Certifications de sécurité et centre de conformité

Décembre 2021

Table des matières

Introduction à l’assurance de la sécurité Apple

Dans le cadre de son engagement à l’égard de la sécurité, Apple collabore régulièrement avec des organisations tierces pour certifier et attester la sécurité de son matériel, de ses logiciels et de ses services. Ces organisations de renommée internationale fournissent à Apple les certifications qui correspondent à chaque version majeure de ses systèmes d’exploitation. De cette façon, elles offrent un gage de confiance, c’est-à-dire l’assurance de la sécurité, selon lequel les besoins de sécurité d’un système sont satisfaits. Pour les secteurs techniques qui ne sont pas acceptés dans le cadre des accords de reconnaissance mutuelle ou pour lesquels aucune norme de certification de sécurité établie n’existe, Apple s’engage à élaborer des normes de sécurité appropriées. Sa mission est de promouvoir une couverture de certifications de sécurité exhaustives acceptée à l’échelle mondiale pour l’ensemble du matériel, des logiciels, des apps et des services Apple.

Des certifications sont souvent nécessaires pour satisfaire aux exigences des lois, des règlements et des normes de l’industrie. Les services comme Apple School Manager et Apple Business Manager sont couverts par les certifications ISO/CEI 27001 et ISO/CEI 27018 d’Apple. Tous les clients, y compris les organismes gouvernementaux, les entreprises et les établissements d’enseignement qui déploient des appareils Apple, peuvent utiliser les certifications du matériel, des systèmes d’exploitation, des logiciels et des services pour démontrer la conformité.

Certifications du matériel

Puisque des logiciels sécurisés requièrent une base de sécurité intégrée dans le matériel, tous les appareils Apple, qu'ils exécutent iOS, iPadOS, macOS, tvOS ou watchOS, sont dotés de capacités de sécurité directement sur la puce. Il s'agit notamment de capacités personnalisées du processeur central qui alimentent les fonctionnalités de sécurité système ainsi que la puce dédiée aux fonctions de sécurité. Le composant le plus important est le coprocesseur Secure Enclave, dont sont dotés tous les appareils iOS, iPadOS, watchOS et tvOS récents ainsi que tous les ordinateurs Mac avec puce Apple et les ordinateurs Mac avec processeur Intel et puce T2 Security d'Apple. Le Secure Enclave est la structure sur laquelle reposent le chiffrement des données au repos, le démarrage sécurisé dans macOS et les données biométriques.

L'engagement d'Apple à l'égard de l'assurance de la sécurité commence par la certification des composants de sécurité fondamentaux de la puce, notamment la racine matérielle de confiance, le démarrage sécurisé, la gestion des clés de protection par le Secure Enclave et l'authentification sécurisée par Touch ID et Face ID. Les fonctionnalités de sécurité des appareils Apple existent grâce à la combinaison de la conception de la puce, du matériel, des logiciels et des services distribués exclusivement par Apple. La certification de ces composants est un élément important de la vérification de l'assurance offerte par Apple.

Pour en savoir plus sur les certifications publiques liées au matériel et aux composants du programme interne associés, consultez les articles :

- Certifications de sécurité pour la puce T2 Security d'Apple
- Certifications de sécurité pour le processeur Secure Enclave

Certifications des logiciels et des apps

Apple dispose de certifications et d'attestations indépendantes pour ses systèmes d'exploitation et ses apps, conformément aux normes FIPS 140-2/-3 des États-Unis pour les modules cryptographiques ainsi qu'aux critères communs pour les systèmes d'exploitation, les apps et les services sur l'appareil. La couverture des systèmes d'exploitation comprend iOS, iPadOS, macOS, sepOS, le programme interne de la puce T2, tvOS et watchOS. Pour les apps, la certification indépendante comprendra initialement le navigateur Safari et l'app Contacts, puis d'autres apps seront ajoutées ultérieurement.

Pour en savoir plus sur les certifications publiques liées aux *systèmes d'exploitation* d'Apple, consultez les articles :

- Certifications de sécurité pour iOS
- Certifications de sécurité pour iPadOS
- Certifications de sécurité pour macOS
- Certifications de sécurité pour tvOS
- Certifications de sécurité pour watchOS

Pour en savoir plus sur les certifications publiques liées aux *apps* Apple, consultez l'article :

- Certifications de sécurité pour les apps Apple

Certifications des services

Apple détient des certifications de sécurité pour soutenir ses clients des secteurs de l'éducation et des entreprises. Ces certifications permettent aux clients d'Apple de respecter leurs obligations réglementaires et contractuelles lorsqu'ils utilisent les services Apple avec le matériel et les logiciels Apple. Elles fournissent à nos clients une attestation indépendante des pratiques d'Apple relatives à la sécurité, à l'environnement et à la confidentialité des informations pour les systèmes concernés.

Pour en savoir plus sur les certifications publiques liées aux *services Internet* Apple, consultez l'article :

- Certifications de sécurité pour les services Internet Apple

Si vous avez des questions au sujet des certifications de sécurité et de confidentialité d'Apple, transmettez-les à security-certifications@apple.com.

Certifications de sécurité du matériel

Aperçu des certifications de sécurité du matériel Apple

Apple détient, entre autres, les certificats de validation de la conformité aux normes FIPS 140-2/-3 des États-Unis pour sepOS et le programme interne de la puce T2. Nous commençons par des *éléments de structure de certification* qui s'appliquent de manière générale à plusieurs plateformes au besoin. Un de ces éléments de structure est la validation de la bibliothèque Corecrypto utilisée pour les déploiements de modules cryptographiques logiciels et matériels dans les systèmes d'exploitation développés par Apple. Un deuxième correspond à la certification du Secure Enclave intégré dans de nombreux appareils Apple. Un troisième correspond à la certification du Secure Element, qui se trouve dans les appareils Apple dotés de Touch ID et ceux dotés de Face ID. Ces éléments de structure de certification matérielle forment la base des certifications générales de sécurité des plateformes.

Validation des algorithmes cryptographiques

La validation de l'exactitude de l'implémentation de nombreux algorithmes cryptographiques ainsi que des fonctions de sécurité connexes est une condition préalable à la validation FIPS 140-3 et favorable à d'autres certifications. La validation est gérée par le Programme de validation des algorithmes cryptographiques (PVAC) du National Institute of Standards and Technology (NIST). Les certificats de validation des implémentations d'Apple sont accessibles à l'aide de l'outil de recherche du PVAC. Pour en savoir plus, consultez le site Web du Programme de validation des algorithmes cryptographiques (PVAC).

Validation des modules cryptographiques : FIPS 140-2/3 (ISO/CEI 19790)

Les modules cryptographiques d'Apple ont été validés à plusieurs reprises par le Programme de validation des modules cryptographiques (PVMC) en fonction de la norme Federal Information Processing Standard (FIPS) 140-2 des États-Unis pour les modules cryptographiques après le lancement de chaque nouvelle version des systèmes d'exploitation depuis 2012. Après chaque version majeure, Apple soumet les modules au PVMC afin de valider la conformité avec la norme. En plus d'être utilisés par les systèmes d'exploitation et les apps d'Apple, ces modules offrent une fonctionnalité cryptographique aux services Apple et peuvent être utilisés par les apps tierces.

Apple atteint le **niveau de sécurité 1** chaque année pour les modules logiciels « Corecrypto pour Intel » et « noyau Corecrypto pour Intel » pour macOS. Pour la puce Apple, les modules « Corecrypto pour ARM » et « noyau Corecrypto pour ARM » s'appliquent à iOS, iPadOS, tvOS et watchOS, et au programme interne de la puce T2 Security d'Apple intégrée dans les ordinateurs Mac.

En 2019, Apple a atteint pour la première fois le **niveau de sécurité 2** de la norme FIPS 140-2 pour le module matériel de cryptographie intégré « Corecrypto Apple : gestion des clés de protection », permettant ainsi l'utilisation approuvée par le gouvernement des États-Unis des clés générées et gérées dans le Secure Enclave. Apple poursuit ses efforts de validation pour le module matériel de cryptographie avec chaque nouvelle version majeure de ses systèmes d'exploitation.

La norme **FIPS 140-3** a été approuvée par le département du Commerce des États-Unis en 2019. La modification la plus notable apportée dans cette version est la spécification des normes ISO/CEI, notamment la norme 19790:2015 et la norme d'essai connexe 24759:2017. Le PVMC a instauré un programme de transition et signalé qu'à partir de 2020, les modules cryptographiques seront validés en fonction de la norme FIPS 140-3. Apple entend conformer ses modules cryptographiques à la norme FIPS 140-3 dans les meilleurs délais.

En ce qui concerne les modules cryptographiques actuellement en phase d'essai et de validation, le PVMC tient à jour deux listes distinctes qui peuvent contenir des informations au sujet des validations proposées. Pour ce qui est des modules cryptographiques en phase d'essai dans un laboratoire agréé, le module peut figurer sur la liste des implémentations à l'essai. Une fois que le laboratoire a terminé les essais et recommande la validation par le PVMC, le module cryptographique d'Apple figure sur la liste des modules en cours de traitement. La phase d'essai du laboratoire est alors terminée et le PVMC n'a plus qu'à la valider. Étant donné que la durée du processus d'évaluation est variable, consultez les deux listes ci-dessus pour déterminer l'état de validation des modules cryptographiques d'Apple entre la date de sortie d'une version majeure du système d'exploitation et l'émission du certificat de validation par le PVMC.

Certifications de produit : Critères communs ISO/CEI 15408

La norme des critères communs (ISO/CEI 15408) est utilisée par de nombreuses organisations comme base pour évaluer le niveau de sécurité des produits informatiques.

Pour connaître les certifications mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC), consultez le portail des critères communs. La norme des critères communs peut également être utilisée en dehors de l'ARCC, dans le cadre de schémas de validation nationaux et privés. En Europe, la reconnaissance mutuelle est régie par l'accord du SOG-IS et l'ARCC.

L'objectif, énoncé par la communauté des critères communs, consiste à établir un ensemble de normes de sécurité reconnu à l'échelle internationale pour fournir une évaluation claire et fiable des capacités de sécurité des produits informatiques. En fournissant une évaluation indépendante de la capacité d'un produit à satisfaire aux normes de sécurité, la certification des critères communs donne aux clients confiance en la sécurité des produits informatiques et permet des décisions plus éclairées.

En vertu de l'ARCC, les pays membres se sont entendus pour reconnaître la certification des produits informatiques avec le même degré de confiance. L'évaluation approfondie des éléments suivants est requise pour obtenir la certification :

- Profils de protection (PP)
- Cibles de sécurité (Security Targets, ST)
- Exigences fonctionnelles de sécurité (Security Functional Requirements, SFR)
- Exigences d'assurance de la sécurité (Security Assurance Requirements, SAR)
- Niveaux d'assurance de l'évaluation (Evaluation Assurance Levels, EAL)

Les profils de protection sont des documents qui précisent les besoins de sécurité d'une classe spécifique d'appareils, comme « Mobility » (mobilité). Ils sont utilisés pour permettre de comparer les évaluations de produits informatiques d'une même classe. L'adhésion à l'ARCC ainsi que la liste de PP continuent de croître chaque année. Cet arrangement permet au développeur de produits de prendre les mesures nécessaires pour obtenir une seule certification en vertu de n'importe lequel des schémas d'autorisation de certificat et de la faire reconnaître par n'importe lequel des signataires utilisateurs de certificats.

