شهادات الأمن ومركز الامتثال

ديسمبر ٢٠٢١

المحتويات

مقدمـة عن ضمان الأمن في Apple

كجزء مـن التزامنـا بالأمـن، تعمل Apple بانتظام مع مؤسسـات تابعة لجهات خارجيـة للمصادقة على أمن أجهزة Apple وبرامجها وخدماتها. تـزود هذه المؤسسـات المعترف بها دوليًا Apple بشـهادات تتوافق مع كل إصدار رئيسـي لنظـام التشـغيل. وبهـذه الطريقـة، فإنها توفر قـدرًا من الثقة - أي ضمان الأمن - لضمـان تلبية الاحتياجات الأمنيـة لنظـام مـا. بالنسـبة إلـى المجالات التقنية التي لـم يتم قبولها بموجـب ترتيبات الاعتراف المتبادل (MRAs) أو التـي تفتقـر إلـى معايير شـهادة الأمن الناضجة، تشـارك Apple في تطوير معايير الأمن المناسـبة. وتتمثل مهمتنـا فـي تحقيـق تغطيـة شـاملة ومقبولة عالميًا لشـهادة الأمن عبر جميع أجهزة Apple وأنظمة تشـغيلها وتطبيقاتها وخدماتها.

غالبًـا مـا تكون الشـهادات ضروريـة لتلبية متطلبات التشـريعات واللوائح والقواعد الصناعية. تتـم تغطية خدمات مثل Apple School Manager و Apple Business Manager بموجب شـهادتي ISO/IEC 27001 و /ISO IEC 27018 مـن Apple. يمكـن لجميـع العملاء، بما في ذلك الوكالات الحكومية والمؤسسـات والمؤسسـات التعليمية التي تنشـر أجهزة Apple، اسـتخدام شـهادات الأجهزة ونظام التشـغيل والبرامج والخدمات لدعم إثبات الامتثال.

شهادات المكونات المادية

نظرًا لأن البرامج الآمنة تتطلب أساسًا من الأمن المضمّن في المكونات المادية، فإن جميع أجهزة Apple - سواء كانت تعمل بنظام iOS أو iPadOS أو macOS أو tvOS أو watchOS - تتمتع بقدرات أمن مصممة في السيليكون. وذلك يشمل إمكانات مخصصة في وحدة المعالجة المركزية تدعم ميزات أمن الأنظمة والسيليكون المخصص للوظائف الأمنية. المكون الأكثر أهمية هو معالج Secure Enclave، والذي يظهر على جميع أجهزة iOS و iPadOS و watchOS و tvOS الحديثة، وعلى جميع أجهزة كمبيوتر Mac التي تحتوي على سيليكون Apple، وأجهزة كمبيوتر Mac المستندة إلى Intel والمزودة برقاقة Apple T2 الأمنية. يوفر Secure Enclave الأساس لتشفير البيانات الثابتة والتمهيد الآمن في macOS والمقاييس الحيوية.

يبدأ التزام Apple بضمان الأمن باعتماد شهادات مكونات الأمن الأساسية في السيليكون بدءًا من جذر الثقة في المكونات المادية، مرورًا بفرض التمهيد الآمن، وصولاً إلى Secure Enclave الذي يوفر مخزنًا آمنًا للمفاتيح، وانتهاءً بالمصادقة الآمنة باستخدام Touch ID و Face ID. أصبحت ميزات الأمن في أجهزة Apple ممكنة من خلال الجمع بين تصميم السيليكون والمكونات المادية والبرامج والخدمات المتوفرة من Apple فقط. يُعد اعتماد هذه المكونات جزءًا مهمًا من التحقق من الضمان الذي تقدمه Apple.

لمزيد من المعلومات حول الشهادات العامة المتعلقة بالمكونات المادية ومكونات البرامج الثابتة المرتبطة، انظر:

- شهادات الأمن لشريحة Apple T2 الأمنية
- شهادات الأمن لمعالج Secure Enclave

شهادات البرامج والتطبيقات

تحتفظ Apple بشهادات وتوثيقات مستقلة حول نظام التشغيل والتطبيقات الخاصة بها بما يتوافق مع معايير معالجة المعلومات الفيدرالية الأمريكية 3-/2-140 (FIPS) لوحدات التشفير والمعايير العامة لأنظمة التشغيل والتطبيقات وخدمات الجهاز. تشمل تغطية أنظمة التشغيل iOS و iPadOS و macOS و sepOS وبرامج T2 الثابتة و tvOS و watchOS. بالنسبة للتطبيقات، ستتضمن الشهادة المستقلة في البداية متصفح Safari وجهات الاتصال، مع اعتماد المزيد من التطبيقات في المستقبل.

للحصول على معلومات حول الشهادات العامة المتعلقة **بأنظمة التشغيل** في Apple، انظر:

- شهادات الأمن لـ iOS
- شهادات الأمن لـ iPadOS
- شهادات الأمن لـ macOS
- شهادات الأمن لـ tvOS
- شهادات الأمن لـ watchOS

للحصول على معلومات حول الشهادات العامة المتعلقة **بتطبيقات** Apple، انظر:

- شهادات الأمن في تطبيقات Apple

شهادات الخدمات

تحتفظ شركة Apple بشهادات الأمن لدعم عملائنا من المؤسسات إلى المنشآت التعليمية. تُمكِّن هذه الشهادات عملاء Apple من الوفاء بالتزاماتهم التنظيمية والتعاقدية عند استخدام خدمات Apple مع برامج Apple ومكوناتها المادية. وتوفر هذه الشهادات لعملائنا تصديقًا مستقلاً حول أمن معلومات Apple والممارسات البيئية وممارسات الخصوصية في أنظمة Apple.

للحصول على معلومات حول الشهادات العامة المتعلقة **بخدمات الإنترنت** في Apple، انظر:

- شهادات أمن خدمات الإنترنت من Apple

للاستفسار حول شهادات الأمن والخصوصية في Apple، تواصل معنا على security-certifications@apple.com.

شـهادات أمن المكونات المادية

نظرة عامة على شهادات أمن المكونات المادية في Apple

تحتفظ Apple بشـهادات التحقـق من صحـة التوافق مع معيار معالجـة المعلومات الفيدرالية 3-/2-140 (FIPS) للبرامـج الثابتـة الخاصـة بـ sepOS و T2 بالإضافة إلى الشـهادات الأخرى. تبدأ Apple **بالكتل البرمجية الإنشـائية للشـهادات** التي تنطبق على نطاق واسـع عبر أنظمة أساسـية متعددة عند الحاجة. الكتلة البرمجية الإنشـائية الأولى هي التحقق من صحة مكتبة التشـفير المسـتخدم لعمليات نشـر وحدة تشـفير البرامج والمكونات المادية داخل أنظمة التشـغيل المطوّرة من Apple. والكتلة البرمجية الإنشـائية الثانية هي شـهادة Secure Enclave، المضمنـة فـي العديـد من أجهزة Apple. والثالثة هي شـهادة Secure Element (SE) الموجودة في أجهزة Apple التـي تحتـوي علـى Touch ID والأجهزة التي تحتوي على Face ID. وتشـكّل الكتل البرمجية الإنشـائية لشـهادة المكونات المادية هذه أساسًـا لشـهادات أمن النظام الأساسي الأوسع.

عمليات التحقق من صحة خوارزمية التشفير

يعـد التحقـق مـن صحـة التنفيذ للعديد من خوارزميات التشـفير ووظائف الأمان ذات الصلة شـرطًا أساسـيًا للتحقق مـن صحـة 3-140 FIPS ودعمًـا للشـهادات الأخرى. وتتم إدارة عملية التحقق بواسـطة برنامـج التحقق من صحة خوارزميـة التشـفير (CAVP) فـي المعهـد الوطنـي للمعايير والتكنولوجيا (NIST). يمكن العثور على شـهادات التحقـق مـن صحـة عمليـات التنفيذ في Apple باسـتخدام أداة البحث في CAVP. لمزيـد من المعلومات، راجع موقـع برنامـج عمليات التحقق من صحة خوارزمية التشـفير (CAVP).

عمليات التحقق من صحة وحدات التشفير: FIPS 140-2/3 (ISO/IEC 19790)

تم التحقق من صحة وحدات التشفير في Apple مرارًا وتكرارًا بواسطة برنامج التحقق من صحة وحدة التشفير (CMVP) بما يتوافق مع معيار معالجة المعلومات الفيدرالية الأمريكية لوحدات التشفير (FIPS 140-2) بعد كل إصدار رئيسي من أنظمة التشغيل منذ ٢.١٢. بعد كل إصدار رئيسي، ترسل Apple الوحدات إلى CMVP للتحقق من صحة التوافق مع المعيار. وتوفر هذه الوحدات، فضلاً عن استخدامها بواسطة أنظمة التشغيل والتطبيقات التابعة لشركة Apple، وظائف تشفير للخدمات المقدمة من Apple وتكون متاحة لتطبيقات الجهات الخارجية لاستخدامها.

تحقق Apple **مستوى الأمن الأول** كل عام للوحدات المستندة لبرامج "وحدة CoreCrypto لـ Intel" و "وحدة CoreCrypto Kernel لـ Intel" لنظام التشغيل macOS. وبالنسبة لسيليكون Apple، "وحدة Corecrypto لـ "ARM و "وحدة Corecrypto Kernel لـ "ARM متوفر لـ iOS و iPadOS و tvOS و watchOS والبرامج الثابتة في رقاقة Apple T2 الأمنية المضمنة في أجهزة كمبيوتر Mac.

في ٢.١٩، حققت Apple **المستوى الأمني الثاني** من FIPS 140-2 الأول لوحدة تشفير المكونات المادية المدمجة التي تم تحديدها على أنها "مخزن المفاتيح الآمن لوحدة Apple Corecrypto" مما يتيح الاستخدام الحكومي المعتمد في الولايات المتحدة الأمريكية للمفاتيح المُنشأة والمُدارة في Secure Enclave. وتواصل Apple السعي نحو إجراء عمليات التحقّق لوحدة تشفير المكونات المادية مع كل إصدار نظام تشغيل رئيسي متواتر.

تم اعتماد FIPS 140-3 من قِبل وزارة التجارة الأمريكية في ٢.١٩. أبرز تغيير في هذا الإصدار من المعايير هو مواصفة معايير ISO/IEC وبالأخص ISO/IEC 19790:2015 ومعيار الاختبار المصاحب ISO/IEC 24759:2017. طرح CMVP برنامج انتقال وأوضح أنه ابتداءً من ٢.٢. سيبدأ التحقق من صحة وحدات التشفير باستخدام FIPS 140-3 كأساس. تهدف وحدات Apple للتشفير إلى تلبية معايير FIPS 140-3 والانتقال إليها في أقرب وقت ممكن.

بالنسبة لوحدات التشفير الموجودة حاليًا في عمليات الاختبار والتحقق من الصحة، يحتفظ CMVP بقائمتين منفصلتين قد تحتويان على معلومات حول عمليات التحقق المقترحة. بالنسبة لوحدات التشفير قيد الاختبار مع مختبر معتمد، قد تسرد قائمة عمليات التنفيذ قيد الاختبار اسم الوحدة. بعد أن ينتهي المختبر من الاختبار ويوصي بالتحقق من الصحة من قِبل CMVP، تظهر وحدات تشفير Apple في قائمة الوحدات قيد المعالجة. ويكتمل حاليًا الاختبار المعملي ويُنتظر التحقق من صحة الاختبار بواسطة CMVP. نظرًا لأن طول عملية التقييم يمكن أن يختلف، انظر إلى قائمتي العملية أعلاه لتحديد الحالة الراهنة لوحدات تشفير Apple بين تاريخ إصدار نظام تشغيل رئيسي وإصدار شهادة التحقق من الصحة بواسطة CMVP.

شهادات المنتج: المعايير العامة (ISO/IEC 15408)

تعد المعايير العامة (ISO/IEC 15408) معيارًا تستخدمه العديد من المؤسسات كأساس لإجراء تقييمات الأمن لمنتجات تقنية المعلومات.

بالنسبة للشهادات التي قد يتم الاعتراف بها بشكل متبادل بموجب اتفاقية الاعتراف بالمعايير العامة الدولية (CCRA)، انظر بوابة المعايير العامة. يمكن أيضًا استخدام مقاييس المعايير العامة خارج CCRA بواسطة مخططات التحقق المحلية والخاصة. في أوروبا، يخضع الاعتراف المتبادل لاتفاقية SOG-IS وكذلك CCRA.

الهدف، كما أوضح مجتمع المعايير العامة، هو تأسيس مجموعة من المعايير الأمنية المعتمدة دوليًا لتوفير تقييم واضح وموثوق للقدرات الأمنية لمنتجات تقنية المعلومات. ومن خلال توفير تقييم مستقل لقدرة المنتج على تلبية المعايير الأمنية، تمنح شهادة المعايير العامة للعملاء ثقة أكبر في أمن منتجات تقنية المعلومات وتؤدي إلى اتخاذ قرارات أكثر استنارة.

ومع اتفاقية الاعتراف بالمعايير العامة (CCRA)، اتفقت الدول الأعضاء على الاعتراف بشهادة منتجات تقنية المعلومات بمستوى الثقة ذاته. التقييمات المطلوبة قبل الحصول على الشهادة واسعة النطاق وتشمل:

- ملفات تعريف الحماية (PPs)
- الأهداف الأمنية (STs)
- المتطلبات الوظيفية الأمنية (SFRs)
- متطلبات ضمان الأمن (SAR)
- مستويات ضمان التقييم (EALs)

ملفات تعريف الحماية (PPs)، عبارة عن مستندات تحدد متطلبات الأمن لفئة من أنواع الأجهزة مثل التنقل، وتُستخدم لتوفير إمكانية المقارنة بين تقييمات منتجات تكنولوجيا المعلومات ضمن نفس الفئة. وتستمر عضوية CCRA جنبًا إلى جنب مع قائمة متزايدة من ملفات تعريف الحماية (PPs) المعتمدة في النمو على أساس سنوي. ويسمح هذا الترتيب لمطور المنتج بالمطالبة بشهادة واحدة بموجب أي من أنظمة تفويض الشهادات وطلب الاعتراف بها من قِبل أيٍ من المُوقِّعين المستهلكين للشهادة.

تحدد الأهداف الأمنية (STs) **ما** سيتم تقييمه عند اعتماد أحد منتجات تكنولوجيا المعلومات. تتم ترجمة الأهداف الأمنية (STs) إلى **متطلبات وظيفية أمنية** (SFRs) أكثر تحديدًا، تُستخدم لتقييم الأهداف الأمنية (STs) بمزيد من التفصيل.

