auf der Evaluierung von Sicherheitstechnologien für Mobilgeräte liegt. Hierzu gehören auch die für die Entwicklung und Aktualisierung von cPPs verantwortlichen iTCs. Apple wird auch künftig Zertifizierungen auf Basis von PPs und cPPs evaluieren und durchführen.

Zertifizierungen für Plattformen von Apple für den nordamerikanischen Markt werden allgemein über die National Information Assurance Partnership (NIAP) durchgeführt, die eine Liste von in der Evaluierung befindlichen Projekten (Products in Evaluation) führt, die jedoch noch nicht zertifiziert sind.

Zusätzlich zu den aufgeführten allgemeinen Plattform-Zertifikaten wurden weitere Zertifikate ausgestellt, um spezifische Sicherheitsanforderungen in bestimmten Märkten aufzuzeigen.

Sicherheitszertifizierungen für Apple-Apps

Hintergrundinformationen zu Zertifizierungen von Apple-Apps

Apple beteiligt sich unter Nutzung der entsprechenden Common Criteria Protection Profiles (PPs) aktiv an den Sicherheitszertifizierungen für Apple-Apps. Diese Evaluierungen bauen auf den von Apple bereits erlangten Zertifizierungen für Hardware und Betriebssysteme auf.

Mit den Apps „Safari“ und „Kontakte“ initiierte Apple im Jahr 2018 Evaluierungen der Anwendungssicherheit für wichtige Apps, die unter iOS 11 ausgeführt werden. Apple setzte diese Evaluierungen mit Apps fort, die unter iOS 12, iOS 13 und iPadOS 13.1 ausgeführt werden. 2021 werden Apps, die unter macOS 11 laufen, einbezogen.

Zertifizierung von kryptografischen Modulen – Status

Die hier aufgeführten Apple-Apps verwenden kryptografische Module für das jeweilige Betriebssystem. Weitere Informationen findest du unter Sicherheitszertifizierungen für iOS, Sicherheitszertifizierungen für iPadOS und Sicherheitszertifizierungen für macOS.

CC-Zertifizierung (Common Criteria) – Status

Das von der National Information Assurance Partnership (NIAP) verwaltete US-Programm führt eine Liste mit in der Evaluierung befindlichen Produkten (Products in Evaluation). Diese Liste enthält Produkte, die momentan in den USA von einer NIAP-autorisierten CCTL-Prüfstelle (Common Criteria Testing Laboratory) evaluiert werden und für die ein Kick-off-Meeting für die Evaluierung oder Ähnliches durchgeführt wurde, bei dem das CCEVS-Management das Produkt offiziell zur Evaluierung zugelassen hat.

Nachdem Produkte zertifiziert wurden, setzt die NIAP die aktuell gültigen Zertifizierungen auf ihre Product Compliant List. Nach 2 Jahren werden diese Zertifizierungen auf Konformität mit der aktuellen Richtlinie zur Aufrechterhaltung der Vertrauenswürdigkeit (Assurance Maintenance Policy) geprüft. Nach Ablauf des für die Aufrechterhaltung der Vertrauenswürdigkeit angegebenen Datums bewegt die NIAP den Eintrag für die Zertifizierung in die Archived Products List.

Im Common Criteria Portal sind Zertifizierungen aufgeführt, die im Rahmen des Common Criteria Recognition Arrangement (CCRA) gegenseitig anerkannt werden können. Das CC-Portal kann Produkte fünf Jahre lang in der Liste der zertifizierten Produkte führen. Für archivierte Zertifizierungen speichert das CC-Portal entsprechende Einträge.

Die Tabelle unten zeigt die Zertifizierungen, die momentan von einer Prüfstelle evaluiert werden oder als CC-konform zertifiziert wurden.

Aktueller Status

- NIAP-Evaluierungen, die als „bereits begonnen“ veröffentlicht wurden, werden unter Products in Evaluation (NIAP) aufgeführt.
- Abgeschlossene und validierte NIAP-Evaluierungen werden in der Product Compliant List aufgeführt.