Les cibles de sécurité définissent *ce* qui sera évalué lors de la certification d'un produit informatique. Elles se traduisent par des *exigences fonctionnelles de sécurité* plus précises, utilisées pour une évaluation plus détaillée.

Les critères communs comprennent également les *exigences d'assurance de la sécurité*. Les *niveaux d'assurance de l'évaluation* sont une mesure communément établie. Ils regroupent les ensembles de SAR couramment utilisés et peuvent être spécifiés dans les PP et les ST pour soutenir la comparabilité.

De nombreux PP plus anciens ont été archivés et sont remplacés par des PP ciblés en cours de développement, qui sont axés sur des solutions et des environnements précis. Dans un effort concerté pour assurer une reconnaissance mutuelle entre tous les membres de l'ARCC, des communautés techniques internationales (iTC) ont été établies pour élaborer et maintenir les profils de protection de collaboration (cPP) conçus dès le départ avec la participation des schémas des signataires de l'ARCC. Des PP ciblant les groupes d'utilisateurs ainsi que des accords de reconnaissance mutuelle autres que l'ARCC continuent d'être élaborés par les parties prenantes appropriées.

Apple a commencé sa quête de certifications en vertu de l'ARCC pour certains cPP au début de 2015. Depuis, elle a obtenu les certifications des critères communs pour chaque version majeure d'iOS et a élargi la couverture pour inclure l'assurance de sécurité fournie par les nouveaux PP.

Apple joue un rôle actif dans les communautés techniques qui se concentrent sur l'évaluation des technologies de sécurité mobile. Cela comprend les iTC responsables de l'élaboration et de la mise à jour des cPP. Nous continuons d'évaluer et d'obtenir des certifications relativement aux PP et aux cPP actuels.

Les certifications des plateformes Apple pour le marché nord-américain sont généralement réalisées avec le National Information Assurance Partnership (NIAP), qui tient à jour une liste des projets en cours d'évaluation qui n'ont pas encore été certifiés.

En plus des certifications de plateformes générales indiquées, d'autres certificats ont été délivrés afin de démontrer les besoins de sécurité propres à certains marchés.

Certifications de sécurité pour le processeur Secure Enclave

Contexte de la certification du Secure Enclave

Le module matériel de cryptographie (*le module cryptographique Apple de la gestion des clés de protection par le SEP*) est intégré dans le système sur puce d'Apple des produits suivants : iPhone et iPad de la série A, ordinateurs Mac avec puce Apple de la série M, Apple Watch de la série S et puces de sécurité de la série T intégrées aux ordinateurs Mac avec processeur Intel à partir de l'iMac Pro lancé en 2017.

En 2018, Apple a synchronisé la validation des modules cryptographiques logiciels avec les systèmes d'exploitation sortis en 2017 (iOS 11, macOS 10.13, tvOS 11 et watchOS 4). Le module cryptographique matériel du SEP détecté comme le module cryptographique de la gestion des clés de protection par le SEP Apple v1.0 a été initialement validé par rapport aux exigences du niveau de sécurité 1 de la norme FIPS 140-2.

En 2019, Apple a validé le module matériel par rapport aux exigences de la norme FIPS 140-2 de niveau de sécurité 2 et a mis à jour l'identifiant de version du module vers la version 9.0 afin de se synchroniser avec les versions de validation des modules utilisateur Corecrypto et des modules noyau Corecrypto correspondants. En 2019, ces versions comprenaient iOS 12, macOS 10.14, tvOS 12 et watchOS 5.

Depuis 2020, Apple poursuit ses efforts de validation pour se conformer à la norme FIPS 140-3, et pour obtenir une assurance supplémentaire du niveau de sécurité 3 pour les exigences en matière de sécurité physique des puces Apple A13, A14, S6 et M1.

Apple participe aussi activement à la validation du module utilisateur Corecrypto et du module noyau Corecrypto pour chaque version majeure d'un système d'exploitation. La validation de la conformité est possible uniquement pour une version finale publiée.

État de la validation des modules cryptographiques

Le Programme de validation des modules cryptographiques (PVMC) tient à jour l'état de validation des modules cryptographiques sur trois listes distinctes, selon leur état du moment :

- Pour figurer sur la liste des implémentations à l'essai du PVMC, le laboratoire doit avoir reçu d'Apple le mandat de procéder à des tests.
- Lorsque les tests sont terminés, que le laboratoire a recommandé la validation par le PVMC et que les frais du PVMC ont été payés, le module est ajouté à la liste des modules en cours de traitement. Cette liste suit la progression des efforts de validation du PVMC en quatre phases :
  - *En attente de révision :* Le module attend l'assignation d'une ressource du PVMC.
  - *En révision :* Les ressources du PVMC effectuent leurs activités de validation.
  - *Coordination :* Le laboratoire et le PVMC résolvent les problèmes détectés.
  - *Finalisation :* Les activités et les formalités liées à la délivrance du certificat sont achevées.
- Lorsqu'ils ont été validés par le PVMC, les modules reçoivent un certificat de conformité et sont ajoutés à la liste des modules cryptographiques validés. Parmi ceux-ci se trouvent :
  - les modules validés qui sont marqués comme actifs;
  - les modules qui, après cinq ans, sont marqués comme historiques;
  - si le certificat d'un module est révoqué pour une raison quelconque, ce dernier est marqué en conséquence.

En 2020, le PVMC a adopté la norme internationale ISO/CEI 19790 comme base pour la norme FIPS 140-3.

Certifications FIPS 140-3

État actuel

Le tableau ci-dessous indique les modules cryptographiques de 2020 et de 2021 actuellement testés par le laboratoire pour vérifier leur conformité avec la norme FIPS 140-3.

Les tests des modules de la gestion des clés de protection (Secure Key Store; SKS) associés aux versions des systèmes d'exploitation de 2020 et 2021 sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement et une fois validés, ils seront déplacés vers la liste des modules cryptographiques validés.

Les tests des modules de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection d'iOS 15 (2021) sont en cours. Ils figurent sur la liste des implémentations à l'essai.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec les versions 2021 d'iOS, d'iPadOS, de macOS, de tvOS et de watchOS *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14, T2, M1, S3-S6) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec les versions 2021 d'iOS, d'iPadOS, de macOS, de tvOS et de watchOS *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A13, A14, S6, M1) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec les versions 2020 d'iOS, d'iPadOS, de macOS, de tvOS et de watchOS *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14, T2, M1, S3-S6) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec les versions 2020 d'iOS, d'iPadOS, de macOS, de tvOS et de watchOS *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A13, A14, S6, M1) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3

Certifications FIPS 140-2

Le tableau ci-dessous indique les modules cryptographiques testés par le laboratoire pour vérifier leur conformité avec la norme FIPS 140-2.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-02-05	*Certificats :* 3811 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v10.0 *Système d'exploitation :* sepOS sous macOS 10.15 Catalina *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-09-10	*Certificats :* 3523 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v9.0 *Système d'exploitation :* sepOS sous macOS 10.14 Mojave *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2019-09-10	*Certificats :* 3223 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v1.0 *Système d'exploitation :* sepOS sous macOS 10.13 High Sierra *Type :* matériel *Niveau de sécurité :* 2

Certifications des critères communs (CC)

Apple participe activement aux évaluations des critères communs dont les profils de protection couvrent la fonctionnalité de sécurité des technologies Apple.

État des certifications des critères communs

Le schéma américain, qui relève du NIAP, tient à jour une liste des produits en évaluation. Cette liste comprend les produits qui, d'une part, sont en cours d'évaluation aux États-Unis avec un laboratoire d'essais selon les critères communs (Common Criteria Testing Laboratory, CCTL) approuvé par le NIAP, et qui, d'autre part, ont fait l'objet d'une réunion d'évaluation préliminaire (ou l'équivalent) où la direction du schéma d'évaluation et de validation lié aux critères communs (Common Criteria Evaluation and Validation Scheme, CCEVS) les a officiellement acceptés pour évaluation.

Après la certification des produits, le NIAP répertorie les certifications valides sur la liste des produits conformes. Au bout de deux ans, ces certifications sont examinées pour vérifier leur conformité avec la politique de maintien de l'assurance actuelle. À l'expiration du maintien de l'assurance, le NIAP fait passer la certification sur sa liste des produits archivés.

Le portail des critères communs répertorie les certifications qui peuvent être mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC). Le portail des CC peut laisser les produits sur la liste des produits certifiés pendant cinq ans. Il tient des dossiers sur les certifications archivées.

Le tableau ci-dessous indique les certifications en cours d'évaluation par un laboratoire, ou celles dont on a confirmé la conformité avec les critères communs.

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : sepOS *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* Secure Enclave d'Apple [2020] *Profils de protection :* CPP_DSC_V1.0 *Matériel :* Secure Enclave (A9-A14, M1, T2, S3-S6) *Logiciel :* sepOS distribué avec iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14 et watchOS 7

Certifications supplémentaires

Le tableau ci-dessous présente les certifications du Secure Enclave qui ne se rapportent ni aux critères communs ni à la norme FIPS 140-3.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2020 *Dates de validation :* 2019-12-07 au 2022-12-26	*Certificats :* CFNR201902910002 (République populaire de Chine : certification technologique des services financiers mobiles) Version en chinois Version en anglais	*Titre :*Environnement d'exécution de confiance du terminal mobile *Système d'exploitation :* iOS 13.5.1 *Spécification :* JR/T 0156-2017

Certifications de sécurité pour la puce T2 Security d'Apple

Contexte de la validation des modules cryptographiques

Apple participe activement à la validation de ses modules logiciels et matériels intégrés pour chaque version majeure d'un système d'exploitation. La validation de la conformité est possible uniquement pour une version finale des modules.

En 2020, le PVMC a adopté la norme internationale ISO/CEI 19790 comme base pour la norme FIPS 140-3 des États-Unis.

En plus d'un processeur Intel, la plupart des ordinateurs Mac lancés depuis 2017 sont dotés de la puce T2 Security d'Apple, un système sur puce Apple. Ces ordinateurs Mac dotés d'une puce T2 utilisent les cinq modules cryptographiques pour de nombreux services sur l'appareil.

- Module utilisateur Corecrypto pour Intel (utilisé par macOS sur les ordinateurs Mac avec processeur Intel)
- Module de noyau Corecrypto pour Intel (utilisé par macOS sur les ordinateurs Mac avec processeur Intel)
- Module utilisateur Corecrypto pour ARM (utilisé par la puce T2)
- Module de noyau Corecrypto pour ARM (utilisé par la puce T2)
- Module cryptographique de la gestion des clés de protection (utilisé par le coprocesseur Secure Enclave intégré dans la puce T2)

Remarque : Les modules sur puce Apple qui fonctionnent avec la puce T2 sont les mêmes que ceux qui fonctionnent avec d'autres puces Apple, telles que les puces de la série A, de la série S et de la série M.

État de la validation des modules cryptographiques

Le Programme de validation des modules cryptographiques (PVMC) tient à jour l'état de validation des modules cryptographiques sur trois listes distinctes, selon leur état du moment :

- Pour figurer sur la liste des implémentations à l'essai du PVMC, le laboratoire doit avoir reçu d'Apple le mandat de procéder à des tests.
- Lorsque les tests sont terminés, que le laboratoire a recommandé la validation par le PVMC et que les frais du PVMC ont été payés, le module est ajouté à la liste des modules en cours de traitement (MIP). Cette liste suit la progression des efforts de validation du PVMC en quatre phases :
  - *En attente de révision :* Le module attend l'assignation d'une ressource du PVMC.
  - *En révision :* Les ressources du PVMC effectuent leurs activités de validation.
  - *Coordination :* Le laboratoire et le PVMC résolvent les problèmes détectés.
  - *Finalisation :* Les activités et les formalités liées à la délivrance du certificat sont achevées.

