أمن أنظمة Apple الأساسية

مايو 2024

المحتويات

مقدمة عن أمن أنظمة Apple الأساسية 5

الالتزام بتحقيق الأمن 7

أمن المكونات المادية والمقاييس الحيوية 8

نظرة عامة على أمن المكونات المادية 8

أمن Apple SoC 9

evalcnE eruceS 01

بصمة الوجه وبصمة الإصبع 81

قطع اتصال مكون الميكروفون المادي 62

البطاقات السريعة في نمط توفير الطاقة 72

أمن الأنظمة 82

نظرة عامة على أمن الأنظمة 82

التمهيد الآمن 92

أمن وحدة تخزين النظام 35

تحديثات البرامج الآمنة 55

تكامل نظام التشغيل 75

تنشيط اتصالات البيانات بشكل آمن 06

التحقق من الملحقات في iPhone و iPad 60

BlastDoor للرسائل والمعرفات 16

أمن نمط المنع على أجهزة Apple 61

الإمكانات الإضافية لأمن الأنظمة في macOS 62

أمن الأنظمة لـ watchOS 73

الإنشاء العشوائي للأرقام 77

جهاز الأبحاث الأمنية من Apple 78

التشفير وحماية البيانات 08

نظرة عامة على التشفير وحماية البيانات 08

رموز الدخول وكلمات السر 18

حماية البيانات 48

خزنة الملفات 79

كيفية حماية Apple لبيانات المستخدمين الشخصية 101

التوقيع الرقمي والتشفير 401

أمن التطبيقات 601

نظرة عامة على أمن التطبيقات 601

أمن التطبيقات في iOS و iPadOS 107

أمن التطبيقات في macOS 113

الميزات الآمنة في تطبيق الملاحظات 811

الميزات الآمنة في تطبيق الاختصارات 911

أمن الخدمات 021

نظرة عامة على أمن الخدمات 021

Apple ID و Apple ID المُدار 121

duolCi 421

إدارة رموز الدخول وكلمات السر 431

yaP elppA 541

استخدام Apple Wallet 159

egasseMi 271

أمن مراسلة الشركات من Apple 175

أمن فيس تايم 671

تحديد الموقع 771

الاستمرارية 081

أمن الشبكات 381
نظرة عامة على أمن الشبكات 381
أمن TLS 183
أمن IPv6 185
أمن الشبكات الخاصة الظاهرية (VPN) 681
أمن Wi-Fi 187
أمن Bluetooth 191
تقنية النطاق فائق العرض في iOS 193
أمن تسجيل الدخول الموحد 391
أمن الإرسال السريع 591
أمن مشاركة كلمة سر Wi-Fi على iPhone و iPad 196
أمن جدار الحماية في macOS 196

أمن مجموعة أدوات المطورين 791
نظرة عامة على أمن مجموعة أدوات المطورين 791
أمن HomeKit 197
أمن SiriKit لـ iOS و iPadOS و watchOS 203
أمن WidgetKit 204
أمن DriverKit لـ macOS 205
أمن ReplayKit في iOS و iPadOS 205
أمن ARKit في iOS و iPadOS 207

إدارة الأجهزة الآمنة 802
نظرة عامة على إدارة الأجهزة الآمنة 802
أمن نموذج الاقتران للـ iPhone والـ iPad 209
إدارة جهاز الجوال 012
أمن أداة إعداد Apple 217
أمن مدة استخدام الجهاز 812

المعجم 022

سجل تاريخ مراجعة المستند 422
سجل تاريخ مراجعة المستند 422

حقوق النشر 432

مقدمة عن أمن أنظمة Apple الأساسـية

تصمم Apple الأمن في صميم أنظمتها الأساسية. بناءً على تجربة إنشاء أكثر أنظمة تشغيل الأجهزة المحمولة تطورًا في العالم، أنشأت Apple هياكل أمنية تلبي المتطلبات الفريدة للجوال والساعة وسطح المكتب والمنزل.

يجمع كل جهاز من أجهزة Apple بين **المكونات المادية** و**البرامج** و**الخدمات** المصممة للعمل معًا لتوفير أقصى درجات الأمن وتسهيل تجربة المستخدم في خدمة الهدف النهائي المتمثل في الحفاظ على أمان المعلومات الشخصية. على سبيل المثال، تعمل الأجهزة الأمنية والأجهزة المزودة بالسيليكون المصممة من قِبل Apple على تشغيل ميزات الأمن المهمة. كما تعمل وسائل حماية البرامج للحفاظ على حماية نظام التشغيل وتطبيقات الجهات الخارجية. وأخيرًا، توفر الخدمات آلية لتحديثات البرامج الأمنية في الوقت المناسب، وتشغيل منظومة محمية للتطبيقات، وتسهيل الاتصالات وعمليات الدفع الآمنة. نتيجة لذلك، لا تحمي أجهزة Apple الجهاز وبياناته فحسب بل النظام البيئي بأكمله، بما في ذلك كل ما يفعله المستخدم محليًا وعلى الشبكات ومع خدمات الإنترنت الرئيسية.

في حين أننا نصمم منتجاتنا لتكون بسيطة وبديهية وذات إمكانيات، فإننا نصممها لتكون آمنة. لا يمكن تعطيل ميزات الأمن الرئيسية، مثل تشفير الجهاز القائم على المكونات المادية، عن طريق الخطأ. الميزات الأخرى، مثل بصمة الوجه وبصمة الإصبع، تعمل على تحسين تجربة المستخدم من خلال جعلها أبسط وأكثر بديهية وأسهل لتأمين الجهاز. ونظرًا لأنه يتم تمكين العديد من هذه الميزات بشكل افتراضي، فلا يحتاج المستخدمون أو أقسام تقنية المعلومات إلى إجراء تكوينات موسَّعة.

توفر هذه الوثائق تفاصيل حول كيفية تطبيق تقنية الأمن وميزاته في أنظمة Apple الأساسية. وتساعد أيضًا المؤسسات على دمج تقنية الأمن وميزاته في أنظمة Apple الأساسية مع سياساتها وتدابيرها الخاصة لتلبية احتياجاتها الأمنية المحددة.

يتم تنظيم المحتوى في مجالات الموضوعات التالية:

- **أمن المكونات المادية والمقاييس الحيوية:** الرقاقات والمكونات المادية التي تشكل أساس الأمن على أجهزة Apple، بما في ذلك رقاقات Apple و Secure Enclave ومحركات التشفير وبصمة الوجه وبصمة الإصبع
- **أمن الأنظمة:** وظائف المكونات المادية والبرامج المتكاملة التي توفر التمهيد الآمن والتحديث والتشغيل المستمر لأنظمة التشغيل في Apple
- **التشفير وحماية البيانات:** البنية والتصميم اللذان يحميان بيانات المستخدم في حالة ضياع الجهاز أو سرقته، أو عند محاولة شخص بلا تصريح أو عملية غير مخوَّلة استخدامه أو تعديله
- **أمن التطبيقات:** البرامج والخدمات التي توفر نظامًا بيئيًا آمنًا للتطبيقات وتمكّن تشغيل التطبيقات بأمان ودون المساس بتكامل النظام الأساسي
- **أمن الخدمات:** خدمات Apple لتحديد الهوية وإدارة كلمات السر وعمليات الدفع والاتصالات والعثور على الأجهزة المفقودة
- **أمن الشبكات:** بروتوكولات الشبكات المعيارية التي توفر مصادقة آمنة وتشفير البيانات أثناء الإرسال
- **أمن مجموعة أدوات المطورين:** إطارات العمل "مجموعة الأدوات" المصممة للإدارة الآمنة والخاصة لكل من المنزل والصحة، بالإضافة إلى توسيع إمكانيات جهاز Apple وخدماتها لتشمل تطبيقات الجهات الخارجية
- **إدارة الأجهزة الآمنة:** الطُرق التي تسمح بإدارة أجهزة Apple وتساعد على منع الاستخدام غير المصرح به وتمكّن المسح عن بُعد في حالة ضياع الجهاز أو سرقته

الالتزام بتحقيق الأمن

تلتزم Apple بالمساعدة في حماية العملاء من خلال تقنيات الخصوصية والأمن الرائدة المصممة لوقاية المعلومات الشخصية، بجانب الأساليب الشاملة التي تساعد في حماية بيانات الشركات في البيئات المؤسسية. وتكافئ Apple الباحثين نظير عملهم في الكشف عن الثغرات الأمنية بتقديم مكافآت Apple للإسهامات الأمنية. تفاصيل البرنامج وفئات المكافآت متوفرة على https://security.Apple.com/bounty/.

إننا نحتفظ بفريق أمني مكرّس لدعم جميع منتجات Apple. يوفر الفريق عمليات تدقيق واختبار أمنية للمنتجات، التي قيد التطوير والتي تم إصدارها على حد سواء. ويوفر فريق Apple أيضًا أدوات وتدريبات أمنية، ويراقب بفعالية التهديدات والتقارير المتعلقة بالمشكلات الأمنية الجديدة. Apple عضو في منتدى فرق الاستجابة للحوادث والأمن (FIRST).

تواصل Apple تخطي حدود الممكن في مجالي الأمن والخصوصية. حيث تستخدم رقاقات Apple المخصصة عبر قائمة المنتجات؛ بدءًا من Apple Watch مرورًا بـ iPhone و iPad وصولًا إلى شرائح سلسلة M في Mac؛ والتي لا يقتصر عملها على الحوسبة الفعالة فقط، بل الأمن أيضًا. على سبيل المثال، تعمل رقاقات Apple على تشكيل الأساس للإقلاع الآمن وبصمة الوجه وبصمة الإصبع وحماية البيانات. بالإضافة إلى ذلك، تساعد ميزات الأمن التي يتم تشغيلها بواسطة رقاقات Apple—مثل حماية تكامل Kernel ورموز مصادقة المؤشر وقيود الأذونات السريعة—على إحباط أنواع الهجمات الإلكترونية الشائعة. لذا، حتى في حالة تنفيذ التعليمات البرمجية للمهاجم بطريقة ما، يتم الحد من الضرر الذي يمكن أن تُحدثه بدرجة كبيرة.

لتحقيق أقصى استفادة من الميزات الأمنية الشاملة المضمنة في أنظمتنا الأساسية، نحث المؤسسات على مراجعة سياسات تقنية المعلومات والأمن لديها للتأكد من أنها تستفيد استفادةً تامةً من طبقات التقنية الأمنية التي توفرها هذه الأنظمة الأساسية.

لمعرفة المزيد حول الإبلاغ عن المشكلات إلى Apple والاشتراك في إشعارات الأمن، راجع الإبلاغ عن ثغرة في الأمان أو الخصوصية.

تؤمن Apple بأن الخصوصية حق أساسي من حقوق الإنسان، ومن ثم وضعت العديد من الضوابط والخيارات المُضمَّنة التي تتيح للمستخدمين تحديد كيفية وتوقيت استخدام التطبيقات لمعلوماتهم، وكذلك المعلومات التي يتم استخدامها. لمعرفة المزيد حول نهج الخصوصية المُتَّبع في Apple وضوابط الخصوصية في أجهزة Apple وسياسة خصوصية Apple، انظر https://www.Apple.com/ae-ar/privacy.

ملاحظة: ما لم يُذكر خلاف ذلك، تغطي هذه الوثائق إصدارات أنظمة التشغيل التالية: iOS 17.3 و iPadOS 17.3 و macOS 14.3 و tvOS 17.3 و watchOS 10.3.

أمن المكونات الماديـة والمقاييس الحيوية

نظرة عامة على أمن المكونات المادية

لكي يكون البرنامج آمنًا، يجب أن يرتكز على المكونات المادية التي تتضمن أمنًا مدمجًا. ولهذا السبب تتمتع أجهزة Apple—المثبت عليها iOS و iPadOS و macOS و tvOS و watchOS—بإمكانات أمنية مصممة برقاقات. تتضمن هذه الإمكانات وحدة المعالجة المركزية (CPU) التي تدعم ميزات أمان النظام، وكذلك السيليكون الإضافي المخصص لوظائف الأمان. علمًا بأن المكونات المادية التي تركز على الأمن تتبع مبدأ دعم الوظائف المحدودة والمُحدّدة بدقة لتقليل الأجزاء المعرضة للهجوم إلى أدنى حد. وتتضمن هذه المكونات ذاكرة ROM للتمهيد، والتي تشكل جذر ثقة في المكونات المادية للتمهيد الآمن، ومحركات AES مخصصة للتشفير وفك التشفير بطريقة فعالة وآمنة، فضلاً عن **Secure Enclave**. Secure Enclave عبارة عن مكون في نظام Apple على شريحة (SoC) يتم تضمينه في جميع أجهزة iPhone و iPad و Apple Watch و Apple TV و HomePod الحديثة وعلى أجهزة Mac المزودة برقاقات Apple وكذلك المزودة بشريحة Apple T2 الأمنية. ويتبع Secure Enclave نفسه المبدأ ذاته الذي يتبعه تصميم نظام SoC، إذ يحتوي على ROM للتمهيد المنفصل خاص به ومحرك AES. يوفر Secure Enclave كذلك الأساس لإنشاء المفاتيح الضرورية لتشفير البيانات غير النشطة وتخزينها بأمان، كما أنه يحمي بيانات المقاييس الحيوية ويُقيّمها بالنسبة إلى كل من بصمة الوجه وبصمة الإصبع.

يجب أن يكون تشفير التخزين سريعًا وفعالاً. في الوقت نفسه، لا يمكنه كشف البيانات (أو **مادة المفاتيح**) التي يستخدمها لإنشاء علاقات مفتاحية مشفرة. ويقوم محرك AES المادي بحل هذه المشكلة عن طريق إجراء التشفير وإلغاء التشفير على الخط بسرعة **أثناء كتابة الملفات أو قراءتها**. توفر قناة خاصة من Secure Enclave مادة مفاتيح ضرورية لمحرك AES دون كشف هذه المعلومات لمعالج التطبيقات (أو وحدة المعالجة المركزية) أو نظام التشغيل العام. ويساعد ذلك على ضمان أن تقوم حماية البيانات وتقنيات خزنة الملفات من Apple بحماية ملفات المستخدمين دون الكشف عن مفاتيح التشفير طويلة الأجل.

صممت Apple التمهيد الآمن لحماية أدنى مستويات البرامج من العبث وللسماح بتحميل برامج نظام التشغيل الموثوقة فقط من Apple عند بدء التشغيل. يبدأ التشغيل الآمن بتعليمات برمجية ثابتة تسمى **Boot ROM** يتم وضعها في أثناء تصنيع شريحة Apple SoC وتُعرف باسم **جذر الثقة في المكونات المادية**. على أجهزة كمبيوتر Mac المزودة بشريحة T2، تبدأ الثقة في التمهيد الآمن لـ macOS بشريحة T2. (تقوم كل من شريحة T2 و Secure Enclave كذلك بتنفيذ عمليات التشغيل الآمن الخاصة بهما باستخدام ذاكرة ROM للتشغيل منفصلة لكل منهما — ويُعد هذا تمثيلاً دقيقًا لكيفية تشغيل شرائح A-series و M1 و M2 بشكل آمن).

يعالج Secure Enclave كذلك بصمة الإصبع وبيانات الوجه من مستشعرات بصمة الوجه وبصمة الإصبع على أجهزة Apple. وهذا يوفر مصادقة آمنة مع الحفاظ على خصوصية وأمن بيانات المستخدم البيومترية. كما يتيح ذلك للمستخدمين الاستفادة من أمن رموز المرور وكلمات السر الأطول والأكثر تعقيدًا، مع سهولة المصادقة السريعة للوصول أو الشراء في العديد من الحالات.

أمن Apple SoC

يشكل السيليكون الذي تصممه Apple بنية عامة في كل منتجات Apple، وأصبح الآن متوفرًا في الـ Mac وكذلك الـ iPhone والـ iPad والـ Apple TV والـ Apple Watch. على مدار عقد من الزمان، كان فريق تصميم السيليكون عالمي المستوى التابع لشركة Apple يعمل على تصميم وتحسين الأنظمة على شرائح (SoCs) في Apple. وقد أسفرت تلك الجهود عن بنية قابلة للتطوير مصممة لكل الأجهزة التي تتصدر المجال من ناحية الإمكانيات الأمنية. وهذا يوفر أساسًا مشتركًا لميزات الأمن التي لا يمكن الحصول عليها إلا من شركة تصمم السيليكون الخاص بها لتشغيله مع برامجها.

صُمم Apple Silicon وصُنع خصوصًا لتمكين ميزات أمان النظام المفصلة أدناه.

الميزة	A10	A11, S3	A12 و A13 و A14 S4 إلى S9	A15 و A16 و A17	M1 و M2 و M3
حماية تكامل Kernel	✓	✓	✓	✓	✓
قيود الأذونات السريعة	✗	✓	✓	✓	✓
حماية تكامل المعالج الثانوي للنظام	✗	✗	✓	✓	✓
رموز مصادقة المؤشر	✗	✗	✓	✓	✓
طبقة حماية الصفحة	✗	✓	✓	✗	✗ راجع الملاحظة 1 أدناه.
Secure Page Table Monitor	✗	✗	✗	✓ راجع الملاحظة 2 أدناه.	✗

الملاحظة 1: تتطلب طبقة حماية الصفحة (PPL) تنفيذ النظام الأساسي للتعليمات البرمجية المُوقّعة والموثوق بها **فقط**، وهذا نموذج أمن لا ينطبق على macOS.

الملاحظة 2: Secure Page Table Monitor (SPTM) مدعوم على A15 و A16 و A17 ويُستخدَم بدلًا من طبقة حماية الصفحة على الأنظمة الأساسية المدعومة.

يقوم السيليكون الذي تصممه Apple أيضًا على وجه التحديد بتمكين إمكانات حماية البيانات الموضحة أدناه.