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssystem: macOS 11 Big Sur *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* macOS 11 Big Sur: Contacts *Protection Profiles (PPs):* PP for Application SW, EP for Web Browsers
Betriebssystem: macOS 11 Big Sur *Zertifizierungsdatum:* —	*Programm-ID:* Noch nicht zertifiziert *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* macOS 11 Big Sur: Safari *Protection Profiles (PPs):* PP for Application SW, EP for Web Browsers
Betriebssysteme: iOS 14, iPadOS 14 *Zertifizierungsdatum:* 20.08.2021	*Programm-ID:* 11191 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple iOS 14 und iPadOS 14: Contacts *Protection Profiles (PPs):* PP for Application SW, EP for Web Browsers
Betriebssysteme: iOS 14, iPadOS 14 *Zertifizierungsdatum:* —	*Programm-ID:* 11192 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple iOS 14 und iPadOS 14: Safari *Protection Profiles (PPs):* PP for Application SW, EP for Web Browsers

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssysteme: iOS 13, iPadOS 13 *Zertifizierungsdatum:* 05.06.2020	*Programm-ID:* 11060 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple iOS 13 und iPadOS 13: Safari *Protection Profiles (PPs):* PP for Application SW, EP for Web Browsers
Betriebssysteme: iOS 13, iPadOS 13 *Zertifizierungsdatum:* 05.06.2020	*Programm-ID:* 11050 *Dokumente:* Certificate (Zertifikat) Security Target (Sicherheitsziel) Guidance (Leitfaden) Validation Report (Validierungsbericht) Assurance Activity Report (Bericht über Prüfaktivitäten)	*Titel:* Apple iOS 13 und iPadOS 13: Contacts *Protection Profiles (PPs):* PP for Application SW

Archivierte Common Criteria-Zertifizierungen für Apple-Apps

Betriebssystem / Zertifizierungsdatum	Programm-ID / Dokumente	Titel / Protection Profiles (PPs)
Betriebssystem: iOS 12 *Zertifizierungsdatum:* 12.06.2019	*Programm-ID:* 10960 *Dokumente:* Security Target (Sicherheitsziel) Guidance (Leitfaden)	*Titel:* iOS 12 Safari *Protection Profiles (PPs):* PP for Application SW, EP for Web Browsers
Betriebssystem: iOS 12 *Zertifizierungsdatum:* 28.02.2019	*Programm-ID:* 10961 *Dokumente:* Security Target (Sicherheitsziel) Guidance (Leitfaden)	*Titel:* iOS 12 Kontakte *Protection Profiles (PPs):* PP for Application SW
Betriebssystem: iOS 11 *Zertifizierungsdatum:* 09.11.2018	*Programm-ID:* 10916 *Dokumente:* Security Target (Sicherheitsziel) Guidance (Leitfaden)	*Titel:* iOS 11 Safari *Protection Profiles (PPs):* PP for Application SW, EP for Web Browsers
Betriebssystem: iOS 11 *Zertifizierungsdatum:* 13.09.2018	*Programm-ID:* 10915 *Dokumente:* Security Target (Sicherheitsziel) Guidance (Leitfaden)	*Titel:* iOS 11 Kontakte *Protection Profiles (PPs):* PP for Application SW

Sicherheitszertifizierungen für Apple-Internetdienste

Apple hält Zertifizierungen in Übereinstimmung mit den Standards ISO/IEC 27001 und ISO/IEC 27018, um es Apple-Kunden zu ermöglichen, ihre gesetzlichen und vertraglichen Verpflichtungen zu erfüllen. Diese Zertifizierungen bieten unseren Kunden eine unabhängige Bewertung der Informationssicherheits- und Datenschutzverfahren von Apple für Systeme im Anwendungsbereich dieser Zertifizierungen.