- Lorsqu'ils ont été validés par le PVMC, les modules reçoivent un certificat de conformité et sont ajoutés à la liste des modules cryptographiques validés. Parmi ceux-ci se trouvent :
  - les modules validés qui sont marqués comme actifs;
  - les modules qui, après cinq ans, sont marqués comme historiques;
  - si le certificat d'un module est révoqué pour une raison quelconque, ce dernier est marqué en conséquence.

Certifications FIPS 140-3

État actuel

Les tests des modules de 2020 de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Les tests des modules de 2021 de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection sont en cours. Ils figurent sur la liste des implémentations à l'essai.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS sous macOS 12 Monterey *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS sous macOS 12 Monterey *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS sous macOS 12 Monterey *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (T2) *Niveau de sécurité :* 2

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS sous macOS 11 Big Sur *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS sous macOS 11 Big Sur *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS sous macOS 11 Big Sur sur processeur Intel *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel *Niveau de sécurité :* 2

Certifications FIPS 140-2

Le tableau ci-dessous indique les modules cryptographiques testés par le laboratoire pour vérifier leur conformité avec la norme FIPS 140-2.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3856 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* sepOS sous macOS 10.15 Catalina *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3855 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* sepOS sous macOS 10.15 Catalina *Type :* logiciel *Niveau de sécurité :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-02-05	*Certificats :* 3811 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Corecrypto Apple v10.0 *Système d'exploitation :* sepOS sous macOS 10.15 Catalina *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-23	*Certificats :* 3438 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* sepOS sous macOS 10.14 Mojave *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-11	*Certificats :* 3433 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* sepOS sous macOS 10.14 Mojave *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-09-10	*Certificats :* 3523 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v9.0 *Système d'exploitation :* sepOS sous macOS 10.14 Mojave *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-22, 2018-07-06	*Certificats :* 3148 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* sepOS sous macOS 10.13 High Sierra *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-17, 2018-07-03	*Certificats :* 3147 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* sepOS sous macOS 10.13 High Sierra *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-07-10	*Certificats :* 3223 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v1.0 *Système d'exploitation :* sepOS sous macOS 10.13 High Sierra *Type :* matériel *Niveau de sécurité :* 2

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2016 *Dates de validation :* 2017-02-01	*Certificats :* 2828 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v7.0 pour iOS *Système d'exploitation :* sepOS sous macOS 10.12 Sierra *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2016 *Dates de validation :* 2017-02-01	*Certificats :* 2827 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v7.0 pour iOS *Système d'exploitation :* sepOS sous macOS 10.12 Sierra *Type :* logiciel *Niveau de sécurité :* 1

Certifications de sécurité des systèmes d’exploitation

Aperçu des certifications de sécurité des systèmes d’exploitation d’Apple

Apple détient, entre autres, les certificats de validation de la conformité aux normes FIPS 140-2/-3 des États-Unis pour sepOS et le programme interne de la puce T2. Nous commençons par des *éléments de structure de certification* qui s’appliquent de manière générale à plusieurs plateformes au besoin. Un de ces éléments de structure est la validation de Corecrypto utilisé pour les déploiements de modules cryptographiques logiciels et matériels dans les systèmes d’exploitation développés par Apple. Un deuxième correspond à la certification du Secure Enclave intégré dans de nombreux appareils Apple. Un troisième correspond à la certification du Secure Element, qui se trouve dans les appareils Apple dotés de Touch ID et ceux dotés de Face ID. Ces éléments de structure de certification matérielle forment la base des certifications générales de sécurité des plateformes.

Validation des algorithmes cryptographiques

La validation de l’exactitude de l’implémentation de nombreux algorithmes cryptographiques ainsi que des fonctions de sécurité connexes est une condition préalable à la validation FIPS 140-3 et favorable à d’autres certifications. La validation est gérée par le Programme de validation des algorithmes cryptographiques (PVAC) du NIST. Les certificats de validation des implémentations d’Apple sont accessibles à l’aide de l’outil de recherche du PVAC.

Validation des modules cryptographiques : FIPS 140-2/3 (ISO/CEI 19790)

La conformité des modules cryptographiques des systèmes d'exploitation Apple a été validée à plusieurs reprises par le Programme de validation des modules cryptographiques (PVMC) en fonction de la norme Federal Information Processing Standard (FIPS) 140-2 des États-Unis après le lancement de chaque nouvelle version des systèmes d'exploitation depuis 2012. Après chaque version majeure, Apple soumet tous les modules au PVMC aux fins de validation cryptographique intégrale. Ces modules validés fournissent des opérations cryptographiques pour les services Apple et peuvent être utilisés par des apps tierces.

Apple atteint le **niveau de sécurité 1** chaque année pour les modules logiciels « Corecrypto pour Intel » et « noyau Corecrypto pour Intel » pour macOS. Pour la puce Apple, les modules « Corecrypto pour ARM » et « noyau Corecrypto pour ARM » s'appliquent à iOS, iPadOS, tvOS et watchOS, et au programme interne de la puce T2 Security d'Apple intégrée dans les ordinateurs Mac.

En 2019, Apple a atteint pour la première fois le **niveau de sécurité 2** de la norme FIPS 140-2 pour le module matériel de cryptographie intégré « Corecrypto Apple : gestion des clés de protection », permettant ainsi l'utilisation approuvée par le gouvernement des États-Unis des clés générées et gérées dans le Secure Enclave. Apple poursuit ses efforts de validation pour le module matériel de cryptographie avec chaque nouvelle version majeure de ses systèmes d'exploitation.

La norme **FIPS 140-3** a été approuvée par le département du Commerce des États-Unis en 2019. La modification la plus notable apportée dans cette version est la spécification des normes ISO/CEI, notamment la norme 19790:2015 et la norme d'essai connexe 24759:2017. Le PVMC a instauré un programme de transition et signalé qu'à partir de 2020, les modules cryptographiques seront validés en fonction de la norme FIPS 140-3. Apple entend conformer ses modules cryptographiques à la norme FIPS 140-3 dans les meilleurs délais.

En ce qui concerne les modules cryptographiques actuellement en phase d'essai et de validation, le PVMC tient à jour deux listes distinctes qui peuvent contenir des informations au sujet des validations proposées. Pour ce qui est des modules cryptographiques en phase d'essai dans un laboratoire agréé, le module peut figurer sur la liste des implémentations à l'essai. Une fois que le laboratoire a terminé les essais et recommande la validation par le PVMC, le module cryptographique d'Apple figure sur la liste des modules en cours de traitement. La phase d'essai du laboratoire est alors terminée et le PVMC n'a plus qu'à la valider. Étant donné que la durée du processus d'évaluation est variable, consultez les deux listes ci-dessus pour déterminer l'état de validation des modules cryptographiques d'Apple entre la date de sortie d'une version majeure du système d'exploitation et l'émission du certificat de validation par le PVMC.

Certifications de produit : Critères communs ISO/CEI 15408

La norme des critères communs (ISO/CEI 15408) est utilisée par de nombreuses organisations comme base pour évaluer le niveau de sécurité des produits informatiques.

Pour connaître les certifications mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC), consultez le portail des critères communs. La norme des critères communs peut également être utilisée en dehors de l'ARCC, dans le cadre de schémas de validation nationaux et privés. En Europe, la reconnaissance mutuelle est régie par l'accord du SOG-IS et l'ARCC.

L'objectif, énoncé par la communauté des critères communs, consiste à établir un ensemble de normes de sécurité reconnu à l'échelle internationale pour fournir une évaluation claire et fiable des capacités de sécurité des produits informatiques. En fournissant une évaluation indépendante de la capacité d'un produit à satisfaire aux normes de sécurité, la certification des critères communs donne aux clients confiance en la sécurité des produits informatiques et permet des décisions plus éclairées.

En vertu de l'ARCC, les pays membres se sont entendus pour reconnaître la certification des produits informatiques avec le même degré de confiance. L'évaluation approfondie des éléments suivants est requise pour obtenir la certification :

- Profils de protection (PP)
- Cibles de sécurité (Security Targets, ST)
- Exigences fonctionnelles de sécurité (Security Functional Requirements, SFR)
- Exigences d'assurance de la sécurité (Security Assurance Requirements, SAR)
- Niveaux d'assurance de l'évaluation (Evaluation Assurance Levels, EAL)

Les profils de protection sont des documents qui précisent les besoins de sécurité d'une classe spécifique d'appareils, comme « Mobility » (mobilité). Ils sont utilisés pour permettre de comparer les évaluations de produits informatiques d'une même classe. L'adhésion à l'ARCC ainsi que la liste de PP continuent de croître chaque année. Cet arrangement permet au développeur de produits de prendre les mesures nécessaires pour obtenir une seule certification en vertu de n'importe lequel des schémas d'autorisation de certificat et de la faire reconnaître par n'importe lequel des signataires utilisateurs de certificats.

Les cibles de sécurité définissent ce qui sera évalué lors de la certification d'un produit informatique. Elles se traduisent par des *exigences fonctionnelles de sécurité* plus précises, utilisées pour une évaluation plus détaillée.

Les critères communs comprennent également les *exigences d'assurance de la sécurité*. Les *niveaux d'assurance de l'évaluation* sont une mesure communément établie. Ils regroupent les ensembles de SAR couramment utilisés et peuvent être spécifiés dans les PP et les ST pour soutenir la comparabilité.

De nombreux PP plus anciens ont été archivés et sont remplacés par des PP ciblés en cours de développement, qui sont axés sur des solutions et des environnements précis. Dans un effort concerté pour assurer une reconnaissance mutuelle entre tous les membres de l'ARCC, des communautés techniques internationales (iTC) ont été établies pour élaborer et maintenir les *profils de protection de collaboration (cPP)* conçus dès le départ avec la participation des schémas des signataires de l'ARCC. Des PP ciblant les groupes d'utilisateurs ainsi que des accords de reconnaissance mutuelle autres que l'ARCC continuent d'être élaborés par les parties prenantes appropriées.

Apple a commencé sa quête de certifications en vertu de l'ARCC pour certains cPP au début de 2015. Depuis, elle a obtenu les certifications des critères communs pour chaque version majeure d'iOS et a élargi la couverture pour inclure l'assurance de sécurité fournie par les nouveaux PP.

Apple joue un rôle actif dans les communautés techniques qui se concentrent sur l'évaluation des technologies de sécurité mobile. Cela comprend les iTC responsables de l'élaboration et de la mise à jour des cPP. Nous continuons d'évaluer et d'obtenir des certifications relativement aux PP et aux cPP actuels.

Les certifications des plateformes Apple pour le marché nord-américain sont généralement réalisées avec le National Information Assurance Partnership (NIAP), qui tient à jour une liste des projets en cours d'évaluation qui n'ont pas encore été certifiés.

En plus des certifications de plateformes générales indiquées, d'autres certificats ont été délivrés afin de démontrer les besoins de sécurité propres à certains marchés.

Certifications de sécurité pour iOS

Contexte de la certification d'iOS

Apple participe activement à la validation de ses modules logiciels et matériels intégrés pour chaque version majeure d'un système d'exploitation. La validation de la conformité est possible uniquement pour une version finale publiée.