كما تتضمن المعايير العامة (CC) **متطلبات ضمان الأمن**. أحد المقاييس الشائعة هو **مستوى ضمان التقييم** (EAL). تجمع مستويات ضمان التقييم (EALs) معًا مجموعات متطلبات ضمان الأمن (SARs) التي تحدث بشكل متكرر ويمكن تحديدها في ملفات تعريف الحماية (PPs) والأهداف الأمنية (STs) لدعم إمكانية للمقارنة.

تمت أرشفة العديد من ملفات تعريف الحماية (PPs) الأقدم ويتم استبدالها بملفات تعريف الحماية (PPs) المستهدفة، والتي يتم تطويرها للتركيز على حلول وبيئات محددة. وفي إطار الجهود المتضافرة الرامية إلى ضمان استمرار الاعتراف المتبادل بين جميع أعضاء CCRA، تم تأسيس المجتمعات الفنية الدولية (iTCs) لتطوير وصيانة ملفات تعريف الحماية التعاونية (cPPs)، والتي يتم تطويرها منذ البداية بمشاركة من الأنظمة المُوقِّعة على CCRA. وتواصل الجهات المعنية جهودها المبذولة لتطوير ملفات تعريف الحماية (PPs) المستهدفة لمجموعات المستخدمين وترتيبات الاعتراف المتبادلة بخلاف CCRA.

بدأت Apple في السعي للحصول على الشهادات بموجب CCRA المُحدّث مع cPPs المحددة ابتداءً من أوائل عام ٢.١٥. ومنذ ذلك الحين حصلت Apple على شهادات المعايير العامة لكل إصدار iOS رئيسي ووسَّعت التغطية لتشمل الضمان الأمني المقدَّم من ملفات تعريف الحماية (PPs) الجديدة.

تلعب Apple دورًا فعالاً داخل المجتمعات التقنية التي تركز على تقييم تقنيات أمن أجهزة الجوال. ويشمل ذلك المجتمعات الفنية الدولية (iTCs) المسؤولة عن تطوير وتحديث ملفات تعريف الحماية التعاونية (cPPs). وتواصل Apple تقييم الشهادات ومعالجتها وفقًا لملفات تعريف PPs و cPPs الحالية.

يتم تنفيذ شهادات أنظمة Apple الأساسية لأسواق أمريكا الشمالية بشكل عام مع شراكة أمن المعلومات الوطني (NIAP) التي تحتفظ بقائمة من المشاريع قيد التقييم حاليًا ولكن لم يتم اعتمادها بعد.

بالإضافة إلى شهادات الأنظمة الأساسية العامة المدرجة، تم إصدار شهادات أخرى لإثبات متطلبات أمن معينة لبعض الأسواق.

شهادات الأمن لمعالج Secure Enclave

خلفية شهادة Secure Enclave

تأتي وحدة تشفير الأجهزة - **وحدة تشفير مخزن المفاتيح الآمن في SEP من** - Apple مضمنة في Apple SOC الموجود في المنتجات التالية: سلسلة A من Apple لـ iPhone و iPad، وسلسلة M لأجهزة كمبيوتر Mac المزودة برقاقة Apple، وسلسلة S لـ Apple Watch، وسلسلة T للرقاقة الأمنية الموجودة في أجهزة كمبيوتر Mac المستندة إلى Intel بدءًا من iMac Pro الذي تم طرحه في عام ٢.١٧.

في عام ٢.١٨، قامت Apple بالمزامنة مع التحقق من صحة وحدات تشفير البرامج مع أنظمة التشغيل المطروحة في عام ٢.١٧: iOS 11 و macOS 10.13 و tvOS 11 و watchOS 4. تم التحقق في البداية من صحة وحدة تشفير مكونات SEP المادية المحددة على أنها وحدة تشفير مخزن المفاتيح الآمن في SEP من Apple إصدار v1.0 وفقًا لمتطلبات المستوى الأمني الأول من FIPS 140-2.

في عام ٢.١٩، قامت Apple بالتحقق من صحة وحدة المكونات المادية وفقًا لمتطلبات المستوى الأمني الثاني من FIPS 140-2 وتحديث معرف إصدار الوحدة إلى v9.0 من أجل المزامنة مع إصدارات عمليات التحقق من صحة وحدات مستخدم corecrypto و corecrypto Kernel المقابلة. في عام 2019، تضمن ذلك iOS 12 و macOS 10.14 و tvOS 12 و watchOS 5.

في عامي ٢.٢٠ و٢.٢١، تسعى Apple إلى التحقق من صحة التوافق مع FIPS 140-3، ومع ضمان إضافي لمستوى الأمان ٣ لمتطلبات الأمان المادية لرقاقات Apple: رقاقات A13 و A14 و S6 و M1.

تشارك Apple أيضًا بفعالية في التحقّق من صحة وحدات مستخدم corecrypto و corecrypto Kernel لكل إصدار رئيسي من نظام التشغيل. لا يمكن إجراء التحقق من صحة التوافق إلا على نسخة الإصدار النهائية.

حالة عملية التحقق من صحة وحدة التشفير

يحتفظ برنامج التحقق من صحة وحدة التشفير (CMVP) بحالة التحقق من صحة وحدات التشفير ضمن الثلاث قوائم منفصلة اعتمادًا على حالتها الحالية:

- لكي يتم الإدراج في قائمة التنفيذ قيد الاختبار في CMVP، يجب أن يتعاقد المختبر مع Apple لتقديم الاختبار.
- بعد اكتمال الاختبار بواسطة المختبر، يكون المختبر قادرًا على التوصية بالتحقق من الصحة بواسطة CMVP، ودفع رسوم CMVP، ثم تُضاف الوحدة إلى قائمة الوحدات قيد المعالجة. تعمل قائمة الوحدات قيد المعالجة MIP على تتبع التقدّم المحرز في جهود التحقق من الصحة بواسطة CMVP في أربع مراحل:
  - **في انتظار المراجعة**: في انتظار تعيين مورد CMVP.
  - **قيد المراجعة**: تعمل موارد CMVP على تنفيذ أنشطة التحقق الخاصة بها.
  - **التنسيق**: يعمل المختبر و CMVP على حل أي مشكلات يتم العثور عليها.
  - **وضع اللمسات الأخيرة**: الأنشطة والإجراءات المتعلقة بإصدار الشهادة.
- بعد التحقّق من الصحة بواسطة CMVP، يتم منح الوحدات شهادة المطابقة وإضافتها إلى قائمة وحدات التشفير التي تم التحقق من صحتها. ويشمل ذلك:
  - الوحدات النمطية التي تم التحقق من صحتها والتي تم تمييزها على أنها نشطة.
  - بعد ٥ سنوات، يتم تمييز الوحدات النمطية على أنها قديمة.
  - إذا تم إلغاء شهادة الوحدة النمطية لسبب ما، فسيتم تمييزها على أنها مُلغاة.

في عام ٢.٢٠، اعتمدت CMVP المعيار الدولي، ISO/IEC 19790، كأساس لمعيار FIPS 140-3.

شهادات FIPS 140-3

الحالة الحالية

يوضح الجدول أدناه وحدات التشفير النمطية لعام ٢.٢ و٢.٢١ التي يتم اختبارها حاليًا بواسطة المختبر للتوافق مع FIPS 140-3.

أكمل مخزن المفاتيح الآمن (SKS) الخاص بنظام التشغيل لعامي ٢.٢ و٢.٢١ الاختبارات المعملية وقد أوصى به المختبر ليتم التحقق من صحته بواسطة CMVP. وهو مدرجة في قائمة الوحدات قيد المعالجة وبمجرد التحقق من صحته سينتقل إلى قائمة وحدات التشفير النمطية التي تم التحقق من صحتها.

تخضع مساحة المستخدم في iOS 15 (٢.٢١)، ومساحة kernel، ومخزن المفاتيح الآمن للاختبارات المعملية. وهي مدرجة في قائمة التنفيذ قيد الاختبار.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع إصدارات ٢.٢١ من iOS و iPadOS و macOS و tvOS و watchOS **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14، T2، M1، S3-S6) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع إصدارات ٢.٢١ من iOS و iPadOS و macOS و tvOS و watchOS **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A13، A14، S6، M1) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣
تاريخ إصدار نظام التشغيل: ٢.٢ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع إصدارات ٢.٢ من iOS و iPadOS و macOS و tvOS و watchOS **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14، T2، M1، S3-S6) **المستوى الأمني العام:** ٢

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع إصدارات ٢.٢. من iOS و iPadOS و macOS و tvOS و watchOS **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A13، A14، S6، M1) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣

شهادات FIPS 140-2

يوضح الجدول أدناه وحدات التشفير النمطية التي تم اختبارها بواسطة المختبر للتوافق مع FIPS 140-2.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢ - ٥ - ٢٠٢١	**الشهادات:** ٣٨١١ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة تشفير مخزن المفاتيح الآمن من Apple الإصدار v1.0 **نظام التشغيل:** sepOS لـ macOS 10.15 Catalina **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢٠١٩	**الشهادات:** ٣٥٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v9.0 **نظام التشغيل:** sepOS لـ macOS 10.14 Mojave **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢٠١٩	**الشهادات:** ٣٢٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v1.0 **نظام التشغيل:** sepOS لـ macOS 10.13 High Sierra **النوع:** المكونات المادية **المستوى الأمني:** ٢

شهادات المعايير العامة (CC)

تشارك Apple بفعالية في تقييمات المعايير العامة حيث تغطي ملفات تعريف الحماية المناسبة وظائف الأمن لتقنية Apple.

حالة شهادة المعايير العامة (CC)

يحتفظ مخطط الولايات المتحدة، الذي تديره NIAP، بقائمة من المنتجات قيد التقييم، وتشمل هذه القائمة المنتجات التي تخضع حاليًا للتقييم في الولايات المتحدة مع مختبر اختبار المعايير العامة (CCTL) المعتمد من NIAP والتي أكملت اجتماع انطلاق التقييم (أو ما يعادله) حيث تقبل إدارة CCEVS رسميًا المنتج قيد التقييم.

بعد اعتماد المنتجات، تُدرج NIAP الشهادات الصالحة حاليًا في قائمة المنتجات المتوافقة. وبعد عامين تتم مراجعة هذه الشهادات للتأكد من توافقها مع السياسة الراهنة للحفاظ على الضمان. بعد انتهاء تاريخ الحفاظ على الضمان، تنقل NIAP قائمة الشهادات إلى قائمة المنتجات المؤرشفة.

تسرد بوابة المعايير العامة الشهادات التي يمكن الاعتراف بها بشكل متبادل بموجب ترتيب الاعتراف بالمعايير العامة (CCRA). قد تحتفظ بوابة المعايير العامة (CC) بالمنتجات في قائمة المنتجات المعتمدة لمدة 0 أعوام، ويتم الاحتفاظ بالسجلات بواسطة بوابة المعايير العامة (CC) في الشهادات المؤرشفة.

يوضح الجدول أدناه الشهادات التي يتم تقييمها حاليًا بواسطة المختبر، أو التي تم اعتمادها على أنها متوافقة مع المعايير العامة.

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: sepOS **تاريخ الشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple Secure Enclave [٢.٢.] **ملفات تعريف الحماية:** CPP_DSC_V1.0 **المكونات المادية:** Secure Enclave (A9-A14، M1، T2، S3-S6) **البرامج:** sepOS الموزَّع مع iOS 14، iPadOS 14، macOS 11 Big Sur، tvOS 14، watchOS 7

الشهادات الإضافية

يوضح الجدول أدناه شهادات Secure Enclave التي لا تستخدم المعايير العامة أو FIPS 140-3.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** ٧ - ١٢ - ٢.١٩ إلى ٢٦ - ١٢ - ٢.٢٢	**الشهادات:** CFNR201902910002 (P.R. الصين: شهادة التكنولوجيا للخدمات المالية المتنقلة) النسخة الصينية النسخة الإنجليزية	**العنوان:** بيئة تنفيذ موثوقة للمحطة المتنقلة **نظام التشغيل:** iOS 13.5.1 **المواصفات:** JR/T 0156-2017

شهادات الأمن لشريحة Apple T2 الأمنية

خلفية عملية التحقق من صحة وحدة التشفير

تشارك Apple بفعالية في التحقق من صحة البرامج المدمجة ووحدات المكونات المادية الخاصة بشركة Apple لكل إصدار رئيسي من نظام التشغيل. لا يمكن إجراء التحقق من صحة التوافق إلا على نسخة إصدار الوحدة النهائية.

في عام ٢٠٢٠، اعتمدت CMVP المعيار الدولي، ISO/IEC 19790، كأساس لمعيار معالجة المعلومات الفيدرالية 140-3 (FIPS).

بالإضافة إلى وحدة معالجة Intelالمركزية، تحتوي معظم أجهزة كمبيوتر Mac منذ عام ٢٠١٧ أيضًا على رقاقة Apple T2 أمنية منفصلة وهي نظام يعتمد على رقاقة Apple من السيليكون (SoC). تستخدم أجهزة كمبيوتر Mac المستندة إلى رقاقة T2 جميع وحدات التشفير الخمس لخدمات متنوعة على الجهاز.

- وحدة مستخدم Corecrypto لـ Intel (مستخدمة بواسطة macOS على أجهزة كمبيوتر Mac المستندة إلى Intel)
- وحدة Corecrypto kernel لـ Intel (مستخدمة بواسطة macOS على أجهزة كمبيوتر Mac المستندة إلى Intel)
- وحدة مستخدم Corecrypto لـ ARM (مستخدمة بواسطة رقاقة T2)
- وحدة Corecrypto kernel لـ ARM (مستخدمة بواسطة رقاقة T2)
- وحدة تشفير مخزن المفاتيح الآمن (مستخدمة بواسطة معالج Secure Enclave المضمن في رقاقة T2)

ملاحظة: الوحدات المستندة إلى سيليكون Apple المثبتة على رقاقة T2 هي نفسها تلك المثبتة على سيليكون Apple الأخرى مثل سلسلة A وسلسلة S وسلسلة M من Apple.