ISO/IEC 27001 und ISO/IEC 27018 sind Teil einer Gruppe von ISMS-Standards (Information Security Management System), die von der Internationalen Organisation für Normung (ISO) herausgegeben werden. Im Rahmen des ISMS von Apple, wurden alle Kontrollanforderungen in Anhang A (Annex A) in die Anwendbarkeitserklärung (SoA; Statement of Applicability) aufgenommen, wie dies in den Standards ISO/IEC 27001 und ISO/IEC 27018 definiert ist. Apple unterzieht sich jährlich einem unabhängigen Testat durch eine autorisierte Registerstelle.

ISO/IEC 27001

ISO/IEC 27001 ist ein Standard für das IT-Sicherheitsmanagement (ISMS; Information Security Management System), der die Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und fortlaufende Verbesserung des IT-Sicherheitsmanagements in einer Organisation festlegt. Der Standard ISO/IEC 27001 umfasst die folgenden Sicherheitsbereiche, die von den ISO/IEC-Zertifizierungen von Apple abgedeckt werden:

- Richtlinien für die Informationssicherheit
- Organisation der Informationssicherheit
- Verwaltung der Werte
- Personalsicherheit
- Physische und umweltbezogene Sicherheit
- Sicherheit der Kommunikation und der Betriebsabläufe
- Zugriffssteuerung
- Anschaffung, Entwicklung und Instandhaltung von Informationssystemen
- Handhabung von Sicherheitsvorfällen
- Aufrechterhaltung des Geschäftsbetriebs (Business Continuity)
- Compliance

ISO/IEC 27018

ISO/IEC 27018 ist ein Verhaltenskodex zum Schutz personenbezogener Daten (PII; Personally Identifiable Information) in öffentlichen Cloud-Umgebungen. Der Standard ISO/IEC 27018 umfasst die folgenden Sicherheitsbereiche, die von den ISO/IEC-Zertifizierungen von Apple abgedeckt werden:

- Zustimmung und Wahlmöglichkeit
- Rechtmäßigkeit des Zwecks und Spezifikation
- Einschränkungen für Datensammlung
- Datenminimierung
- Einschränkung der Verwendung, Aufbewahrung und Offenlegung
- Genauigkeit und Qualität
- Offenheit, Transparenz und Informationspflicht
- Individuelle Teilnahme und Zugang
- Rechenschaftspflicht
- Informationssicherheit
- Einhaltung des Datenschutzes

Von ISO/IEC 27001 und ISO/IEC 27018 abgedeckte Apple-Dienste

Die ISO/IEC 27001- und ISO/IEC 27018-Zertifizierungen von Apple decken die folgenden Dienste ab:

- Apple Geschäftschat
- Apple Business Manager
- Apple Push-Benachrichtigungsdienst (APNS)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork-Dienste
- Verwaltete Apple-IDs
- Schoolwork
- Siri

Zertifizierungen

Der Nachweis für die ISO/IEC 27001- und 27018-Zertifizierung von Apple ist bei unserer Registerstelle erhältlich.

Um die Zertifizierungen von Apple anzuzeigen, gehe auf der Website der British Standards Institution (BSI) zur Certificate and Client Directory search, gib „Apple“ im Suchfeld „Company“ ein, klicke auf „Search“ und wähle dann die gewünschten Suchergebnisse zum Anzeigen der Zertifizierungen aus.

Hinweis: Informationen zu nicht von Apple hergestellten Produkten oder nicht von Apple kontrollierten oder geprüften unabhängigen Websites stellen keine Empfehlung oder Billigung dar. Apple übernimmt keine Verantwortung für die Auswahl, Leistung oder Nutzung von Websites und Produkten Dritter. Apple gibt keine Zusicherungen bezüglich der Genauigkeit oder Zuverlässigkeit der Websites Dritter ab. Kontaktiere den jeweiligen Anbieter, um weitere Informationen zu erhalten.