État de la validation des modules cryptographiques pour iOS

Le Programme de validation des modules cryptographiques (PVMC) tient à jour l'état de validation des modules cryptographiques sur trois listes distinctes, selon leur état du moment :

- Pour figurer sur la liste des implémentations à l'essai du PVMC, le laboratoire doit avoir reçu d'Apple le mandat de procéder à des tests.
- Lorsque les tests sont terminés, que le laboratoire a recommandé la validation par le PVMC et que les frais du PVMC ont été payés, le module est ajouté à la liste des modules en cours de traitement (MIP). Cette liste suit la progression des efforts de validation du PVMC en quatre phases :
  - *En attente de révision :* Le module attend l'assignation d'une ressource du PVMC.
  - *En révision :* Les ressources du PVMC effectuent leurs activités de validation.
  - *Coordination :* Le laboratoire et le PVMC résolvent les problèmes détectés.
  - *Finalisation :* Les activités et les formalités liées à la délivrance du certificat sont achevées.
- Lorsqu'ils ont été validés par le PVMC, les modules reçoivent un certificat de conformité et sont ajoutés à la liste des modules cryptographiques validés. Parmi ceux-ci se trouvent :
  - les modules validés qui sont marqués comme actifs;
  - les modules qui, après cinq ans, sont marqués comme historiques;
  - si le certificat d'un module est révoqué pour une raison quelconque, ce dernier est marqué en conséquence.

En 2020, le PVMC a adopté la norme internationale ISO/CEI 19790 comme base pour la norme FIPS 140-3.

Certifications FIPS 140-3

État actuel

Les tests de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection d'iOS 14 (2020) sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Les tests des modules de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection d'iOS 15 (2021) sont en cours. Ils figurent sur la liste des implémentations à l'essai.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* iOS 15 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* iOS 15 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec iOS 15 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec iOS 15 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A13, A14, A15) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* iOS 14 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* iOS 14 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec iOS 14 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec iOS 14 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A13-A14) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3

Certifications FIPS 140-2

Le tableau ci-dessous indique les modules cryptographiques actuellement testés par le laboratoire ou qui l'ont été pour vérifier leur conformité avec la norme FIPS 140-2.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3856 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* iOS 13 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3855 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* iOS 13 *Type :* logiciel *Niveau de sécurité :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-02-05	*Certificats :* 3811 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v10.0 *Système d'exploitation :* sepOS distribué avec iOS 13 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-23	*Certificats :* 3438 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* iOS 12 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-11	*Certificats :* 3433 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* iOS 12 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-09-10	*Certificats :* 3523 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v9.0 *Système d'exploitation :* sepOS distribué avec iOS 12 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-22, 2018-07-06	*Certificats :* 3148 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* iOS 11 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-17, 2018-07-03	*Certificats :* 3147 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* iOS 11 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2019-09-10	*Certificats :* 3223 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v1.0 *Système d'exploitation :* sepOS distribué avec iOS 11 *Type :* matériel *Niveau de sécurité :* 2

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2016 *Dates de validation :* 2017-02-01	*Certificats :* 2828 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v7.0 pour iOS *Système d'exploitation :* iOS 10 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2016 *Dates de validation :* 2017-02-01	*Certificats :* 2827 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v7.0 pour iOS *Système d'exploitation :* iOS 10 *Type :* logiciel *Niveau de sécurité :* 1

Anciennes versions

Les certificats datant de plus de cinq ans sont répertoriés par le PVMC avec l'état historique. Ces anciennes versions d'iOS disposaient de la validation des modules cryptographiques :

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

Contexte de la certification des critères communs (CC)

Apple participe activement à l'évaluation d'iOS pour chaque version majeure du système d'exploitation. L'évaluation ne peut être effectuée que par rapport à la version finale du système d'exploitation. Avant iPadOS 13.1, iPadOS s'appelait iOS.

État des certifications des critères communs

Le schéma américain, qui relève du NIAP, tient à jour une liste des produits en évaluation. Cette liste comprend les produits qui, d'une part, sont en cours d'évaluation aux États-Unis avec un laboratoire d'essais selon les critères communs (Common Criteria Testing Laboratory, CCTL) approuvé par le NIAP, et qui, d'autre part, ont fait l'objet d'une réunion d'évaluation préliminaire (ou l'équivalent) où la direction du schéma d'évaluation et de validation lié aux critères communs (Common Criteria Evaluation and Validation Scheme, CCEVS) les a officiellement acceptés pour évaluation.

Après la certification des produits, le NIAP répertorie les certifications valides sur la liste des produits conformes. Au bout de deux ans, ces certifications sont examinées pour vérifier leur conformité avec la politique de maintien de l'assurance actuelle. À l'expiration du maintien de l'assurance, le NIAP fait passer la certification sur sa liste des produits archivés.

Le portail des critères communs répertorie les certifications qui peuvent être mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC). Le portail des CC peut laisser les produits sur la liste des produits certifiés pendant cinq ans. Il tient des dossiers sur les certifications archivées.

Le tableau ci-dessous indique les certifications en cours d'évaluation par un laboratoire, ou celles dont on a confirmé la conformité avec les critères communs.

État actuel

Les tests de laboratoire pour les évaluations auprès du NIAP visant iOS 15 sont en cours. Pour obtenir les renseignements les plus récents, consultez la liste des produits en évaluation et la liste des produits conformes.

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : iOS 15 *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* —	*Titre :* Apple iOS 15 : iPhone *Profils de protection :* bases des appareils mobiles (modules PP à confirmer)
Système d'exploitation : iOS 14 *Date de certification :* 2021-09-01	*ID du schéma :* 11146 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* Apple iOS 14 : iPhone *Profils de protection :* bases des appareils mobiles, module de client VPN, module PP pour clients de réseau local sans fil, EP pour agent de GAM
Système d'exploitation : iOS 13 *Date de certification :* 2020-11-06	*ID du schéma :* 11036 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* iOS 13 d'Apple sur iPhone *Profils de protection :* bases des appareils mobiles, module de client VPN, EP pour clients de réseau local sans fil, EP pour agent de GAM

Certifications archivées des critères communs pour iOS

Ces anciennes versions d'iOS disposaient de la validation des critères communs. Elles sont archivées par le NIAP en fonction de sa politique :

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : iOS 12 *Date de certification :* 2019-03-14	*ID du schéma :* 10937 *Documents :* Cible de sécurité Guide	*Titre :* iPhone doté d'iOS 12 *Profils de protection :* bases des appareils mobiles, module de client VPN, EP pour client de réseau local sans fil, EP pour agent de GAM
Système d'exploitation : iOS 11 *Date de certification :* 2018-07-17	*ID du schéma :* 10851 *Documents :* Cible de sécurité Guide	*Titre :* Apple iOS 11 *Profils de protection :* bases des appareils mobiles, EP pour client de réseau local sans fil, EP pour agent de GAM
Système d'exploitation : iOS 10 *Date de certification :* 2017-07-27	*ID du schéma :* 10782 *Documents :* Cible de sécurité Guide	*Titre :* iOS 10.2 sur les appareils iPhone et iPad *Profils de protection :* bases des appareils mobiles, EP pour client de réseau local sans fil, EP pour agent de GAM
Système d'exploitation : iOS 10 *Date de certification :* 2017-07-27	*ID du schéma :* 10792 *Documents :* Cible de sécurité Guide	*Titre :* iOS 10.2, client VPN sur les appareils iPhone et iPad *Profils de protection :* Client VPN (PP)
Système d'exploitation : iOS 9 *Date de certification :* 2016-10-14	*ID du schéma :* 10725 *Documents :* Cible de sécurité Guide	*Titre :* iOS 9.3.2 avec agent de GMA *Profils de protection :* bases des appareils mobiles, EP pour agent de GAM
Système d'exploitation : iOS 9 *Date de certification :* 2016-10-13	*ID du schéma :* 10714 *Documents :* Cible de sécurité Guide	*Titre :* Client VPN du système d'exploitation sur iPhone et iPad *Profils de protection :* Client VPN (PP)
Système d'exploitation : iOS 9 *Date de certification :* 2016-01-28	*ID du schéma :* 10695 *Documents :* Cible de sécurité Guide	*Titre :* iOS 9 *Profils de protection :* bases des appareils mobiles

Certifications de sécurité pour iPadOS

Contexte de la certification d'iPadOS

Apple participe activement à la validation de ses systèmes d'exploitation pour chaque version majeure à l'aide de profils de protection de collaboration et des niveaux de sécurité conformes à la norme FIPS 140-3. La validation de la conformité est possible uniquement pour une version finale publiée.

Remarque : En 2019, le système d'exploitation des appareils iPad est devenu iPadOS. Avant iPadOS 13.1, iPadOS s'appelait iOS.

État de la validation des modules cryptographiques pour iPadOS

Le Programme de validation des modules cryptographiques (PVMC) tient à jour l'état de validation des modules cryptographiques sur trois listes distinctes, selon leur état du moment :

- Pour figurer sur la liste des implémentations à l'essai du PVMC, le laboratoire doit avoir reçu d'Apple le mandat de procéder à des tests.
- Lorsque les tests sont terminés, que le laboratoire a recommandé la validation par le PVMC et que les frais du PVMC ont été payés, le module est ajouté à la liste des modules en cours de traitement (MIP). Cette liste suit la progression des efforts de validation du PVMC en quatre phases :
  - *En attente de révision :* Le module attend l'assignation d'une ressource du PVMC.
  - *En révision :* Les ressources du PVMC effectuent leurs activités de validation.
  - *Coordination :* Le laboratoire et le PVMC résolvent les problèmes détectés.
  - *Finalisation :* Les activités et les formalités liées à la délivrance du certificat sont achevées.
- Lorsqu'ils ont été validés par le PVMC, les modules reçoivent un certificat de conformité et sont ajoutés à la liste des modules cryptographiques validés. Parmi ceux-ci se trouvent :
  - les modules validés qui sont marqués comme actifs;
  - les modules qui, après cinq ans, sont marqués comme historiques;
  - si le certificat d'un module est révoqué pour une raison quelconque, ce dernier est marqué en conséquence.

En 2020, le PVMC a adopté la norme internationale ISO/CEI 19790 comme base pour la norme FIPS 140-3.

Certifications FIPS 140-3

État actuel

Les tests de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection d'iPadOS 14 (2020) sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Les tests des modules de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection d'iPadOS 15 (2021) sont en cours. Ils figurent sur la liste des implémentations à l'essai.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* iPadOS 15 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* iPadOS 15 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec iPadOS 15 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14, M1) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec iPadOS 15 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14, M1) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* iPadOS 14 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* iPadOS 14 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec iPadOS 14 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14, M1) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec iPadOS 14 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A9-A14, M1) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3

Certifications FIPS 140-2

Le tableau ci-dessous indique les modules cryptographiques actuellement testés par le laboratoire ou qui l'ont été pour vérifier leur conformité avec la norme FIPS 140-2.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3856 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* iPadOS 13 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3855 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* iPadOS 13 *Type :* logiciel *Niveau de sécurité :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-02-05	*Certificats :* 3811 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Corecrypto Apple v10.0 *Système d'exploitation :* sepOS distribué avec iPadOS 13 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-23	*Certificats :* 3438 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* iOS 12 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-11	*Certificats :* 3433 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* iOS 12 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-09-10	*Certificats :* 3523 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v9.0 *Système d'exploitation :* sepOS distribué avec iOS 12 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-22, 2018-07-06	*Certificats :* 3148 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* iOS 11 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-17, 2018-07-03	*Certificats :* 3147 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* iOS 11 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2019-09-10	*Certificats :* 3223 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v1.0 *Système d'exploitation :* sepOS distribué avec iOS 11 *Type :* matériel *Niveau de sécurité :* 2

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2016 *Dates de validation :* 2017-02-01	*Certificats :* 2828 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v7.0 pour iOS *Système d'exploitation :* iOS 10 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2016 *Dates de validation :* 2017-02-01	*Certificats :* 2827 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v7.0 pour iOS *Système d'exploitation :* iOS 10 *Type :* logiciel *Niveau de sécurité :* 1

Anciennes versions

Les certificats datant de plus de cinq ans sont répertoriés par le PVMC avec l'état historique. Ces anciennes versions d'iOS disposaient de la validation des modules cryptographiques :

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

Contexte de la certification des critères communs (CC)

Apple participe activement à l'évaluation d'iPadOS pour chaque version majeure du système d'exploitation. L'évaluation ne peut être effectuée que par rapport à la version finale du système d'exploitation.