حالة عملية التحقق من صحة وحدة التشفير

يحتفظ برنامج التحقق من صحة وحدة التشفير (CMVP) بحالة التحقق من صحة وحدات التشفير ضمن الثلاث قوائم منفصلة اعتمادًا على حالتها الحالية:

- لكي يتم الإدراج في قائمة التنفيذ قيد الاختبار في CMVP، يجب أن يتعاقد المختبر مع Apple لتقديم الاختبار.
- بعد اكتمال الاختبار بواسطة المختبر، يكون المختبر قادرًا على التوصية بالتحقق من الصحة بواسطة CMVP، ودفع رسوم CMVP، ثم تُضاف الوحدة إلى قائمة الوحدات قيد المعالجة (MIP). تعمل قائمة الوحدات قيد المعالجة MIPعلى تتبع التقدّم المحرز في جهود التحقق من الصحة بواسطة CMVPفي أربع مراحل:
- **في انتظار المراجعة:** في انتظار تعيين مورد CMVP.
- **قيد المراجعة:** تعمل موارد CMVP على تنفيذ أنشطة التحقق الخاصة بها.
- **التنسيق:** يعمل المختبر و CMVP على حل أي مشكلات يتم العثور عليها.
- **وضع اللمسات الأخيرة:** الأنشطة والإجراءات المتعلقة بإصدار الشهادة.
- بعد التحقّق من الصحة بواسطة CMVP، يتم منح الوحدات شهادة المطابقة وإضافتها إلى قائمة وحدات

التشفير التي تم التحقق من صحتها. ويشمل ذلك:

- الوحدات النمطية التي تم التحقق من صحتها والتي تم تمييزها على أنها نشطة.
- بعد 0 سنوات، يتم تمييز الوحدات النمطية على أنها قديمة.
- إذا تم إلغاء شهادة الوحدة النمطية لسبب ما، فسيتم تمييزها على أنها مُلغاة.

شهادات FIPS 140-3

الحالة الحالية

أكملت الوحدات النمطية لعام ٢.٢. لمساحة المستخدم، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

تخضع الوحدات النمطية لعام ٢.٢. لمساحة المستخدم، ومساحة kernel، ومخزن المفاتيح الآمن للاختبارات المعملية. وهي مدرجة في قائمة التنفيذ قيد الاختبار.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** sepOS لـ macOS 12 Monterey **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** sepOS لـ macOS 12 Monterey **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** sepOS لـ macOS 12 Monterey **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (T2) **المستوى الأمني:** ٢

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS لـ macOS 11 Big Sur **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS لـ macOS 11 Big Sur **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS لـ macOS 11 Big Sur على Intel **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية **المستوى الأمني:** ٢

شهادات FIPS 140-2

يوضح الجدول أدناه وحدات التشفير النمطية التي تم اختبارها بواسطة المختبر للتوافق مع FIPS 140-2.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢٠٢١	**الشهادات:** ٣٨٥٦ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** sepOS لـ macOS 10.15 Catalina **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢٠٢١	**الشهادات:** ٣٨٥٥ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v10.0 لـ ARM **نظام التشغيل:** sepOS لـ macOS 10.15 Catalina **النوع:** البرامج **المستوى الأمني:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٥ - ٢ - ٢.٢١	**الشهادات:** ٣٨١١ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة تشفير مخزن المفاتيح الآمن Apple Corecrypto الإصدار v10.0 **نظام التشغيل:** sepOS لـ macOS 10.15 Catalina **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ٢٣ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Corecrypto الإصدار v9.0 لـ ARM **نظام التشغيل:** sepOS لـ macOS 10.14 Mojave **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١١ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v9.0 لـ ARM **نظام التشغيل:** sepOS لـ macOS 10.14 Mojave **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢.١٩	**الشهادات:** ٣٥٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v9.0 **نظام التشغيل:** sepOS لـ macOS 10.14 Mojave **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ٢٢ - ٥ - ٢.١٨، ٦ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** sepOS لـ macOS 10.13 High Sierra **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ١٧ - ٥ - ٢.١٨، ٣ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v8.0 لـ ARM **نظام التشغيل:** sepOS لـ macOS 10.13 High Sierra **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ١٠ - ٧ - ٢.١٨	**الشهادات:** ٣٢٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v1.0 **نظام التشغيل:** sepOS لـ macOS 10.13 High Sierra **النوع:** المكونات المادية **المستوى الأمني:** ٢

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٦ **تواريخ التحقق من الصحة:** ١ - ٢ - ٢.١٧	**الشهادات:** ٢٨٢٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple iOS Corecrypto Kernel الإصدار v7.0 **نظام التشغيل:** sepOS لـ macOS 10.12 Sierra **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٦ **تواريخ التحقق من الصحة:** ١ - ٢ - ٢.١٧	**الشهادات:** ٢٨٢٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple iOS Corecrypto Kernel الإصدار v7.0 **نظام التشغيل:** sepOS لـ macOS 10.12 Sierra **النوع:** البرامج **المستوى الأمني:** ١

شـهادات أمن أنظمة التشغيل

نظرة عامة على شهادات أمن أنظمة التشغيل في Apple

تحتفظ Apple بشـهادات التحقق من صحـة التوافق مع معيار معالجـة المعلومات الفيدرالية 3-/2-140 (FIPS) للبرامـج الثابتـة الخاصـة بـ sepOS و T2 بالإضافة إلى الشـهادات الأخرى. تبدأ Apple **بالكتل البرمجية الإنشـائية للشـهادات** التي تنطبق على نطاق واسـع عبر أنظمة أساسـية متعددة عند الحاجة. الكتلة البرمجية الإنشـائية الأولى هي التحقق من صحة التشـفير المسـتخدم لعمليات نشـر وحدة تشـفير البرامج والمكونات المادية داخل أنظمة التشـغيل المطوّرة من Apple. والكتلة البرمجية الإنشـائية الثانية هي شـهادة Secure Enclave، المضمنـة فـي العديـد من أجهزة Apple. والثالثة هي شـهادة Secure Element (SE) الموجودة في أجهزة Apple التـي تحتـوي علـى Touch ID والأجهزة التي تحتوي على Face ID. وتشـكّل الكتل البرمجية الإنشـائية لشـهادة المكونات المادية هذه أساسًـا لشـهادات أمن النظام الأساسي الأوسع.

عمليات التحقق من صحة خوارزمية التشفير

يعـد التحقـق مـن صحـة التنفيذ للعديد من خوارزميات التشـفير ووظائف الأمان ذات الصلة شـرطًا أساسـيًا للتحقق مـن صحـة FIPS 140-3 ودعمًـا للشـهادات الأخرى. وتتم إدارة عملية التحقق بواسـطة برنامـج التحقق من صحة خوارزميـة التشـفير (CAVP) فـي NIST. يمكـن العثور على شـهادات التحقق من صحة عمليـات التنفيذ في Apple باسـتخدام أداة البحث في CAVP.

عمليات التحقق من صحة وحدات التشفير: FIPS 140-2/3 (ISO/IEC 19790)

تم التحقق من صحة وحدات التشفير في أنظمة تشغيل Apple مرارًا وتكرارًا بواسطة برنامج التحقق من صحة وحدة التشفير (CMVP) بما يتوافق مع معايير معالجة المعلومات الفيدرالية الأمريكية 140-2 (FIPS) بعد كل إصدار رئيسي من أنظمة التشغيل منذ ٢.١٢. بعد كل إصدار رئيسي، تقدم Apple جميع الوحدات إلى CMVP للتحقق من صحة التشفير بالكامل. وتوفر هذه الوحدات التي تم التحقق منها عمليات تشفير للخدمات التي توفرها Apple، وتكون متوفرة للاستخدام بواسطة التطبيقات التابعة لجهات خارجية.

تحقق Apple **مستوى الأمن الأول** كل عام للوحدات المستندة لبرامج "وحدة CoreCrypto لـ Intel" و "وحدة CoreCrypto Kernel لـ Intel" لنظام التشغيل macOS. وبالنسبة لسيليكون Apple، "وحدة Corecrypto لـ ARM" و "وحدة Corecrypto Kernel لـ ARM" متوفر لـ iOS و iPadOS و tvOS و watchOS والبرامج الثابتة في رقاقة Apple T2 الأمنية المضمنة في أجهزة كمبيوتر Mac.

في ٢.١٩، حققت Apple **المستوى الأمني الثاني** من FIPS 140-2 الأول لوحدة تشفير المكونات المادية المدمجة التي تم تحديدها على أنها "مخزن المفاتيح الآمن لوحدة Apple Corecrypto" مما يتيح الاستخدام الحكومي المعتمد في الولايات المتحدة الأمريكية للمفاتيح المُنشأة والمُدارة في Secure Enclave. وتواصل Apple السعي نحو إجراء عمليات التحقّق لوحدة تشفير المكونات المادية مع كل إصدار نظام تشغيل رئيسي متواتر.

تم اعتماد FIPS 140-3 من قِبل وزارة التجارة الأمريكية في ٢.١٩. أبرز تغيير في هذا الإصدار من المعايير هو مواصفة معايير ISO/IEC وبالأخص ISO/IEC 19790:2015 ومعيار الاختبار المصاحب ISO/IEC 24759:2017. طرح CMVP برنامج انتقال وأوضح أنه ابتداءً من ٢.٢٠ سيبدأ التحقق من صحة وحدات التشفير باستخدام FIPS 140-3 كأساس. تهدف وحدات Apple للتشفير إلى تلبية معايير FIPS 140-3 والانتقال إليها في أقرب وقت ممكن.

بالنسبة لوحدات التشفير الموجودة حاليًا في عمليات الاختبار والتحقق من الصحة، يحتفظ CMVP بقائمتين منفصلتين قد تحتويان على معلومات حول عمليات التحقق المقترحة. بالنسبة لوحدات التشفير قيد الاختبار مع مختبر معتمد، قد تسرد قائمة عمليات التنفيذ قيد الاختبار اسم الوحدة. بعد أن ينتهي المختبر من الاختبار ويوصي بالتحقق من الصحة من قِبل CMVP، تظهر وحدات تشفير Apple في قائمة الوحدات قيد المعالجة. ويكتمل حاليًا الاختبار المعملي ويُنتظر التحقق من صحة الاختبار بواسطة CMVP. نظرًا لأن طول عملية التقييم يمكن أن يختلف، انظر إلى قائمتي العملية أعلاه لتحديد الحالة الراهنة لوحدات تشفير Apple بين تاريخ إصدار نظام تشغيل رئيسي وإصدار شهادة التحقق من الصحة بواسطة CMVP.

شهادات المنتج: المعايير العامة (ISO/IEC 15408)

تعد المعايير العامة (ISO/IEC 15408) معيارًا تستخدمه العديد من المؤسسات كأساس لإجراء تقييمات الأمن لمنتجات تقنية المعلومات.

بالنسبة للشهادات التي قد يتم الاعتراف بها بشكل متبادل بموجب اتفاقية الاعتراف بالمعايير العامة الدولية (CCRA)، انظر بوابة المعايير العامة. يمكن أيضًا استخدام مقاييس المعايير العامة خارج CCRA بواسطة مخططات التحقق المحلية والخاصة. في أوروبا، يخضع الاعتراف المتبادل لاتفاقية SOG-IS وكذلك CCRA.

الهدف، كما أوضح مجتمع المعايير العامة، هو تأسيس مجموعة من المعايير الأمنية المعتمدة دوليًا لتوفير تقييم واضح وموثوق للقدرات الأمنية لمنتجات تقنية المعلومات. ومن خلال توفير تقييم مستقل لقدرة المنتج على تلبية المعايير الأمنية، تمنح شهادة المعايير العامة للعملاء ثقة أكبر في أمن منتجات تقنية المعلومات وتؤدي إلى اتخاذ قرارات أكثر استنارة.

ومع اتفاقية الاعتراف بالمعايير العامة (CCRA)، اتفقت الدول الأعضاء على الاعتراف بشهادة منتجات تقنية المعلومات بمستوى الثقة ذاته. التقييمات المطلوبة قبل الحصول على الشهادة واسعة النطاق وتشمل:

- ملفات تعريف الحماية (PPs)
- الأهداف الأمنية (STs)
- المتطلبات الوظيفية الأمنية (SFRs)
- متطلبات ضمان الأمن (SAR)
- مستويات ضمان التقييم (EALs)

ملفات تعريف الحماية (PPs)، عبارة عن مستندات تحدد متطلبات الأمن لفئة من أنواع الأجهزة مثل التنقل، وتُستخدم لتوفير إمكانية المقارنة بين تقييمات منتجات تكنولوجيا المعلومات ضمن نفس الفئة. وتستمر عضوية CCRAجنبًا إلى جنب مع قائمة متزايدة من ملفات تعريف الحماية (PPs) المعتمدة في النمو على أساس سنوي. ويسمح هذا الترتيب لمطور المنتج بالمطالبة بشهادة واحدة بموجب أي من أنظمة تفويض الشهادات وطلب الاعتراف بها من قِبل أيٍ من المُوقِّعين المستهلكين للشهادة.

تحدد الأهداف الأمنية (STs) **ما** سيتم تقييمه عند اعتماد أحد منتجات تكنولوجيا المعلومات. تتم ترجمة الأهداف الأمنية (STs) إلى **متطلبات وظيفية أمنية** (SFRs) أكثر تحديدًا، تُستخدم لتقييم الأهداف الأمنية (STs) بمزيد من التفصيل.

كما تتضمن المعايير العامة (CC) **متطلبات ضمان الأمن**. أحد المقاييس الشائعة هو **مستوى ضمان التقييم** (EAL). تجمع مستويات ضمان التقييم (EALs) معًا مجموعات متطلبات ضمان الأمن (SARs) التي تحدث بشكل متكرر ويمكن تحديدها في ملفات تعريف الحماية (PPs) والأهداف الأمنية (STs) لدعم إمكانية للمقارنة.

تمت أرشفة العديد من ملفات تعريف الحماية (PPs) الأقدم ويتم استبدالها بملفات تعريف الحماية (PPs) المستهدفة، والتي يتم تطويرها للتركيز على حلول وبيئات محددة. وفي إطار الجهود المتضافرة الرامية إلى ضمان استمرار الاعتراف المتبادل بين جميع أعضاء CCRA، تم تأسيس المجتمعات الفنية الدولية (iTCs) لتطوير وصيانة **ملفات تعريف الحماية التعاونية** (cPPs)، والتي يتم تطويرها منذ البداية بمشاركة من الأنظمة المُوقِّعة على CCRA. وتواصل الجهات المعنية جهودها المبذولة لتطوير ملفات تعريف الحماية (PPs) المستهدفة لمجموعات المستخدمين وترتيبات الاعتراف المتبادلة بخلاف CCRA.

بدأت Apple في السعي للحصول على الشهادات بموجب CCRA المُحدّث مع cPPs المحددة ابتداءً من أوائل عام ٢.١٥. ومنذ ذلك الحين حصلت Apple على شهادات المعايير العامة لكل إصدار iOS رئيسي ووسَّعت التغطية لتشمل الضمان الأمني المقدَّم من ملفات تعريف الحماية (PPs) الجديدة.

تلعب Apple دورًا فعالاً داخل المجتمعات التقنية التي تركز على تقييم تقنيات أمن أجهزة الجوال. ويشمل ذلك المجتمعات الفنية الدولية (iTCs) المسؤولة عن تطوير وتحديث ملفات تعريف الحماية التعاونية (cPPs). وتواصل Apple تقييم الشهادات ومعالجتها وفقًا لملفات تعريف PPs و cPPs الحالية.