macOS Security Compliance Project

Das macOS Security Compliance Project (mSCP) ist ein Open Source-Projekt, mit dem ein programmatischer Ansatz für die Erstellung von Sicherheitsleitfäden bereitgestellt werden soll. Hierbei handelt es sich um ein Gemeinschaftsprojekt, das sich aus staatlichen IT-Sicherheitskräften des National Institute of Standards and Technology (NIST), der National Aeronautics and Space Administration (NASA), der Defense Information Systems Agency (DISA) und dem Los Alamos National Laboratory (LANL) zusammensetzt. Das Projekt verwendet eine Reihe von getesteten und validierten Steuerungen für macOS und überprüft diese Steuerungen mit allen Sicherheitsleitfaden, die von diesem Projekt unterstützt werden. Darüber hinaus kann dieses Projekt als Ressource für die unkomplizierte Erstellung von angepassten Sicherheitsgrundlagen für technische Sicherheitssteuerungen verwendet werden. Hierfür kommt eine Bibliothek mit getesteten und validierten atomaren Operationen (Konfigurationseinstellungen) zum Einsatz. Das Projekt stellt angepasste Dokumentationen, Skripte, Konfigurationsprofile und Audit-Checklisten auf Basis der verwendeten Grundlagen bereit.

Das mSCP kann Ergebnisse produzieren, die in Verbindung mit Management- und Sicherheitstools verwendet werden können, um Compliance sicherzustellen. Die Konfigurationseinstellungen in diesem Projekt unterstützen die folgenden grundlegenden Richtlinien:

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

Weitere Informationen:

- Eine Übersicht über alle Regeln im Projekt ist hier zu finden.
- Weitere Informationen über das Projekt und die Verwendung sind im Wiki des macOS Security Compliance Project zu finden.
- Weitere Informationen zum Konfigurieren des Projekts für die Verwendung sind hier zu finden: Getting to Know the macOS Security Compliance Project, Part 1 und Getting to Know the macOS Security Compliance Project, Part 2.
- Weitere Informationen zum Unterstützen der Projektentwicklung sind im Leitfaden für Mitwirkende zu finden.

Revisionsverlauf des Dokuments

Datum	Zusammenfassung
Mittwoch, 27. Oktober 2021	Aktualisierte Themen: • Sicherheitszertifizierungen für den Secure Enclave-Prozessor (SEP) • Sicherheitszertifizierungen für iOS • Sicherheitszertifizierungen für macOS
Dienstag, 17. August 2021	Aktualisierte Themen: • Sicherheitszertifizierungen für den Secure Enclave-Prozessor (SEP) • Sicherheitszertifizierungen für den Apple T2-Sicherheits-Chip • Sicherheitszertifizierungen für iOS • Sicherheitszertifizierungen für iPadOS • Sicherheitszertifizierungen für macOS • Sicherheitszertifizierungen für tvOS • Sicherheitszertifizierungen für watchOS • Sicherheitszertifizierungen für Apple-Apps • Sicherheitszertifizierungen • macOS Security Compliance Project

Datum	Zusammenfassung
Montag, 26. April 2021	Hinzugefügte Themen: • macOS Security Compliance Project Aktualisierte Themen: • Sicherheitszertifizierungen für den Apple T2-Sicherheits-Chip: Neue FIPS 140-2-Zertifizierung, 3811 • Sicherheitszertifizierungen für den Secure Enclave-Prozessor (SEP): Neue FIPS 140-2-Zertifizierung, 3811, und neue Tabelle für zusätzliche Zertifizierungen. • Sicherheitszertifizierungen für iOS: Neue FIPS 140-2-Zertifizierung, 3811, Programm-ID 11146 für iOS 14 in Evaluierung • Sicherheitszertifizierungen für iPadOS: Neue FIPS 140-2-Zertifizierung, 3811, Programm-ID 11147 für iPadOS 14 in Evaluierung • Sicherheitszertifizierungen für macOS: Neue FIPS 140-2-Zertifizierung, 3811. • Sicherheitszertifizierungen für tvOS: Neue FIPS 140-2-Zertifizierungen, 3811. • Sicherheitszertifizierungen für watchOS: Neue FIPS 140-2-Zertifizierungen, 3811. • Sicherheitszertifizierungen für Apple-Apps: Aktualisierung des Common Criteria-Status und neue Tabelle für archivierte Common Criteria-Zertifizierungen.