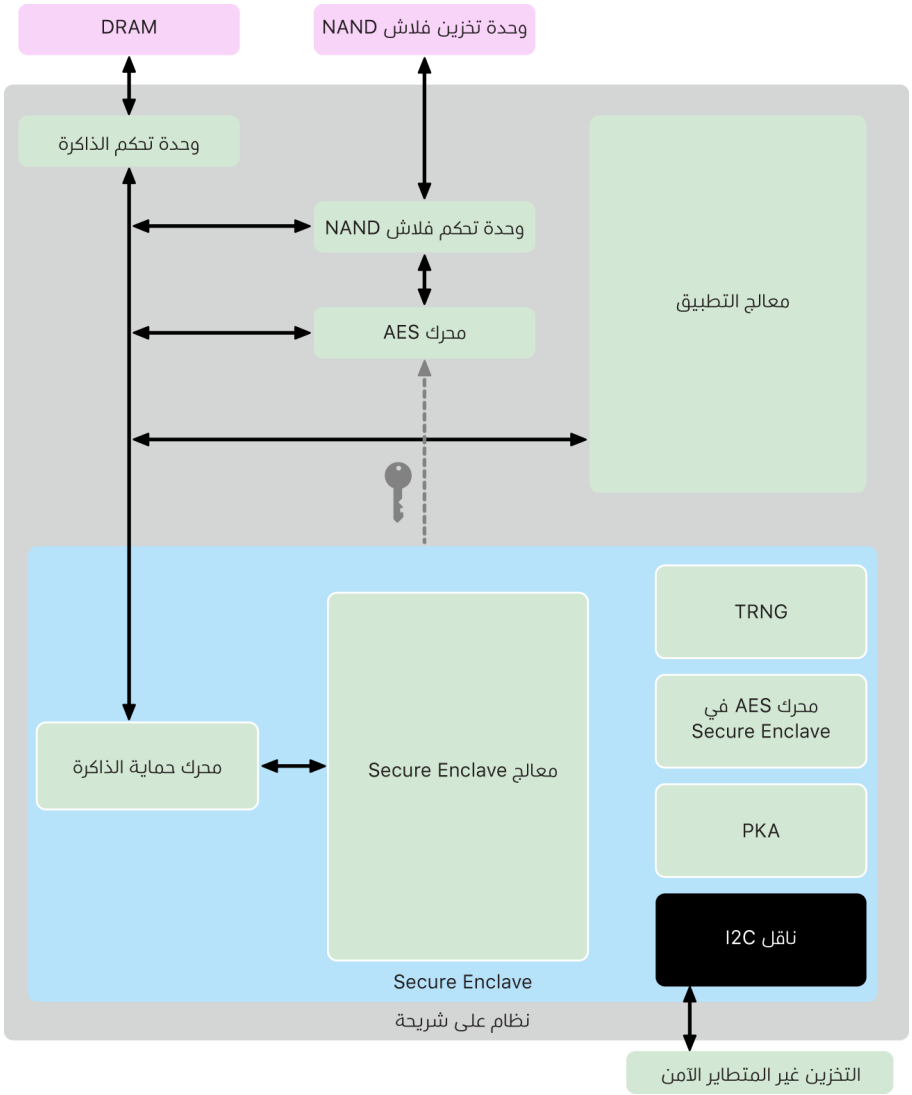
الميزة	A10 و A11 S3	A12 إلى A17 S4 إلى S9 M1 و M2 و M3
حماية المفاتيح المؤمنة (SKP)	✓	✓
recoveryOS - محمي بكل فئات حماية البيانات	✓	✓
أنماط التمهيد البديلة لكل من DFU والتشخيصات والتحديث - حماية البيانات من الفئة A و B و C	✗	✓

Secure Enclave

Secure Enclave هو نظام فرعي آمن مخصص للإصدارات الأحدث من iPhone و iPad و Mac و Apple TV و Apple Watch و HomePod.

نظرة عامة

Secure Enclave عبارة عن نظام فرعي آمن مخصص مُدمج في الأنظمة على الشرائح (SoCs) التي تقدمها Apple. ويتم عزل Secure Enclave عن المعالج الرئيسي لتوفير طبقة إضافية من الأمن، وهو مصمم للحفاظ على أمن بيانات المستخدم الحساسة حتى عند اختراق نواة معالج التطبيقات. ويتبع مبادئ التصميم ذاتها التي يتبعها SoC—ذاكرة ROM للتمهيد لإنشاء جذر الثقة للمكونات المادية، ومحرك AES لعمليات التشفير الفعالة والآمنة، والذاكرة المحمية. بالرغم من أن Secure Enclave لا يتضمن التخزين، ولكنه يشتمل على آلية لتخزين المعلومات بأمان على وحدة التخزين المتصلة بشكل منفصل عن تخزين فلاش NAND المُستخدم من قبل معالج التطبيقات ونظام التشغيل.



ويعد Secure Enclave ميزة من ميزات المكونات المادية في معظم إصدارات الـ iPhone والـ iPad والـ Mac والـ Apple TV والـ Apple Watch والـ HomePod، وهي:

- iPhone 5s أو أحدث
- iPad Air أو أحدث
- أجهزة كمبيوتر Mac المزودة بسيليكون Apple
- أجهزة كمبيوتر Macbook Pro التي تحتوي على شريط اللمس (2016 و 2017) المزودة بشريحة Apple T1
- أجهزة كمبيوتر Mac المستندة إلى Intel التي تحتوي على شريحة Apple T2 الأمنية
- Apple TV HD أو أحدث
- Apple Watch Series 1 أو أحدث
- HomePod و HomePod mini

معالج Secure Enclave

يوفر معالج Secure Enclave قوة الحوسبة الرئيسية لـ Secure Enclave. ولتوفير أقصى مستوى من العزلة، تم تخصيص معالج Secure Enclave لاستخدام Secure Enclave فقط. يساعد ذلك في منع هجمات القنوات الجانبية التي تعتمد على البرامج الضارة التي تشترك في نفس محور التنفيذ مثل البرامج المستهدفة المعرضة للهجوم.

يقوم معالج Secure Enclave بتشغيل إصدار L4 microkernel مخصص لـ Apple. وقد تم تصميمه للعمل بكفاءة على سرعة ساعة أقل، ما يساعد على حمايته من هجمات الساعة والطاقة. يتضمن معالج Secure Enclave، بدءًا من A11 و S4، محركًا بذاكرة محمية وذاكرة مشفرة مع إمكانات مكافحة إعادة التشغيل والتمهيد الآمن ومولد الأرقام العشوائي المخصص ومحرك AES الخاص به.

محرك حماية الذاكرة

يعمل Secure Enclave من منطقة مخصصة بذاكرة DRAM في الجهاز. وتعمل طبقات الحماية المتعددة على عزل ذاكرة Secure Enclave المحمية عن معالج التطبيقات.

عند بدء تشغيل الجهاز، يقوم Boot ROM في Secure Enclave بإنشاء مفتاح حماية ذاكرة مؤقت عشوائي لمحرك حماية الذاكرة. وعندما يكتب Secure Enclave في منطقة الذاكرة المخصصة له، يعمل محرك حماية الذاكرة على تشفير كتلة الذاكرة باستخدام AES في نمط Mac XEX (xor-encrypt-xor)، ويحتسب علامة المصادقة للذاكرة الخاصة برمز مصادقة الرسائل المستندة إلى التشفير (CMAC). ويخزّن محرك حماية الذاكرة علامة المصادقة بجانب الذاكرة المشفرة. عندما يقرأ Secure Enclave الذاكرة، يتحقق محرك حماية الذاكرة من علامة المصادقة. وفي حالة تطابق علامة المصادقة، يعمل محرك حماية الذاكرة على فك تشفير كتلة الذاكرة. أما إذا لم تتطابق العلامة، يشير محرك حماية الذاكرة إلى خطأ في Secure Enclave. بعد حدوث خطأ في مصادقة الذاكرة، يتوقف Secure Enclave عن قبول الطلبات حتى تتم إعادة تشغيل النظام.

بدءًا من أنظمة SoCs من الفئة A11 و S4 المتوفرة من Apple، يضيف محرك حماية الذاكرة ميزة حماية إعادة التشغيل لذاكرة Secure Enclave. للمساعدة على منع إعادة تشغيل البيانات ذات الأهمية الأمنية، يخزّن محرك حماية الذاكرة رقمًا فريدًا لمرة واحدة يسمى **قيمة غير قابلة لإعادة التشغيل** لكتلة الذاكرة بجانب علامة المصادقة. يتم استخدام القيمة غير القابلة لإعادة التشغيل كمفتاح إضافي لعلامة مصادقة CMAC. تتم حماية القيم غير القابلة لإعادة التشغيل لجميع كتل الذاكرة باستخدام شجرة تكامل متجذرة في ذاكرة SRAM المخصصة داخل Secure Enclave. بالنسبة إلى عمليات الكتابة، **يحدّث** محرك حماية الذاكرة القيمة غير القابلة لإعادة التشغيل وكل مستوى من شجرة التكامل وصولاً إلى SRAM. بالنسبة إلى عمليات الكتابة، **يتحقق** محرك حماية الذاكرة من القيمة غير القابلة لإعادة التشغيل وكل مستوى من شجرة التكامل وصولاً إلى SRAM. يتم التعامل مع حالات عدم تطابق القيمة غير القابلة لإعادة التشغيل بشكل مشابه لحالات عدم تطابق علامة المصادقة.

على الـ Apple A14 أو M1 أو SoCS الأحدث، يدعم محرك حماية الذاكرة وجود مفتاحين لحماية الذاكرة المؤقتة. يتم استخدام الأول للبيانات الخاصة في Secure Enclave، بينما يتم استخدام الثاني للبيانات المشتركة مع المحرك العصبي الآمن.

يعمل محرك حماية الذاكرة بشكل مضمن وشفاف في Secure Enclave. يقرأ Secure Enclave الذاكرة ويكتب فيها كما لو كانت ذاكرة DRAM عادية غير مشفرة، بينما لا يرى أي مراقب خارج Secure Enclave سوى الإصدار المُشفّر والمُصادَق عليه من الذاكرة فقط. وينتج عن ذلك حماية قوية للذاكرة بدون مقايضات الأداء أو تعقيدات البرامج.

Boot ROM في Secure Enclave

تحتوي Secure Enclave على Boot ROM مخصص لـ Secure Enclave. وعلى غرار Boot ROM في معالج التطبيقات، فإن Secure Enclave Boot ROM عبارة عن تعليمة برمجية ثابتة تؤسس لجذر الثقة في المكونات المادية في Secure Enclave.

عند بدء تشغيل النظام، يعمل iBoot على تعيين منطقة مخصصة من الذاكرة إلى Secure Enclave. قبل استخدام الذاكرة، يقوم Boot ROM في Secure Enclave بتهيئة محرك حماية الذاكرة لتوفير حماية تشفير لذاكرة Secure Enclave المحمية.

ثم يُرسِل معالج التطبيقات صورة sepOS إلى Boot ROM في Secure Enclave. وبعد نسخ صورة sepOS في الذاكرة المحمية الخاصة بـ Secure Enclave، يتحقق Boot ROM في Secure Enclave من تجزئة التشفير وتوقيع الصورة للتحقق من أن صورة sepOS مصرح لها بالعمل على الجهاز. إذا تم توقيع صورة sepOS بشكل صحيح للعمل على الجهاز، فإن Boot ROM في Secure Enclave ينقل التحكم إلى sepOS. إذا كان التوقيع غير صالح، فقد تم تصميم Boot ROM في Secure Enclave لمنع أي استخدام إضافي لـ Secure Enclave حتى إعادة تعيين الشريحة التالية.

في Apple A10 وأنظمة SoCs الأحدث، يعمل Boot ROM في Secure Enclave على قفل تجزئة sepOS في سجل مخصص لهذا الغرض. يستخدم مُسرّع المفتاح العام هذه التجزئة للمفاتيح المرتبطة بنظام التشغيل (المرتبطة بنظام التشغيل).

مراقب التمهيد في Secure Enclave

في Apple A13 وأنظمة SoCs الأحدث، يشتمل Secure Enclave على مراقب تمهيد تم تصميمه لضمان تكامل أقوى في تجزئة sepOS التي تم تمهيدها.

عند بدء تشغيل النظام، يعمل تكوين حماية تكامل المعالج الثانوي للنظام (SCIP) الخاص بمعالج Secure Enclave للمساعدة على منع معالج Secure Enclave من تنفيذ أي تعليمة برمجية بخلاف Boot ROM في Secure Enclave. يساعد مراقب التمهيد على منع Secure Enclave من تعديل تكوين SCIP مباشرةً. لجعل صورة sepOS التي تم تحميلها قابلة للتنفيذ، يرسل Boot ROM في Secure Enclave طلبًا إلى مراقب التمهيد يتضمن عنوان وحجم صورة sepOS التي تم تحميلها. عند استلام الطلب، يقوم مراقب التمهيد بإعادة تعيين معالج Secure Enclave، وتجزئة صورة sepOS التي تم تحميلها، وتحديث إعدادات SCIP للسماح بتنفيذ صورة sepOS التي تم تحميلها، وبدء التنفيذ داخل التعليمة البرمجية التي تم تحميلها حديثًا. ومع استمرار النظام في التمهيد، يتم استخدام هذه العملية نفسها كلما تم جعل تعليمة برمجية جديدة قابلةً للتنفيذ. وفي كل مرة، يعمل مراقب التمهيد على تحديث تجزئة تشغيل في عملية التمهيد. يتضمن مراقب التمهيد أيضًا معامِلات أمن مهمة في تجزئة التشغيل.

عند اكتمال التمهيد، يقوم مراقب التمهيد بإنهاء تجزئة التشغيل وإرسالها إلى مُسرّع المفتاح العام لاستخدامها مع المفاتيح المرتبطة بنظام التشغيل. وهذه العملية مصممة بحيث لا يمكن تجاوز ربط مفتاح نظام التشغيل حتى مع وجود ثغرة أمنية في Boot ROM في Secure Enclave.

مولّد الأرقام العشوائية الحقيقية

يُستخدم مولّد الأرقام العشوائية الحقيقية (TRNG) لإنشاء بيانات عشوائية آمنة. ويستخدم Secure Enclave مولّد TRNG عندما يُنشئ مفتاح تشفير عشوائيًا أو جذر مفتاح عشوائيًا أو إنتروبيا أخرى. يعتمد TRNG على عدة مذبذبات حلقية تمت معالجتها لاحقًا باستخدام CTR_DRBG (خوارزمية تستند إلى تشفير الكُتل في نمط العدّاد).

مفاتيح التشفير الجذرية

يحتوي Secure Enclave على مفتاح تشفير جذري للمعرف الفريد (UID). ويكون UID فريدًا لكل جهاز على حدة ولا يرتبط بأي معرف آخر على الجهاز.

ويتم دمج UID المُنشأ عشوائيًا في النظام وقت تصنيع SoC. بدءًا من A9 SoC، يتم إنشاء UID من خلال Secure Enclave TRNG أثناء التصنيع ويتم كتابته إلى المنصهرات باستخدام عملية برمجية تجري بالكامل في Secure Enclave. تحمي هذه العملية معرّف المستخدم من أن يكون مرئيًا خارج الجهاز أثناء التصنيع وبالتالي لا يتوفر للوصول إليه أو تخزينه من قِبل Apple أو أي من مورديها.

تستخدم صورة sepOS معرف UID لحماية الأسرار الخاصة بالجهاز. ويتيح المعرف الفريد ربط البيانات بشكل مشفر بجهاز معين. على سبيل المثال، يتضمن التسلسل الهرمي للمفتاح الذي يحمي نظام الملفات المعرف الفريد، لذلك إذا تم نقل شرائح تخزين SSD الداخلية فعليًا من جهاز إلى آخر، فلن يكون الوصول إلى الملفات ممكنًا. تتضمن الأسرار الأخرى المحمية الخاصة بالجهاز بيانات بصمة الوجه أو بصمة الإصبع. في أي Mac، لا يتلقى هذا المستوى من التشفير سوى التخزين الداخلي الكامل المرتبط بمحرك AES. على سبيل المثال، لا يتم تشفير أجهزة التخزين الخارجية المتصلة عبر USB أو وحدة التخزين المستندة إلى PCIe المضافة إلى 2019 Mac Pro بهذه الطريقة.

كما يتضمن Secure Enclave معرف مجموعة (GID) للجهاز، ويكون مشتركًا لجميع الأجهزة التي تستخدم SoC معينًا (على سبيل المثال، تشترك جميع الأجهزة التي تستخدم Apple A15 SoC في معرف GID ذاته).

ولا يتوفر UID و GID عبر مجموعة إجراءات الاختبار المشتركة (JTAG) أو واجهات تصحيح الأخطاء الأخرى.

محرك AES في Secure Enclave

محرك AES في Secure Enclave عبارة عن كتلة مادية تُستخدم لإجراء تشفير متماثل استنادًا إلى تشفير AES. وقد تم تصميم محرك AES لمقاومة تسرُّب المعلومات باستخدام التوقيت وتحليل الطاقة الثابتة (SPA). بدءًا من A9 SoC، يتضمن محرك AES أيضًا إجراءات مضادة لتحليل الطاقة الديناميكية (DPA).

يدعم محرك AES مفاتيح المكونات المادية والبرامج. يتم اشتقاق مفاتيح المكونات المادية من معرّف UID أو GID الخاصين بـ Secure Enclave. وتظل هذه المفاتيح داخل محرك AES ولا تكون مرئية حتى لبرنامج sepOS. بالرغم من أن البرنامج يمكنه طلب عمليات التشفير وفك التشفير باستخدام مفاتيح المكونات المادية، فإنه لا يمكنه استخراج المفاتيح.

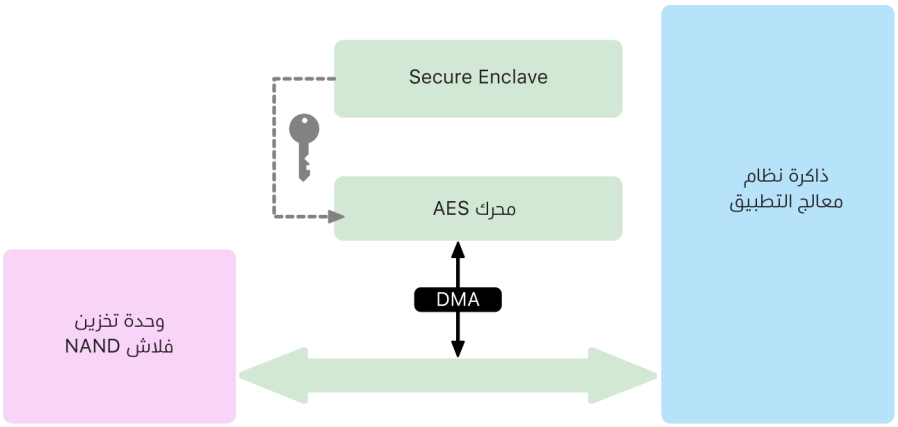
في Apple A10 وأنظمة SoCs الأحدث، يتضمن محرك AES وحدات بت جذرية قابلة للقفل تعمل على تنويع المفاتيح المشتقة من UID أو GID. وهذا يسمح بأن يكون الوصول إلى البيانات مشروطًا بوضع التشغيل على الجهاز. على سبيل المثال، تُستخدم وحدات البت الجذرية القابلة للقفل لرفض الوصول إلى البيانات المحمية بكلمة سر عند التشغيل من نمط تحديث البرنامج الثابت للجهاز (DFU). لمزيد من المعلومات، انظر رموز الدخول وكلمات السر.