État des certifications des critères communs

Le schéma américain, qui relève du NIAP, tient à jour une liste des produits en évaluation. Cette liste comprend les produits qui, d'une part, sont en cours d'évaluation aux États-Unis avec un laboratoire d'essais selon les critères communs (Common Criteria Testing Laboratory, CCTL) approuvé par le NIAP, et qui, d'autre part, ont fait l'objet d'une réunion d'évaluation préliminaire (ou l'équivalent) où la direction du schéma d'évaluation et de validation lié aux critères communs (Common Criteria Evaluation and Validation Scheme, CCEVS) les a officiellement acceptés pour évaluation.

Après la certification des produits, le NIAP répertorie les certifications valides sur la liste des produits conformes. Au bout de deux ans, ces certifications sont examinées pour vérifier leur conformité avec la politique de maintien de l'assurance actuelle. À l'expiration du maintien de l'assurance, le NIAP fait passer la certification sur sa liste des produits archivés.

Le portail des critères communs répertorie les certifications qui peuvent être mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC). Le portail des CC peut laisser les produits sur la liste des produits certifiés pendant cinq ans. Il tient des dossiers sur les certifications archivées.

Le tableau ci-dessous indique les certifications en cours d'évaluation par un laboratoire, ou celles dont on a confirmé la conformité avec les critères communs.

État actuel

Les tests de laboratoire pour les évaluations auprès du NIAP visant iPadOS 15 sont en cours. Pour obtenir les renseignements les plus récents, consultez la liste des produits en évaluation et la liste des produits conformes.

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : iPadOS 15 *Date de certification :* 2019-03-14	*ID du schéma :* — *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* iPad doté d'iOS 12 *Profils de protection :* bases des appareils mobiles, module de client VPN, EP pour client de réseau local sans fil, EP pour agent de GAM
Système d'exploitation : iPadOS 14 *Date de certification :* 2021-09-01	*ID du schéma :* 11147 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* Apple iPadOS 14 : iPad *Profils de protection :* bases des appareils mobiles, module de client VPN, EP pour client de réseau local sans fil, EP pour agent de GAM
Système d'exploitation : iPadOS 13 *Date de certification :* 2020-11-06	*ID du schéma :* 11036 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* iPadOS 13 sur les appareils mobiles iPad *Profils de protection :* bases des appareils mobiles, module de client VPN, EP pour client de réseau local sans fil, EP pour agent de GAM

Anciennes versions

Ces anciennes versions d'iOS disposaient de la validation des critères communs. Elles sont archivées par le NIAP en fonction de sa politique :

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

Certifications de sécurité pour macOS

Contexte de la certification de macOS

Apple participe activement à la validation de ses systèmes d'exploitation pour chaque version majeure à l'aide de profils de protection de collaboration et des niveaux de sécurité conformes à la norme FIPS 140-3. La validation de la conformité est possible uniquement pour une version finale publiée.

État de la validation des modules cryptographiques pour macOS

Le Programme de validation des modules cryptographiques (PVMC) tient à jour l'état de validation des modules cryptographiques sur trois listes distinctes, selon leur état du moment :

- Pour figurer sur la liste des implémentations à l'essai du PVMC, le laboratoire doit avoir reçu d'Apple le mandat de procéder à des tests.
- Lorsque les tests sont terminés, que le laboratoire a recommandé la validation par le PVMC et que les frais du PVMC ont été payés, le module est ajouté à la liste des modules en cours de traitement (MIP). Cette liste suit la progression des efforts de validation du PVMC en quatre phases :
  - *En attente de révision :* Le module attend l'assignation d'une ressource du PVMC.
  - *En révision :* Les ressources du PVMC effectuent leurs activités de validation.
  - *Coordination :* Le laboratoire et le PVMC résolvent les problèmes détectés.
  - *Finalisation :* Les activités et les formalités liées à la délivrance du certificat sont achevées.
- Lorsqu'ils ont été validés par le PVMC, les modules reçoivent un certificat de conformité et sont ajoutés à la liste des modules cryptographiques validés. Parmi ceux-ci se trouvent :
  - les modules validés qui sont marqués comme actifs;
  - les modules qui, après cinq ans, sont marqués comme historiques;
  - si le certificat d'un module est révoqué pour une raison quelconque, ce dernier est marqué en conséquence.

En 2020, le PVMC a adopté la norme internationale ISO/CEI 19790 comme base pour la norme FIPS 140-3.

Pour les ordinateurs Mac, le tableau ci-dessous indique quels modules cryptographiques s'appliquent à quelle technologie de Mac.

Module cryptographique	Ordinateur Mac avec puce Apple	Ordinateurs Mac avec puce T2 Security d'Apple	Ordinateurs Mac avec processeur Intel sans puce T2 Security d'Apple
Espace utilisateur puce Apple	✓		
Noyau puce Apple	✓		
Espace utilisateur Intel		✓	✓
Noyau Intel		✓	✓
Gestion des clés de protection	✓	✓	

Certifications FIPS 140-3

En 2020, Apple a lancé des ordinateurs Mac avec puce Apple. L'applicabilité des modules cryptographiques pour les ordinateurs Mac avec puce Apple ou processeur Intel est indiquée dans la colonne « Renseignements sur le module » du tableau ci-dessous.

Remarque : Les puces T2 Security d'Apple sont présentes dans de nombreux ordinateurs Mac avec processeur Intel. Pour en savoir plus sur les certifications de la puce T2, consultez Certifications de sécurité pour la puce T2 Security d'Apple.

Client SSH de macOS

OpenSSH peut être configuré pour l'utilisation des modules dont la conformité avec les normes FIPS 140-3 a été validée avec des algorithmes FIPS 140-3 particuliers. Les organisations peuvent exécuter un programme d'installation signé et authentifié disponible auprès d'Apple au moyen du mot de passe *FIPS140Mode*. Le programme d'installation insère deux fichiers sur le Mac :

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

macOS utilise ensuite ces fichiers pour restreindre les codes accessibles par OpenSSH à ceux validés par le NIST et s'assure que le client OpenSSH utilise le module cryptographique validé fourni en fonction de la plateforme. Les administrateurs peuvent aussi créer leurs propres fichiers. Pour en savoir plus, consultez la page de manuel `apple_ssh_and_fips` sous macOS 12.0.1 ou version ultérieure.

État actuel

Les tests de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de macOS 11 Big Sur sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Les tests des modules de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de macOS 12 Monterey sont en cours. Ils figurent sur la liste des implémentations à l'essai.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* macOS 12 Monterey sur puce Apple *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* macOS 12 Monterey sur puce Apple *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* macOS 12 Monterey sur processeur Intel *Environnement :* Intel, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* macOS 12 Monterey sur processeur Intel *Environnement :* Intel, noyau, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Systèmes d'exploitation :* sepOS distribué avec macOS 12 Monterey sur puce Apple, sepOS distribué avec macOS 12 Monterey sur processeur Intel avec puce T2 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (M1 et T2) *Niveau de sécurité :* 2

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec macOS 12 Monterey sur puce Apple *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (M1) *Niveau de sécurité :* 2 *Niveau de sécurité physique :* 3
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* macOS 11 Big Sur sur processeur Intel *Environnement :* Intel, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* macOS 11 Big Sur sur processeur Intel *Environnement :* Intel, noyau, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* macOS 11 Big Sur sur puce Apple *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* macOS 11 Big Sur sur puce Apple *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Systèmes d'exploitation :* sepOS distribué avec macOS 11 Big Sur sur puce Apple, sepOS distribué avec macOS 11 Big Sur sur processeur Intel *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (M1) *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec macOS 11 Big Sur sur puce Apple *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (M1) *Niveau de sécurité :* 2 *Niveau de sécurité physique :* 3

Certifications FIPS 140-2

Le tableau ci-dessous indique les modules cryptographiques actuellement testés par le laboratoire ou qui l'ont été pour vérifier leur conformité avec la norme FIPS 140-2.

Les tests de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de macOS 10.15 Catalina sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Remarque : Les puces T2 Security d'Apple sont présentes dans de nombreux ordinateurs Mac avec processeur Intel. Pour en savoir plus sur les certifications de la puce T2, consultez Certifications de sécurité pour la puce T2 Security d'Apple.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-24	*Certificats :* 3859 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module espace utilisateur Corecrypto Apple pour Intel (ccv10) *Système d'exploitation :* macOS 10.15 Catalina *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-24	*Certificats :* 3858 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v10.0 pour Intel (ccv10) *Système d'exploitation :* macOS 10.15 Catalina *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-12	*Certificats :* 3402 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v9.0 pour Intel *Système d'exploitation :* macOS 10.14 Mojave *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-12	*Certificats :* 3431 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v9.0 pour Intel *Système d'exploitation :* macOS 10.14 Mojave *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-22	*Certificats :* 3155 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v8.0 pour Intel *Système d'exploitation :* macOS 10.13 High Sierra *Type :* logiciel *Niveau de sécurité :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-22	*Certificats :* 3156 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v8.0 pour Intel *Système d'exploitation :* macOS 10.13 High Sierra *Type :* logiciel *Niveau de sécurité :* 1

Anciennes versions

Ces anciennes versions d'OS X et de macOS disposaient de la validation des modules cryptographiques. Celles datant de plus de cinq ans sont répertoriées par le PVMC avec l'état historique :

- 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

Contexte de la certification des critères communs (CC)

Apple participe activement à l'évaluation de macOS pour chaque version majeure du système d'exploitation. L'évaluation ne peut être effectuée que par rapport à la version finale du système d'exploitation.

État des certifications des critères communs

Le schéma américain, qui relève du NIAP, tient à jour une liste des produits en évaluation. Cette liste comprend les produits qui, d'une part, sont en cours d'évaluation aux États-Unis avec un laboratoire d'essais selon les critères communs (Common Criteria Testing Laboratory, CCTL) approuvé par le NIAP, et qui, d'autre part, ont fait l'objet d'une réunion d'évaluation préliminaire (ou l'équivalent) où la direction du schéma d'évaluation et de validation lié aux critères communs (Common Criteria Evaluation and Validation Scheme, CCEVS) les a officiellement acceptés pour évaluation.

Après la certification des produits, le NIAP répertorie les certifications valides sur la liste des produits conformes. Au bout de deux ans, ces certifications sont examinées pour vérifier leur conformité avec la politique de maintien de l'assurance actuelle. À l'expiration du maintien de l'assurance, le NIAP fait passer la certification sur sa liste des produits archivés.

Le portail des critères communs répertorie les certifications qui peuvent être mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC). Le portail des CC peut laisser les produits sur la liste des produits certifiés pendant cinq ans. Il tient des dossiers sur les certifications archivées.