يتم تنفيذ شهادات أنظمة Appleالأساسية لأسواق أمريكا الشمالية بشكل عام مع شراكة أمن المعلومات الوطني (NIAP) التي تحتفظ بقائمة من المشاريع قيد التقييم حاليًا ولكن لم يتم اعتمادها بعد.

بالإضافة إلى شهادات الأنظمة الأساسية العامة المدرجة، تم إصدار شهادات أخرى لإثبات متطلبات أمن معينة لبعض الأسواق.

شهادات الأمن لـ iOS

خلفية شهادة iOS

تشارك Apple بفعالية في التحقق من صحة البرامج المدمجة ووحدات المكونات المادية الخاصة بشركة Apple لكل إصدار رئيسي من نظام التشغيل. لا يمكن إجراء التحقق من صحة التوافق إلا على نسخة الإصدار النهائية.

حالة عملية التحقق من صحة وحدة التشفير في iOS

يحتفظ برنامج التحقق من صحة وحدة التشفير (CMVP) بحالة التحقق من صحة وحدات التشفير ضمن الثلاث قوائم منفصلة اعتمادًا على حالتها الحالية:

- لكي يتم الإدراج في قائمة التنفيذ قيد الاختبار في CMVP، يجب أن يتعاقد المختبر مع Apple لتقديم الاختبار.
- بعد اكتمال الاختبار بواسطة المختبر، يكون المختبر قادرًا على التوصية بالتحقق من الصحة بواسطة CMVP، ودفع رسوم CMVP، ثم تُضاف الوحدة إلى قائمة الوحدات قيد المعالجة (MIP). تعمل قائمة الوحدات قيد المعالجة MIP على تتبع التقدّم المحرز في جهود التحقق من الصحة بواسطة CMVP في أربع مراحل:
  - **في انتظار المراجعة:** في انتظار تعيين مورد CMVP.
  - **قيد المراجعة:** تعمل موارد CMVP على تنفيذ أنشطة التحقق الخاصة بها.
  - **التنسيق:** يعمل المختبر و CMVP على حل أي مشكلات يتم العثور عليها.
  - **وضع اللمسات الأخيرة:** الأنشطة والإجراءات المتعلقة بإصدار الشهادة.
- بعد التحقّق من الصحة بواسطة CMVP، يتم منح الوحدات شهادة المطابقة وإضافتها إلى قائمة وحدات التشفير التي تم التحقق من صحتها. ويشمل ذلك:
  - الوحدات النمطية التي تم التحقق من صحتها والتي تم تمييزها على أنها نشطة.
  - بعد ٥ سنوات، يتم تمييز الوحدات النمطية على أنها قديمة.
  - إذا تم إلغاء شهادة الوحدة النمطية لسبب ما، فسيتم تمييزها على أنها مُلغاة.

في عام ٢٠٢٠، اعتمدت CMVP المعيار الدولي، ISO/IEC 19790، كأساس لمعيار FIPS 140-3.

شهادات FIPS 140-3

الحالة الحالية

أكملت مساحة المستخدم في iOS 14 (٢.٢.)، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

تخضع مساحة المستخدم في iOS 15 (٢.٢١)، ومساحة kernel، ومخزن المفاتيح الآمن للاختبارات المعملية. وهي مدرجة في قائمة التنفيذ قيد الاختبار.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** iOS 15 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** iOS 15 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع iOS 15 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع iOS 15 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A13، A14، A15) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** iOS 14 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢٠٢٠. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** iOS 14 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢٠٢٠. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع iOS 14 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٢٠٢٠. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع iOS 14 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A13-A14) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣

شهادات FIPS 140-2

يوضح الجدول أدناه وحدات التشفير النمطية التي يتم اختبارها حاليًا والتي تم اختبارها بواسطة المختبر للتوافق مع FIPS 140-2.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢.٢١	**الشهادات:** ٣٨٥٦ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** iOS 13 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢.٢١	**الشهادات:** ٣٨٥٥ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v10.0 لـ ARM **نظام التشغيل:** iOS 13 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٥ - ٢ - ٢.٢١	**الشهادات:** ٣٨١١ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة تشفير مخزن المفاتيح الآمن من Apple الإصدار v1.0 **نظام التشغيل:** sepOS الموزَّع مع iOS 13 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ٢٣ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v9.0 لـ ARM **نظام التشغيل:** iOS 12 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١١ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Corecrypto الإصدار v9.0 لـ ARM **نظام التشغيل:** iOS 12 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢.١٩	**الشهادات:** ٣٥٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v9.0 **نظام التشغيل:** sepOS الموزَّع مع iOS 12 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ٢٢ - ٥ - ٢.١٨، ٦ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** iOS 11 **النوع:** البرامج **المستوى الأمني:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ١٧ - ٥ - ٢.١٨، ٣ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v8.0 لـ ARM **نظام التشغيل:** iOS 11 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ١. - ٩ - ٢.١٩	**الشهادات:** ٣٢٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v1.0 **نظام التشغيل:** sepOS الموزَّع مع iOS 11 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٦ **تواريخ التحقق من الصحة:** ١ - ٢ - ٢.١٧	**الشهادات:** ٢٨٢٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple iOS Corecrypto Kernel الإصدار v7.0 **نظام التشغيل:** iOS 10 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٦ **تواريخ التحقق من الصحة:** ١ - ٢ - ٢.١٧	**الشهادات:** ٢٨٢٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple iOS Corecrypto Kernel الإصدار v7.0 **نظام التشغيل:** iOS 10 **النوع:** البرامج **المستوى الأمني:** ١

الإصدارات السابقة

وتُدرَج الإصدارات الأقدم من ٥ سنوات بواسطة CMVP ضمن حالة قديمة. تحتوي إصدارات iOS السابقة هذه على عمليات التحقق من صحة وحدة التشفير:

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

خلفية شهادة المعايير العامة (CC)

تشارك Apple بفعالية في تقييم iOS لكل إصدار رئيسي من نظام التشغيل. ولا يمكن إجراء التقييم إلا على نسخة نهائية من نظام التشغيل تم طرحها للجمهور. قبل iPadOS 13.1، كان يطلق مسمى iOS على iPadOS.

حالة شهادة المعايير العامة (CC)

يحتفظ مخطط الولايات المتحدة، الذي تديره NIAP، بقائمة من المنتجات قيد التقييم، وتشمل هذه القائمة المنتجات التي تخضع حاليًا للتقييم في الولايات المتحدة مع مختبر اختبار المعايير العامة (CCTL) المعتمد من NIAP والتي أكملت اجتماع انطلاق التقييم (أو ما يعادله) حيث تقبل إدارة CCEVS رسميًا المنتج قيد التقييم.

بعد اعتماد المنتجات، تُدرج NIAP الشهادات الصالحة حاليًا في قائمة المنتجات المتوافقة. وبعد عامين تتم مراجعة هذه الشهادات للتأكد من توافقها مع السياسة الراهنة للحفاظ على الضمان. بعد انتهاء تاريخ الحفاظ على الضمان، تنقل NIAP قائمة الشهادات إلى قائمة المنتجات المؤرشفة.

تسرد بوابة المعايير العامة الشهادات التي يمكن الاعتراف بها بشكل متبادل بموجب ترتيب الاعتراف بالمعايير العامة (CCRA). قد تحتفظ بوابة المعايير العامة (CC) بالمنتجات في قائمة المنتجات المعتمدة لمدة ٥ أعوام، ويتم الاحتفاظ بالسجلات بواسطة بوابة المعايير العامة (CC) في الشهادات المؤرشفة.

يوضح الجدول أدناه الشهادات التي يتم تقييمها حاليًا بواسطة المختبر، أو التي تم اعتمادها على أنها متوافقة مع المعايير العامة.

الحالة الحالية

تُجرَى حاليًا الاختبارات المعملية للتقييمات باستخدام NIAP لـ iOS 15. لحصول على أحدث المعلومات، انظر المنتجات قيد التقييم (NIAP) وقائمة المنتجات المتوافقة.

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: iOS 15 **تاريخالشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** —	**العنوان:** Apple iOS 15: أجهزة iPhone **ملفات تعريف الحماية:** أساسيات الجهاز الجوال (سيتم تأكيد وحدات PP-Modules)
نظام التشغيل: iOS 14 **تاريخالشهادة:** ١ - ٩ - ٢٠٢١	**معرف النظام:** ١١١٤٦ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple iOS 14: أجهزة iPhone **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، وحدة عميل VPN، وحدة PP لعملاء WLAN، عميل MDM EP
نظام التشغيل: iOS 13 **تاريخالشهادة:** ٦ - ١١ - ٢٠٢٠	**معرف النظام:** ١١٠٣٦ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple iOS 13 على iPhone **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، وحدة عميل VPN، وحدة EP لعملاء WLAN، عميل MDM EP

شهادات المعايير العامة المؤرشفة لـ iOS

تحتوي إصدارات iOS السابقة هذه على عمليات تقييم المعايير العامة. تتم أرشفتها بواسطة NIAP وفقًا لسياسة NIAP:

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: iOS 12 **تاريخالشهادة:** ١٤ - ٣ - ٢٠١٩	**معرف النظام:** ١.٩٣٧ **المستندات:** الهدف الأمني الإرشاد	**العنوان:** iPhone مثبت عليه iOS 12 **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، وحدة عميل VPN، عميل الشبكة المحلية اللاسلكية EP، عميل MDM EP
نظام التشغيل: iOS 11 **تاريخالشهادة:** ١٧ - ٧ - ٢٠١٨	**معرف النظام:** ١.٨٥١ **المستندات:** الهدف الأمني الإرشاد	**العنوان:** Apple iOS 11 **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، عميل الشبكة المحلية اللاسلكية EP، عميل MDM EP
نظام التشغيل: iOS 10 **تاريخالشهادة:** ٢٧ - ٧ - ٢٠١٧	**معرف النظام:** ١.٧٨٢ **المستندات:** الهدف الأمني، الإرشاد	**العنوان:** iOS 10.2 على أجهزة iPhone و iPad **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، عميل الشبكة المحلية اللاسلكية EP، عميل MDM EP
نظام التشغيل: iOS 10 **تاريخالشهادة:** ٢٧ - ٧ - ٢٠١٧	**معرف النظام:** ١.٧٩٢ **المستندات:** الهدف الأمني، الإرشاد	**العنوان:** عميل VPN لـ iOS 10.2 على iPhone و iPad **ملفات تعريف الحماية:** وحدةPP لعميل VPN
نظام التشغيل: iOS 9 **تاريخالشهادة:** ١٤ - ١٠ - ٢٠١٦	**معرف النظام:** ١.٧٢٥ **المستندات:** الهدف الأمني، الإرشاد	**العنوان:** iOS 9.3.2 مع عميل MDM **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، عميل MDM EP
نظام التشغيل: iOS 9 **تاريخالشهادة:** ١٣ - ١٠ - ٢٠١٦	**معرف النظام:** ١.٧١٤ **المستندات:** الهدف الأمني، الإرشاد	**العنوان:** عميل VPN لنظام التشغيل على iPhone و iPad **ملفات تعريف الحماية:** وحدة PP لعميل VPN
نظام التشغيل: iOS 9 **تاريخالشهادة:** ٢٨ - ١ - ٢٠١٦	**معرف النظام:** ١.٦٩٥ **المستندات:** الهدف الأمني، الإرشاد	**العنوان:** iOS 9 **ملفات تعريف الحماية:** أساسيات الجهاز الجوال

شهادات الأمن لـ iPadOS

خلفية شهادة iPadOS

تشارك Apple تشارك في التحقق من صحة أنظمة تشغيل Apple لكل إصدار رئيسي من نظام التشغيل، باستخدام ملفات تعريف حماية تعاونية مناسبة ومستويات أمن FIPS 140-3. لا يمكن إجراء التحقق من صحة التوافق إلا على نسخة الإصدار النهائية.

ملاحظة: في عام ٢٠١٩، تم تغيير اسم نظام التشغيل لأجهزة iPad إلى iPadOS. قبل iPadOS 13.1 ، كان يطلق مسمى iOS على iPadOS.

حالة عملية التحقق من صحة وحدة التشفير في iPadOS

يحتفظ برنامج التحقق من صحة وحدة التشفير (CMVP) بحالة التحقق من صحة وحدات التشفير ضمن الثلاث قوائم منفصلة اعتمادًا على حالتها الحالية:

- لكي يتم الإدراج في قائمة التنفيذ قيد الاختبار في CMVP، يجب أن يتعاقد المختبر مع Apple لتقديم الاختبار.
- بعد اكتمال الاختبار بواسطة المختبر، يكون المختبر قادرًا على التوصية بالتحقق من الصحة بواسطة CMVP، ودفع رسوم CMVP، ثم تُضاف الوحدة إلى قائمة الوحدات قيد المعالجة (MIP). تعمل قائمة الوحدات قيد المعالجة MIP على تتبع التقدّم المحرز في جهود التحقق من الصحة بواسطة CMVP في أربع مراحل:
  - **في انتظار المراجعة:** في انتظار تعيين مورد CMVP.
  - **قيد المراجعة:** تعمل موارد CMVP على تنفيذ أنشطة التحقق الخاصة بها.
  - **التنسيق:** يعمل المختبر و CMVP على حل أي مشكلات يتم العثور عليها.
  - **وضع اللمسات الأخيرة:** الأنشطة والإجراءات المتعلقة بإصدار الشهادة.
- بعد التحقّق من الصحة بواسطة CMVP، يتم منح الوحدات شهادة المطابقة وإضافتها إلى قائمة وحدات التشفير التي تم التحقق من صحتها. ويشمل ذلك:
  - الوحدات النمطية التي تم التحقق من صحتها والتي تم تمييزها على أنها نشطة.
  - بعد ٥ سنوات، يتم تمييز الوحدات النمطية على أنها قديمة.
  - إذا تم إلغاء شهادة الوحدة النمطية لسبب ما، فسيتم تمييزها على أنها مُلغاة.

في عام ٢٠٢٠، اعتمدت CMVP المعيار الدولي، ISO/IEC 19790، كأساس لمعيار FIPS 140-3.