Glossar

Apple Business Manager Ein webbasiertes Portal, das einfach in der Handhabung ist und IT-Administratoren die Möglichkeit bietet, Apple-Geräte, die ihre Organisation direkt bei Apple oder einem teilnehmenden autorisierten Apple-Vertriebspartner oder Anbieter erworben hat, schnell und effizient bereitzustellen. Geräte können automatisch in der organisationseigenen Lösung für die Mobilgeräteverwaltung (Mobile Device Management, MDM) registriert werden, ohne dass sie vor der Übergabe an die Benutzer in die Hand genommen und vorbereitet werden müssen.

Apple Push-Benachrichtigungsdienst (APNS) Ein globaler Dienst von Apple, der Push-Benachrichtigungen an Apple-Geräte sendet.

Apple School Manager Ein webbasiertes Portal, das einfach in der Handhabung ist und IT-Administratoren die Möglichkeit bietet, Apple-Geräte, die ihre Organisation direkt bei Apple oder einem teilnehmenden autorisierten Apple-Vertriebspartner oder Anbieter erworben hat, schnell und effizient bereitzustellen. Geräte können automatisch in der organisationseigenen Lösung für die Mobilgeräteverwaltung (Mobile Device Management, MDM) registriert werden, ohne dass sie vor der Übergabe an die Benutzer in die Hand genommen und vorbereitet werden müssen.

collaborative Protection Profile (cPP) Ein von einer internationalen Technical Community (iTC) entwickeltes Schutzprofil (Protection Profile). iTCs sind Expertengruppen, die mit der Erstellung von cPPs beauftragt werden.

Common Criteria (CC) Ein Standard, der die allgemeinen Konzepte und Grundsätze für die Evaluierung der IT-Sicherheit festlegt und die allgemeinen Evaluierungskriterien vorgibt. Hierzu gehören Kataloge mit Sicherheitsanforderungen in einer standardisierten Sprache.

Common Criteria Recognition Arrangement (CCRA) Ein internationales Abkommen zur gegenseitigen Anerkennung von Schutzprofilen und Zertifikaten, das die Richtlinien und Anforderungen für die internationale Anerkennung von Zertifikaten definiert, die gemäß den Anforderungen des ISO/IEC 15408- oder des Common Criteria-Standards erteilt wurden.

corecrypto Eine Bibliothek, die Implementierungen kryptografischer Primitive (Low-Level) bereitstellt. Dabei ist zu beachten, dass corecrypto keine direkten Programmierschnittstellen für Entwickler bereitstellt und von den Entwicklern über bereitgestellte APIs genutzt wird. Der corecrypto-Quellcode ist öffentlich zugänglich, damit seine Sicherheitsmerkmale und die korrekte Funktionsweise geprüft werden können.

Cryptographic Algorithm Validation Program (CAVP) Eine vom NIST (National Institute of Standards and Technology) betriebene Initiative zur Bereitstellung von Validierungstests für zertifizierte kryptografische Algorithmen (beispielsweise FIPS-Zertifikat und NIST-Empfehlung) und deren individuelle Komponenten.

Cryptographic Module Validation Program (CMVP) Eine von den Regierungen der USA und Kanadas ins Leben gerufene Initiative zur Validierung der Konformität mit dem FIPS 140-3-Standard.

Federal Information Processing Standard (FIPS) Publikationen, die vom National Institute of Standards and Technology (NIST) erstellt werden, weil sie entweder gesetzlich vorgeschrieben sind oder es zwingend erforderliche gesetzliche Anforderungen an die Cybersicherheit gibt (oder in beiden Fällen).

Full Disk Encryption (FDE) Die Verschlüsselung aller Daten auf einem Speichermedium.