محرك AES

يحتوي كل جهاز Apple مزود بـ Secure Enclave أيضًا على محرك تشفير AES256 مخصص (محرك AES) مضمّن في مسار الوصول إلى الذاكرة المباشرة (DMA) بين تخزين فلاش NAND (غير المتطاير) وذاكرة النظام الرئيسية، مما يجعل تشفير الملفات عالي الكفاءة. في معالج A9 أو معالجات السلسلة A الأحدث، يوجد النظام الفرعي لتخزين الفلاش على ناقل معزول لا يُسمح له بالوصول إلى الذاكرة التي تحتوي على بيانات المستخدم من خلال محرك تشفير DMA.

في وقت التمهيد، تقوم sepOS بإنشاء مفتاح تغليف عشوائي باستخدام TRNG. وينقل Secure Enclave هذا المفتاح إلى محرك AES باستخدام واصلات مخصصة مصممة لمنع الوصول إليه بواسطة أي برنامج خارج Secure Enclave. بعد ذلك، تستطيع sepOS استخدام مفتاح التغليف العشوائي لتغليف مفاتيح الملفات لاستخدامها بواسطة برنامج تشغيل نظام ملفات معالج التطبيقات. عندما يقوم برنامج تشغيل نظام الملفات بقراءة ملف أو كتابته، يرسل المفتاح المغلّف إلى محرك AES، والذي يقوم بفك تغليف المفتاح. لا يعرض محرك AES المفتاح غير المُغلّف للبرنامج أبدًا.

ملاحظة: محرك AES عبارة عن مكون منفصل عن كل من Secure Enclave ومحرك AES في Secure Enclave، ولكن تشغيله مرتبط بشكل وثيق بـ Secure Enclave كما هو موضح أدناه.



مُسرّع المفتاح العام

مُسرّع المفتاح العام (PKA) عبارة عن كتلة مادية تُستخدم لإجراء عمليات التشفير غير المتماثل. يدعم PKA خوارزميات التوقيع والتشفير RSA و ECC (منحنى القطع الناقص). صُمّم PKA لمقاومة تسرُّب المعلومات عبر التوقيت وهجمات القناة الجانبية مثل SPA و DPA.

يدعم PKA مفاتيح البرامج والمكونات المادية. يتم اشتقاق مفاتيح المكونات المادية من معرّف UID أو GID الخاصين بـ Secure Enclave. وتظل هذه المفاتيح داخل PKA ولا تكون مرئية حتى لبرنامج sepOS.

بدءًا من A13 SoCs، ثبت أن تطبيقات تشفير PKA صحيحة رياضيًا باستخدام تقنيات التحقق الرسمية.

على Apple A10 وأنظمة SocS الأحدث، يدعم PKA المفاتيح المرتبطة بنظام التشغيل، ويُشار إليه أيضًا باسم حماية المفاتيح المؤمنة (SKP). يتم إنشاء هذه المفاتيح باستخدام مجموعة من UID للجهاز وتجزئة sepOS التي تعمل على الجهاز. يتم توفير التجزئة بواسطة Boot ROM في Secure Enclave، أو من خلال مراقب التمهيد في Secure Enclave على Apple A13 وأنظمة SoCs الأحدث. تُستخدم هذه المفاتيح أيضًا للتحقق من إصدار sepOS عند تقديم طلبات إلى خدمات Apple معينة، كما تُستخدم أيضًا لتحسين أمن البيانات المحمية برمز دخول من خلال المساعدة على منع الوصول إلى مادة المفاتيح في حالة إجراء تغييرات مهمة على النظام من دون تفويض من المستخدم.

التخزين غير المتطاير الآمن

تم تزويد Secure Enclave بجهاز تخزين غير متطاير آمن مخصص. يتم توصيل التخزين غير المتطاير الآمن بـ Secure Enclave باستخدام ناقل I2C مخصص، بحيث لا يمكن الوصول إليه إلا من خلال Secure Enclave. جميع مفاتيح تشفير بيانات المستخدم متجذرة في الإنتروبيا المخزنة في التخزين غير المتطاير في Secure Enclave.

في الأجهزة المثبت عليها A12 و S4 وأنظمة SoCs الأحدث، يتم إقران Secure Enclave مع مكون تخزين آمن لتخزين الإنتروبيا. تم تصميم مكون التخزين الآمن ذاته مع تعليمات ROM برمجية ثابتة ومولّد أرقام عشوائية مادي ومفتاح تشفير فريد لكل جهاز ومحركات تشفير واكتشاف العبث المادي. يتواصل Secure Enclave ومكون التخزين الآمن باستخدام بروتوكول مشفر ومصادق عليه يوفر الوصول الحصري إلى الإنتروبيا.

تم تزويد الأجهزة التي تم إصدارها لأول مرة في خريف 2020 أو أحدث بمكون تخزين آمن من الجيل الثاني. ويضيف مكون التخزين الآمن من الجيل الثاني صناديق قفل ذات عدّاد. يُخزّن كل صندوق قفل ذي عدّاد قيمةً عشوائيةً من 128 بت، ومُتحقِّق من رمز الدخول من 128 بت، وعدّاد من 8 بت، وقيمة محاولات قصوى من 8 بت. ويتم الوصول إلى صناديق القفل ذات العدّاد عبر بروتوكول مشفر ومصادق عليه.

تحمل صناديق القفل ذات العدّاد الإنتروبيا اللازمة لفتح قفل بيانات المستخدم المحمية برمز دخول. للوصول إلى بيانات المستخدم، يجب على Secure Enclave المقترن اشتقاق قيمة إنتروبيا لرمز الدخول الصحيح من رمز الدخول الخاص بالمستخدم ومعرف UID الخاص بـ Secure Enclave. لا يمكن التعرف على رمز دخول المستخدم باستخدام محاولات فتح القفل المرسلة من مصدر غير Secure Enclave المقترن. إذا تم تجاوز حد محاولات إدخال رمز الدخول (على سبيل المثال، 10 محاولات على الـ iPhone)، يتم مسح البيانات المحمية برمز الدخول بالكامل بواسطة مكون التخزين الآمن.

لإنشاء صندوق قفل ذي عدّاد، يرسل Secure Enclave إلى مكون التخزين الآمن قيمة إنتروبيا رمز الدخول وقيمة الحد الأقصى للمحاولات. ويقوم مكون التخزين الآمن بإنشاء قيمة عشوائية باستخدام مُولّد الأرقام العشوائية الخاص بها. ثم تستخرج قيمة تحقق من رمز الدخول وقيمة إنتروبيا لصندوق القفل من إنتروبيا رمز الدخول المرفق ومفتاح التشفير الفريد لمكون التخزين الآمن والقيمة العشوائية. يعمل مكون التخزين الآمن على تهيئة صندوق القفل ذي العدّاد بعدد 0، وقيمة الحد الأقصى للمحاولات المُقدّمة، وقيمة التحقُّق المشتقة، والقيمة العشوائية. يقوم مكون التخزين الآمن بعد ذلك بإرجاع قيمة إنتروبيا صندوق القفل المنشأة إلى Secure Enclave.

لاسترداد قيمة إنتروبيا صندوق القفل من صندوق قفل ذي عدّاد لاحقًا، يرسل Secure Enclave إنتروبيا رمز الدخول إلى مكون التخزين الآمن. يعمل مكون التخزين الآمن أولاً على زيادة عدّاد صندوق القفل. وإذا تجاوز العداد المتزايد القيمة القصوى لعدد المحاولات، فإن مكون التخزين الآمن يطمس صندوق القفل ذا العدّاد. إذا لم يتم الوصول إلى الحد الأقصى لعدد المحاولات، يحاول مكون التخزين الآمن اشتقاق قيمة التحقق من رمز الدخول وقيمة إنتروبيا صندوق القفل باستخدام نفس الخوارزمية المستخدمة لإنشاء صندوق القفل ذي العدّاد. إذا كانت قيمة التحقق من رمز الدخول المشتقة مطابقة لقيمة التحقق من رمز الدخول المخزنة، يُرجع مكون التخزين الآمن قيمة إنتروبيا صندوق القفل إلى Secure Enclave ويُعيد تعيين العدّاد إلى 0.

تكون المفاتيح المستخدمة للوصول إلى البيانات المحمية بكلمة سر متجذرةً في إنتروبيا المُخزّنة في صناديق القفل ذات العدّاد. لمزيد من المعلومات، انظر نظرة عامة على حماية البيانات.

يتم استخدام التخزين غير المتطاير الآمن لكل الخدمات المضادة لإعادة التشغيل في Secure Enclave. تُستخدم الخدمات غير القابلة لإعادة التشغيل على Secure Enclave لإبطال البيانات عبر الأحداث التي تميّز الحدود غير القابلة لإعادة التشغيل، بما في ذلك، على سبيل المثال لا الحصر، ما يلي:

- تغيير رمز الدخول
- تمكين أو تعطيل بصمة الوجه أو بصمة الإصبع
- إضافة وجه في بصمة الوجه أو بصمة إصبع في بصمة الإصبع أو إزالتهما
- إعادة تعيين بصمة الوجه أو بصمة الإصبع
- إضافة أو إزالة بطاقة Apple Pay
- مسح جميع المحتويات والإعدادات

في البُنى التي لا تحتوي على مكون تخزين آمن، يتم استخدام ذاكرة EEPROM (ذاكرة للقراءة فقط قابلة للمسح والبرمجة كهربائيًا) لتوفير خدمات تخزين آمنة في Secure Enclave. وكما هو الحال مع مكونات التخزين الآمنة، فإن ذاكرة EEPROM يتم إرفاقها والوصول إليها فقط من Secure Enclave، ولكنها لا تحتوي على ميزات أمن مادية مخصصة ولا تضمن الوصول الحصري إلى إنتروبيا (باستثناء خصائص التوصيل المادي) أو وظيفة صندوق القفل ذي العدّاد.

المحرك العصبي الآمن

على الأجهزة المزودة ببصمة الوجه (لا تتضمن بصمة الإصبع)، يحول المحرك العصبي الآمن الصور ثنائية الأبعاد وخرائط العمق إلى تمثيل رياضي لوجه المستخدم.

على A11 وحتى A13 SoCs، تم دمج المحرك العصبي الآمن في Secure Enclave. يستخدم المحرك العصبي الآمن الوصول المباشر للذاكرة (DMA) لتحقيق أداء عالٍ. تقوم وحدة إدارة ذاكرة إدخال/إخراج (IOMMU) بتقييد الواقعة تحت سيطرة نواة sepOS هذا الوصول المباشر إلى مناطق الذاكرة المصرح بها.

بدءًا من A14 أو M1 أو أحدث، يتم تطبيق المحرك العصبي الآمن كنمط آمن في المحرك العصبي لمعالج التطبيقات. تقوم وحدة تحكم أمن المكونات المادية المخصصة بالتبديل بين مهام معالج التطبيقات ومهام Secure Enclave، وإعادة تعيين حالة المحرك العصبي في كل انتقال للحفاظ على أمن بيانات بصمة الوجه. ويقوم محرك مخصص بتطبيق تشفير الذاكرة والمصادقة والتحكم في الوصول. في الوقت نفسه، يستخدم مفتاح تشفير ونطاق ذاكرة منفصلين لقصر المحرك العصبي الآمن على مناطق الذاكرة المصرح بها.

برامج مراقبة الطاقة والساعة

صُمِّمت جميع الأجهزة الإلكترونية لتعمل في نطاق جهد وتردد محدود. يمكن أن تتعطل الأجهزة الإلكترونية عند تشغيلها خارج هذا الغلاف، ومن ثم قد يتم تجاوز ضوابط الأمن. صُمِّم Secure Enclave بدوائر مراقبة للمساعدة على ضمان بقاء الجهد والتردد في نطاق آمن. وصُمِّمت دوائر المراقبة هذه بحيث يكون لها غلاف تشغيل أكبر بكثير من باقي Secure Enclave. إذا اكتشفت الشاشات نقطة تشغيل غير قانونية، فإن الساعات في Secure Enclave تتوقف تلقائيًا ولا يُعاد تشغيلها حتى تتم إعادة تعيين SoC التالية.

ملخص ميزة Secure Enclave

ملاحظة: تتضمن منتجات A12 و A13 و S4 و S5 التي تم إصدارها لأول مرة في خريف 2020 الجيل الثاني من مكون التخزين الآمن، بينما تتضمن المنتجات الأقدم التي تعتمد على SoCs الجيل الأول من مكون التخزين الآمن.

SoC	محرك حماية الذاكرة	التخزين الآمن	محرك AES	PKA
A8	التشفير والمصادقة	EEPROM	نعم	لا
A9	التشفير والمصادقة	EEPROM	حماية DPA	نعم
A10	التشفير والمصادقة	EEPROM	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
A11	التشفير والمصادقة ومنع إعادة التشغيل	EEPROM	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
A12 (أجهزة Apple التي تم إصدارها قبل خريف 2020)	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الأول	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
A12 (أجهزة Apple التي تم إصدارها بعد خريف 2020)	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الثاني	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
A13 (أجهزة Apple التي تم إصدارها قبل خريف 2020)	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الأول	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل ومراقب التمهيد
A13 (أجهزة Apple التي تم إصدارها بعد خريف 2020)	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الثاني	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل ومراقب التمهيد
A14 إلى A17	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الثاني	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل ومراقب التمهيد
S3	التشفير والمصادقة	EEPROM	حماية DPA ووحدات البت الجذرية القابلة للقفل	نعم
S4	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الأول	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
S5 (أجهزة Apple التي تم إصدارها قبل خريف 2020)	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الأول	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
S5 (أجهزة Apple التي تم إصدارها بعد خريف 2020)	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الثاني	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل

SoC	محرك حماية الذاكرة	التخزين الآمن	محرك AES	PKA
S6 إلى S9	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الثاني	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
T2	التشفير والمصادقة	EEPROM	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل
M1 و M2 و M3	التشفير والمصادقة ومنع إعادة التشغيل	مكون التخزين الآمن من الجيل الثاني	حماية DPA ووحدات البت الجذرية القابلة للقفل	المفاتيح المرتبطة بنظام التشغيل ومراقب التمهيد

بصمة الوجه وبصمة الإصبع

أمن بصمة الوجه وبصمة الإصبع

تعد رموز الدخول وكلمات السر ضرورية لأمان أجهزة Apple. في الوقت نفسه، يحتاج المستخدمون إلى التمتع بإمكانية الوصول السلس إلى أجهزتهم، غالبًا أكثر من مائة مرة في اليوم. توفر المصادقة البيومترية طريقة للاحتفاظ بالأمن الذي يوفره رمز الدخول القوي؛ أو حتى تعزيز رمز الدخول أو كلمة السر حيث لن يلزم إدخال أيهما يدويًا؛ مع توفير رفاهية فتح القفل السريع بضغطة إصبع أو مجرد نظرة. ولا يحل بصمة الوجه وبصمة الإصبع محل رمز الدخول أو كلمة السر، ولكن في معظم الحالات يجعلان الوصول أسرع وأسهل.

تعتمد بنية أمان المقاييس الحيوية من Apple على فصل صارم للمسؤوليات بين مستشعر المقاييس الحيوية و Secure Enclave، واتصال آمن بين الاثنين. يلتقط المستشعر صورة المقاييس الحيوية وينقلها بأمان إلى Secure Enclave. أثناء التسجيل، يعمل Secure Enclave على معالجة بيانات قوالب بصمة الوجه وبصمة الإصبع المقابلة وتشفيرها وتخزينها. أثناء المطابقة، يقارن Secure Enclave البيانات الواردة من مستشعر المقاييس الحيوية بالقوالب المخزنة لتحديد ما إذا كان سيتم فتح قفل الجهاز أو الرد بأن المطابقة صالحة (لـ Apple Pay وداخل التطبيق والاستخدامات الأخرى لكل من بصمة الوجه وبصمة الإصبع). تدعم البنية الأساسية الأجهزة التي تتضمن كلاً من المستشعر و Secure Enclave (مثل iPhone و iPad والعديد من أنظمة Mac)، فضلاً عن القدرة على فصل المستشعر ماديًا إلى جهاز طرفي يتم إقرانه بأمان بـ Secure Enclave في Mac مزود برقاقات Apple.

أمن بصمة الوجه

بنظرة بسيطة، يفتح بصمة الوجه قفل أجهزة Apple المدعومة بشكل آمن. ويوفر مصادقة بديهية وآمنة يتم تمكينها من خلال نظام كاميرا العمق الحقيقي الذي يستخدم تقنيات متقدمة لرسم خريطة هندسية لوجه المستخدم بدقة. يستخدم بصمة الوجه شبكات عصبية لتحديد الانتباه والمطابقة ومكافحة تزييف الهوية، بحيث يمكن للمستخدم فتح قفل هاتفه بنظرة خاطفة، حتى عند ارتداء قناع عند استخدام الأجهزة المدعومة. ويتكيف بصمة الوجه تلقائيًا مع التغييرات في المظهر، ويحمي خصوصية وأمن بيانات المقاييس الحيوية للمستخدم بعناية.

تم تصميم بصمة الوجه لتأكيد انتباه المستخدم وتوفير مصادقة قوية مع خفض معدل المطابقة الخاطئة ومكافحة تزييف الهوية الرقمي والمادي.

تبحث كاميرا العمق الحقيقي تلقائيًا عن وجه المستخدم عندما يُنبّه المستخدم جهاز Apple الذي يحتوي على بصمة الوجه (عن طريق رفعها أو الضغط على الشاشة)، وكذلك عندما تحاول هذه الأجهزة مصادقة المستخدم لعرض إشعار وارد أو عندما يطلب أي تطبيق مدعوم مصادقة بصمة الوجه. بعد اكتشاف الوجه، تؤكد بصمة الوجه الانتباه والعزم على فتح القفل عن طريق اكتشاف أن عيني المستخدم مفتوحتان وأن انتباهه موجه نحو جهازه؛ ويتم تعطيل فحص انتباه بصمة الوجه عند تنشيط التعليق الصوتي، لتسهيلات الاستخدام؛ ويمكن تعطيله بشكل منفصل، إذا لزم الأمر. يلزم كشف الانتباه دائمًا عند استخدام بصمة الوجه عند ارتداء قناع.