شهادات FIPS 140-3

الحالة الحالية

أكملت مساحة المستخدم في iPadOS 14 (٢.٢.)، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

تخضع مساحة المستخدم في iPadOS 15 (٢.٢١)، ومساحة kernel، ومخزن المفاتيح الآمن للاختبارات المعملية. وهي مدرجة في قائمة التنفيذ قيد الاختبار.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** iPadOS 15 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** iPadOS 15 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع iPadOS 15 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14، M1) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع iPadOS 15 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14، M1) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** iPadOS 14 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** iPadOS 14 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع iPadOS 14 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14، M1) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع iPadOS 14 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A9-A14، M1) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣

شهادات FIPS 140-2

يوضح الجدول أدناه وحدات التشفير النمطية التي يتم اختبارها حاليًا والتي تم اختبارها بواسطة المختبر للتوافق مع FIPS 140-2.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢.٢١	**الشهادات:** ٣٨٥٦ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** iPadOS 13 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢.٢١	**الشهادات:** ٣٨٥٥ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v10.0 لـ ARM **نظام التشغيل:** iPadOS 13 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٥ - ٢ - ٢.٢١	**الشهادات:** ٣٨١١ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة تشفير مخزن المفاتيح الآمن Apple Corecrypto الإصدار v10.0 **نظام التشغيل:** sepOS الموزَّع مع iPadOS 13 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ٢٣ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v9.0 لـ ARM **نظام التشغيل:** iOS 12 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١١ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Corecrypto الإصدار v9.0 لـ ARM **نظام التشغيل:** iOS 12 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢.١٩	**الشهادات:** ٣٥٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v9.0 **نظام التشغيل:** sepOS الموزَّع مع iOS 12 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ٢٢ - ٥ - ٢.١٨، ٦ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** iOS 11 **النوع:** البرامج **المستوى الأمني:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ١٧ - ٥ - ٢.١٨، ٣ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v8.0 لـ ARM **نظام التشغيل:** iOS 11 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ١. - ٩ - ٢.١٩	**الشهادات:** ٣٢٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v1.0 **نظام التشغيل:** sepOS الموزَّع مع iOS 11 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٦ **تواريخ التحقق من الصحة:** ١ - ٢ - ٢.١٧	**الشهادات:** ٢٨٢٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple iOS Corecrypto Kernel الإصدار v7.0 **نظام التشغيل:** iOS 10 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٦ **تواريخ التحقق من الصحة:** ١ - ٢ - ٢.١٧	**الشهادات:** ٢٨٢٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple iOS Corecrypto Kernel الإصدار v7.0 **نظام التشغيل:** iOS 10 **النوع:** البرامج **المستوى الأمني:** ١

الإصدارات السابقة

وتُدرَج الإصدارات الأقدم من ٥ سنوات بواسطة CMVP ضمن حالة قديمة. تحتوي إصدارات iOS السابقة هذه على عمليات التحقق من صحة وحدة التشفير:

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

خلفية شهادة المعايير العامة (CC)

تشارك Apple بفعالية في تقييم iPadOS لكل إصدار رئيسي من نظام التشغيل. ولا يمكن إجراء التقييم إلا على نسخة نهائية من نظام التشغيل تم طرحها للجمهور.

حالة شهادة المعايير العامة (CC)

يحتفظ مخطط الولايات المتحدة، الذي تديره NIAP، بقائمة من المنتجات قيد التقييم، وتشمل هذه القائمة المنتجات التي تخضع حاليًا للتقييم في الولايات المتحدة مع مختبر اختبار المعايير العامة (CCTL) المعتمد من NIAP والتي أكملت اجتماع انطلاق التقييم (أو ما يعادله) حيث تقبل إدارة CCEVS رسميًا المنتج قيد التقييم.

بعد اعتماد المنتجات، تُدرج NIAP الشهادات الصالحة حاليًا في قائمة المنتجات المتوافقة. وبعد عامين تتم مراجعة هذه الشهادات للتأكد من توافقها مع السياسة الراهنة للحفاظ على الضمان. بعد انتهاء تاريخ الحفاظ على الضمان، تنقل NIAP قائمة الشهادات إلى قائمة المنتجات المؤرشفة.

تسرد بوابة المعايير العامة الشهادات التي يمكن الاعتراف بها بشكل متبادل بموجب اتفاقية الاعتراف بالمعايير العامة (CCRA). قد تحتفظ بوابة المعايير العامة (CC) بالمنتجات في قائمة المنتجات المعتمدة لمدة ٥ أعوام، ويتم الاحتفاظ بالسجلات بواسطة بوابة المعايير العامة (CC) في الشهادات المؤرشفة.

يوضح الجدول أدناه الشهادات التي يتم تقييمها حاليًا بواسطة المختبر، أو التي تم اعتمادها على أنها متوافقة مع المعايير العامة.

الحالة الحالية

تُجرَى حاليًا الاختبارات المعملية للتقييمات باستخدام NIAP لـ iPadOS 15. لحصول على أحدث المعلومات، انظر المنتجات قيد التقييم (NIAP) وقائمة المنتجات المتوافقة.

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: iPadOS 15 **تاريخالشهادة:** ١٤ - ٣ - ٢٠١٩	**معرف النظام:** — **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** iPad مثبت عليه iOS 12 **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، وحدة عميل VPN، عميل الشبكة المحلية اللاسلكية EP، عميل MDM EP
نظام التشغيل: iPadOS 14 **تاريخالشهادة:** ١ - ٩ - ٢٠٢١	**معرف النظام:** ١١١٤٧ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple iPadOS 14: أجهزة iPad **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، وحدة عميل VPN، عميل الشبكة المحلية اللاسلكية EP، عميل MDM EP

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: iPadOS 13 **تاريخالشهادة:** ٦ - ١١ - ٢٠٢٠	**معرف النظام:** ١١.٣٦ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** iPadOS 13 على أجهزة iPad الجوالة **ملفات تعريف الحماية:** أساسيات الجهاز الجوال، وحدة عميل VPN، عميل الشبكة المحلية اللاسلكية EP، عميل MDM EP

الإصدارات السابقة

تحتوي إصدارات iOS السابقة هذه على عمليات تقييم المعايير العامة. تتم أرشفتها بواسطة NIAP وفقًا لسياسة NIAP:

- iOS 12 (معرف النظام: ١.٩٣٧)
- iOS 11 (معرف النظام: ١.٨٥١)
- iOS 10 (معرف النظام: ١.٧٧٨٢، ١.٧٩٢)
- iOS 9 (معرف النظام: ١.٧٢٥، ١.٧١٤، ١.٦٩٥)

شهادات الأمن لـ macOS

خلفية شهادة macOS

تشارك Apple تشارك في التحقق من صحة أنظمة تشغيل Apple لكل إصدار رئيسي من نظام التشغيل، باستخدام ملفات تعريف حماية تعاونية مناسبة ومستويات أمن FIPS 140-3. لا يمكن إجراء التحقق من صحة التوافق إلا على نسخة الإصدار النهائية.

حالة عملية التحقق من صحة وحدة التشفير في macOS

يحتفظ برنامج التحقق من صحة وحدة التشفير (CMVP) بحالة التحقق من صحة وحدات التشفير ضمن الثلاث قوائم منفصلة اعتمادًا على حالتها الحالية:

- لكي يتم الإدراج في قائمة التنفيذ قيد الاختبار في CMVP، يجب أن يتعاقد المختبر مع Apple لتقديم الاختبار.
- بعد اكتمال الاختبار بواسطة المختبر، يكون المختبر قادرًا على التوصية بالتحقق من الصحة بواسطة CMVP، ودفع رسوم CMVP، ثم تُضاف الوحدة إلى قائمة الوحدات قيد المعالجة (MIP). تعمل قائمة الوحدات قيد المعالجة MIP على تتبع التقدّم المحرز في جهود التحقق من الصحة بواسطة CMVP في أربع مراحل:
- **في انتظار المراجعة**: في انتظار تعيين مورد CMVP.
- **قيد المراجعة**: تعمل موارد CMVP على تنفيذ أنشطة التحقق الخاصة بها.
- **التنسيق**: يعمل المختبر و CMVP على حل أي مشكلات يتم العثور عليها.
- **وضع اللمسات الأخيرة**: الأنشطة والإجراءات المتعلقة بإصدار الشهادة.
- بعد التحقّق من الصحة بواسطة CMVP، يتم منح الوحدات شهادة المطابقة وإضافتها إلى قائمة وحدات التشفير التي تم التحقق من صحتها. ويشمل ذلك:
- الوحدات النمطية التي تم التحقق من صحتها والتي تم تمييزها على أنها نشطة.
- بعد ٥ سنوات، يتم تمييز الوحدات النمطية على أنها قديمة.
- إذا تم إلغاء شهادة الوحدة النمطية لسبب ما، فسيتم تمييزها على أنها مُلغاة.

في عام ٢٠٢٠، اعتمدت CMVP المعيار الدولي، ISO/IEC 19790، كأساس لمعيار FIPS 140-3.

بالنسبة لأجهزة كمبيوتر Apple Mac، يوضح الجدول أدناه وحدات التشفير التي تنطبق على تقنية Mac.

وحدة التشفير	أجهزة كمبيوتر Macالمزودة بسيليكون Apple	أجهزة كمبيوتر Macالمزودة برقاقة Apple T2 أمنية	أجهزة كمبيوتر Macالمستندة إلى Intelولا تحتوي على رقاقة Apple T2الأمنية
مساحة مستخدم سيليكون Apple	✓		
Kernel سيليكون Apple	✓		
مساحة مستخدم Intel		✓	✓
Intel Kernel		✓	✓
تخزين المفاتيح الآمن	✓	✓	

شهادات FIPS 140-3

في عام ٢٠٢٠، أصدرت Apple أجهزة كمبيوتر Mac المستندة إلى سيليكون Apple. يشار إلى إمكانية تطبيق وحدات التشفير على أجهزة كمبيوتر رقاقات Apple أو أجهزة كمبيوتر Mac المستندة إلى Intel في عمود "معلومات الوحدة النمطية" في الجدول أدناه.

ملاحظة: يتم تضمين رقائق Apple T2 الأمنية في العديد من أجهزة كمبيوتر Mac المستندة إلى Intel. للحصول على معلومات حول شهادات رقاقة T2، انظر شهادات الأمن لشريحة Apple T2 الأمنية.

عميل macOS ssh

يمكن تكوين OpenSSH لاستخدام وحدات FIPS 140-3 التي تم التحقق من صحتها لخوارزميات FIPS 140-3 المحددة. يمكن للمؤسسات تشغيل مُثبِّت موقَّع وموثق ومتاح من Apple باستخدام كلمة السر FIPS140Mode. يضع المُثبِّت ملفين على جهاز Mac:

- fips_ssh_config: يتم وضعه في /private/etc/ssh/ssh_config.d/
- fips_sshd_config: يتم وضعه في /private/etc/ssh/sshd_config.d/

يستخدم macOS بعد ذلك هذه الملفات لتقييد الشفرات المتاحة لـ OpenSSH على تلك التي تم التحقق من صحتها من قبل NIST والتأكد من أن عميل OpenSSH يستخدم وحدة التشفير التي يوفرها النظام الأساسي والتي تم التحقق من صحتها. يمكن للمسؤولين أيضًا إنشاء ملفاتهم الخاصة. لمزيد من المعلومات، انظر صفحة apple_ssh_and_fips في macOS 12.0.1 أو أحدث.

الحالة الحالية

أكملت مساحة المستخدم في macOS 11 Big Sur، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

تخضع مساحة المستخدم في macOS 12 Monterey، ومساحة kernel، ومخزن المفاتيح الآمن للاختبارات المعملية. وهي مدرجة في قائمة التنفيذ قيد الاختبار.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢٠٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** macOS 12 Monterey على رقاقات Apple **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢٠٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** macOS 12 Monterey على رقاقات Apple **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢٠٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** macOS 12 Monterey على Intel **البيئة:** Intel، المتسخدم، البرامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢٠٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** macOS 12 Monterey على Intel **البيئة:** Intel، Kernel، البرامج **النوع:** البرامج **المستوى الأمني:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢٠٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** sepOS الموزَّع مع macOS 12 Monterey على رقاقات Apple، sepOS الموزَّع مع macOS 12 Monterey على Intel مع T2 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (M1 و T2) **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢٠٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12.0 **نظام التشغيل:** sepOS الموزَّع مع macOS 12 Monterey على رقاقات Apple **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (M1) **المستوى الأمني:** ٢ **المستوى الأمني المادي:** ٣
تاريخ إصدار نظام التشغيل: ٢٠٢٠ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** macOS 11 Big Sur على Intel **البيئة:** Intel، المتسخدم، البرامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢٠٢٠ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** macOS 11 Big Sur على Intel **البيئة:** Intel، Kernel، البرامج **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢٠٢٠ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** macOS 11 Big Sur على رقاقات Apple **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢٠٢٠. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** macOS 11 Big Sur على رقاقات Apple **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني:** ا
تاريخ إصدار نظام التشغيل: ٢٠٢٠. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع macOS 11 Big Sur على رقاقات Apple، sepOS الموزَّع مع macOS 11 Big Sur على Intel **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (M1) **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢٠٢٠. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع macOS 11 Big Sur على رقاقات Apple **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (M1) **المستوى الأمني:** ٢ **المستوى الأمني المادي:** ٣

شهادات FIPS 140-2

يوضح الجدول أدناه وحدات التشفير النمطية التي يتم اختبارها حاليًا والتي تم اختبارها بواسطة المختبر للتوافق مع FIPS 140-2.

أكملت مساحة المستخدم في macOS 10.15 Catalina، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

ملاحظة: يتم تضمين رقائق Apple T2 الأمنية في العديد من أجهزة كمبيوتر Mac المستندة إلى Intel. للحصول على معلومات حول شهادات رقاقة T2، انظر شهادات الأمن لشريحة Apple T2 الأمنية.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٤ - ٣ - ٢.٢١	**الشهادات:** ٣٨٥٩ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مساحة مستخدم Apple Corecrypto لـ Intel (ccv10) **نظام التشغيل:** macOS 10.15 Catalina **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٤ - ٣ - ٢.٢١	**الشهادات:** ٣٨٥٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v10.0 لـ Intel (ccv10) **نظام التشغيل:** macOS 10.15 Catalina **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٢ - ٤ - ٢.١٩	**الشهادات:** ٣٤٠٢ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v9.0 لـ Intel **نظام التشغيل:** macOS 10.14 Mojave **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٢ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣١ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v9.0 لـ Intel **نظام التشغيل:** macOS 10.14 Mojave **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٢٢ - ٣ - ٢.١٨	**الشهادات:** ٣١٥٥ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ Intel **نظام التشغيل:** macOS 10.13 High Sierra **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٢٢ - ٣ - ٢.١٨	**الشهادات:** ٣١٥٦ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v8.0 لـ Intel **نظام التشغيل:** macOS 10.13 High Sierra **النوع:** البرامج **المستوى الأمني:** ١

الإصدارات السابقة

تحتوي إصدارات OS X و macOS السابقة هذه على عمليات التحقق من صحة وحدة التشفير. ويتم إدراج الإصدارات الأقدم من 5 سنوات بواسطة CMVP ضمن حالة قديمة:

- 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

خلفية شهادة المعايير العامة (CC)

تشارك Apple بفعالية في تقييم macOS لكل إصدار رئيسي من نظام التشغيل. ولا يمكن إجراء التقييم إلا على نسخة نهائية من نظام التشغيل تم طرحها للجمهور.