Le tableau ci-dessous indique les certifications en cours d'évaluation par un laboratoire, ou celles dont on a confirmé la conformité avec les critères communs.

État actuel

Les évaluations avec le NIAP pour macOS 11 et macOS 12 utilisant les profils de protection pour système d'exploitation d'usage général et chiffrement complet du disque (AA et EE) sont en cours.

Pour obtenir les renseignements les plus récents, consultez la liste des produits en évaluation et la liste des produits conformes.

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : macOS 12 Monterey *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* —	*Titre :* Apple FileVault 2 sous macOS 12 Monterey *Profils de protection :* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (profils de protection à confirmer)
Système d'exploitation : macOS 12 Monterey *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* —	*Titre :* macOS 12 Monterey *Profils de protection :* PP_OS_V4.21 (profils de protection à confirmer)

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : macOS 11 Big Sur *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* Apple FileVault 2 sous macOS 11 Big Sur *Profils de protection :* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Système d'exploitation : macOS 11 Big Sur *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* Apple macOS 11 Big Sur *Profils de protection :* PP_OS_V4.21
Système d'exploitation : macOS 10.15 Catalina *Date de certification :* 2021-04-29	*ID du schéma :* 11078 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* Apple FileVault 2 sur les ordinateurs dotés d'une puce T2 sous macOS 10.15 Catalina *Profils de protection :* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Système d'exploitation : macOS 10.15 Catalina *Date de certification :* 2020-09-23	*ID du schéma :* 11077 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* macOS 10.15 Catalina *Profils de protection :* PP_OS_V4.21

Certifications de sécurité pour tvOS

Contexte de la certification de tvOS

Apple participe activement à la validation des modules cryptographiques associés à chaque version majeure de tvOS. La validation de la conformité est possible uniquement pour une version finale publiée.

État de la validation des modules cryptographiques pour tvOS

Le Programme de validation des modules cryptographiques (PVMC) tient à jour l'état de validation des modules cryptographiques sur trois listes distinctes, selon leur état du moment :

- Pour figurer sur la liste des implémentations à l'essai du PVMC, le laboratoire doit avoir reçu d'Apple le mandat de procéder à des tests.
- Lorsque les tests sont terminés, que le laboratoire a recommandé la validation par le PVMC et que les frais du PVMC ont été payés, le module est ajouté à la liste des modules en cours de traitement (MIP). Cette liste suit la progression des efforts de validation du PVMC en quatre phases :
  - *En attente de révision :* Le module attend l'assignation d'une ressource du PVMC.
  - *En révision :* Les ressources du PVMC effectuent leurs activités de validation.
  - *Coordination :* Le laboratoire et le PVMC résolvent les problèmes détectés.
  - *Finalisation :* Les activités et les formalités liées à la délivrance du certificat sont achevées.
- Lorsqu'ils ont été validés par le PVMC, les modules reçoivent un certificat de conformité et sont ajoutés à la liste des modules cryptographiques validés. Parmi ceux-ci se trouvent :
  - les modules validés qui sont marqués comme actifs;
  - les modules qui, après cinq ans, sont marqués comme historiques;
  - si le certificat d'un module est révoqué pour une raison quelconque, ce dernier est marqué en conséquence.

En 2020, le PVMC a adopté la norme internationale ISO/CEI 19790 comme base pour la norme FIPS 140-3.

Certifications FIPS 140-3

État actuel

Les tests de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de tvOS 14 (2020) sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Les tests des modules de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de tvOS 15 (2021) sont en cours. Ils figurent sur la liste des implémentations à l'essai.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* tvOS 15 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* tvOS 15 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec tvOS 15 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A10, A12) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* tvOS 14 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* tvOS 14 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec tvOS 14 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (A10, A12) *Niveau de sécurité globale :* 2

Certifications FIPS 140-2

Le tableau ci-dessous indique les modules cryptographiques actuellement testés par le laboratoire ou qui l'ont été pour vérifier leur conformité avec la norme FIPS 140-2.

Les tests de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de tvOS 13 (2019) sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3856 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* tvOS 13 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-03-23	*Certificats :* 3855 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* tvOS 13 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-02-05	*Certificats :* 3811 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v10.0 *Système d'exploitation :* sepOS distribué avec tvOS 13 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-23	*Certificats :* 3438 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* tvOS 12 *Type :* logiciel *Niveau de sécurité :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-11	*Certificats :* 3433 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* tvOS 12 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-09-10	*Certificats :* 3523 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v9.0 *Système d'exploitation :* sepOS distribué avec tvOS 12 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-22, 2018-07-06	*Certificats :* 3148 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* tvOS 11 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-17, 2018-07-03	*Certificats :* 3147 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* tvOS 11 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2019-09-10	*Certificats :* 3223 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v1.0 *Système d'exploitation :* sepOS distribué avec tvOS 11 *Type :* matériel *Niveau de sécurité :* 2

Certifications de sécurité pour watchOS

Contexte de la certification de watchOS

Apple participe activement à la validation des modules cryptographiques associés à chaque version majeure de watchOS. La validation de la conformité est possible uniquement pour une version finale publiée.

État de la validation des modules cryptographiques pour watchOS

Le Programme de validation des modules cryptographiques (PVMC) tient à jour l'état de validation des modules cryptographiques sur trois listes distinctes, selon leur état du moment :

- Pour figurer sur la liste des implémentations à l'essai du PVMC, le laboratoire doit avoir reçu d'Apple le mandat de procéder à des tests.
- Lorsque les tests sont terminés, que le laboratoire a recommandé la validation par le PVMC et que les frais du PVMC ont été payés, le module est ajouté à la liste des modules en cours de traitement (MIP). Cette liste suit la progression des efforts de validation du PVMC en quatre phases :
  - *En attente de révision :* Le module attend l'assignation d'une ressource du PVMC.
  - *En révision :* Les ressources du PVMC effectuent leurs activités de validation.
  - *Coordination :* Le laboratoire et le PVMC résolvent les problèmes détectés.
  - *Finalisation :* Les activités et les formalités liées à la délivrance du certificat sont achevées.
- Lorsqu'ils ont été validés par le PVMC, les modules reçoivent un certificat de conformité et sont ajoutés à la liste des modules cryptographiques validés. Parmi ceux-ci se trouvent :
  - les modules validés qui sont marqués comme actifs;
  - les modules qui, après cinq ans, sont marqués comme historiques;
  - si le certificat d'un module est révoqué pour une raison quelconque, ce dernier est marqué en conséquence.

En 2020, le PVMC a adopté la norme internationale ISO/CEI 19790 comme base pour la norme FIPS 140-3.

Certifications FIPS 140-3

État actuel

Les tests de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de watchOS 7 (2020) sont terminés et le laboratoire a recommandé leur validation au PVMC. Ils figurent sur la liste des modules en cours de traitement.

Les tests des modules de l'espace utilisateur, de l'espace de noyau et de la gestion des clés de protection de watchOS 8 (2021) sont en cours. Ils figurent sur la liste des implémentations à l'essai.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* watchOS 8 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* watchOS 8 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec watchOS 8 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (S3, S4, S5, S6) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2021 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v12.0 *Système d'exploitation :* sepOS distribué avec watchOS 8 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (S6) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* watchOS 7 *Environnement :* puce Apple, utilisateur, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* watchOS 7 *Environnement :* puce Apple, noyau, logiciel *Type :* logiciel *Niveau de sécurité globale :* 1
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec watchOS 7 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (S3, S4, S5, S6) *Niveau de sécurité globale :* 2
Date de lancement du système d'exploitation : 2020 *Dates de validation :* —	*Certificats :* Pas encore certifié *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module Corecrypto Apple v11.1 *Système d'exploitation :* sepOS distribué avec watchOS 7 *Environnement :* puce Apple, gestion des clés de protection, matériel *Type :* matériel (S6) *Niveau de sécurité globale :* 2 *Niveau de sécurité physique :* 3

Certifications FIPS 140-2

Le tableau ci-dessous indique les modules cryptographiques actuellement testés par le laboratoire ou qui l'ont été pour vérifier leur conformité avec la norme FIPS 140-2.

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* —	*Certificats :* 3856 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* watchOS 6 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2019 *Dates de validation :* —	*Certificats :* 3855 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v10.0 pour ARM *Système d'exploitation :* watchOS 6 *Type :* logiciel *Niveau de sécurité :* 1

Dates	Certificats et documents	Renseignements sur le module
Date de lancement du système d'exploitation : 2019 *Dates de validation :* 2021-02-05	*Certificats :* 3811 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v10.0 *Système d'exploitation :* sepOS distribué avec watchOS 6 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-23	*Certificats :* 3438 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* watchOS 5 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-04-11	*Certificats :* 3433 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v9.0 pour ARM *Système d'exploitation :* watchOS 5 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2018 *Dates de validation :* 2019-09-10	*Certificats :* 3523 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v9.0 *Système d'exploitation :* sepOS distribué avec watchOS 5 *Type :* matériel *Niveau de sécurité :* 2
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-22, 2018-07-06	*Certificats :* 3148 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module utilisateur Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* watchOS 4 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2018-03-09, 2018-05-17, 2018-07-03	*Certificats :* 3147 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module noyau Corecrypto Apple v8.0 pour ARM *Système d'exploitation :* watchOS 4 *Type :* logiciel *Niveau de sécurité :* 1
Date de lancement du système d'exploitation : 2017 *Dates de validation :* 2019-09-10	*Certificats :* 3223 *Documents :* Certificat Politique de sécurité Guide du rôle de responsable du chiffrement	*Titre :* Module cryptographique pour la gestion des clés de protection Apple v1.0 *Système d'exploitation :* sepOS distribué avec watchOS 4 *Type :* matériel *Niveau de sécurité :* 2

Certifications de sécurité des logiciels

Aperçu des certifications de sécurité des logiciels Apple

Apple détient, entre autres, les certificats de validation de la conformité aux normes FIPS 140-2/-3 des États-Unis pour sepOS et le programme interne de la puce T2. Nous commençons par des *éléments de structure de certification* qui s'appliquent de manière générale à plusieurs plateformes au besoin. Un de ces éléments de structure est la validation de Corecrypto utilisé pour les déploiements de modules cryptographiques logiciels et matériels dans les systèmes d'exploitation développés par Apple. Un deuxième correspond à la certification du Secure Enclave intégré dans de nombreux appareils Apple. Un troisième correspond à la certification du Secure Element, qui se trouve dans les appareils Apple dotés de Touch ID et ceux dotés de Face ID. Ces éléments de structure de certification matérielle forment la base des certifications générales de sécurité des plateformes.

Certifications de produit : Critères communs ISO/CEI 15408

La norme des critères communs (ISO/CEI 15408) est utilisée par de nombreuses organisations comme base pour évaluer le niveau de sécurité des produits informatiques.

Pour connaître les certifications mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC), consultez le portail des critères communs. La norme des critères communs peut également être utilisée en dehors de l'ARCC, dans le cadre de schémas de validation nationaux et privés. En Europe, la reconnaissance mutuelle est régie par l'accord du SOG-IS et l'ARCC.

L'objectif, énoncé par la communauté des critères communs, consiste à établir un ensemble de normes de sécurité reconnu à l'échelle internationale pour fournir une évaluation claire et fiable des capacités de sécurité des produits informatiques. En fournissant une évaluation indépendante de la capacité d'un produit à satisfaire aux normes de sécurité, la certification des critères communs donne aux clients confiance en la sécurité des produits informatiques et permet des décisions plus éclairées.