بعد أن تؤكد كاميرا العمق الحقيقي وجود وجه منتبه، تعرض وتقرأ آلاف النقاط بالأشعة تحت الحمراء لتشكيل خريطة عمق للوجه، بجانب صورة ثنائية الأبعاد بالأشعة تحت الحمراء. وتُستخدم هذه البيانات لإنشاء تسلسل من الصور ثنائية الأبعاد وخرائط العمق يتم توقيعها رقميًا وإرسالها إلى Secure Enclave. لمواجهة عمليات تزييف الهوية الرقمية والمادية، تعمل كاميرا العمق الحقيقي على عشوائية تسلسل الصور ثنائية الأبعاد ولقطات خريطة العمق، وترسم نمطًا عشوائيًا خاصًا بالجهاز. يحوّل جزء من المحرك العصبي الآمن؛ المحمي داخل Secure Enclave؛ هذه البيانات إلى تمثيل رياضي ويقارن هذا التمثيل ببيانات الوجه المسجلة. وتمثّل بيانات الوجه المسجلة هذه في حد ذاتها تمثيلاً رياضيًا لوجه المستخدم الذي تم التقاطه عبر مجموعة متنوعة من الأشكال.

أمن بصمة الإصبع

بصمة الإصبع هو نظام استشعار بصمات الأصابع الذي يجعل الوصول الآمن إلى أجهزة Apple المدعومة أسرع وأسهل. تقرأ هذه التقنية بيانات بصمة الإصبع من أي زاوية وتتعلم المزيد عن بصمة إصبع المستخدم مع مرور الوقت، مع استمرار المستشعر في توسيع خريطة بصمة الإصبع كلما تم التعرف على عُقد متداخلة إضافية مع كل استخدام.

يمكن فتح قفل أجهزة Apple المزودة بمستشعر بصمة الإصبع باستخدام بصمة إصبع. لا يحل بصمة الإصبع محل الحاجة إلى رمز دخول الجهاز أو كلمة سر المستخدم، حيث يظل أحدهما مطلوبًا بعد بدء تشغيل الجهاز أو إعادة تشغيله أو تسجيل الخروج منه (على أي Mac). في بعض التطبيقات، يمكن أيضًا استخدام بصمة الإصبع بدلاً من رمز دخول الجهاز أو كلمة سر المستخدم، على سبيل المثال لفتح قفل الملاحظات المحمية بكلمة سر في تطبيق الملاحظات وفتح قفل مواقع الويب المحمية بسلسلة المفاتيح وفتح قفل كلمات سر التطبيقات المدعومة. ومع ذلك، يلزم دائمًا إدخال رمز دخول الجهاز أو كلمة سر المستخدم في بعض السيناريوهات (على سبيل المثال، لتغيير رمز دخول الجهاز الموجود أو كلمة سر المستخدم الموجودة أو لإزالة تسجيلات بصمات الأصابع الموجودة أو إنشاء تسجيلات جديدة).

عندما يكتشف مستشعر بصمة الإصبع لمسة إصبع، يشغّل مصفوفة التصوير المتقدمة لمسح الإصبع ويرسل نسخة المسح إلى Secure Enclave. تختلف القناة المستخدمة لتأمين هذا الاتصال، اعتمادًا على ما إذا كان مستشعر بصمة الإصبع مضمنًا في الجهاز مع Secure Enclave أو موجودًا في جهاز طرفي منفصل.

أثناء توجيه المسح النقطي لبصمات الأصابع للتحليل، يتم تخزينه مؤقتًا في ذاكرة مشفرة داخل Secure Enclave ومن ثم يتم تجاهله. يستخدم التحليل تعيين زاوية تدفق النتوء تحت الجلد، وهي عملية تتسم بفقدان البيانات بحيث إنها تتجاهل "البيانات التفصيلية للإصبع" التي قد تكون مطلوبة لإعادة بناء بصمة إصبع المستخدم الفعلية. أثناء التسجيل، يتم تخزين خريطة العُقد الناتجة بتنسيق مشفر لا يمكن قراءته إلا بواسطة Secure Enclave كقالب للمقارنة به في عمليات المطابقة المستقبلية، ولكن بدون أي معلومات هوية. ولا تغادر هذه البيانات الجهاز أبدًا. ولا تُرسل إلى Apple، ولا يتم تضمينها في النُسخ الاحتياطية للجهاز.

أمن قناة بصمة الإصبع المضمنة

يتم الاتصال بين Secure Enclave ومستشعر بصمة الإصبع المضمن عبر ناقل واجهة طرفية تسلسلية. ويقوم المعالج بإعادة توجيه البيانات إلى Secure Enclave ولكن لا يمكنه قراءتها. ويتم تشفيرها ومصادقتها باستخدام مفتاح جلسة يتم التفاوض عليه باستخدام مفتاح مشترك يتم توفيره لكل مستشعر بصمة الإصبع و Secure Enclave المقابل له في المصنع. لكل مستشعر بصمة الإصبع، يكون المفتاح المشترك قويًا وعشوائيًا ومختلفًا. يستخدم تبادل مفتاح الجلسة تغليف مفتاح AES، حيث يوفر كلا الجانبين مفتاحًا عشوائيًا ينشئ مفتاح الجلسة ويستخدم تشفير النقل الذي يوفر المصادقة والسرية (باستخدام AES-CCM).

لوحة مفاتيح ماجيك المزودة ببصمة الإصبع

توفر لوحة مفاتيح ماجيك المزودة بنظام بصمة الإصبع (وكذلك لوحة مفاتيح ماجيك المزودة ببصمة الإصبع ولوحة المفاتيح الرقمية) مستشعر بصمة الإصبع في لوحة مفاتيح خارجية يمكن استخدامها مع أي Mac مزود برقاقات Apple. تؤدي لوحة مفاتيح ماجيك المزودة ببصمة الإصبع دور مستشعر المقاييس الحيوية؛ لا تخزن قوالب المقاييس الحيوية ولا تقوم بإجراء المطابقة الحيوية، أو تفرض سياسات الأمان (على سبيل المثال، الاضطرار إلى إدخال كلمة السر بعد 48 ساعة دون فتح القفل). يجب أن يتم إقران مستشعر بصمة الإصبع في لوحة مفاتيح ماجيك المزودة ببصمة الإصبع بشكل آمن مع Secure Enclave على Mac قبل تمكين استخدامه، ثم يقوم Secure Enclave بإجراء عمليات التسجيل والمطابقة ويفرض سياسات الأمن بالطريقة ذاتها التي يُستخدم بها في مستشعر بصمة الإصبع مضمن. تعمل Apple على تنفيذ عملية الاقتران في المصنع لأي لوحة مفاتيح ماجيك مزودة ببصمة الإصبع التي تأتي برفقة أي جهاز Mac. يمكن أيضًا إجراء الاقتران بواسطة المستخدم إذا لزم الأمر. يمكن إقران لوحة مفاتيح ماجيك المزودة ببصمة الإصبع بشكل آمن مع جهاز Mac واحد فقط في كل مرة، ولكن يستطيع Mac الحفاظ على الاقتران الآمن مع ما يصل إلى خمس لوحات مفاتيح لوحة مفاتيح ماجيك مختلفة مزودة ببصمة الإصبع.

تتوافق لوحة مفاتيح ماجيك المزودة ببصمة الإصبع ومستشعرات بصمة الإصبع المضمنة. إذا تم وضع إصبع تم تسجيله في مستشعر بصمة الإصبع مضمن بأي Mac على لوحة مفاتيح ماجيك مزودة ببصمة الإصبع، فإن Secure Enclave في Mac تعالج المطابقة بنجاح، والعكس صحيح.

لدعم الاقتران الآمن وبالتالي الاتصال بين Secure Enclave ولوحة مفاتيح ماجيك المزودة ببصمة الإصبع على Mac، تم تجهيز لوحة المفاتيح بجهاز مُسرّع المفتاح العام (PKA)، لتوفير التوثيق، وبمفاتيح مستندة إلى الأجهزة، لتنفيذ عمليات التشفير اللازمة.

الاقتران الآمن

قبل أن تتمكن من استخدام لوحة مفاتيح ماجيك المزودة ببصمة الإصبع لتنفيذ عمليات بصمة الإصبع، يجب إقرانها بأمان مع Mac. للإقران، فإن Secure Enclave على Mac وحزمة PKA في لوحة مفاتيح ماجيك المزودة ببصمة الإصبع تتبادلان المفاتيح العامة، المتجذرة في Apple CA الموثوق بها، وتستخدمان مفاتيح التوثيق المحمولة بالأجهزة ومفتاح ECDH سريع الزوال لتوثيق هويتهما بشكل آمن. على Mac، تكون هذه البيانات محمية بواسطة Secure Enclave؛ وعلى لوحة مفاتيح ماجيك المزودة ببصمة الإصبع، تكون هذه البيانات محمية بواسطة حزمة PKA. بعد الاقتران الآمن، يتم تشفير جميع بيانات بصمة الإصبع المتصلة بين Mac ولوحة مفاتيح ماجيك المزودة ببصمة الإصبع بواسطة AES-GCM بطول مفتاح 256 بت، باستخدام مفاتيح ECDH سريعة الزوال التي تستخدم منحنى NIST P-256 استنادًا إلى الهويات المخزنة. لمزيد من المعلومات عن استخدام لوحة المفاتيح في النمط اللاسلكي، انظر أمن Bluetooth.

غرض الإقران الآمن

لإجراء بعض عمليات بصمة الإصبع لأول مرة، مثل تسجيل بصمة إصبع جديدة، يجب على المستخدم تأكيد غرضه ماديًا لاستخدام لوحة مفاتيح ماجيك مزودة ببصمة الإصبع مع Mac. يتم تأكيد الغرض المادي بالضغط مرتين على زر الطاقة في Mac عند الإشارة إليه بواسطة واجهة المستخدم، أو عن طريق مطابقة بصمة إصبع تم تسجيلها سابقًا مع Mac بنجاح. لمزيد من المعلومات، انظر الغرض الآمن والاتصالات الآمنة مع Secure Enclave.

يمكن مصادقة معاملات Apple Pay بمطابقة بصمة الإصبع أو عن طريق إدخال كلمة سر مستخدم macOS والضغط مرتين على زر بصمة الإصبع في لوحة مفاتيح ماجيك المزودة ببصمة الإصبع. يعمل الأخير على تمكين المستخدم من تأكيد الغرض المادي حتى دون مطابقة بصمة الإصبع.

أمن قناة لوحة مفاتيح ماجيك المزودة ببصمة الإصبع

للمساعدة على ضمان وجود قناة اتصال آمنة بين مستشعر بصمة الإصبع في لوحة مفاتيح ماجيك مزودة ببصمة الإصبع و Secure Enclave على Mac المقترن، يلزم ما يلي:

- الاقتران الآمن بين لوحة مفاتيح ماجيك مزودة بحزمة PKA الخاصة ببصمة الإصبع و Secure Enclave كما هو موضح أعلاه
- قناة آمنة بين لوحة مفاتيح ماجيك المزودة بمستشعر بصمة الإصبع وحزمة PKA الخاصة بها

تم إنشاء القناة الآمنة بين لوحة مفاتيح ماجيك المزودة بمستشعر بصمة الإصبع وحزمة PKA الخاصة بها في المصنع باستخدام مفتاح فريد مشترك بين الاثنين. (تلك هي التقنية نفسها المستخدمة لإنشاء القناة الآمنة بين Secure Enclave على Mac والمستشعر المضمن به، على أجهزة كمبيوتر Mac المزودة ببصمة الإصبع مضمن).

بصمة الوجه وبصمة الإصبع ورموز المرور وكلمات السر

لاستخدام بصمة الوجه أو بصمة الإصبع، يتعين على المستخدم إعداد جهازه بحيث يلزم إدخال رمز دخول أو كلمة سر لفتح القفل. عندما يكتشف بصمة الوجه أو بصمة الإصبع مطابقة ناجحة، يتم إلغاء قفل جهاز المستخدم دون طلب رمز الدخول أو كلمة السر للجهاز. وهذا يُضفي مزيدًا من القابلية التطبيقية على استخدام رمز دخول أو كلمة سر أطول وأكثر تعقيدًا حيث إنه لا يتعين على المستخدم إدخال أيهما بهذا الشكل المتكرر. لا يحل بصمة الوجه وبصمة الإصبع محل رمز الدخول أو كلمة السر للمستخدم؛ ولكنهما يوفران وصولاً سهلاً إلى الجهاز ضمن حدود مدروسة وقيود زمنية. ويعد ذلك مهمًا لأن رمز الدخول القوي أو كلمة السر القوية بمثابة الأساس الذي يشكّل كيفية عمل جهاز iPhone أو iPad أو Mac أو Apple Watch الخاص بالمستخدم على حماية بيانات المستخدم بطريقة مشفرة.

متى يلزم وجود رمز الدخول أو كلمة السر للجهاز

يستطيع المستخدم استخدام رمز الدخول أو كلمة السر في أي وقت بدلاً من بصمة الوجه أو بصمة الإصبع، لكن ثمة حالات لا يُسمح فيها باستخدام المقاييس الحيوية. دائمًا ما تتطلب العمليات الحساسة للأمن التالية إدخال رمز دخول أو كلمة سر:

- تحديث البرامج
- مسح الجهاز
- عرض إعدادات رمز الدخول أو تغييرها
- تثبيت ملفات تعريف التكوين
- فتح قفل جزء الخصوصية والأمن في إعدادات النظام (macOS 13 أو أحدث) على Mac

- فتح قفل جزء الأمن والخصوصية في تفضيلات النظام (macOS 12 أو أقدم) على Mac
- فتح قفل جزء "المستخدمون والمجموعات" في إعدادات النظام (macOS 13 أو أحدث) على Mac (في حالة تشغيل خزنة الملفات)
- فتح قفل جزء "المستخدمون والمجموعات" في تفضيلات النظام (macOS 12 أو أقدم) على Mac (في حالة تشغيل خزنة الملفات)

يلزم كذلك إدخال رمز المرور أو كلمة السر إذا كان الجهاز في أي من الحالات الآتية:

- تشغيل الجهاز أو إعادة تشغيله.
- تسجيل خروج المستخدم من حسابه على الـ Mac (أو عدم تسجيل دخوله حتى اللحظة).
- عدم فتح قفل المستخدم لجهازه لأكثر من 48 ساعة.
- عدم استخدام المستخدم رمز الدخول أو كلمة السر لفتح قفل جهازه لمدة 156 ساعة (ستة أيام ونصف)، وعدم استخدام المستخدم المقاييس الحيوية لفتح قفل جهازه خلال 4 ساعات.
- استقبال الجهاز لأمر قفل عن بُعد.
- يمكن للمستخدم إنهاء إيقاف التشغيل/طوارئ SOS بالضغط مطولاً على أي من زري مستوى الصوت وزر إسبات/تنبيه في نفس الوقت لمدة ثانيتين ثم الضغط على إلغاء.
- تتوفر خمس محاولات غير ناجحة لمطابقة المقاييس الحيوية (لسهولة الاستخدام، قد يعرض الجهاز إدخال رمز دخول أو كلمة سر بدلاً من استخدام المقاييس الحيوية بعد عدد أقل من المحاولات الفاشلة).

عند تمكين بصمة الوجه على iPhone مع ارتداء قناع، يكون متاحًا لمدة 6.5 ساعات بعد أحد إجراءات المستخدم الآتية:

- محاولة ناجحة لمطابقة بصمة الوجه (باستخدام قناع أو من دونه)
- التحقق من صحة رمز المرور للجهاز
- فتح الجهاز باستخدام Apple Watch

عند تنفيذ أي من تلك الإجراءات، تطول الفترة لمدة 6.5 ساعات إضافية.

عند تمكين بصمة الوجه أو بصمة الإصبع على iPhone أو iPad، يتم قفل الجهاز فورًا عند الضغط على إسبات/تنبيه، ويتم قفل الجهاز في كل مرة يدخل فيها حالة الإسبات. يتطلب بصمة الوجه وبصمة الإصبع مطابقة ناجحة—أو استخدام رمز الدخول اختياريًا—مع كل تنبيه.

تُعد احتمالية فتح شخص عشوائي من السكان لـ iPhone أو iPad للمستخدم أقل من 1 في 1,000,000 باستخدام بصمة الوجه—بما في ذلك تشغيل بصمة الوجه مع ارتداء قناع. بالنسبة إلى طرز iPhone و iPad و Mac الخاصة بالمستخدم والمزودة ببصمة الإصبع وتلك المقترنة بلوحة مفاتيح ماجيك، فإن الاحتمالية أقل من 1 في 50,000. وتزداد هذه الاحتمالية مع وجود العديد من بصمات الأصابع المسجلة (حتى 1 من 10000 مع خمس بصمات أصابع) أو الهيئات (حتى 1 من 500000 مع هيئتين). لمزيد من الحماية، يسمح كل من بصمة الوجه وبصمة الإصبع بخمس محاولات مطابقة غير ناجحة فقط قبل المطالبة بإدخال رمز دخول أو كلمة سر للوصول إلى جهاز المستخدم أو حسابه. عند استخدام بصمة الوجه، تكون احتمالية المطابقة الخاطئة أعلى في الحالات الآتية:

- التوائم والأشقاء الذين يشبهون المستخدم
- الأطفال الذين تقل أعمارهم عن 13 عامًا (حيث إن ملامح وجوههم المميزة ربما لم تتطور بشكل كامل)

تزداد احتمالية المطابقة الخاطئة في تلك الحالتين عند استخدام بصمة الوجه مع ارتداء قناع. إذا شعر المستخدم بالقلق إزاء مطابقة خاطئة، توصي Apple باستخدام رمز دخول للمصادقة.

أمن مطابقة الوجوه

تتم مطابقة الوجوه داخل Secure Enclave باستخدام الشبكات العصبية المدربة خصوصًا لهذا الغرض. طورت Apple شبكات عصبية لمطابقة الوجوه باستخدام أكثر من مليار صورة، بما في ذلك صور الأشعة تحت الحمراء (IR) والصور العميقة التي تم جمعها في الدراسات التي أُجريت بموافقة المشاركين المستنيرة. بعد ذلك، عملت Apple مع المشاركين من جميع أنحاء العالم لتضمين مجموعة تمثيلية من الأشخاص، مع مراعاة الجنس والعمر والعرق وعوامل أخرى. تمت زيادة الدراسات حسب الحاجة لتوفير درجة عالية من الدقة على مجموعة متنوعة من المستخدمين. تم تصميم بصمة الوجه للعمل في ظل وجود القبعات والأوشحة والنظارات والعدسات اللاصقة والعديد من النظارات الشمسية. يدعم نظام بصمة الوجه كذلك فتح القفل باستخدام قناع على أجهزة iPhone بدءًا من iPhone 12 وiOS 15.4 أو أحدث. علاوة على ذلك، تم تصميمه للعمل في البيئات الداخلية والخارجية وحتى في الظلام الدامس. كما توجد شبكة عصبية إضافية مدرّبة على اكتشاف ومكافحة تزييف الهوية تدافع ضد محاولات فتح قفل الجهاز باستخدام الصور أو الأقنعة. يتم تشفير بيانات بصمة الوجه، بما في ذلك التمثيلات الرياضية لوجه المستخدم، ولا تكون متاحة إلا لـ Secure Enclave. ولا تغادر هذه البيانات الجهاز أبدًا. ولا تُرسل إلى Apple، ولا يتم تضمينها في النُسخ الاحتياطية للجهاز. يتم حفظ بيانات بصمة الوجه الآتية، مشفرةً للاستخدام بواسطة Secure Enclave فقط، أثناء التشغيل العادي:

- التمثيلات الرياضية لوجه المستخدم المحسوبة أثناء التسجيل
- التمثيلات الرياضية لوجه المستخدم المحسوبة أثناء بعض محاولات فتح القفل إذا رأى بصمة الوجه أنها مفيدة لرفع مستوى المطابقة المستقبلية

لا تُحفَظ صور الوجه الملتقطة أثناء التشغيل العادي، ولكن يتم تجاهلها على الفور بعد حساب التمثيل الرياضي إمّا للتسجيل في بيانات بصمة الوجه وإمّا للمقارنة مع بيانات بصمة الوجهالمسجَّلة.