حالة شهادة المعايير العامة (CC)

يحتفظ مخطط الولايات المتحدة، الذي تديره NIAP، بقائمة من المنتجات قيد التقييم، وتشمل هذه القائمة المنتجات التي تخضع حاليًا للتقييم في الولايات المتحدة مع مختبر اختبار المعايير العامة (CCTL) المعتمد من NIAP والتي أكملت اجتماع انطلاق التقييم (أو ما يعادله) حيث تقبل إدارة CCEVS رسميًا المنتج قيد التقييم.

بعد اعتماد المنتجات، تُدرج NIAP الشهادات الصالحة حاليًا في قائمة المنتجات المتوافقة. وبعد عامين تتم مراجعة هذه الشهادات للتأكد من توافقها مع السياسة الراهنة للحفاظ على الضمان. بعد انتهاء تاريخ الحفاظ على الضمان، تنقل NIAP قائمة الشهادات إلى قائمة المنتجات المؤرشفة.

تسرد بوابة المعايير العامة الشهادات التي يمكن الاعتراف بها بشكل متبادل بموجب اتفاقية الاعتراف بالمعايير العامة (CCRA). قد تحتفظ بوابة المعايير العامة (CC) بالمنتجات في قائمة المنتجات المعتمدة لمدة ٥ أعوام، ويتم الاحتفاظ بالسجلات بواسطة بوابة المعايير العامة (CC) في الشهادات المؤرشفة.

يوضح الجدول أدناه الشهادات التي يتم تقييمها حاليًا بواسطة المختبر، أو التي تم اعتمادها على أنها متوافقة مع المعايير العامة.

الحالة الحالية

تُجرَى حاليًا التقييمات باستخدام NIAP لـ macOS 11 و macOS 12 باستخدام نظام التشغيل للأغراض العامة وملفات تعريف الحماية للتشفير الكامل للقرص (FDE) (AA و EE).

لحصول على أحدث المعلومات، انظر المنتجات قيد التقييم (NIAP) وقائمة المنتجات المتوافقة.

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: macOS 12 Monterey **تاريخ الشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** —	**العنوان:** Apple FileVault 2 مع macOS 12 Monterey **ملفات تعريف الحماية:** _CPP_FDE_ AA_V2.0E, CPP_FDE_EE_V2.0E (سيتم تأكيد وحدات PPs)
نظام التشغيل: macOS 12 Monterey **تاريخ الشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** —	**العنوان:** macOS 12 Monterey **ملفات تعريف الحماية:** PP_OS_V4.21 (سيتم تأكيد وحدات PPs)
نظام التشغيل: macOS 11 Big Sur **تاريخ الشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple FileVault 2 مع macOS 11 Big Sur **ملفات تعريف الحماية:** _CPP_FDE AA_V2.0E, CPP_FDE_EE_V2.0E
نظام التشغيل: macOS 11 Big Sur **تاريخ الشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple macOS 11 Big Sur **ملفات تعريف الحماية:** PP_OS_V4.21
نظام التشغيل: macOS 10.15 Catalina **تاريخ الشهادة:** ٢٩ - ٤ - ٢٠٢١	**معرف النظام:** ١١.٧٨ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple FileVault 2 على أجهزة كمبيوتر T2 المثبَّت عليها macOS 10.15 Catalina **ملفات تعريف الحماية:** _CPP_FDE AA_V2.0E, CPP_FDE_EE_V2.0E

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: macOS 10.15 Catalina **تاريخ الشهادة:** ٢٣ - ٩ - ٢٠٢٠	**معرف النظام:** ١١.٧٧ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** macOS 10.15 Catalina **ملفات تعريف الحماية:** PP_OS_V4.21

شهادات الأمن لـ tvOS

خلفية شهادة tvOS

تشارك Apple بفعالية في التحقق من صحة وحدات التشفير المرتبطة بكل إصدار رئيسي من tvOS. لا يمكن إجراء التحقق من صحة التوافق إلا على نسخة الإصدار النهائية.

حالة عملية التحقق من صحة وحدة التشفير في tvOS

يحتفظ برنامج التحقق من صحة وحدة التشفير (CMVP) بحالة التحقق من صحة وحدات التشفير ضمن الثلاث قوائم منفصلة اعتمادًا على حالتها الحالية:

- لكي يتم الإدراج في قائمة التنفيذ قيد الاختبار في CMVP، يجب أن يتعاقد المختبر معApple لتقديم الاختبار.
- بعد اكتمال الاختبار بواسطة المختبر، يكون المختبر قادرًا على التوصية بالتحقق من الصحة بواسطة CMVP، ودفع رسوم CMVP، ثم تُضاف الوحدة إلى قائمة الوحدات قيد المعالجة (MIP). تعمل قائمة الوحدات قيد المعالجة MIP على تتبع التقدّم المحرز في جهود التحقق من الصحة بواسطة CMVP في أربع مراحل:
  - **في انتظار المراجعة**: في انتظار تعيين مورد CMVP.
  - **قيد المراجعة**: تعمل موارد CMVP على تنفيذ أنشطة التحقق الخاصة بها.
  - **التنسيق**: يعمل المختبر و CMVP على حل أي مشكلات يتم العثور عليها.
  - **وضع اللمسات الأخيرة**: الأنشطة والإجراءات المتعلقة بإصدار الشهادة.
- بعد التحقّق من الصحة بواسطة CMVP، يتم منح الوحدات شهادة المطابقة وإضافتها إلى قائمة وحدات التشفير التي تم التحقق من صحتها. ويشمل ذلك:
  - الوحدات النمطية التي تم التحقق من صحتها والتي تم تمييزها على أنها نشطة.
  - بعد ٥ سنوات، يتم تمييز الوحدات النمطية على أنها قديمة.
  - إذا تم إلغاء شهادة الوحدة النمطية لسبب ما، فسيتم تمييزها على أنها مُلغاة.

في عام ٢٠٢٠، اعتمدت CMVP المعيار الدولي، ISO/IEC 19790، كأساس لمعيار FIPS 140-3.

شهادات FIPS 140-3

الحالة الحالية

أكملت مساحة المستخدم في tvOS 14 (٢.٢.)، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

تخضع مساحة المستخدم في tvOS 15 (٢.٢١)، ومساحة kernel، ومخزن المفاتيح الآمن للاختبارات المعملية. وهي مدرجة في قائمة التنفيذ قيد الاختبار.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** tvOS 15 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** tvOS 15 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع tvOS 15 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A10، A12) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** tvOS 14 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** tvOS 14 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypt الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع tvOS 14 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (A10، A12) **المستوى الأمني العام:** ٢

شهادات FIPS 140-2

يوضح الجدول أدناه وحدات التشفير النمطية التي يتم اختبارها حاليًا والتي تم اختبارها بواسطة المختبر للتوافق مع FIPS 140-2.

أكملت مساحة المستخدم في tvOS 13 (٢.١٩)، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢٠٢١	**الشهادات:** ٣٨٥٦ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** tvOS 13 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٢٣ - ٣ - ٢٠٢١	**الشهادات:** ٣٨٥٥ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypt Kernel الإصدار v10.0 لـ ARM **نظام التشغيل:** tvOS 13 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٥ - ٢ - ٢٠٢١	**الشهادات:** ٣٨١١ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة تشفير مخزن المفاتيح الآمن من Appleالإصدار v1.0 **نظام التشغيل:** sepOS الموزَّع مع tvOS 13 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ٢٣ - ٤ - ٢٠١٩	**الشهادات:** ٣٤٣٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypt Kernel الإصدار v9.0 لـ ARM **نظام التشغيل:** tvOS 12 **النوع:** البرامج **المستوى الأمني:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١١ - ٤ - ٢.١٩	**الشهادات:** ٣٤٣٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Corecrypto الإصدار v9.0 لـ ARM **نظام التشغيل:** tvOS 12 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢.١٩	**الشهادات:** ٣٥٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v9.0 **نظام التشغيل:** sepOS الموزَّع مع tvOS 12 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ٢٢ - ٥ - ٢.١٨، ٦ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** tvOS 11 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ١٧ - ٥ - ٢.١٨، ٣ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v8.0 لـ ARM **نظام التشغيل:** tvOS 11 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢.١٩	**الشهادات:** ٣٢٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v1.0 **نظام التشغيل:** sepOS الموزَّع مع tvOS 11 **النوع:** المكونات المادية **المستوى الأمني:** ٢

شهادات الأمن لـ watchOS

خلفية شهادة watchOS

تشارك Apple بفعالية في التحقق من صحة وحدات التشفير المرتبطة بكل إصدار رئيسي من watchOS. لا يمكن إجراء التحقق من صحة التوافق إلا على نسخة الإصدار النهائية.

حالة عملية التحقق من صحة وحدة التشفير في watchOS

يحتفظ برنامج التحقق من صحة وحدة التشفير (CMVP) بحالة التحقق من صحة وحدات التشفير ضمن الثلاث قوائم منفصلة اعتمادًا على حالتها الحالية:

- لكي يتم الإدراج في قائمة التنفيذ قيد الاختبار في CMVP، يجب أن يتعاقد المختبر مع Apple لتقديم الاختبار.
- بعد اكتمال الاختبار بواسطة المختبر، يكون المختبر قادرًا على التوصية بالتحقق من الصحة بواسطة CMVP، ودفع رسوم CMVP، ثم تُضاف الوحدة إلى قائمة الوحدات قيد المعالجة (MIP). تعمل قائمة الوحدات قيد المعالجة MIPعلى تتبع التقدّم المحرز في جهود التحقق من الصحة بواسطة CMVP في أربع مراحل:
  - **في انتظار المراجعة**: في انتظار تعيين مورد CMVP.
  - **قيد المراجعة**: تعمل موارد CMVP على تنفيذ أنشطة التحقق الخاصة بها.
  - **التنسيق**: يعمل المختبر و CMVP على حل أي مشكلات يتم العثور عليها.
  - **وضع اللمسات الأخيرة**: الأنشطة والإجراءات المتعلقة بإصدار الشهادة.
- بعد التحقّق من الصحة بواسطة CMVP، يتم منح الوحدات شهادة المطابقة وإضافتها إلى قائمة وحدات التشفير التي تم التحقق من صحتها. ويشمل ذلك:
  - الوحدات النمطية التي تم التحقق من صحتها والتي تم تمييزها على أنها نشطة.
  - بعد ٥ سنوات، يتم تمييز الوحدات النمطية على أنها قديمة.
  - إذا تم إلغاء شهادة الوحدة النمطية لسبب ما، فسيتم تمييزها على أنها مُلغاة.

في عام ٢٠٢٠، اعتمدت CMVP المعيار الدولي، ISO/IEC 19790، كأساس لمعيار FIPS 140-3.

شهادات FIPS 140-3

الحالة الحالية

أكملت مساحة المستخدم في watchOS 7 (٧.٢.٠)، ومساحة kernel، ومخزن المفاتيح الآمن الاختبارات المعملية وقد أوصى بها المختبر ليتم التحقق من صحتها بواسطة CMVP. وهي مدرجة في قائمة الوحدات قيد المعالجة.

تخضع مساحة المستخدم في watchOS 8 (٨.٢.١)، ومساحة kernel، ومخزن المفاتيح الآمن للاختبارات المعملية. وهي مدرجة في قائمة التنفيذ قيد الاختبار.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٨.٢.١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** watchOS 8 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٨.٢.١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** watchOS 8 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٨.٢.١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع watchOS 8 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (S3، S4، S5، S6) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٨.٢.١ **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v12 **نظام التشغيل:** sepOS الموزَّع مع watchOS 8 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (S6) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** watchOS 7 **البيئة:** سيليكون Apple، المستخدم، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** watchOS 7 **البيئة:** سيليكون Apple، Kernel، البرنامج **النوع:** البرامج **المستوى الأمني العام:** ١
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع watchOS 7 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (S3، S4، S5، S6) **المستوى الأمني العام:** ٢
تاريخ إصدار نظام التشغيل: ٢.٢. **تواريخ التحقق من الصحة:** —	**الشهادات:** غير معتمدة بعد **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto الإصدار v11.1 **نظام التشغيل:** sepOS الموزَّع مع watchOS 7 **البيئة:** رقاقات Apple، مخزن المفاتيح الآمن، المكونات المادية **النوع:** المكونات المادية (S6) **المستوى الأمني العام:** ٢ **المستوى الأمني المادي:** ٣

شهادات FIPS 140-2

يوضح الجدول أدناه وحدات التشفير النمطية التي يتم اختبارها حاليًا والتي تم اختبارها بواسطة المختبر للتوافق مع FIPS 140-2.

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** —	**الشهادات:** ٣٨٥٦ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** watchOS 6 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** —	**الشهادات:** ٣٨٥٥ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v10.0 لـ ARM **نظام التشغيل:** watchOS 6 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٩ **تواريخ التحقق من الصحة:** ٥ - ٢ - ٢٠٢١	**الشهادات:** ٣٨١١ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة تشفير مخزن المفاتيح الآمن من Apple الإصدار v1.0 **نظام التشغيل:** sepOS الموزَّع مع watchOS 6 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ٢٣ - ٤ - ٢٠١٩	**الشهادات:** ٣٤٣٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v9.0 لـ ARM **نظام التشغيل:** watchOS 5 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١١ - ٤ - ٢٠١٩	**الشهادات:** ٣٤٣٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Corecrypto الإصدار v9.0 لـ ARM **نظام التشغيل:** watchOS 5 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٨ **تواريخ التحقق من الصحة:** ١٠ - ٩ - ٢٠١٩	**الشهادات:** ٣٥٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v9.0 **نظام التشغيل:** sepOS الموزَّع مع watchOS 5 **النوع:** المكونات المادية **المستوى الأمني:** ٢
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢٠١٨، ٢٢ - ٥ - ٢٠١٨، ٦ - ٧ - ٢٠١٨	**الشهادات:** ٣١٤٨ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة مستخدم Apple Core Crypto الإصدار v8.0 لـ ARM **نظام التشغيل:** watchOS 4 **النوع:** البرامج **المستوى الأمني:** ١

التواريخ	الشهادات /المستندات	معلومات الوحدة النمطية
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ٩ - ٣ - ٢.١٨، ١٧ - ٥ - ٢.١٨، ٣ - ٧ - ٢.١٨	**الشهادات:** ٣١٤٧ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** وحدة Apple Corecrypto Kernel الإصدار v8.0 لـ ARM **نظام التشغيل:** watchOS 4 **النوع:** البرامج **المستوى الأمني:** ١
تاريخ إصدار نظام التشغيل: ٢.١٧ **تواريخ التحقق من الصحة:** ١. - ٩ - ٢.١٩	**الشهادات:** ٣٢٢٣ **المستندات:** الشهادة سياسة الأمن إرشادات مسؤول التشفير	**العنوان:** Apple Secure Key Store Cryptographic Module v1.0 **نظام التشغيل:** sepOS الموزَّع مع watchOS 4 **النوع:** المكونات المادية **المستوى الأمني:** ٢

شهادات أمن البرامج

نظرة عامة على شهادات أمن البرامج في Apple

تحتفظ Apple بشهادات التحقق من صحة التوافق مع معيار معالجة المعلومات الفيدرالية 3-/2-140 (FIPS) للبرامج الثابتة الخاصة بـ sepOS و T2 بالإضافة إلى الشهادات الأخرى. تبدأ Apple **بالكتل البرمجية الإنشائية للشهادات** التي تنطبق على نطاق واسع عبر أنظمة أساسية متعددة عند الحاجة. الكتلة البرمجية الإنشائية الأولى هي التحقق من صحة التشفير المستخدم لعمليات نشر وحدة تشفير البرامج والمكونات المادية داخل أنظمة التشغيل المطوَّرة من Apple. والكتلة البرمجية الإنشائية الثانية هي شهادة Secure Enclave، المضمنة في العديد من أجهزة Apple. والثالثة هي شهادة Secure Element (SE) الموجودة في أجهزة Apple التي تحتوي على Touch ID والأجهزة التي تحتوي على Face ID. وتشكّل الكتل البرمجية الإنشائية لشهادة المكونات المادية هذه أساسًا لشهادات أمن النظام الأساسي الأوسع.