Implementation under Test (IUT) Ein kryptografisches Modul, das gerade von einer Prüfstelle getestet wird.

Information Security Management System (ISMS) Eine Reihe von Richtlinien und Verfahren für die Informationssicherheit, die den Anwendungsbereich und auch die Grenzen eines Sicherheitsprogramms regeln, das zum Schutz von Informationen und Systemen eingesetzt wird und die Informationssicherheit systematisch über den gesamten Lebenszyklus der Informationen und/oder Systeme verwaltet.

international Technical Community (iTC) Ein Gremium, das für die Entwicklung von PPs (Protection Profiles) oder cPPs (collaborative Protection Profiles) im Rahmen des CCRA (Common Criteria Recognition Arrangement) verantwortlich ist.

IPsec-VPN-Client Ein Client in einem Protection Profile, der eine sichere IPsec-Verbindung zwischen einer physischen oder virtuellen Host-Plattform und einem anderen Standort bereitstellt.

Kryptografisches Modul Die Hardware, Software und/oder Firmware, die kryptografische Funktionen bereitstellt und die Anforderungen eines festgelegten Standards für kryptografische Module erfüllt.

Mobilgeräteverwaltung (Mobile Device Management, MDM) Ein Dienst, mit dem registrierte Geräte per Fernzugriff (remote) verwaltet werden können. Nach dem Registrieren eines Geräts kann der Benutzer den MDM-Dienst über das Netzwerk verwenden, um ohne Benutzerinteraktion Einstellungen zu konfigurieren und andere Aufgaben auf dem Gerät auszuführen.

Modules in Process (MIP) Eine Liste, die vom Cryptographic Module Validation Program (CMVP) verwaltet wird und kryptografische Module enthält, die sich momentan im CMVP-Validierungsprozess befinden.

National Information Assurance Partnership (NIAP) Eine Initiative der US-Regierung, die für die US-Implementierung des CC-Standards (Common Criteria) und für die Verwaltung des NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) zuständig ist.

National Institute of Standards and Technology (NIST) Eine US-Bundesbehörde, die dem Handelsministerium unterstellt ist und zu deren Verantwortungsbereich die Weiterentwicklung von Messtechniken, Standards und Technologien gehört.

Protection Profile (PP) Ein Dokument, in dem die Sicherheitsprobleme und Sicherheitsanforderungen für eine bestimmte Produktklasse definiert sind.

Secure Element (SE) Ein Siliziumchip, der in viele Apple-Geräte integriert ist und Funktionen wie Apple Pay unterstützt.

Secure Enclave Processor (SEP) Ein in einen SoC (System-on-Chip) integrierter Coprozessor.

Security Level (SL) Die vier generellen Sicherheitsstufen (Security Levels) – 1 bis 4 – sind im ISO/IEC 19790-Standard definiert und beschreiben die geltenden Sicherheitsanforderungen. Level 4 ist die höchste Sicherheitsstufe.

Security Target (ST) Ein Dokument, in dem die Sicherheitsprobleme und Sicherheitsanforderungen für ein bestimmtes Produkt definiert sind.

Senior Officials Group Information Systems Security (SOG-IS) Ein Gremium, das ein Abkommen zur gegenseitigen Anerkennung von Schutzprofilen und Zertifikaten durch mehrere europäische Staaten verwaltet.

sepOS Die Firmware der Secure Enclave basiert auf einer von Apple angepassten Version des L4-Mikrokernels.

Statement of Applicability (SOA) Ein Dokument, das die im Rahmen eines ISMS implementierten Sicherheitsvorkehrungen beschreibt und zur Unterstützung einer ISO/IEC 27001-Zertifizierung erstellt wird.

System on Chip (SoC) Ein integrierter Schaltkreis (IC), der mehrere Komponenten in einem einzigen Chip zusammenfasst.

T2 Ein Apple-Sicherheits-Chip, der seit 2017 in einigen Intel-basierten Mac-Computern verbaut wird.

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

D028-00499-B