تحسين مطابقات بصمة الوجه

لتحسين أداء المطابقة ومواكبة التغييرات الطبيعية للوجه والشكل، يعمل بصمة الوجه على زيادة التمثيل الرياضي المخزّن لديه مع مرور الوقت. عقب المطابقة الناجحة، قد يستخدم بصمة الوجه التمثيل الرياضي المحسوب حديثًا—إذا كانت جودته كافية—لعدد محدود من المطابقات الإضافية قبل تجاهل تلك البيانات. وعلى العكس من ذلك، إذا فشل بصمة الوجه في التعرف على الوجه، لكن جودة المطابقة أعلى من حد معين وأدخل المستخدم رمز الدخول عقب المحاولة الفاشلة مباشرةً، يأخذ نظام بصمة الوجه عملية التقاط أخرى ويزيد من بيانات بصمة الوجه المسجَّلة لديه باستخدام التمثيل الرياضي المحسوب حديثًا. يتم تجاهل بيانات بصمة الوجه الجديدة إذا توقف المستخدم عن المطابقة معها أو بعد عدد محدود من المطابقات؛ كما يتم تجاهل البيانات الجديدة عند تحديد خيار إعادة تعيين بصمة الوجه. تتيح عمليات إثراء البيانات هذه لبصمة الوجه مواكبة التغييرات الهائلة في شعر وجه المستخدم أو استخدامه الماكياج، مع تقليل نسبة القبول الخاطئ.

استخدامات بصمة الوجه وبصمة الإصبع

فتح قفل جهاز أو حساب مستخدم

عند إيقاف تشغيل بصمة الوجه أو بصمة الإصبع، عند قفل الجهاز أو الحساب، يتم تجاهل مفاتيح أعلى فئة من حماية البيانات—المخزنة في Secure Enclave. يتعذر الوصول إلى الملفات وعناصر سلسلة المفاتيح الموجودة في تلك الفئة حتى يفتح المستخدم قفل الجهاز أو الحساب بإدخال رمز الدخول أو كلمة السر.

عند تشغيل بصمة الوجه أو بصمة الإصبع، لا يتم تجاهل المفاتيح عند قفل الجهاز أو الحساب؛ وبدلاً من ذلك، يتم تغليفها بمفتاح تم توفيره لنظام بصمة الوجه أو بصمة الإصبع الفرعي داخل Secure Enclave. وإذا اكتشف الجهاز مطابقة ناجحة عندما يحاول المستخدم فتح قفل الجهاز أو الحساب، يوفر الجهازُ المفتاحَ لإلغاء تغليف مفاتيح حماية البيانات، ويتم فتح قفل الجهاز أو الحساب. توفر هذه العملية حماية إضافية من خلال طلب التعاون بين النظامين الفرعيين لحماية البيانات وبصمة الوجه أو بصمة الإصبع لفتح الجهاز.

عند إعادة تشغيل الجهاز، تُفقد المفاتيح المطلوبة لبصمة الوجه أو بصمة الإصبع لفتح الجهاز أو الحساب؛ تتجاهلها Secure Enclave بعد استيفاء أي شرط يتطلب إدخال رمز الدخول أو كلمة السر.

تأمين الشراء باستخدام Apple Pay

يمكن للمستخدم كذلك استخدام بصمة الوجه وبصمة الإصبع مع Apple Pay لإجراء عمليات شراء سهلة وآمنة في المتاجر والتطبيقات وعلى الويب:

- **استخدام بصمة الوجه في المتاجر:** لتخويل الدفع في المتاجر باستخدام بصمة الوجه، يجب على المستخدم أولاً تأكيد نيته للدفع من خلال النقر مرتين على الزر الجانبي. ويلتقط هذا النقر المزدوج نية المستخدم باستخدام إيماءة فعلية مرتبطة مباشرة بـ Secure Enclave ومقاومة لأي عملية تزييف تتم من خلال العمليات الضارة. ثم يقوم المستخدم بالمصادقة باستخدام بصمة الوجه قبل وضع الجهاز بالقرب من قارئ الدفع غير التلامسي. يمكن تحديد طريقة دفع مختلفة عبر Apple Pay بعد مصادقة بصمة الوجه، التي تتطلب إعادة المصادقة، ولكن لن يتعين على المستخدم النقر مرتين على الزر الجانبي مرة أخرى.
- **استخدام بصمة الوجه في التطبيقات وعلى الويب:** لإجراء عملية دفع داخل التطبيقات وعلى الويب، يؤكد المستخدم نية الدفع من خلال النقر مرتين على الزر الجانبي، ثم يقوم بالمصادقة باستخدام بصمة الوجه لتخويل الدفع. إذا لم تكتمل معاملة Apple Pay في غضون 60 ثانية من النقر مرتين على الزر الجانبي، يجب على المستخدم إعادة تأكيد نية الدفع من خلال النقر مرتين مجددًا.
- **استخدام بصمة الإصبع:** مع بصمة الإصبع، يتم تأكيد نية الدفع باستخدام إيماءة تنشيط مستشعر بصمة الإصبع مدمجة مع مطابقة ناجحة لبصمة إصبع المستخدم.

استخدام واجهات برمجة التطبيقات المقدمة من النظام

يمكن أن تستخدم تطبيقات الجهات الخارجية واجهات API التي يوفرها النظام لمطالبة المستخدم بالمصادقة باستخدام بصمة الوجه أو بصمة الإصبع أو رمز الدخول أو كلمة السر، بينما التطبيقات التي تدعم بصمة الإصبع تدعم بصمة الوجه تلقائيًا دون أي تغييرات. عند استخدام بصمة الوجه أو بصمة الإصبع، يتم إعلام التطبيق فقط بما إذا كانت المصادقة ناجحة أم لا؛ ولا يمكنه الوصول إلى بصمة الوجه أو بصمة الإصبع أو البيانات المرتبطة بالمستخدم المسجل.

حماية عناصر سلسلة المفاتيح

يمكن كذلك حماية عناصر سلسلة المفاتيح باستخدام بصمة الوجه أو بصمة الإصبع، بحيث لا يتم إصدارها إلا بواسطة Secure Enclave فقط عن طريق مطابقة ناجحة أو رمز دخول الجهاز أو كلمة سر الحساب. تتوفر لدى مطوري التطبيق واجهات API للتحقق من تعيين رمز الدخول أو كلمة السر بواسطة المستخدم، قبل طلب بصمة الوجه أو بصمة الإصبع أو رمز الدخول أو كلمة السر لفتح عناصر سلسلة المفاتيح. يمكن لمطوري التطبيقات القيام بأي مما يلي:

- المطالبة بألا تعود عمليات API للمصادقة إلى كلمة سر التطبيق أو رمز دخول الجهاز. كما يمكنهم الاستعلام عما إذا كان المستخدم مسجلاً أم لا، ما يسمح باستخدام بصمة الوجه أو بصمة الإصبع كعامل ثانٍ في التطبيقات الحساسة أمنيًا.
- إنشاء واستخدام مفاتيح منحنى القطع الناقص (ECC) داخل Secure Enclave بحيث يمكن حمايتها بواسطة بصمة الوجه أو بصمة الإصبع. يتم تنفيذ العمليات التي تحتوي على هذه المفاتيح دائمًا داخل Secure Enclave بعد أن تصرّح باستخدامها.

إجراء عمليات الشراء والموافقة عليها

يمكن للمستخدمين كذلك تكوين بصمة الوجه أو بصمة الإصبع للموافقة على عمليات الشراء من iTunes Store و App Store و Apple Books والمزيد، بحيث لا يضطر المستخدمون إلى إدخال كلمة سر Apple ID الخاصة بهم. عند إجراء عمليات الشراء، يتحقق Secure Enclave من حدوث المصادقة البيومترية، ثم يطلق مفاتيح ECC المستخدمة لتوقيع طلب المتجر.

الغرض الآمن والاتصالات الآمنة مع Secure Enclave

يوفر الغرض الآمن طريقة لتأكيد غرض المستخدم دون أي تفاعل مع نظام التشغيل أو معالج التطبيقات. ويكون الاتصال عبارة عن رابط مادي - من زر مادي إلى Secure Enclave - يتوفر في التالي:

- iPhone X أو أحدث
- Apple Watch Series 1 أو أحدث
- iPad Pro (كل الطرز)
- iPad Air (2020)
- أجهزة كمبيوتر Mac المزودة بسيليكون Apple

باستخدام هذا الرابط، يمكن للمستخدم تأكيد غرضه في إكمال عملية ما بطريقة تم تصميمها بحيث لا يمكن حتى للبرامج التي تتمتع بامتيازات جذرية أو تعمل في ملحقات kernel أن تكون مخادعة.

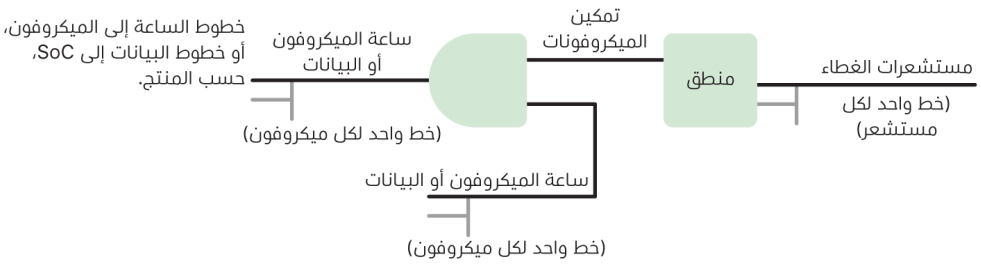
تُستخدم هذه الميزة لتأكيد غرض المستخدم أثناء معاملات Apple Pay وعند الانتهاء من إقران لوحة مفاتيح ماجيك مزودة ببصمة الإصبع على أي Mac مزود برقاقات Apple. يشير الضغط مرتين على الزر المناسب (لبصمة الوجه) أو المسح الضوئي لبصمة الإصبع (لبصمة الإصبع) عندما يُطلب منك ذلك من خلال واجهة المستخدم إلى تأكيد غرض المستخدم. لمزيد من المعلومات، انظر تأمين الشراء باستخدام Apple Pay. يتم دعم آلية مماثلة - تعتمد على Secure Enclave وبرامج T2 الثابتة - في طرز MacBook المزودة بشريحة Apple T2 الأمنية ولا تحتوي على شريط اللمس.

قطع اتصال مكون الميكروفون المادي

تتميز جميع أجهزة الـ Mac المحمولة المزودة بسيليكون Apple وجميع أجهزة الـ Mac المحمولة المزودة بشريحة Apple T2 الأمنية بقطع اتصال المكونات المادية الذي يضمن تعطيل الميكروفون كلما تم إغلاق الغطاء. على كل أجهزة كمبيوتر Macbook Pro و Macbook Air المحمولة مقاس 13 بوصة المزودة بشريحة T2، وجميع أجهزة MacBook المحمولة المزودة بشريحة T2 من 2019 أو أحدث، وأجهزة Mac المحمولة المزودة بسيليكون Apple، يتم تنفيذ قطع الاتصال هذا في المكونات المادية وحدها. تم تصميم قطع الاتصال لمنع أي برنامج—حتى البرامج التي تتمتع بامتيازات الجذر أو النواة في macOS، وحتى البرامج على شريحة T2 أو برنامج ثابت آخر—من إشراك الميكروفون عندما يكون الغطاء مغلقًا. (لا يتم قطع اتصال الكاميرا في المكونات المادية، لأن مجال الرؤية لديها محجوب تمامًا مع إغلاق الغطاء.)

تتميز طرز الـ iPad بدءًا من 2020 أيضًا بفصل مكون الميكروفون المادي. عند توصيل حافظة متوافقة مع MFi (مثل تلك التي تبيعها Apple) بـ iPad وإغلاقها، يتم فصل الميكروفون في المكونات المادية. وقد تم تصميم ذلك لمنع إتاحة بيانات صوت الميكروفون لأي برنامج، حتى مع امتيازات الجذر أو النواة في iPadOS أو أي برنامج ثابت للجهاز.

يتم تنفيذ وسائل الحماية في هذا القسم مباشرةً باستخدام منطق المكونات المادية، وفقًا لمخطط الدائرة التالي:



في كل منتج به فصل مادي للميكروفون، يكتشف مستشعر الغطاء الإغلاق المادي للغطاء أو العلبة باستخدام بعض الخصائص المادية (على سبيل المثال، مستشعر تأثير القاعة أو مستشعر زاوية المفصلة) للتفاعل. بالنسبة لأجهزة الاستشعار التي تكون المعايرة ضرورية فيها، يتم تعيين المعامِلات أثناء إنتاج الجهاز وتتضمن عملية المعايرة قفلاً ماديًا لا يمكن التراجع عنه نتيجة لأي تغييرات لاحقة على المعامِلات الحساسة على المستشعر. تصدر هذه المستشعرات إشارة مكونات مادية مباشرة تمر عبر مجموعة بسيطة من منطق المكونات المادية غير القابلة لإعادة البرمجة. يوفر هذا المنطق تنبيهًا و/أو تباطؤًا و/أو تأخيرًا يصل إلى 500 مللي ثانية قبل تعطيل الميكروفون. وحسب طراز المنتج، يمكن تنفيذ هذه الإشارة إما عن طريق تعطيل الخطوط التي تنقل البيانات بين الميكروفون والنظام على الشريحة (SoC) أو عن طريق تعطيل أحد خطوط الإدخال إلى وحدة الميكروفون التي تتيح لها أن تكون نشطة، على سبيل المثال، خط الساعة أو أداة تحكم فعالة مماثلة.

البطاقات السريعة في نمط توفير الطاقة

إذا لم يتم تشغيل iOS لأن الـ iPhone يحتاج إلى الشحن، فربما لا تزال هناك طاقة كافية في البطارية لدعم معاملات البطاقة السريعة. أجهزة الـ iPhone المدعومة تدعم هذه الميزة تلقائيًا مع:

- بطاقات الدفع أو المواصلات المصممة كبطاقات ترانزيت سريع
- بطاقات الوصول التي تم تشغيل النمط السريع عليها

عند الضغط على الزر الجانبي، تظهر أيقونة البطارية أن الطاقة منخفضة، ويشير النص إلى أن البطاقات السريعة متوفرة للاستخدام. تنفّذ وحدة تحكم في الاتصال قريب المدى معاملات البطاقة السريعة في ظل نفس الظروف التي يتم فيها تشغيل iOS، باستثناء أنه يتم الإشارة إلى المعاملات بإشعار حسي فقط (لا يتم عرض إشعار مرئي). على iPhone SE الجيل الثاني، قد تستغرق المعاملات المكتملة بضع ثوانٍ لتظهر على الشاشة. لا تتوفر هذه الميزة عند تنفيذ إيقاف تشغيل مبدوء من مستخدم قياسي.

أمن الأنظمة

نظرة عامة على أمن الأنظمة

بناءً على الإمكانات الفريدة للمكونات المادية في Apple، يكون أمن الأنظمة مسؤولاً عن التحكم في الوصول إلى موارد النظام في أجهزة Apple دون المساس بسهولة الاستخدام. ويشمل أمن الأنظمة عملية التمهيد وتحديثات البرامج وحماية موارد نظام الكمبيوتر مثل وحدة المعالجة المركزية والذاكرة والقرص والبرامج والبيانات المخزنة.

الإصدارات الأحدث من أنظمة تشغيل Apple هي الأكثر أمنًا. يعد **التمهيد الآمن** جزءًا مهمًا من أمن Apple، والذي يحمي النظام من الإصابة بالبرامج الضارة في وقت التمهيد. يبدأ الإقلاع الآمن في الرقاقات وينشئ سلسلة ثقة من خلال البرامج، حيث تم تصميم كل خطوة لضمان عمل الخطوة التالية بشكل صحيح قبل تسليم التحكم. لا يدعم نموذج الأمن هذا التمهيد الافتراضي لأجهزة Apple فحسب، بل يدعم أيضًا الأنماط المختلفة للاستعادة والتحديثات في الوقت المناسب على أجهزة Apple. وتعمل المكونات الفرعية، مثل Secure Enclave، على تنفيذ عملية الإقلاع الآمن الخاصة بها للمساعدة على ضمان عدم إقلاع سوى التعليمات البرمجية التي تعرف Apple أنها جيدة. صمم نظام التحديث للمساعدة على منع هجمات الإرجاع إلى إصدار أقدم، بحيث لا يمكن إرجاع الأجهزة إلى إصدار أقدم من نظام التشغيل (والذي يعرف المهاجم كيفية اختراقه) كوسيلة لسرقة بيانات المستخدم.

تتضمن أيضًا أجهزة Apple وسائل حماية التمهيد ووقت التشغيل بحيث تحافظ على سلامتها أثناء التشغيل المستمر. توفر الرقاقات التي صمّمتها Apple على iPhone و iPad و Mac المزودة برقاقات Apple و Apple Watch و Apple TV و HomePod بنيةً عامةً لحماية سلامة أنظمة التشغيل. ويضم macOS أيضًا مجموعة موسعة وقابلة للتكوين من إمكانيات الحماية لدعم نموذج الحوسبة المختلف الذي يتميز به، فضلًا عن الإمكانيات المدعومة على جميع الأنظمة الأساسية لمكونات Mac المادية.