شهادات المنتج: المعايير العامة (ISO/IEC 15408)

تعد المعايير العامة (ISO/IEC 15408) معيارًا تستخدمه العديد من المؤسسات كأساس لإجراء تقييمات الأمن لمنتجات تقنية المعلومات.

بالنسبة للشهادات التي قد يتم الاعتراف بها بشكل متبادل بموجب اتفاقية الاعتراف بالمعايير العامة الدولية (CCRA)، انظر بوابة المعايير العامة. يمكن أيضًا استخدام مقاييس المعايير العامة خارج CCRA بواسطة مخططات التحقق المحلية والخاصة. في أوروبا، يخضع الاعتراف المتبادل لاتفاقية SOG-IS وكذلك CCRA.

الهدف، كما أوضح مجتمع المعايير العامة، هو تأسيس مجموعة من المعايير الأمنية المعتمدة دوليًا لتوفير تقييم واضح وموثوق للقدرات الأمنية لمنتجات تقنية المعلومات. ومن خلال توفير تقييم مستقل لقدرة المنتج على تلبية المعايير الأمنية، تمنح شهادة المعايير العامة للعملاء ثقة أكبر في أمن منتجات تقنية المعلومات وتؤدي إلى اتخاذ قرارات أكثر استنارة.

ومع اتفاقية الاعتراف بالمعايير العامة (CCRA)، اتفقت الدول الأعضاء على الاعتراف بشهادة منتجات تقنية المعلومات بمستوى الثقة ذاته. التقييمات المطلوبة قبل الحصول على الشهادة واسعة النطاق وتشمل:

- ملفات تعريف الحماية (PPs)
- الأهداف الأمنية (STs)
- المتطلبات الوظيفية الأمنية (SFRs)
- متطلبات ضمان الأمن (SAR)
- مستويات ضمان التقييم (EALs)

ملفات تعريف الحماية (PPs)، عبارة عن مستندات تحدد متطلبات الأمن لفئة من أنواع الأجهزة مثل التنقل، وتُستخدم لتوفير إمكانية المقارنة بين تقييمات منتجات تكنولوجيا المعلومات ضمن نفس الفئة. وتستمر عضوية CCRA جنبًا إلى جنب مع قائمة متزايدة من ملفات تعريف الحماية (PPs) المعتمدة في النمو على أساس سنوي. ويسمح هذا الترتيب لمطور المنتج بالمطالبة بشهادة واحدة بموجب أي من أنظمة تفويض الشهادات وطلب الاعتراف بها من قِبل أيٍ من المُوقِّعين المستهلكين للشهادة.

تحدد الأهداف الأمنية (STs) **ما** سيتم تقييمه عند اعتماد أحد منتجات تكنولوجيا المعلومات. تتم ترجمة الأهداف الأمنية (STs) إلى **متطلبات وظيفية أمنية** (SFRs) أكثر تحديدًا، تُستخدم لتقييم الأهداف الأمنية (STs) بمزيد من التفصيل.

كما تتضمن المعايير العامة (CC) **متطلبات ضمان الأمن**. أحد المقاييس الشائعة هو **مستوى ضمان التقييم** (EAL). تجمع مستويات ضمان التقييم (EALs) معًا مجموعات متطلبات ضمان الأمن (SARs) التي تحدث بشكل متكرر ويمكن تحديدها في ملفات تعريف الحماية (PPs) والأهداف الأمنية (STs) لدعم إمكانية للمقارنة.

تمت أرشفة العديد من ملفات تعريف الحماية (PPs) الأقدم ويتم استبدالها بملفات تعريف الحماية (PPs) المستهدفة، والتي يتم تطويرها للتركيز على حلول وبيئات محددة. وفي إطار الجهود المتضافرة الرامية إلى ضمان استمرار الاعتراف المتبادل بين جميع أعضاء CCRA، تم تأسيس المجتمعات الفنية الدولية (iTCs) لتطوير وصيانة ملفات تعريف الحماية التعاونية (cPPs)، والتي يتم تطويرها منذ البداية بمشاركة من الأنظمة المُوقِّعة على CCRA. وتواصل الجهات المعنية جهودها المبذولة لتطوير ملفات تعريف الحماية (PPs) المستهدفة لمجموعات المستخدمين وترتيبات الاعتراف المتبادلة بخلاف CCRA.

بدأت Apple في السعي للحصول على الشهادات بموجب CCRA المُحدّث مع cPPs المحددة ابتداءً من أوائل عام 2015. ومنذ ذلك الحين حصلت Apple على شهادات المعايير العامة لكل إصدار iOS رئيسي ووسَّعت التغطية لتشمل الضمان الأمني المقدَّم من ملفات تعريف الحماية (PPs) الجديدة.

تلعب Apple دورًا فعالاً داخل المجتمعات التقنية التي تركز على تقييم تقنيات أمن أجهزة الجوال. ويشمل ذلك المجتمعات الفنية الدولية (iTCs) المسؤولة عن تطوير وتحديث ملفات تعريف الحماية التعاونية (cPPs). وتواصل Apple تقييم الشهادات ومعالجتها وفقًا لملفات تعريف PPs و cPPs الحالية.

يتم تنفيذ شهادات أنظمة Apple الأساسية لأسواق أمريكا الشمالية بشكل عام مع شراكة أمن المعلومات الوطني (NIAP) التي تحتفظ بقائمة من المشاريع قيد التقييم حاليًا ولكن لم يتم اعتمادها بعد.

بالإضافة إلى شهادات الأنظمة الأساسية العامة المدرجة، تم إصدار شهادات أخرى لإثبات متطلبات أمن معينة لبعض الأسواق.

شهادات الأمن في تطبيقات Apple

خلفية شهادة تطبيقات Apple

تشارك Apple بفعالية في شهادات الأمن الخاصة بتطبيقات Apple باستخدام ملفات تعريف حماية المعايير العامة (PPs) المناسبة. وتستند هذه التقييمات إلى شهادات المكونات المادية وأنظمة التشغيل التي حصلت عليها Apple.

في عام ٢٠١٨، بدأت Apple إجراء تقييمات أمنية للتطبيقات الرئيسية المُثبّتة على iOS 11 باستخدام تطبيقي متصفح Safari وجهات الاتصال. وقد واصلت Apple إجراء هذه التقييمات على التطبيقات المُثبّتة على iOS 12 و iOS 13 و iPadOS 13.1. في عام ٢٠٢١، أُضيفت تغطية للتطبيقات التي تعمل على macOS 11.

حالة شهادات صحة وحدة التشفير

تُستخدم تطبيقات Apple المدرجة هنا وحدات التشفير لنظام التشغيل المطبق. لمزيد من المعلومات، انظر شهادات الأمن لـ iOS وشهادات الأمن لـ iPadOS وشهادات الأمن لـ macOS.

حالة شهادة المعايير العامة (CC)

يحتفظ مخطط الولايات المتحدة، الذي تديره NIAP، بقائمة من المنتجات قيد التقييم، وتشمل هذه القائمة المنتجات التي تخضع حاليًا للتقييم في الولايات المتحدة مع مختبر اختبار المعايير العامة (CCTL) المعتمد من NIAP والتي أكملت اجتماع انطلاق التقييم (أو ما يعادله) حيث تقبل إدارة CCEVS رسميًا المنتج قيد التقييم.

بعد اعتماد المنتجات، تُدرج NIAP الشهادات الصالحة حاليًا في قائمة المنتجات المتوافقة. وبعد عامين تتم مراجعة هذه الشهادات للتأكد من توافقها مع السياسة الراهنة للحفاظ على الضمان. بعد انتهاء تاريخ الحفاظ على الضمان، تنقل NIAP قائمة الشهادات إلى قائمة المنتجات المؤرشفة.

تسرد بوابة المعايير العامة الشهادات التي يمكن الاعتراف بها بشكل متبادل بموجب اتفاقية الاعتراف بالمعايير العامة (CCRA). قد تحتفظ بوابة المعايير العامة (CC) بالمنتجات في قائمة المنتجات المعتمدة لمدة ٥ أعوام، ويتم الاحتفاظ بالسجلات بواسطة بوابة المعايير العامة (CC) في الشهادات المؤرشفة.

يوضح الجدول أدناه الشهادات التي يتم تقييمها حاليًا بواسطة المختبر، أو التي تم اعتمادها على أنها متوافقة مع المعايير العامة.

الحالة الحالية

- التقييمات مع NIAP التي تم نشرها على أنها جارية مدرجة في المنتجات قيد التقييم (NIAP).
- التقييمات التي اكتملت وتم التحقق من صحتها مدرجة في قائمة NIAP المتوافقة مع المنتج.

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: macOS 11 Big Sur **تاريخ الشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** macOS 11 Big Sur: جهات الاتصال **ملفات تعريف الحماية:** PP لتطبيق ،SW EP لمتصفحات الويب
نظام التشغيل: macOS 11 Big Sur **تاريخ الشهادة:** —	**معرف النظام:** غير معتمدة بعد **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** macOS 11 Big Sur: Safari **ملفات تعريف الحماية:** PP لتطبيق ،SW EP لمتصفحات الويب
نظام التشغيل: iOS 14 و iPadOS 14 **تاريخالشهادة:** ٢٠٢١ - ٨ - ٢.	**معرف النظام:** ١١١٩١ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple iOS 14 و iPadOS 14: جهات الاتصال **ملفات تعريف الحماية:** PP لتطبيق ،SW EP لمتصفحات الويب
نظام التشغيل: iOS 14 و iPadOS 14 **تاريخالشهادة:** —	**معرف النظام:** ١١١٩٢ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple iOS 14 و iPadOS 14: Safari **ملفات تعريف الحماية:** PP لتطبيق ،SW EP لمتصفحات الويب
نظام التشغيل: iOS 13 و iPadOS 13 **تاريخالشهادة:** ٢٠٢٠ - ٦ - ٥	**معرف النظام:** ١١.٦. **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple iOS 13 و iPadOS 13: Safari **ملفات تعريف الحماية:** PP لتطبيق ،SW EP لمتصفحات الويب

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: iOS 13 و iPadOS 13 **تاريخالشهادة:** ٥ - ٦ - ٢٠٢٠	**معرف النظام:** ١١.٥ **المستندات:** الشهادة الهدف الأمني الإرشاد تقرير التقييم تقرير نشاط الضمان	**العنوان:** Apple iOS 13 و iPadOS 13: جهات الاتصال **ملفات تعريف الحماية:** PP لتطبيق SW

شهادات المعايير العامة المؤرشفة لتطبيقات Apple

نظام التشغيل /تاريخ الشهادة	معرف النظام /المستندات	العنوان /ملفات تعريف الحماية
نظام التشغيل: iOS 12 **تاريخالشهادة:** ١٢ - ٦ - ٢٠١٩	**معرف النظام:** ١.٩٦ **المستندات:** الهدف الأمني الإرشاد	**العنوان:** iOS 12 Safari **ملفات تعريف الحماية:** PP لتطبيق SW، EP لمتصفحات الويب
نظام التشغيل: iOS 12 **تاريخالشهادة:** ٢٨ - ٢ - ٢٠١٩	**معرف النظام:** ١.٩٦١ **المستندات:** الهدف الأمني الإرشاد	**العنوان:** iOS 12 جهات الاتصال **ملفات تعريف الحماية:** PP لتطبيق SW
نظام التشغيل: iOS 11 **تاريخالشهادة:** ٩ - ١١ - ٢٠١٨	**معرف النظام:** ١.٩١٦ **المستندات:** الهدف الأمني الإرشاد	**العنوان:** iOS 11 Safari **ملفات تعريف الحماية:** PP لتطبيق SW، EP لمتصفحات الويب
نظام التشغيل: iOS 11 **تاريخالشهادة:** ١٣ - ٩ - ٢٠١٨	**معرف النظام:** ١.٩١٥ **المستندات:** الهدف الأمني الإرشاد	**العنوان:** iOS 11 جهات الاتصال **ملفات تعريف الحماية:** PPلتطبيق SW

شـهادات أمن خدمات الإنترنت من Apple

تحتفظ شـركة Apple بالشـهادات على أسـاس الامتثال لمعياري ISO/IEC 27001 و ISO/IEC 27018 لتمكين عمـلاء Apple مـن تلبيـة التزاماتهـم التنظيمية والتعاقدية. وتوفر هذه الشـهادات لعملائنا توثيقًا مسـتقلاً حول ممارسـات أمـن وخصوصيـة المعلومات التـي تنتهجها Appleللأنظمـة الواقعة ضمن النطاق.

تُعـد ISO/IEC 27001 و ISO/IEC 27018 جـزءًا مـن مجموعة معايير نظام إدارة أمـن المعلومات (ISMS) التي نشـرتها المنظمـة الدوليـة للمعاييـر (ISO). كجزء مـن نظام ISMS من Apple، تم تضمين جميـع متطلبات التحكم فـي الملحـق أ فـي بيـان قابليـة التطبيق على النحـو المحدد في معايير ISO/IEC 27001 وISO/IEC 27018 . تخضع Apple لشـهادة مسـتقلة من جهة تسـجيل معتمدة بشـكل سنوي.