En vertu de l'ARCC, les pays membres se sont entendus pour reconnaître la certification des produits informatiques avec le même degré de confiance. L'évaluation approfondie des éléments suivants est requise pour obtenir la certification :

- Profils de protection (PP)
- Cibles de sécurité (Security Targets, ST)
- Exigences fonctionnelles de sécurité (Security Functional Requirements, SFR)
- Exigences d'assurance de la sécurité (Security Assurance Requirements, SAR)
- Niveaux d'assurance de l'évaluation (Evaluation Assurance Levels, EAL)

Les profils de protection sont des documents qui précisent les besoins de sécurité d'une classe spécifique d'appareils, comme « Mobility » (mobilité). Ils sont utilisés pour permettre de comparer les évaluations de produits informatiques d'une même classe. L'adhésion à l'ARCC ainsi que la liste de PP continuent de croître chaque année. Cet arrangement permet au développeur de produits de prendre les mesures nécessaires pour obtenir une seule certification en vertu de n'importe lequel des schémas d'autorisation de certificat et de la faire reconnaître par n'importe lequel des signataires utilisateurs de certificats.

Les cibles de sécurité définissent *ce* qui sera évalué lors de la certification d'un produit informatique. Elles se traduisent par des *exigences fonctionnelles de sécurité* plus précises, utilisées pour une évaluation plus détaillée.

Les critères communs comprennent également les *exigences d'assurance de la sécurité*. Les *niveaux d'assurance de l'évaluation* sont une mesure communément établie. Ils regroupent les ensembles de SAR couramment utilisés et peuvent être spécifiés dans les PP et les ST pour soutenir la comparabilité.

De nombreux PP plus anciens ont été archivés et sont remplacés par des PP ciblés en cours de développement, qui sont axés sur des solutions et des environnements précis. Dans un effort concerté pour assurer une reconnaissance mutuelle entre tous les membres de l'ARCC, des communautés techniques internationales (iTC) ont été établies pour élaborer et maintenir les profils de protection de collaboration (cPP) conçus dès le départ avec la participation des schémas des signataires de l'ARCC. Des PP ciblant les groupes d'utilisateurs ainsi que des accords de reconnaissance mutuelle autres que l'ARCC continuent d'être élaborés par les parties prenantes appropriées.

Apple a commencé sa quête de certifications en vertu de l'ARCC pour certains cPP au début de 2015. Depuis, elle a obtenu les certifications des critères communs pour chaque version majeure d'iOS et a élargi la couverture pour inclure l'assurance de sécurité fournie par les nouveaux PP.

Apple joue un rôle actif dans les communautés techniques qui se concentrent sur l'évaluation des technologies de sécurité mobile. Cela comprend les iTC responsables de l'élaboration et de la mise à jour des cPP. Nous continuons d'évaluer et d'obtenir des certifications relativement aux PP et aux cPP actuels.

Les certifications des plateformes Apple pour le marché nord-américain sont généralement réalisées avec le National Information Assurance Partnership (NIAP), qui tient à jour une liste des projets en cours d'évaluation qui n'ont pas encore été certifiés.

En plus des certifications de plateformes générales indiquées, d'autres certificats ont été délivrés afin de démontrer les besoins de sécurité propres à certains marchés.

Certifications de sécurité pour les apps Apple

Contexte de la certification des apps Apple

Apple participe activement à la certification de la sécurité des apps Apple à l'aide des profils de protection (PP) liés aux critères communs appropriés. Ces évaluations s'appuient sur les certifications du matériel et des systèmes d'exploitation qu'Apple a obtenues.

En 2018, la société a lancé des évaluations de la sécurité des apps pour les applications clés fonctionnant sous iOS 11 avec le navigateur Safari et l'app Contacts. Elle a continué ces évaluations sur les apps fonctionnant sous iOS 12, iOS 13 et iPadOS 13.1. La couverture pour les apps sous macOS 11 est actuellement en cours d'ajout.

État des certifications des modules cryptographiques

Les apps Apple mentionnées ici utilisent les modules cryptographiques pour le système d'exploitation applicable. Pour en savoir plus, consultez Certifications de sécurité pour iOS, Certifications de sécurité pour iPadOS et Certifications de sécurité pour macOS.

État des certifications des critères communs

Le schéma américain, qui relève du NIAP, tient à jour une liste des produits en évaluation. Cette liste comprend les produits qui, d'une part, sont en cours d'évaluation aux États-Unis avec un laboratoire d'essais selon les critères communs (Common Criteria Testing Laboratory, CCTL) approuvé par le NIAP, et qui, d'autre part, ont fait l'objet d'une réunion d'évaluation préliminaire (ou l'équivalent) où la direction du schéma d'évaluation et de validation lié aux critères communs (Common Criteria Evaluation and Validation Scheme, CCEVS) les a officiellement acceptés pour évaluation.

Après la certification des produits, le NIAP répertorie les certifications valides sur la liste des produits conformes. Au bout de deux ans, ces certifications sont examinées pour vérifier leur conformité avec la politique de maintien de l'assurance actuelle. À l'expiration du maintien de l'assurance, le NIAP fait passer la certification sur sa liste des produits archivés.

Le portail des critères communs répertorie les certifications qui peuvent être mutuellement reconnues en vertu de l'arrangement international de reconnaissance des critères communs (ARCC). Le portail des CC peut laisser les produits sur la liste des produits certifiés pendant cinq ans. Il tient des dossiers sur les certifications archivées.

Le tableau ci-dessous indique les certifications en cours d'évaluation par un laboratoire, ou celles dont on a confirmé la conformité avec les critères communs.

État actuel

- Les évaluations auprès du NIAP publiées comme étant en cours sont inscrites sur la liste des produits en évaluation.
- Le NIAP inscrit les évaluations terminées et validées sur sa liste des produits conformes.

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : macOS 11 Big Sur *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* macOS 11 Big Sur : Contacts *Profils de protection :* PP pour logiciels d'application, paquet étendu (Extended Package, EP) pour navigateurs Web
Système d'exploitation : macOS 11 Big Sur *Date de certification :* —	*ID du schéma :* Pas encore certifié *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* macOS 11 Big Sur : Safari *Profils de protection :* PP pour logiciels d'application, paquet étendu (Extended Package, EP) pour navigateurs Web
Systèmes d'exploitation : iOS 14, iPadOS 14 *Date de certification :* 2021-08-20	*ID du schéma :* 11191 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* iOS 14 et iPadOS 14 d'Apple : Contacts *Profils de protection :* PP pour logiciels d'application, paquet étendu (Extended Package, EP) pour navigateurs Web
Systèmes d'exploitation : iOS 14, iPadOS 14 *Date de certification :* —	*ID du schéma :* 11192 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* iOS 14 et iPadOS 14 d'Apple : Safari *Profils de protection :* PP pour logiciels d'application, paquet étendu (Extended Package, EP) pour navigateurs Web
Systèmes d'exploitation : iOS 13, iPadOS 13 *Date de certification :* 2020-06-05	*ID du schéma :* 11060 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* iOS 13 et iPadOS 13 d'Apple : Safari *Profils de protection :* PP pour logiciels d'application, paquet étendu (Extended Package, EP) pour navigateurs Web
Systèmes d'exploitation : iOS 13, iPadOS 13 *Date de certification :* 2020-06-05	*ID du schéma :* 11050 *Documents :* Certificat Cible de sécurité Guide Rapport de validation Rapport d'activité d'assurance	*Titre :* iOS 13 et iPadOS 13 d'Apple : Contacts *Profils de protection :* PP pour logiciels d'application

Certifications des critères communs archivées pour les apps Apple

Système d'exploitation et date de certification	ID du schéma et documents	Titre et profils de protection
Système d'exploitation : iOS 12 *Date de certification :* 2019-06-12	*ID du schéma :* 10960 *Documents :* Cible de sécurité Guide	*Titre :* Safari sous iOS 12 *Profils de protection :* PP pour logiciels d'application, paquet étendu (Extended Package, EP) pour navigateurs Web
Système d'exploitation : iOS 12 *Date de certification :* 2019-02-28	*ID du schéma :* 10961 *Documents :* Cible de sécurité Guide	*Titre :* Contacts sous iOS 12 *Profils de protection :* PP pour logiciels d'application
Système d'exploitation : iOS 11 *Date de certification :* 2018-11-09	*ID du schéma :* 10916 *Documents :* Cible de sécurité Guide	*Titre :* Safari sous iOS 11 *Profils de protection :* PP pour logiciels d'application, paquet étendu (Extended Package, EP) pour navigateurs Web
Système d'exploitation : iOS 11 *Date de certification :* 2018-09-13	*ID du schéma :* 10915 *Documents :* Cible de sécurité Guide	*Titre :* Contacts sous iOS 11 *Profils de protection :* PP pour logiciels d'application

Certifications de sécurité pour les services Internet Apple

Apple dispose de certifications de conformité avec les normes ISO/CEI 27001 et ISO/CEI 27018 pour permettre à ses clients de remplir leurs obligations réglementaires et contractuelles. Ces certifications fournissent à nos clients une attestation indépendante des pratiques d'Apple relatives à la sécurité de l'information et à la confidentialité pour les systèmes concernés.

Les normes ISO/CEI 27001 et ISO/CEI 27018 appartiennent à une famille de normes de systèmes de gestion de la sécurité de l'information (SGSI) publiées par l'Organisation internationale de normalisation (ISO). Pour le SGSI d'Apple, toutes les exigences de contrôle de l'annexe A sont incluses dans la déclaration d'applicabilité conformément à la définition présente dans les normes ISO/CEI 27001 et 27018. Apple fait l'objet d'une attestation indépendante délivrée annuellement par un organisme de certification agréé.

Norme ISO/CEI 27001

La norme ISO/CEI 27001 concerne les SGSI et précise les exigences relatives à la création, à la mise en place, à la maintenance et à l'amélioration continue d'un SGSI au sein d'une organisation. La norme ISO/CEI 27001 comprend les domaines de sécurité suivants couverts par les certifications ISO/CEI d'Apple :

- Politiques de sécurité de l'information
- Organisation de la sécurité de l'information
- Gestion des ressources
- Sécurité des ressources humaines
- Sécurité physique et environnementale
- Gestion des communications et des opérations
- Contrôle d'accès
- Acquisition, développement et maintenance des systèmes d'information
- Gestion des incidents de sécurité de l'information
- Gestion de la continuité des activités
- Conformité

Norme ISO/CEI 27018

La norme ISO/CEI 27018 est un code de pratique pour la protection des renseignements nominatifs dans les environnements infonuagiques publics. Elle comprend les domaines de sécurité suivants couverts par les certifications ISO/CEI d'Apple :

- Consentement et choix
- Spécification et légitimité des finalités
- Limitation de collecte
- Minimisation des données
- Limitation d'utilisation, de conservation et de diffusion
- Exactitude et qualité
- Ouverture, transparence et notification
- Participation et accès individuels
- Responsabilité
- Sécurité de l'information
- Respect de la confidentialité

Services Apple couverts par les normes ISO/CEI 27001 et ISO/CEI 27018

Les certifications ISO/CEI 27001 et 27018 d'Apple couvrent les services suivants :

- Clavardage commercial d'Apple
- Apple Business Manager
- Service de notifications Push d'Apple (APN)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- Services iWork
- Identifiants Apple gérés
- Pour l'école
- Siri

Certifications

Les preuves de certification ISO/CEI 27001 et 27018 d'Apple sont disponibles auprès de notre organisme de certification.