التمهيد الآمن

عملية التمهيد على أجهزة iPhone و iPad

تحتوي كل خطوة من خطوات عملية بدء التشغيل على مكونات موقّعة بطريقة مشفرة من قِبل Apple لتمكين فحص التكامل بحيث لا يتابع التمهيد عمله إلا بعد التحقق من سلسلة الثقة. تتضمن هذه المكونات مُحمّلات الإقلاع و Kernel وملحقات Kernel والبرامج الثابتة للنطاق الأساسي الخلوي. وقد صُمّمت سلسلة التمهيد الآمن هذه لضمان عدم العبث بأدنى مستويات البرامج.

عند تشغيل جهاز iPhone و iPad، يقوم معالج التطبيق الخاص به على الفور بتنفيذ التعليمات البرمجية من ذاكرة للقراءة فقط يُشار إليها باسم Boot ROM. يتم وضع هذه التعليمات البرمجية الثابتة، المعروفة باسم **جذر الثقة** في المكونات المادية، أثناء تصنيع الشريحة وتتم الثقة بها ضمنيًا. تحتوي تعليمات Boot ROM البرمجية على المفتاح العام للجهة الموثقة Apple Root (CA) الذي يُستخدم للتحقق من أن مُحمّل الإقلاع iBoot موقع من قِبل Apple قبل السماح له بالتحميل. هذه هي الخطوة الأولى في سلسلة الثقة، حيث تتحقق كل خطوة من توقيع الخطوة التالية من قِبل Apple. عندما ينتهي iBoot من مهامه، يقوم بالتحقق من kernel في iOS أو iPadOS وتشغيله. بالنسبة إلى الأجهزة التي تتضمن معالج A9 أو إصدارًا أقدم من سلسلة A، يتم تحميل مرحلة إضافية من محمّل إقلاع المستوى الأدنى (LLB) ويتم التحقق منها بواسطة Boot ROM ويحمّل بدوره iBoot ويتحقق منه.

تتم معالجة الفشل في تحميل المراحل التالية أو التحقق منها بشكل مختلف حسب المكونات المادية:

- **لا يستطيع Boot ROM تحميل LLB (الأجهزة القديمة):** وضع ترقية البرنامج الثابت للجهاز (DFU)
- **LLB أو iBoot:** وضع الاسترداد

في كلتا الحالتين، يجب أن يكون الجهاز متصلاً بفايندر (في macOS 10.15 أو أحدث) أو iTunes (في macOS 10.14 أو أقدم) عبر USB وأن تتم استعادته إلى إعدادات المصنع الافتراضية.

يُستخدم سجل تقدّم التمهيد (BPR) بواسطة Secure Enclave لتقييد الوصول إلى بيانات المستخدم في أوضاع مختلفة ويتم تحديثه قبل الدخول في الأوضاع التالية:

- **وضع DFU:** يعيّن بواسطة Boot ROM على الأجهزة التي تحتوي على Apple A12 أو SoCs أحدث
- **وضع الاسترداد:** يعيّن بواسطة iBoot على الأجهزة التي تحتوي على A10 أو S2 أو SoCs أحدث

على الأجهزة ذات الوصول الخلوي، يقوم النظام الفرعي للنطاق الأساسي الخلوي بإجراء تمهيد آمن إضافي باستخدام البرامج والمفاتيح الموقعة التي تم التحقق منها بواسطة معالج النطاق الأساسي.

يُنفّذ Secure Enclave أيضًا عملية تمهيد آمنة تفحص برنامجها (sepOS) وتتأكد من صحته وتوقيعه بواسطة Apple.

تنفيذ iBoot الآمن للذاكرة

في iOS 14 و iPadOS 14 أو أحدث، قامت Apple بتعديل سلسلة أدوات برنامج C التحويلي المستخدمة لتصميم مُحمّل إقلاع iBoot لتحسين مستوى أمنه. تم تصميم سلسلة الأدوات المعدلة لتنفيذ التعليمات البرمجية لمنع مشكلات الذاكرة والأمان التي تحدث عادةً في برامج C. على سبيل المثال، فإنها تساعد في منع معظم الثغرات في الفئات التالية:

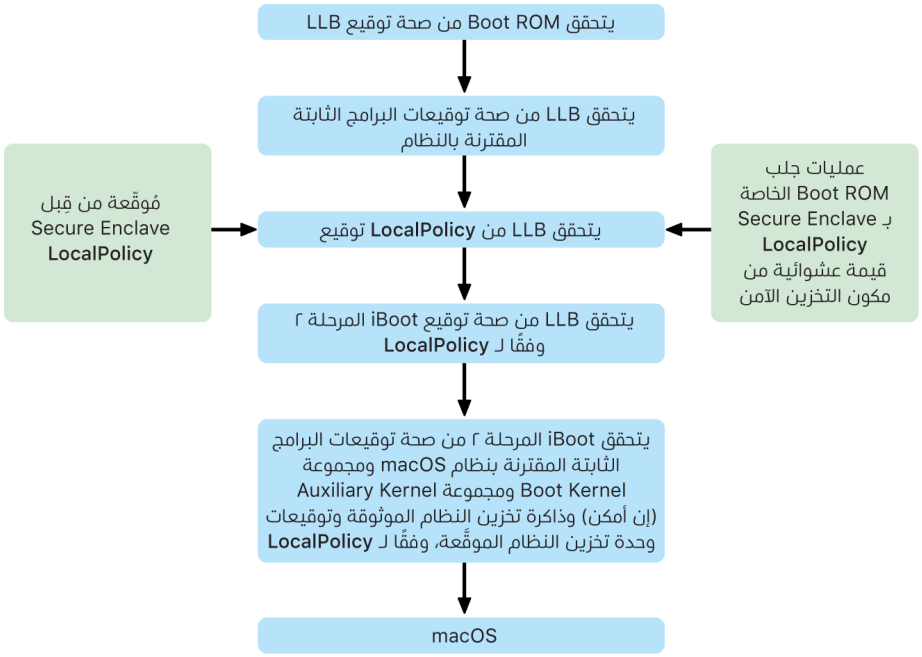
- تجاوز سعة المخزن المؤقت، وذلك من خلال التأكد من أن جميع المؤشرات تحمل معلومات الحدود التي يتم التحقق منها عند الوصول إلى الذاكرة
- استغلال كومة الذاكرة المؤقتة، عن طريق فصل بيانات كومة الذاكرة المؤقتة عن بيانات التعريف الخاصة بها والكشف الدقيق عن حالات الخطأ مثل التحرُّر المزدوج من الأخطاء
- الارتباك في تحديد النوع، من خلال التأكد من أن جميع المؤشرات تحمل معلومات نوع وقت التشغيل التي يتم التحقق منها أثناء عمليات توجيه المؤشر
- الارتباك في تحديد النوع الناتج عن أخطاء الاستخدام بعد التحرّر، وذلك عن طريق فصل كل تخصيصات الذاكرة الديناميكية حسب النوع الثابت.

هذه التقنية متوفرة على iPhone المزود بشريحة بايونك A13 أو أحدث، و iPad المزود بشريحة بايونك A14 أو أحدث.

أجهزة كمبيوتر Mac المزودة بسيليكون Apple

عملية التمهيد في أجهزة كمبيوتر Mac المزودة بسيليكون Apple

عند تشغيل كمبيوتر Mac مزود بسيليكون Apple، يقوم بعملية تمهيد مشابهة كثيرًا لعملية تمهيد الـ iPhone والـ iPad.



تعمل الشريحة على تنفيذ التعليمات البرمجية من Boot ROM في الخطوة الأولى في سلسلة الثقة. ويعمل التمهيد الآمن في macOS على Mac مزود بسيليكون Apple على التحقق من التعليمات البرمجية لنظام التشغيل نفسه، وكذلك سياسات الأمن وحتى عناصر kexts (المدعومة، لكن غير موصى بها) التي يقوم المستخدمون المصرح لهم بتكوينها.

عند تشغيل LLB (محمّل إقلاع المستوى الأدنى)، فإنه يتحقق من صحة التوقيعات ويحمّل البرامج الثابتة المقترنة بالنظام لمحاور intra-SoC، مثل وحدة التخزين وشاشة العرض وإدارة النظام ووحدات تحكم ثندربولت. ويتحمل LLB أيضًا مسؤولية تحميل LocalPolicy، وهو ملف موقع بواسطة معالج Secure Enclave. يصف ملف LocalPolicy التكوين الذي اختاره المستخدم لسياسات أمن تمهيد النظام ووقت التشغيل. تتمتع LocalPolicy بنفس تنسيق بنية البيانات الذي تتمتع به جميع كائنات التمهيد الأخرى، ولكن يتم توقيعها محليًا بواسطة مفتاح خاص يتوفر فقط داخل Secure Enclave الخاص بجهاز كمبيوتر معين، بدلاً من توقيعها بواسطة خادم Apple مركزي (مثل تحديثات البرامج).

للمساعدة على منع إعادة تشغيل أي LocalPolicy سابقة، يجب أن يبحث محمّل إقلاع المستوى الأدنى (LLB) عن قيمة غير قابلة لإعادة التشغيل من مكون التخزين الآمن المرتبط بـ Secure Enclave. للقيام بذلك، يستخدم Boot ROM في Secure Enclave ويتأكد من أن القيمة غير القابلة لإعادة التشغيل في LocalPolicy تطابق القيمة غير القابلة لإعادة التشغيل في مكون التخزين الآمن. ويساعد هذا الإجراء على منع إعادة تطبيق LocalPolicy قديمة—كان من الممكن تكوينها لتوفير مستوى أمني أقل—على النظام بعد ترقية المستوى الأمني. والنتيجة هي أن التمهيد الآمن على Mac مزود بسيليكون Apple يساعد على الحماية من التراجع إلى إصدارات نظام التشغيل الأقدم، وكذلك الحماية ضد خفض سياسات الأمان.

تكتشف LocalPolicy ما إذا كان نظام التشغيل قد تم تكوينه لتوفير التأمين الكامل أو المنخفض أو الأقل تقييدًا.

- **التأمين الكامل:** يتصرف النظام مثل iOS و iPadOS، ويسمح فقط ببرنامج التمهيد الذي كان معروفًا أنه الأحدث في وقت التثبيت.
- **التأمين المنخفض:** يتم توجيه LLB إلى الثقة في التوقيعات "العالمية" المرفقة مع نظام التشغيل. ويسمح ذلك للنظام بتشغيل إصدارات أقدم من macOS. نظرًا لأن الإصدارات الأقدم من macOS تحتوي حتمًا على ثغرات أمنية لم يتم إصلاحها، يتم وصف وضع الأمن هذا على أنه **منخفض**. وهذا هو أيضًا مستوى السياسة المطلوب لدعم تمهيد ملحقات kernel (kexts).
- **التأمين الأقل تقييدًا:** يتصرف النظام مثل سلوك التأمين المنخفض من حيث أنه يستخدم التحقق من التوقيعات العالمية لـ iBoot وما بعده، ولكنه يخبر iBoot أيضًا بأنه يجب عليه قبول بعض كائنات التمهيد التي يتم توقيعها بواسطة Secure Enclave بنفس المفتاح المستخدم لتوقيع LocalPolicy. يدعم مستوى السياسة هذا المستخدمين في إنشاء ملحقات XNU kernels المخصصة الخاصة بهم وتوقيعها وتمهيدها.

إذا أشارت LocalPolicy إلى LLB بأن نظام التشغيل المحدد يعمل في التأمين الكامل، يقوم LLB بتقييم التوقيع المخصص لـ iBoot. إذا كان يعمل في التأمين المنخفض أو التأمين الأقل تقييدًا، فإنه يقيّم التوقيع العام. تؤدي أي أخطاء في التحقق من التوقيع إلى قيام النظام بالتمهيد إلى recoveryOS لتوفير خيارات الإصلاح.

بعد تسليم LLB إلى iBoot، يقوم بتحميل البرامج الثابتة المقترنة بـ macOS مثل تلك الخاصة بالمحرك العصبي الآمن والمعالج دائم التشغيل والبرامج الثابتة الأخرى. ويبحث iBoot أيضًا عن معلومات حول LocalPolicy التي تم تسليمها إليه من LLB. إذا كانت LocalPolicy تشير إلى أنه يجب أن يكون هناك مجموعة Kernel مساعدة (AuxKC)، فإن iBoot يبحث عنه في نظام الملفات، ويتحقق من توقيعه بواسطة Secure Enclave بنفس المفتاح الموجود في LocalPolicy ويتحقق من تطابق التجزئة الخاص به مع التجزئة المخزنة في LocalPolicy. إذا تم التحقق من AuxKC، فسيضعه iBoot في الذاكرة مع مجموعة Boot Kernel، قبل تأمين منطقة الذاكرة الكاملة التي تغطي مجموعة Boot Kernel و AuxKC باستخدام حماية تكامل المعالج الثانوي للنظام (CTRR). إذا أشارت السياسة إلى وجوب وجود AuxKC في حين أنها غير موجودة، فسيستمر النظام في التمهيد إلى macOS بدونها. كما أن iBoot مسؤول أيضًا عن التحقق من تجزئة الجذر الخاصة بوحدة تخزين النظام الموقَّعة (SSV)، للتحقق من أن نظام الملفات الذي سيقوم kernel بتحميله قد تم التحقق من سلامته بالكامل.

أنماط التمهيد في أجهزة كمبيوتر Mac المزودة بسيليكون Apple

تحتوي أجهزة كمبيوتر Mac المزودة بسيليكون Apple على أنماط التمهيد الموضحة أدناه.

الوضع	مجموعة المفاتيح	الوصف
macOS	من حالة إيقاف التشغيل، اضغط على زر الطاقة و**اتركه**.	1. يُسلّم Boot ROM إلى LLB. 2. يقوم LLB بتحميل البرامج الثابتة المقترنة بالنظام وسياسة Local Policy لنظام macOS المحدد. 3. يقوم LLB بتأمين إشارة في سجل تقدّم التمهيد (BPR) بأنه يقوم بالتمهيد إلى macOS، ثم يُسلّم إلى iBoot. 4. يقوم iBoot بتحميل البرامج الثابتة المقترنة بـ macOS وذاكرة التخزين المؤقت الموثوق بها وشجرة الجهاز ومجموعة Boot Kernel. 5. إذا سمحت LocalPolicy بذلك، يقوم iBoot بتحميل مجموعة Kernel المساعدة (AuxKC) من kexts التابعة لجهات خارجية. 6. إذا لم تقم LocalPolicy بتعطيله، يتحقق iBoot من تجزئة توقيع الجذر لوحدة تخزين النظام الموقَّعة (SSV).
recoveryOS المقترن	من حالة إيقاف التشغيل، اضغط **مطولاً** على زر الطاقة.	1. يُسلّم Boot ROM إلى LLB. 2. يقوم LLB بتحميل البرامج الثابتة المقترنة بالنظام وسياسة Local Policy لـ recoveryOS. 3. يقوم LLB بتأمين إشارة في سجل تقدّم التمهيد بأنه يقوم بالتمهيد إلى recoveryOS المقترن، ثم يُسلّم إلى iBoot لـ recoveryOS المقترن. 4. يقوم iBoot بتحميل البرامج الثابتة المقترنة بـ macOS وذاكرة التخزين المؤقت الموثوق بها وشجرة الجهاز ومجموعة Boot Kernel. 5. إذا فشل تمهيد recoveryOS المقترن، تتم محاولة التمهيد في recoveryOS الاحتياطي.

الوضع	مجموعة المفاتيح	الوصف
recoveryOS الاحتياطي	من حالة إيقاف التشغيل، **اضغط مرتين مطولاً** على زر الطاقة.	1. يُسلّم Boot ROM إلى LLB. 2. يقوم LLB بتحميل البرامج الثابتة المقترنة بالنظام وسياسة Local Policy لـ recoveryOS. 3. يقوم LLB بتأمين إشارة في سجل تقدّم التمهيد بأنه يقوم بالتمهيد إلى recoveryOS المقترن، ثم يُسلّم إلى iBoot لـ recoveryOS. 4. يقوم iBoot بتحميل البرامج الثابتة المقترنة بـ macOS وذاكرة التخزين المؤقت الموثوق بها وشجرة الجهاز ومجموعة Boot Kernel.
النمط الآمن	قم بالتمهيد إلى نظام recoveryOS كما هو مذكور أعلاه، ثم اضغط مطولاً على **مفتاح العالي** أثناء تحديد وحدة تخزين بدء التشغيل.	1. يتم التمهيد إلى recoveryOS كما ورد أعلاه. 2. يؤدي الضغط على مفتاح العالي أثناء تحديد وحدة تخزين إلى قيام تطبيق BootPicker باعتماد macOS هذا للتشغيل، كالمعتاد؛ كما يقوم بتعيين متغير `nvram` يخبر iBoot بعدم تحميل AuxKC في التمهيد التالي. 3. يقوم النظام بإعادة التشغيل والإقلاع إلى وحدة التخزين المستهدفة، لكن لا يقوم iBoot بتحميل AuxKC.

قيود recoveryOS المقترن

على الـ macOS 12.0.1 أو الأحدث، يقوم كل تثبيت جديد على macOS بتثبيت إصدار recoveryOS مقترن بمجموعة وحدات التخزين APFS المطابقة. يُعد هذا التصميم مألوفًا لمستخدمي أجهزة كمبيوتر Mac المستندة إلى Intel، لكن على الـ Mac المزود برقاقات Apple، فإنه يوفر ضمانات أمن وتوافق إضافية. ونظرًا إلى أن كل تثبيت على macOS يحتوي الآن على recoveryOS مقترن ومخصص، فإن هذا يساعد على ضمان عدم إمكانية تنفيذ عمليات خفض مستوى الأمن إلا من خلال recoveryOS المقترن المخصص. وهذا بدوره يساعد على حماية عمليات تثبيت الإصدارات الأحدث من macOS من العبث الذي يتم بدؤه من الإصدارات الأقدم من macOS والعكس صحيح.

يتم فرض قيود الاقتران على النحو الآتي:

- يتم إقران جميع عمليات تثبيت macOS 11 بـ recoveryOS. إذا تم تحديد تثبيت macOS 11 للتمهيد افتراضيًا، فسيتم تمهيد recoveryOS بالضغط باستمرار على مفتاح التشغيل في وقت التمهيد على الـ Mac المزود برقاقات Apple. يمكن لـ recoveryOS خفض مستوى إعدادات الأمن لأي عمليات تثبيت على macOS 11، ولكن ليس لأي عمليات تثبيت على macOS 12.0.1.
- إذا تم تحديد تثبيت macOS 12.0.1 أو أحدث للتمهيد افتراضيًا، فسيتم تمهيد recoveryOS المقترن بالضغط باستمرار على مفتاح التشغيل في وقت تشغيل Mac. يمكن لـ recoveryOS المقترن خفض مستوى إعدادات الأمن لعملية التثبيت على macOS المقترن، ولكن ليس لأي عملية تثبيت على macOS آخر.