ISO/IEC 27001

ISO/IEC 27001 هـو معيـار لنظـام إدارة أمـن المعلومات يحدد متطلبات إنشـاء نظـام إدارة أمن المعلومات في المؤسسـة وتنفيذه وصيانته وتحسـينه باسـتمرار. يشـتمل معيار ISO/IEC 27001 على مجالات الأمن التالية التي تغطيها شـهادات ISO/IEC الخاصة بشـركة Apple:

- سياسـة أمن المعلومات
- تنظيـم أمن المعلومات
- إدارة الأصول
- أمن الموارد البشـرية
- الأمـن المادي والبيئي
- إدارة الاتصـالات والعمليات
- التحكـم في الوصول
- اقتنـاء أنظمة المعلومـات وتطويرها وصيانتها
- إدارة حـوادث أمن المعلومات
- إدارة اسـتمرارية العمل
- الامتثال

ISO/IEC 27018

ISO/IEC 27018 عبارة عن مدونة ممارسات لحماية معلومات التعريف الشخصية (PII) في البيئات السحابية العامة. يشتمل معيار ISO/IEC 27018 على مجالات الأمن التالية التي تغطيها شهادات ISO/IEC الخاصة بشركة Apple:

- الموافقة والاختيار
- مشروعية الغرض ومواصفاته
- قيود جمع المعلومات
- التقليل من البيانات
- قيود استخدام البيانات والاحتفاظ بها والإفصاح عنها
- الدقة والجودة
- الانفتاح والشفافية والإشعار
- المشاركة الفردية والوصول
- المساءلة
- أمن المعلومات
- الامتثال للخصوصية

خدمات Appleالتي يغطيها المعياران ISO/IEC 27001 و ISO/IEC 27018

تغطي شهادتا ISO/IEC 27001 و ISO/IEC 27018 الخاصتان بشركة Apple الخدمات التالية:

- محادثات الشركات من Apple
- Apple Business Manager
- خدمة إشعارات Push من Apple (APNs)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- خدمات iWork
- حسابات Apple ID المُدارة
- Schoolwork
- Siri

الشهادات

يتوفر دليل شهادتي ISO/IEC 27001 و ISO/IEC 27018 الخاصتين بشركة Apple في سجلاتنا.

لعرض شهادات Apple، انتقل إلى البحث في الشهادة ودليل العميل على موقع المعهد البريطاني للمعايير (BSI)، أدخل Apple في حقل بحث الشركة، انقر على زر البحث، ثم حدد نتائج البحث لعرض الشهادات.

ملاحظة: يتم توفير معلومات حول المنتجات التي لم تصنعها Apple، أو مواقع الويب المستقلة التي لا تخضع لرقابة Apple أو اختباراتها، دون توصية أو إجازة. ولا تتحمل Apple أي مسؤولية فيما يتعلق باختيار أو أداء أو استخدام مواقع أو منتجات تابعة لجهات خارجية. ولا تقدم Apple أي إقرارات فيما يتعلق بدقة أو موثوقية مواقع الويب التابعة لجهات خارجية. اتصل بالبائع للحصول على معلومات إضافية.

مشـروع الامتثال الأمني لـ macOS

يعد مشروع الامتثال الأمني لـ macOS (mSCP) جهدًا مفتوح المصدر لتوفير نهج برمجي لإنشاء الإرشادات الأمنية. هذا مشروع مشترك بين موظفي أمن تكنولوجيا المعلومات التشغيليين الفيدراليين من المعهد الوطني للمعايير والتكنولوجيا (NIST) والإدارة الوطنية للملاحة الجوية والفضاء (ناسا) ووكالة أنظمة معلومات الدفاع (DISA) ومختبر لوس ألاموس الوطني (LANL). يستخدم المشروع مجموعة من عناصر التحكم التي تم اختبارها والتحقق من صحتها لنظام macOS ويقوم بتعيين عناصر التحكم هذه على أي دليل أمن يدعمه المشروع. بالإضافة إلى ذلك، يمكن استخدام هذا المشروع كمصدر لإنشاء خطوط أساس أمنية مخصصة لعناصر تحكم الأمن الفنية بسهولة من خلال الاستفادة من مكتبة الإجراءات الذرية التي تم اختبارها والتحقق من صحتها (إعدادات التكوين). وينتج عن المشروع وثائق مخصصة ونصوص وملفات تعريف التكوين وقائمة تدقيق بناءً على خط الأساس المستخدم.

يمكن لـ mSCP إنتاج محتوى يُستخدَم مع أدوات الإدارة والأمن لتحقيق الامتثال. تدعم إعدادات التكوين في هذا المشروع خطوط الأساس الإرشادية التالية:

المؤسسة	خطوط الأساس المدعومة
المعهد الوطني للمعايير والتكنولوجيا (NIST)، الإصدار الخاص(SP) 800-53، ضوابط الأمن الموصى بها لأنظمة المعلومات الفيدرالية والمنظمات، المراجعة 5	800-53 مرتفع، 800-53 متوسط، 800-53 منخفض
المعهد الوطني للمعايير والتكنولوجيا (NIST)، الإصدار الخاص (SP) 800-171، حماية المعلومات غير المصنفة الخاضعة للرقابة في الأنظمة والمنظمات غير الفيدرالية المراجعة 2	800-171
وكالة أنظمة معلومات الدفاع (DISA)، دليل التنفيذ الفني للأمن لـ Apple macOS 11 STIG macOS 11	STIG
لجنة تعليمات أنظمة الأمن القومي 1253 (CNSSI)، تصنيف الأمن وتحديد التحكم لأنظمة الأمن القومي	1253

معلومات إضافية:

- خط الأساس لمراجعة جميع القواعد في المشروع متاح هنا.
- لمعرفة المزيد حول المشروع والاستخدام، انظر نص الويكي الخاص بمشروع الامتثال الأمني لـ macOS.
- لإعداد المشروع للاستخدام، انظر: التعرف على مشروع الامتثال الأمني لـ macOS، الجزء ١ والتعرف على مشروع الامتثال الأمني لـ macOS، الجزء ٢.
- إذا كنت مهتمًا بدعم تطوير المشروع، فانظر إرشادات المساهم.

سجل تاريخ مراجعة المستند

التاريخ	الملخص
٢٧ أكتوبر ٢٠٢١	الموضوعات المُحدّثة: • شهادات الأمن لمعالج Secure Enclave • شهادات الأمن لـ iOS • شهادات الأمن لـ macOS
١٧ أغسطس ٢٠٢١	الموضوعات المُحدّثة: • شهادات الأمن لمعالج Secure Enclave • شهادات الأمن لشريحة Apple T2 الأمنية • شهادات الأمن لـ iOS • شهادات الأمن لـ iPadOS • شهادات الأمن لـ macOS • شهادات الأمن لـ tvOS • شهادات الأمن لـ watchOS • شهادات الأمن في تطبيقات Apple • شهادات الأمن • مشروع الامتثال الأمني لـ macOS
٢٦ أبريل ٢٠٢١	الموضوع المضاف: • مشروع الامتثال الأمني لـ macOS الموضوعات المُحدّثة: • شهادات الأمن لرقاقة Apple T2 الأمنية: شهادة FIPS 140-2 جديدة، 3811 • شهادات الأمن لمعالج Secure Enclave: شهادة FIPS 140-2 جديدة، 3811 وجدول جديد للشهادات الإضافية. • شهادات الأمن لـ iOS: شهادات FIPS 140-2 جديدة، 3811، معرف نظام 11146 iOS 14 قيد التقييم • شهادات الأمن لـ iPadOS: شهادات FIPS 140-2 جديدة، 3811، معرف نظام 11147 iPadOS 14 قيد التقييم • شهادات الأمن لـ macOS: شهادة FIPS 140-2 جديدة، 3811. • شهادات الأمن لـ tvOS: شهادات FIPS 140-2 جديدة، 3811. • شهادات الأمن لـ watchOS: شهادات FIPS 140-2 جديدة، 3811. • شهادات الأمن في تطبيقات Apple: تحديثات لحالة المعايير العامة، وجدول جديد لشهادات المعايير العامة المؤرشفة.

المعجم

اتفاقية الاعتراف بالمعايير العامة (CCRA) ترتيب اعتراف متبادل يحدد السياسات والمتطلبات للاعتراف الدولي بالشهادات الصادرة وفقًا لسلسلة ISO/IEC 15408 أو مقاييس المعايير العامة.

إدارة جهاز الجوال (MDM) خدمة تتيح للمستخدم إدارة الأجهزة المسجلة عن بُعد. بعد تسجيل الجهاز، يمكن للمستخدم استخدام خدمة MDM عبر الشبكة لتكوين الإعدادات وتنفيذ مهام أخرى على الجهاز دون تدخل المستخدم.

التشفير الكامل للقرص (FDE) تشفير جميع البيانات الموجودة على وحدة تخزين.

التنفيذ قيد الاختبار (IUT) وحدة تشفير يتم اختبارها بواسطة المختبر.

المجتمع التقني الدولي (iTC) مجموعة مسؤولة عن تطوير ملفات تعريف الحماية أو ملفات تعريف الحماية التعاونية تحت رعاية اتفاقية الاعتراف بالمعايير العامة (CCRA).

المستوى الأمني (SL) المستويات الأمنية الأربعة الشاملة (١ - ٤) التي تم تحديدها في ISO/IEC 19790 لوصف مجموعات متطلبات الأمن المعمول بها. المستوى ٤ هو الأكثر صرامة.

المعايير العامة (CC) معيار يحدد المفاهيم والمبادئ العامة لتقييم أمن تقنية المعلومات ويحدد نموذجًا عامًا للتقييم. يتضمن كتالوجات لمتطلبات الأمن بلغة موحدة.

المعهد الوطني للمعايير والتكنولوجيا (NIST) جزء من وزارة التجارة الأمريكية مسؤول عن النهوض بعلوم القياس والمعايير والتكنولوجيا.

الهدف الأمني (ST) وثيقة تحدد مشكلة الأمن ومتطلبات الأمن لمنتج معين.

الوحدات قيد المعالجة (MIP) قائمة يحتفظ بها برنامج التحقق من صحة وحدة التشفير (CMVP) لوحدات التشفير حاليًا في عملية التحقق من صحة CMVP.

أمن نظم المعلومات لمجموعة كبار المسؤولين (SOG-IS) مجموعة تدير اتفاقية الاعتراف المتبادل بين عدة دول أوروبية.

برنامج التحقق من صحة وحدة التشفير (CMVP) مؤسسة تديرها الحكومتان الأمريكية والكندية للتحقق من التوافق مع معيار FIPS 140-3.

برنامج عمليات التحقق من صحة خوارزمية التشفير (CAVP) مؤسسة تديرها NIST لتوفير اختبار التحقق من صحة خوارزميات التشفير المعتمدة (مثل المعتمدة من FIPS والموصى بها من قِبلNIST) ومكوناتها الفردية.

بيان قابلية التطبيق (SOA) وثيقة تصف الضوابط الأمنية المطبقة في نطاق ISMS، والتي تم إنتاجها لدعم شهادة ISO/IEC 27001.

خدمة إشعارات Push من Apple (APNs) خدمة عالمية تقدمها Apple تُسلّم الإشعارات الموجهة إلى أجهزة Apple.

شراكة أمن المعلومات الوطني (NIAP) منظمة تابعة للحكومة الأمريكية مسؤولة عن تشغيل تنفيذ الولايات المتحدة لمقياس المعايير المشتركة وإدارة خطة تقييم المعايير العامة والتحقق من صحتها (CCEVS) التابعة لـ NIAP.

عميل VPN IPsec في ملف تعريف الحماية، عميل يوفر اتصال IPsec آمنًا بين نظام أساسي مضيف فعلي أو ظاهري وموقع بعيد.

معالج Secure Enclave (SEP) معالج مشترك مُصنع داخل نظام على رقاقة (SoC).

معيار معالجة المعلومات الفيدرالية (FIPS) المنشورات التي طورها المعهد الوطني للمعايير والتكنولوجيا، إما عند الاقتضاء بموجب القانون، أو عندما تكون هناك متطلبات ملزمة للحكومة الفيدرالية للأمن الإلكتروني، أو كليهما.

ملف تعريف الحماية التعاونية (cPP) ملف حماية تم تطويره بواسطة مجتمع تقني دولي، وهو مجموعة من الخبراء المكلفين بإنشاء cPPs.

ملفات تعريف الحماية (PP) وثيقة تحدد مشكلة الأمن ومتطلبات الأمن لفئة معينة من المنتجات.

نظام إدارة أمن المعلومات (ISMS) مجموعة من سياسات وإجراءات أمن المعلومات التي تحكم حدود برنامج الأمن المصمم لحماية نطاق من المعلومات والأنظمة من خلال إدارة أمن المعلومات بشكل منهجي طوال دورة حياة المعلومات و/أو النظام.

نظام على شريحة (SoC) دائرة متكاملة (IC) تضم مكونات متعددة في شريحة واحدة.

وحدة التشفير الأجهزة و/أو البرامج و/أو البرامج الثابتة التي توفر وظائف التشفير وتفي بمتطلبات معيار وحدة التشفير المحددة.

Apple Business Manager بوابة ويب بسيطة مخصصة لمسؤولي تقنية المعلومات، لتوفر للمؤسسات طريقة سريعة ومبسطة لنشر أجهزة Appleالتي اشترتها مباشرةً من Apple أو من موزع مشارك معتمد من Apple أو من شركة اتصالات. يمكنها تسجيل الأجهزة تلقائيًا في حل إدارة جهاز الجوال (MDM) الخاص بها دون الحاجة إلى لمس الأجهزة فعليًا أو تحضيرها قبل أن يحصل عليها المستخدمون.

Apple School Manager بوابة ويب بسيطة مخصصة لمسؤولي تقنية المعلومات، لتوفر للمؤسسات طريقة سريعة ومبسطة لنشر أجهزة Apple التي اشترتها مباشرةً من Apple أو من موزع مشارك معتمد من Apple أو من شركة اتصالات. يمكنها تسجيل الأجهزة تلقائيًا في حل إدارة جهاز الجوال (MDM) الخاص بها دون الحاجة إلى لمس الأجهزة فعليًا أو تحضيرها قبل أن يحصل عليها المستخدمون.

corecrypto مكتبة توفر تطبيقات للتشفيرات الأولية منخفضة المستوى. لاحظ أن corecrypto لا توفر واجهات برمجة مباشرة للمطورين ويتم استخدامها من خلال واجهات API المقدمة للمطورين. كود المصدر الخاص بـ corecrypto متاح للجمهور للسماح بالتحقق من خصائصه الأمنية وعمله بشكل صحيح.

Secure Element (SE) رقاقة سيليكون مدمجة في العديد من أجهزة Apple تدعم وظائف مثل Apple Pay.

sepOS برنامج Secure Enclave الثابت، استنادًا إلى إصدار L4 microkernel مخصص لـ Apple.

T2 رقاقة أمن من Apple مضمنة في بعض أجهزة كمبيوتر Mac التي تعمل بنظام Intel منذ عام ٢٠١٧.

Apple Inc.

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

AB028-00499-B