Pour consulter les certifications d'Apple, consultez la page Recherche de certificats et de clients dans le répertoire sur le site Web de British Standards Institution (BSI), entrez Apple dans le champ de recherche Company (Entreprise), cliquez sur le bouton Search (Rechercher), puis sélectionnez les résultats de recherche pour afficher les certificats.

Remarque : Les renseignements sur les produits qui ne sont pas fabriqués par Apple ou les sites Web indépendants qui ne sont ni gérés ni vérifiés par Apple sont fournis sans recommandation ni approbation. Apple se dégage de toute responsabilité quant à la sélection, au bon fonctionnement ou à l'utilisation de sites Web ou produits de tiers. Apple n'offre aucune garantie quant à l'exactitude ou à la fiabilité des informations présentées sur les sites Web de tiers. Pour obtenir plus d'information, communiquez avec le fournisseur.

Projet de conformité de macOS en matière de sécurité

Le projet de conformité de macOS en matière de sécurité (mSCOP, macOS Security Compliance Project) est une initiative dont le code source est libre qui consiste à adopter une approche programmatique de génération de recommandations concernant la sécurité. Il s'agit d'un projet collectif auquel participent les personnels de sécurité en TI du NIST (National Institute of Standards and Technology), de la NASA (National Aeronautics and Space Administration), de la DISA (Defense Information Systems Agency) et du LANL (Los Alamos National Laboratory) à l'échelle fédérale. Le projet utilise un ensemble de contrôles testés et validés pour macOS et met ces contrôles en correspondance avec tout guide de sécurité qu'il prend en charge. Par ailleurs, ce projet peut être utilisé pour créer facilement des références de sécurité personnalisées relatives aux contrôles de sécurité techniques en exploitant une bibliothèque d'actions atomiques testées et validées (réglages de configuration). Le projet produit des documents, des scripts, des profils de configuration et des listes d'audit personnalisés en fonction de la référence utilisée.

Le mSCP peut produire du contenu utilisable conjointement avec les outils de gestion et de sécurité pour atteindre les objectifs de conformité. Les réglages de configuration dans le cadre de ce projet prennent en charge les références d'assistance suivantes :

Organisation	Références prises en charge
Publication spéciale (SP, Special Publication) 800-53 du NIST (National Institute of Standards and Technology) : Recommended Security Controls for Federal Information Systems and Organizations (contrôles de sécurité recommandés pour les organisations et les systèmes d'information fédéraux), révision 5	800-53 élevé, 800-53 modéré, 800-53 faible
Publication spéciale (SP, Special Publication) 800-171 du NIST (National Institute of Standards and Technology) : Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (protection des informations publiques contrôlées dans les organisations et systèmes non fédéraux), révision 2	800-171
STIG pour macOS 11 de l'Agence des systèmes d'information de la Défense (DISA, Defense Information Systems Agency), Guide d'implémentation technique de sécurité (STIG, Security Technical Implementation Guide) pour macOS 11 d'Apple	STIG
Comité sur les instructions des systèmes de sécurité nationale (CNSSI, Committee on National Security Systems Instruction) 1253, catégorisation de sécurité et sélection des contrôles des systèmes de sécurité nationale	1253

Informations supplémentaires :

- Voici une référence qui permet de réviser toutes les règles du projet.
- Pour en savoir plus sur le projet et son utilisation, consultez le wiki du projet de conformité de macOS en matière de sécurité.
- Pour configurer le projet pour l'utiliser, consultez : Apprendre à connaître le projet de conformité de macOS en matière de sécurité, 1re partie et Apprendre à connaître le projet de conformité de macOS en matière de sécurité, 2e partie.
- Si vous souhaitez soutenir le développement du projet, consultez les conseils pour le contributeur.

Historique des révisions des documents

Date	Résumé
27 octobre 2021	Sujets mis à jour : • Certifications de sécurité pour le processeur Secure Enclave • Certifications de sécurité pour iOS • Certifications de sécurité pour macOS
17 août 2021	Sujets mis à jour : • Certifications de sécurité pour le processeur Secure Enclave • Certifications de sécurité pour la puce T2 Security d'Apple • Certifications de sécurité pour iOS • Certifications de sécurité pour iPadOS • Certifications de sécurité pour macOS • Certifications de sécurité pour tvOS • Certifications de sécurité pour watchOS • Certifications de sécurité pour les apps Apple • Certifications de sécurité • Projet de conformité de macOS en matière de sécurité

Date	Résumé
26 avril 2021	Sujet ajouté : • Projet de conformité de macOS en matière de sécurité Sujets mis à jour : • Certifications de sécurité pour la puce T2 Security d'Apple : Nouvelles certifications FIPS 140-2, 3811 • Certifications de sécurité pour le processeur Secure Enclave : Nouvelles certifications FIPS 140-2, 3811 et nouveau tableau des certifications supplémentaires • Certifications de sécurité pour iOS : Nouvelles certifications FIPS 140-2, 3811, schéma identifiant 11146 pour iOS 14 en cours d'évaluation • Certifications de sécurité pour iPadOS : Nouvelles certifications FIPS 140-2, 3811, schéma identifiant 11147 pour iPadOS 14 en cours d'évaluation • Certifications de sécurité pour macOS : Nouvelle certification FIPS 140-2, 3811 • Certifications de sécurité pour tvOS : Nouvelles certifications FIPS 140-2, 3811 • Certifications de sécurité pour watchOS : Nouvelles certifications FIPS 140-2, 3811 • Certifications de sécurité pour les apps Apple : Mises à jour apportées à l'état des critères communs et ajout d'un tableau présentant les certifications archivées des critères communs

Glossaire

Apple Business Manager Portail Web simple destiné aux administrateurs de TI. Il offre une façon rapide et simplifiée de déployer des appareils Apple que les organisations ont achetés directement auprès d'Apple, ou d'un revendeur ou opérateur agréé Apple participant. Les TI peuvent automatiser l'inscription des appareils à leur solution de gestion des appareils mobiles (GAM) et remettre les appareils aux utilisateurs sans avoir à les manipuler ou à les préparer.

Apple School Manager Portail Web simple destiné aux administrateurs de TI. Il offre une façon rapide et simplifiée de déployer des appareils Apple que les organisations ont achetés directement auprès d'Apple, ou d'un revendeur ou opérateur agréé Apple participant. Les TI peuvent automatiser l'inscription des appareils à leur solution de gestion des appareils mobiles (GAM) et remettre les appareils aux utilisateurs sans avoir à les manipuler ou à les préparer.

Arrangement de reconnaissance des critères communs (ARCC) Accord de reconnaissance mutuelle qui établit les politiques et les exigences relatives à la reconnaissance internationale des certificats délivrés conformément aux normes des critères communs ISO/CEI 15408.

chiffrement complet du disque Chiffrement de l'intégralité des données d'un volume de stockage.

cible de sécurité (Security Target, ST) Document qui indique les problèmes et les besoins de sécurité d'un produit particulier.

client VPN IPsec Dans un profil de protection, un client qui offre une connexion sécurisée par protocole IPsec entre une plateforme hôte physique ou virtuelle et un lieu éloigné.

communauté technique internationale (international Technical Community, iTC) Groupe responsable de l'élaboration des profils de protection ou des profils de protection de collaboration sous l'égide de l'Arrangement de reconnaissance des critères communs (ARCC).

Corecrypto Bibliothèque qui fournit des implémentations de primitives cryptographiques de bas niveau. Il est à noter que Corecrypto n'offre pas directement d'interfaces de programmation aux développeurs. Ces derniers l'utilisent plutôt par l'intermédiaire d'interfaces de programmation d'applications (API) qui leur sont fournies. Le code source de Corecrypto est accessible au public afin de permettre la vérification de ses caractéristiques de sécurité et de son fonctionnement.

critères communs (CC) Norme qui établit les concepts et les principes généraux relatifs à l'évaluation de la sécurité informatique en plus de préciser un modèle général pour l'évaluation. Elle comprend des catalogues répertoriant les exigences de sécurité dans un langage normalisé.

déclaration d'applicabilité Document qui décrit les contrôles de sécurité mis en œuvre dans le cadre d'un SGSI, produit pour soutenir une certification ISO/CEI 27001.

gestion des appareils mobiles (GAM) Service qui permet de gérer à distance les appareils inscrits. Une fois un appareil inscrit, on peut utiliser le service de GAM sur le réseau pour configurer les réglages et accomplir d'autres tâches sur l'appareil sans interaction avec l'utilisateur.

implémentation à l'essai (Implementation Under Test, IUT) Module cryptographique en cours de test par un laboratoire.

module cryptographique Matériel, logiciel ou programme interne qui offre des fonctions cryptographiques et satisfait aux exigences d'une norme donnée relative aux modules cryptographiques.

modules en cours de traitement (Modules in Process, MIP) Liste tenue à jour par le Programme de validation des modules cryptographiques (PVMC) répertoriant tous les modules cryptographiques actuellement soumis à son processus de validation.

National Information Assurance Partnership (NIAP) Organisation du gouvernement américain responsable de la mise en application de la norme des critères communs aux États-Unis et de la gestion de son schéma d'évaluation et de validation lié aux critères communs (Common Criteria Evaluation and Validation Scheme, CCEVS).

National Institute of Standards and Technology (NIST) Service du département du Commerce des États-Unis chargé de faire avancer la métrologie, y compris ses normes et ses technologies.

niveaux de sécurité Les quatre niveaux de sécurité globale (1 à 4) définis par la norme ISO/CEI 19790 pour décrire des ensembles des besoins de sécurité applicables, le niveau 4 étant le plus strict.

norme FIPS (Federal Information Processing Standard) Publications conçues par le National Institute of Standards and Technology lorsque la loi l'exige ou que des exigences du gouvernement fédéral en matière de cybersécurité le justifient.

processeur Secure Enclave (Secure Enclave Processor, SEP) Coprocesseur fabriqué à l'intérieur d'un système sur puce.

profil de protection (PP) Document qui indique les problèmes et les besoins de sécurité d'une classe de produits spécifique.

profil de protection de collaboration (collaborative Protection Profile, cPP) Profil de protection conçu par une communauté technique internationale regroupant des experts chargés de la création des cPP.

Programme de validation des algorithmes cryptographiques (PVAC) Organisation dirigée par le NIST qui effectue des tests de validation sur les algorithmes cryptographiques approuvés (par exemple, ceux conformes aux normes FIPS et recommandés par le NIST) et leurs composants individuels.

Programme de validation des modules cryptographiques (PVMC) Organisation dirigée par les gouvernements des États-Unis et du Canada pour valider la conformité avec la norme FIPS 140-3.

Secure Element Puce de silicium intégrée dans de nombreux appareils Apple qui prend en charge des fonctions comme Apple Pay.

Senior Officials Group Information Systems Security (SOG-IS) Groupe qui gère un accord de reconnaissance mutuelle entre plusieurs nations européennes.

sepOS Programme interne du Secure Enclave, qui repose sur une version personnalisée par Apple du micronoyau L4.

service de notifications Push d'Apple (APN) Service mondial offert par Apple pour fournir des notifications de type Push aux appareils Apple.

système de gestion de la sécurité de l'information (SGSI) Ensemble de règlements et de procédures sur la sécurité de l'information qui régit les limites d'un programme de sécurité conçu pour protéger un éventail de renseignements et de systèmes en gérant la sécurité de l'information tout au long du cycle de vie de l'information ou du système.

système sur puce Circuit intégré qui incorpore divers composants dans une seule puce.

T2 Puce de sécurité d'Apple présente dans certains ordinateurs Mac avec processeur Intel depuis 2017.

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

C028-00499-B