للإقلاع إلى recoveryOS المقترن لأي عملية تثبيت على macOS، يجب تحديد هذا التثبيت كإعداد افتراضي، ويتم ذلك باستخدام عام > قرص بدء التشغيل في إعدادات النظام (macOS 13 أو أحدث) أو قرص بدء التشغيل في تفضيلات النظام (macOS 12 أو أقدم) أو عن طريق بدء أي recoveryOS مع الضغط باستمرار على الخيار في أثناء تحديد وحدة تخزين.

ملاحظة: لا يستطيع recoveryOS الاحتياطي خفض مستوى أي عمليات تثبيت على الـ macOS.

تتحكم سياسة أمن قرص بدء التشغيل في أجهزة كمبيوتر Mac المزودة بسيليكون Apple

نظرة عامة

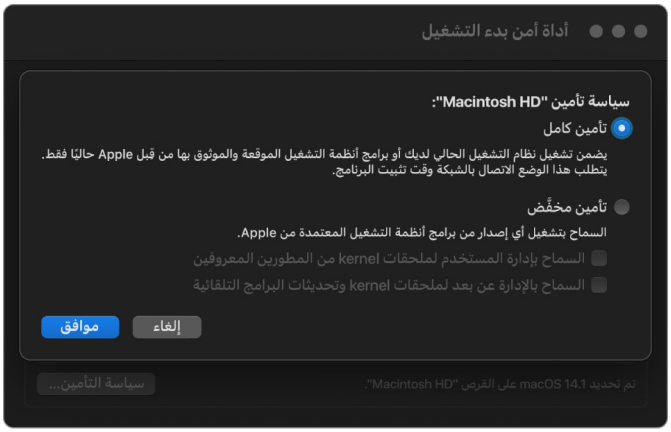
على عكس سياسات الأمن على أجهزة كمبيوتر Mac المستندة إلى Intel، فإن سياسات الأمن على أجهزة كمبيوتر Mac المزودة بسيليكون Apple تناسب كل نظام تشغيل مثبت. وهذا يعني أن العديد من مثيلات macOS المثبتة التي لها إصدارات وسياسات أمن مختلفة تكون مدعومة على Mac ذاته. ولهذا السبب، تمت إضافة **منتقي نظام التشغيل** إلى أداة أمن بدء التشغيل.

في أجهزة كمبيوتر Mac المزودة بسيليكون Apple، تشير أداة أمن النظام إلى حالة الأمن الكلية التي تم تكوينها بواسطة المستخدم لنظام macOS مثل تمهيد kext أو تكوين حماية تكامل النظام (SIP). إذا كان تغيير إعدادات الأمن سيؤدي إلى تدهور الحالة الأمنية بشكل كبير أو تسهيل اختراق النظام، يجب على المستخدم الدخول إلى وضع recoveryOS من خلال الضغط مطولاً على زر الطاقة (حتى لا تتمكن البرامج الضارة من تشغيل الإشارة، بحيث تقتصر إمكانية تنفيذ ذلك على التدخل البشري المادي فقط)، لإجراء التغيير. ولهذا السبب، فإن أي Mac مزود بسيليكون Apple لن يشترط (أو يدعم) وجود كلمة سر خاصة بالبرنامج الثابت أيضًا، فكل التغييرات المهمة يتم تمريرها بالفعل من خلال تفويض المستخدم. لمزيد من المعلومات حول SIP، انظر حماية تكامل النظام.

يمكن تعيين التأمين الكامل والتأمين المنخفض باستخدام أداة أمن بدء التشغيل من recoveryOS. ولكن التأمين الأقل تقييدًا لا يمكن الوصول إليه إلا من خلال أدوات سطر الأوامر للمستخدمين الذين يقبلون مخاطر جعل الـ Mac الخاص بهم أقل تأمينًا.

سياسة التأمين الكامل

"تأمين كامل" هو الإعداد الافتراضي، ويتصرف مثل iOS و iPadOS. في الوقت الذي يتم فيه تنزيل البرنامج وإعداده للتثبيت، بدلاً من استخدام التوقيع العام الذي يتوفر مع البرنامج، يتواصل macOS مع نفس خادم توقيع Apple المستخدم في iOS و iPadOS ويطلب توقيعًا جديدًا "بطابع شخصي". يتم تخصيص توقيع عندما يتضمن معرف الشريحة الحصري (ECID) -وهو معرف فريد خاص بوحدة المعالجة المركزية من Apple في هذه الحالة- كجزء من طلب التوقيع. ويكون التوقيع الذي يرجع من خادم التوقيع فريدًا وقابلاً للاستخدام فقط بواسطة وحدة المعالجة المركزية من Apple المعينة هذه. عندما تكون سياسة التأمين الكامل سارية المفعول، يضمن Boot ROM و LLB أن لا يكون التوقيع المحدد موقعًا من قِبل Apple فحسب، بل تم توقيعه لهذا الـ Mac بالتحديد، ويربط هذا الإصدار من macOS بشكل أساسي مع ذلك الـ Mac.

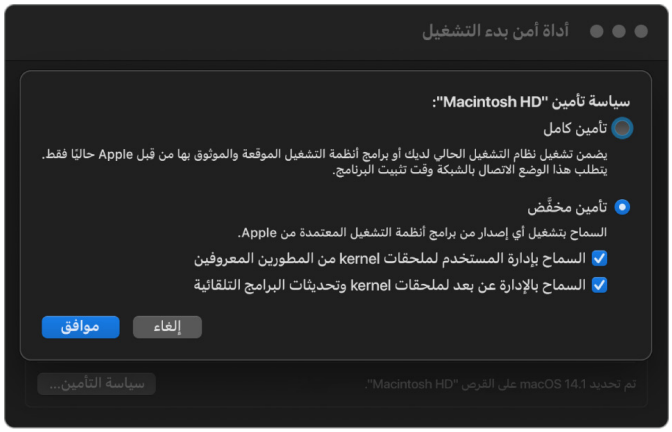


يوفر استخدام خادم توقيع على الإنترنت أيضًا حماية أفضل ضد هجمات التراجع مقارنةً بأساليب التوقيع العام النموذجية. في نظام التوقيع العام، كان من الممكن أن تتعرض الحقبة الأمنية للتراجع عدة مرات، لكن أي نظام لم يشهد أحدث البرامج الثابتة أبدًا لن يعرف ذلك. على سبيل المثال، الكمبيوتر الذي يعتقد حاليًا أنه موجود في الحقبة الأمنية 1 يقبل البرامج من الحقبة الأمنية 2، حتى إذا كانت الحقبة الأمنية الفعلية الحالية هي 5. باستخدام نظام التوقيع عبر الإنترنت من سيليكون Apple، يمكن لخادم التوقيع رفض إنشاء توقيعات إلا للبرامج الموجودة في أحدث حقبة أمنية.

بالإضافة إلى ذلك، إذا اكتشف أحد المهاجمين ثغرة أمنية بعد تغيير الحقبة الأمنية، فلن يتمكن ببساطة من انتقاء البرامج العُرضة للتهديدات من حقبة سابقة من النظام أ وتطبيقها على النظام ب لمهاجمته. حقيقة أن البرامج العرضة للتهديدات من حقبة قديمة قد تم تخصيصها للنظام أ يمنعها من أن تكون قابلة للنقل وبالتالي يمنع استخدامها لمهاجمة النظام ب. تعمل كل هذه الآليات معًا لتوفير ضمانات أقوى بكثير تمنع المهاجمين من وضع البرامج العرضة للتهديدات عن قصد على Mac للتحايل على وسائل الحماية التي توفرها أحدث البرامج. ولكن المستخدم الذي يمتلك اسم مستخدم وكلمة سر كمسؤول للـ Mac يظل بإمكانه دائمًا اختيار سياسة الأمن التي تناسب حالات الاستخدام الخاصة به.

سياسة التأمين المنخفض

يشبه سلوك التأمين المنخفض سلوك التأمين المتوسط على أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة T2، حيث يقوم فيها البائع (في هذه الحالة، Apple) بإنشاء توقيع رقمي للتعليمة البرمجية لتأكيد صدورها من البائع. يساعد هذا التصميم على منع المهاجمين من إدخال تعليمات برمجية غير موقعة. تشير Apple إلى هذا التوقيع على أنه توقيع "عام"، لأنه يمكن استخدامه على أي Mac، لأي فترة زمنية، لأجهزة كمبيوتر Mac التي تم تعيين سياسة التأمين المنخفض بها حاليًا. لا يوفر التأمين المنخفض في حد ذاته الحماية من هجمات التراجع على الرغم من أن التغييرات غير المصرح بها في نظام التشغيل قد تؤدي إلى جعل الوصول إلى بيانات المستخدم غير ممكن. لمزيد من المعلومات، انظر ملحقات Kernel في أجهزة كمبيوتر Mac المزودة بسيليكون Apple.



بالإضافة إلى تمكين المستخدمين من تشغيل إصدارات أقدم من macOS، فإن التأمين المنخفض مطلوب للإجراءات الأخرى التي يمكنها تعريض أمن نظام المستخدم للخطر، مثل تقديم ملحقات kernel التابعة لجهات خارجية (kexts). تتمتع Kexts بنفس الامتيازات التي تتمتع بها kernel، وبالتالي فإن أي ثغرات أمنية في kexts التابعة لجهات خارجية يمكن أن تؤدي إلى اختراق نظام التشغيل بالكامل. وهذا هو السبب في تشجيع المطورين بشدة على اعتماد ملحقات النظام، قبل إزالة دعم kext من macOS لأجهزة كمبيوتر Mac المستقبلية المزودة بسيليكون Apple. حتى عند تمكين kexts التابعة لجهات الخارجية، فلا يمكن تحميلها في kernel عند الطلب. بدلاً من ذلك، يتم دمج kexts في مجموعة Kernel المساعدة (AuxKC) التي يتم تخزين علامة تجزئتها في LocalPolicy، ومن ثَم يتطلب ذلك إعادة تشغيل. لمزيد من المعلومات حول إنشاء AuxKC، انظر توسيع ملحق kernel بشكل آمن في macOS.

سياسة التأمين الأقل تقييدًا

التأمين الأقل تقييدًا مخصص للمستخدمين الذين يقبلون المجازفة بتعريض الـ Mac لحالة أمنية دون المستوى المفترض. ويختلف هذا النمط عن نمط "بلا تأمين" على أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة T2. باستخدام التأمين الأقل تقييدًا، لا يزال التحقق من التوقيع يتم على طول سلسلة التمهيد الآمن بالكامل، ولكن يتم تعيين السياسة على إشارات أقل تقييدًا إلى iBoot بأنه يجب أن يقبل كائنات التمهيد الموقعة محليًا من قِبل Secure Enclave، مثل ذاكرة التخزين المؤقت لملحقات مجموعة Boot Kernel التي يُنشئها المستخدم ويتم تصميمها من مصدر ملحق XNU kernel مخصص. بهذه الطريقة، يوفر "التأمين الأقل تقييدًا" أيضًا قدرة معمارية لتشغيل kernel عشوائي "غير موثوق به مطلقًا على نظام التشغيل". عند تحميل مجموعة Boot Kernel مخصصة أو نظام تشغيل غير موثوق به بالكامل على النظام، تصبح بعض مفاتيح فك التشفير غير متاحة. وقد تم تصميم ذلك لمنع أنظمة التشغيل غير الموثوق بها تمامًا من الوصول إلى البيانات من أنظمة التشغيل الموثوق بها.

هام: لا توفر Apple ملحقات XNU المخصصة أو تدعمها.

هناك طريقة أخرى تختلف بها سياسة "التأمين الأقل تقييدًا" عن سياسية "بلا تأمين" على أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة T2: لقد صارت شرطًا أساسيًا لبعض التراجعات الأمنية التي كانت في الماضي يمكن السيطرة عليها بشكل مستقل. والجدير بالذكر أن تعطيل حماية تكامل النظام (SIP) على أجهزة كمبيوتر Mac المزودة بسيليكون Apple يتطلب من المستخدم الإقرار بأنه يضع النظام في نمط التأمين الأقل تقييدًا. ويكون ذلك مطلوبًا لأن تعطيل SIP يؤدي دائمًا إلى وضع النظام في حالة تجعل اختراق kernel أسهل بكثير. على وجه الخصوص، يؤدي تعطيل SIP على أجهزة كمبيوتر Mac المزودة بسيليكون Apple إلى تعطيل فرض توقيع kext أثناء وقت إنشاء AuxKC، مما يسمح بتحميل أي kext عشوائي في ذاكرة kernel. تم إجراء تحسين آخر على SIP على أجهزة كمبيوتر Mac المزودة بسيليكون Apple حيث تم نقل مخزن السياسات من NVRAM إلى LocalPolicy. ومن ثم فإن تعطيل SIP يتطلب مصادقةً من قِبل مستخدم لديه حق الوصول إلى مفتاح توقيع LocalPolicy، من recoveryOS (الذي يتم الوصول إليه عن طريق الضغط مطولاً على زر الطاقة). هذا يجعل الأمر أكثر صعوبة على مهاجم البرامج فقط، أو حتى المهاجم الموجود فعليًا، لتعطيل SIP.

ليس من الممكن إرجاع مستوى الأمن إلى التأمين الأقل تقييدًا من تطبيق أداة أمن بدء التشغيل. ولا يمكن للمستخدم خفض مستوى الأمن إلا من خلال تشغيل أدوات سطر الأوامر من الوحدة الطرفية في recoveryOS، مثل `csrutil` (لتعطيل SIP). بعد أن يقوم المستخدم بخفض مستوى الأمن، تنعكس حقيقة حدوث ذلك في أداة أمن بدء التشغيل، وبالتالي يمكن للمستخدم تعيين الأمان بسهولة إلى نمط أكثر أمنًا.

ملاحظة: جهاز Mac المزود بسيليكون Apple لا يتطلب أو يدعم سياسة معينة لتمهيد الوسائط لأن كل عمليات التمهيد يتم تنفيذها محليًا من الناحية الفنية. إذا اختار المستخدم الإقلاع من وسائط خارجية، فيجب أولاً تخصيص إصدار نظام التشغيل هذا باستخدام عملية إعادة تشغيل مُصادق عليها من recoveryOS. وتؤدي إعادة التشغيل هذه إلى إنشاء ملف LocalPolicy على محرك الأقراص الداخلي الذي يُستخدم لإجراء إقلاع موثوق به من نظام التشغيل المُخزَّن على الوسائط الخارجية. وهذا يعني أن تكوين بدء التشغيل من الوسائط الخارجية يتم تمكينه بشكل صريح دائمًا على أساس كل نظام تشغيل، ويتطلب بالفعل مصادقة المستخدم، لذا فلا يلزم وجود تكوين آمن إضافي.

إنشاء مفتاح توقيع LocalPolicy وإدارته

الإنشاء

عند تثبيت macOS لأول مرة في المصنع، أو عند إجراء تثبيت-محو مُقيّد، يقوم الـ Mac بتشغيل التعليمات البرمجية من قرص RAM للاستعادة المؤقتة لتهيئة الحالة الافتراضية. أثناء هذه العملية، تنشئ بيئة الاستعادة زوجًا جديدًا من المفاتيح العامة والخاصة يتم الاحتفاظ بها في Secure Enclave. ويُشار إلى المفتاح الخاص باسم **مفتاح هوية المالك (OIK)**. في حالة وجود أي OIK بالفعل، يتم إتلافه كجزء من هذه العملية. تعمل بيئة الاستعادة أيضًا على تهيئة المفتاح المستخدم لقفل التنشيط؛ **مفتاح هوية المستخدم (UIK)**. يوجد جزء من هذه العملية يكون فريدًا لأجهزة كمبيوتر Mac المزودة بسيليكون Apple، وهو أنه عندما تُطلب شهادة UIK لقفل التنشيط، يتم تضمين مجموعة من القيود المطلوبة التي سيتم فرضها في وقت التحقق في LocalPolicy. وإذا لم يتمكن الجهاز من الحصول على UIK مُعتمدة لقفل التنشيط (على سبيل المثال، نظرًا لأن الجهاز مرتبط حاليًا بحساب "العثور على الـ Mac" وتم الإبلاغ عن فقدانه)، فلن يتمكن من المضي قدمًا لإنشاء سياسة محلية. إذا تم إصدار **شهادة هوية مستخدم (ucrt)** لجهاز ما، فإن هذه الشهادة تحتوي على قيود السياسة المفروضة على الخادم وقيود السياسة التي يطلبها المستخدم بامتداد X.509 v3.

عندما يتم استرداد قفل تنشيط`ucrt`/ بنجاح، يتم تخزينه في قاعدة بيانات على جانب الخادم وإعادته كذلك إلى الجهاز. وبعد أن يحتوي الجهاز على ucrt، يتم إرسال طلب شهادة للمفتاح العام الذي يتوافق مع OIK إلى خادم **مرجع التوثيق الأساسي (BAA)**. ويتحقق BAA من طلب شهادة OIK باستخدام المفتاح العام من شهادة ucrt المخزنة في قاعدة بيانات BAA التي يمكن الوصول إليها. إذا تمكّن BAA من التحقق من الشهادة، فإنه يصادق على المفتاح العام، ويُعيد **شهادة هوية المالك (OIC)** الموقَّعة من قِبل BAA وتحتوي على القيود المخزنة في ucrt. ويتم إرسال OIC مرة أخرى إلى Secure Enclave. منذ ذلك الحين، كلما وقّع Secure Enclave على LocalPolicy جديدة، فإنه يربط OIC بـ Image4. تحتوي LLB على ثقة مضمنة في شهادة BAA الجذرية، مما يجعلها تثق في OIC، مما يجعلها تثق في توقيع LocalPolicy العام.

قيود RemotePolicy

تحتوي جميع ملفات Image4، وليست السياسات المحلية فقط، على قيود على تقييم ملف بيانات Image4. وهذه القيود يتم ترميزها باستخدام معرفات كائنات خاصة (OID) في شهادة الطرف. تبحث مكتبة التحقق من Image4 عن OID الخاص بقيد الشهادة الخاصة من شهادة أثناء تقييم التوقيع، ومن ثم تعمل على تقييم القيود المحددة فيه آليًا. وتكون القيود على الأشكال التالية:

- يجب وجود X
- يجب عدم وجود X
- يجب أن يحتوي X قيمة معينة

لذلك، على سبيل المثال، بالنسبة للتوقيعات "الشخصية"، ستحتوي قيود الشهادة على القيد "يجب وجود ECID"؛ وبالنسبة للتوقيعات "العامة"، ستحتوي على القيد "يجب عدم وجود ECID". تم تصميم هذه القيود لتضمن أن تكون جميع ملفات Image4 المُوقّعة بواسطة مفتاح معين متوافقة مع متطلبات معينة لتجنب إنشاء ملف بيانات Image4 مُوقّع بشكل خاطئ.

في سياق كل LocalPolicy، يُشار إلى قيود شهادة Image4 هذه باسم **RemotePolicy**. يمكن أن توجد RemotePolicy مختلفة لسياسات LocalPolicies في بيئات التمهيد المختلفة. وتُستخدم RemotePolicy لتقييد LocalPolicy على recoveryOS بحيث عند تمهيد recoveryOS يمكن أن تتصرف فقط كما لو كانت تقوم بالتمهيد وفقًا لسياسة التأمين الكامل. ويؤدي ذلك إلى زيادة الثقة في سلامة بيئة تمهيد recoveryOS كمكان يمكن تغيير السياسة منه. تقوم RemotePolicy بتقييد LocalPolicy لاحتواء ECID الخاص بـ Mac الذي تم إنشاء LocalPolicy عليه، والتجزئة العشوائية للسياسة البعيدة (`rpnh`) المحددة المخزنة في مكون التخزين الآمن على هذا الـ Mac. يتغير `rpnh`، وبالتالي RemotePolicy، فقط عند اتخاذ إجراءات لميزة العثور على الـ Mac وقفل التنشيط، مثل التسجيل وإلغاء التسجيل والقفل عن بُعد والمسح عن بُعد. يتم تحديد قيود السياسة البعيدة وتخصيصها في وقت اعتماد شهادة مفتاح هوية المستخدم (UIK) ويتم تسجيلها في شهادة هوية المستخدم الصادرة (ucrt). ويتم تحديد بعض قيود السياسة البعيدة، مثل ECID و ChipID و BoardID، بواسطة الخادم. وقد تم تصميم ذلك لمنع جهاز واحد من توقيع ملفات LocalPolicy لجهاز آخر. قد يتم تحديد قيود السياسة البعيدة الأخرى بواسطة الجهاز لمنع خفض المستوى الأمني للسياسة المحلية دون توفير كل من المصادقة المحلية المطلوبة للوصول إلى OIK الحالي والمصادقة عن بُعد للحساب الذي تم قفل تنشيط الجهاز له.

محتويات ملف LocalPolicy لأجهزة كمبيوتر Mac المزودة بسيليكون Apple

LocalPolicy هو ملف Image4 موقّع بواسطة Secure Enclave. بينما Image4 عبارة عن تنسيق بنية بيانات مُشفّر بواسطة DER (Abstract Syntax Notation One) ASN.1 يُستخدم لوصف معلومات حول كائنات سلسلة التمهيد الآمن على أنظمة Apple الأساسية. في نموذج التمهيد الآمن المستند إلى Image4، يتم طلب سياسات الأمن في وقت تثبيت البرنامج الذي يتم بدؤه بواسطة طلب توقيع إلى خادم توقيع Apple مركزي. إذا كانت السياسة مقبولة، يقوم خادم التوقيع بإرجاع ملف Image4 مُوقَّع يحتوي على مجموعة متنوعة من تسلسلات الرموز المكونة من أربعة أحرف (4CC). ويتم تقييم ملفات Image4 المُوقَّعة ورموز 4CCs هذه في وقت التمهيد بواسطة برنامج مثل Boot ROM أو LLB.

تسليم الملكية بين أنظمة التشغيل

يُشار إلى الوصول إلى مفتاح هوية المالك (OIK) باسم "الملكية". وتكون الملكية مطلوبة للسماح للمستخدمين بإعادة توقيع LocalPolicy بعد إجراء تغييرات في السياسة أو البرنامج. وتتم حماية OIK بنفس التسلسل الهرمي للمفاتيح كما هو موضح في حماية المفاتيح المؤمنة (SKP)، مع حماية OIK بنفس مفتاح تشفير المفاتيح (KEK) المستخدم في مفتاح تشفير وحدة التخزين (VEK). وهذا يعني أنه عادةً ما يكون محميًا بكلمات سر المستخدم وقياسات نظام التشغيل والسياسة. يوجد OIK واحد فقط لجميع أنظمة التشغيل على الـ Mac. لذلك، عند تثبيت نظام تشغيل ثانٍ، يلزم الحصول على موافقة صريحة من المستخدمين على نظام التشغيل الأول لتسليم الملكية إلى المستخدمين في نظام التشغيل الثاني. ومع ذلك، فإن المستخدمين غير موجودين حتى الآن لنظام التشغيل الثاني، عند تشغيل المُثبت من نظام التشغيل الأول. ولا يتم إنشاء المستخدمين في أنظمة التشغيل بشكل طبيعي حتى يتم تمهيد نظام التشغيل وتشغيل مساعد الإعداد. وبالتالي، يلزم اتخاذ إجراءين جديدين عند تثبيت نظام تشغيل ثانٍ على Mac مزود بسيليكون Apple:

- إنشاء LocalPolicy لنظام التشغيل الثاني
- تحضير "مستخدم تثبيت" لتسليم الملكية

عند تشغيل مساعد التثبيت والتثبيت المستهدف لوحدة تخزين فارغة ثانوية، تظهر مطالبة لسؤال المستخدم عمّا إذا كان يرغب في نسخ مستخدم من وحدة التخزين الحالية ليكون المستخدم الأول لوحدة التخزين الثانية أم لا. إذا وافق المستخدم، فإن "مستخدم التثبيت" الذي يتم إنشاؤه يكون، في الواقع، KEK مشتق من كلمة سر المستخدم المحدد ومفاتيح المكونات المادية، والذي يُستخدم بعد ذلك لتشفير OIK عند تسليمه إلى نظام التشغيل الثاني. ثم من داخل مساعد تثبيت نظام التشغيل الثاني، يطلب كلمة سر هذا المستخدم للسماح له بالوصول إلى OIK في Secure Enclave لنظام التشغيل الجديد. إذا اختار المستخدمون عدم نسخ مستخدم، فستظل عملية إنشاء مستخدم التثبيت جاريةً بالطريقة ذاتها، ولكن يتم استخدام كلمة سر فارغة بدلاً من كلمة سر المستخدم. وهذا التدفق الثاني موجود لبعض سيناريوهات إدارة النظام. ومع ذلك، يجب على المستخدمين الذين يرغبون في إجراء عمليات تثبيت متعددة وحدات التخزين ويريدون إجراء تسليم الملكية بالطريقة الأكثر أمانًا أن يختاروا دائمًا نسخ مستخدم من نظام التشغيل الأول إلى نظام التشغيل الثاني.

LocalPolicy على Mac مزود بسيليكون Apple

بالنسبة إلى أجهزة كمبيوتر Mac المزودة بسيليكون Apple، تم تفويض عنصر التحكم في سياسة الأمن المحلية ليكون تطبيقًا يعمل في Secure Enclave. ويمكن لهذا البرنامج استخدام بيانات اعتماد المستخدم ووضع التمهيد لوحدة المعالجة المركزية الأساسية لتحديد من يمكنه تغيير سياسة الأمن وتحديد بيئة التمهيد التي تسمح بذلك. ويساعد ذلك على منع البرامج الضارة من استخدام عناصر التحكم في سياسة الأمن ضد المستخدم من خلال خفض مستواها للحصول على مزيد من الامتيازات.

خصائص ملف بيانات LocalPolicy

يحتوي ملف LocalPolicy على بعض رموز 4CCs الهيكلية الموجودة في معظم ملفات Image4 - مثل لوحة أو معرّف الطراز (BORD)، مما يشير إلى شريحة Apple معينة (CHIP)، أو معرّف الشريحة الحصري (ECID). لكن عناصر 4CCs الواردة أدناه تركز فقط على سياسات الأمن التي يمكن للمستخدمين تكوينها.

ملاحظة: تستخدم Apple مصطلح **recoveryOS One True (1TR) المقترن** للإشارة إلى التمهيد في recoveryOS المقترن باستخدام زر طاقة مادي بضغطة واحدة مطولاً. ويختلف هذا عن تمهيد recoveryOS العادي الذي يحدث باستخدام NVRAM أو الضغط المزدوج مطولاً أو عند حدوث أخطاء عند بدء التشغيل. يؤدي الضغط على الزر المادي من نوع معين إلى زيادة الثقة في أن بيئة التمهيد لا يمكن الوصول إليها بواسطة مهاجم برمجي فقط استطاع اختراق macOS.

التجزئة العشوائية لـ LocalPolicy (lpnh)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** يتم استخدام `lpnh` لمكافحة إعادة تشغيل LocalPolicy. وهذه هي تجزئة SHA384 الخاصة بالقيمة العشوائية لـ LocalPolicy (LPN) التي يتم تخزينها في مكون التخزين الآمن ويمكن الوصول إليها باستخدام Boot ROM في Secure Enclave أو في Secure Enclave. ولا تكون القيمة غير القابلة لإعادة التشغيل مرئية مطلقًا لمعالج التطبيقات، ولكن تكون مرئية لـ sepOS فقط. سيحتاج المهاجم الذي يريد إقناع LLB بأن LocalPolicy السابقة التي تم اكتشافها كانت صالحة، وإلى وضع قيمة في مكون التخزين الآمن التي يتم تجزئتها بنفس قيمة `lpnh` الموجودة في LocalPolicy التي يريد إعادة تشغيلها. عادةً ما يوجد LPN واحد صالح على النظام—باستثناء أثناء تحديثات البرامج، عندما يوجد اثنان صالحان في الوقت نفسه—للسماح بإمكانية العودة إلى تمهيد البرنامج القديم في حالة حدوث خطأ في التحديث. عند تغيير أي LocalPolicy لأي نظام تشغيل، تتم إعادة توقيع كل السياسات بقيمة **lpnh** الجديدة المطابقة لـ LPN الجديد الموجود في مكون التخزين الآمن. يحدث هذا التغيير عندما يغير المستخدم إعدادات الأمان أو ينشئ أنظمة تشغيل جديدة باستخدام LocalPolicy جديدة لكل منها.

التجزئة العشوائية للسياسة البعيدة (rpnh)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** تعمل `rpnh` بالطريقة نفسها التي تعمل بها `lpnh`، ولكن لا يتم تحديثها إلا عند تحديث السياسة البعيدة، مثلاً عند تغيير حالة التسجيل في تطبيق تحديد الموقع. يحدث هذا التغيير عندما يغير المستخدم حالة تطبيق تحديد الموقع على الـ Mac الخاص به.

التجزئة العشوائية لـ recoveryOS (ronh)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** تعمل `ronh` بالطريقة نفسها التي تعمل بها lpnh، ولكن تكون موجودة بشكل حصري في LocalPolicy لنظام recoveryOS. ويتم تحديثها عند تحديث نظام recoveryOS، مثلما يحدث عند تحديث البرامج. يتم استخدام قيمة منفصلة غير قابلة لإعادة التشغيل من `lpnh` و `rpnh` بحيث عندما يتم وضع الجهاز في حالة تعطيل بواسطة تطبيق تحديد الموقع، يمكن تعطيل أنظمة التشغيل الحالية (عن طريق إزالة LPN و RPN من مكون التخزين الآمن)، مع الاستمرار في ترك نظام recoveryOS قابلًا للإقلاع. وبهذه الطريقة، يمكن إعادة تمكين أنظمة التشغيل عندما يثبت مالك النظام سيطرته على النظام عن طريق إدخال كلمة سر iCloud الخاصة به المستخدمة لحسابه في تطبيق تحديد الموقع. يحدث هذا التغيير عندما يقوم المستخدم بتحديث نظام recoveryOS أو إنشاء أنظمة تشغيل جديدة.

تجزئة ملف بيانات Image4 للمرحلة التالية (nsih)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** يمثل حقل **nsih** تجزئة SHA384 لبنية بيانات ملف بيانات Image4 التي تصف macOS الذي تم تمهيده. يحتوي ملف بيانات Image4 الخاص بـ macOS على قياسات لكل كائنات التمهيد، مثل iBoot وذاكرة التخزين المؤقت الموثوق بها وشجرة الجهاز ومجموعة Boot Kernel وتجزئة جذر وحدة تخزين النظام الموقَّعة (SSV). عند توجيه LLB إلى تمهيد macOS معين، تم تصميم ذلك ليضمن أن تكون تجزئة ملف بيانات Image4 الخاصة بـ macOS المرفقة مع iBoot مطابقة لما تم التقاطه في حقل `nsih` في LocalPolicy. وبهذه الطريقة، تكتشف `nsih` هدف المستخدم في نظام التشغيل الذي أنشأ المستخدم سياسة LocalPolicy لها. يُغيّر المستخدمون قيمة `nsih` ضمنيًا عند تنفيذ تحديث للبرامج.

تجزئة ملف بيانات Image4 الخاص بـ Cryptex1 (spih)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** يمثل حقل `spih` تجزئة SHA384 لهيكل بيانات ملف Image4 الخاص بـ Cryptex1. يحتوي ملف بيانات Image4 الخاص بـ Cryptex1 على قياسات وحدة التشفير وعمليات تأمين نظام الملفات وذاكرة التخزين المؤقت الموثوق بها المرتبطة. عند بدء تشغيل macOS، يضمن ملحق XNU kernel وطبقة حماية الصفحة أن تكون تجزئة ملف بيانات Image4 الخاص بـ Cryptex1 مطابقة لما نشره iBoot من حقل `spih` في LocalPolicy. يُغيّر المستخدمون قيمة `spih` ضمنيًا عند تثبيت الاستجابة الأمنية السريعة أو إجراء تحديث للبرامج. يمكن تحديث تجزئة ملف بيانات Image4 الخاص بـ Cryptex1 بشكل مستقل عن تجزئة ملف بيانات Image4 للمرحلة التالية.

إنشاء Cryptex1 (stng)

- **النوع:** عدد صحيح غير مُوقَّع من 64 بت
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** حقل `stng` هو قيمة عدّاد تمثل وقت آخر تحديث لتجزئة ملف بيانات Image4 الخاص بـ Cryptex1 في LocalPolicy. يوفر قيمة منع إعادة التشغيل بدلًا من `lpnh` أثناء تقييم طبقة حماية الصفحة للسياسة المحلية لتطبيق التشفير الوارد. يزيد المستخدمون من قيمة `stng` ضمنيًا عند تثبيت الاستجابة الأمنية السريعة وإجراء تحديث للبرامج.

تجزئة سياسة ذاكرة التخزين المؤقت لملحقات Kernel المساعدة (AuxKC) (auxp)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** macOS
- **الوصف:** `auxp` عبارة عن تجزئة SHA384 لسياسة قائمة kext المصرح بها من قِبل المستخدم (UAKL). وتُستخدم وقت إنشاء AuxKC للمساعدة على ضمان تضمين kexts المُصرّح بها من قِبل المستخدم فقط في AuxKC. ويُعدّ `smb2` شرطًا أساسيًا لإعداد هذا الحقل. ويغيّر المستخدمون قيمة `auxp` ضمنيًا عندما يغيّرون UAKL من خلال الموافقة على kext من الخصوصية والأمن في إعدادات النظام (macOS 13 أو أحدث) أو جزء الأمن والخصوصية في تفضيلات النظام (macOS 12 أو أقدم).

تجزئة ملف بيانات Image4 لذاكرة التخزين المؤقت لملحقات Kernel المساعدة (AuxKC) (auxi)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** macOS
- **الوصف:** بعد أن يتحقق النظام من تطابق تجزئة UAKL مع محتويات الحقل `auxp` في LocalPolicy، يطلب توقيع AuxKC بواسطة تطبيق معالج Secure Enclave المسؤول عن توقيع LocalPolicy. ثم تُوضع تجزئة SHA384 الخاصة بتوقيع ملف بيانات AuxKC Image4 في LocalPolicy، لتجنب احتمال خلط ومطابقة AuxKCs المُوقّعة سابقًا مع نظام تشغيل في وقت التمهيد. إذا عثر iBoot على حقل `auxi` في LocalPolicy، يحاول تحميل AuxKC من وحدة التخزين ويتحقق من صحة توقيعه. ويتحقق أيضًا من تطابق تجزئة ملف بيانات Image4 المرفق بـ AuxKC مع القيمة الموجودة في حقل `auxi`. إذا فشل تحميل AuxKC لأي سبب من الأسباب، يستمر النظام في التمهيد بدون كائن التمهيد هذا، وبالتالي بدون تحميل أي ملفات kexts تابعة لجهات خارجية. يعتبر الحقل `auxp` شرطًا أساسيًا لتعيين الحقل auxi في LocalPolicy. ويغيّر المستخدمون قيمة `auxi` ضمنيًا عندما يغيّرون UAKL من خلال الموافقة على kext من الخصوصية والأمن في إعدادات النظام (macOS 13 أو أحدث) أو جزء الأمن والخصوصية في تفضيلات النظام (macOS 12 أو أقدم).

تجزئة إيصال ذاكرة التخزين المؤقت لملحقات Kernel المساعدة (AuxKC) (auxr)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** macOS
- **الوصف:** `auxr` عبارة عن تجزئة SHA384 لإيصال AuxKC، تشير إلى مجموعة kexts الدقيقة التي تم تضمينها في AuxKC. يمكن أن يكون إيصال AuxKC مجموعة فرعية من UAKL، لأنه يمكن استبعاد kexts من AuxKC حتى لو كانت مصرحًا بها من قِبل المستخدم، إذا كانت معروفة بأنها تُستخدم لتنفيذ الهجمات. بالإضافة إلى ذلك، قد تؤدي بعض kexts التي يمكن استخدامها لكسر حدود kernel الخاصة بالمستخدم إلى تقليل الوظائف مثل عدم القدرة على استخدام Apple Pay أو تشغيل محتوى 4K و HDR. أما المستخدمون الذين يرغبون في الحصول على هذه الإمكانيات، فعليهم باختيار تضمين AuxKC أكثر تقييدًا. يعتبر الحقل `auxp` شرطًا أساسيًا لتعيين الحقل `auxr` في LocalPolicy. ويغيّر المستخدمون قيمة `auxr` ضمنيًا عند إنشاء AuxKC جديد من الخصوصية والأمن في إعدادات النظام (macOS 13 أو أحدث) أو جزء الأمن والخصوصية في تفضيلات النظام (macOS 12 أو أقدم).

تجزئة ملف بيانات CustomOS لـ Image4 (coih)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** 1TR
- **الوصف:** تُعد `coih` تجزئة SHA384 لملف بيانات Image4 على CustomOS. تُستخدم حمولة ملف البيانات هذا بواسطة iBoot (بدلاً من XNU kernel) لنقل التحكم. يغير المستخدمون قيمة `coih` ضمنيًا عند استخدام أداة سطر الأوامر `kmutil configure-boot` في 1TR.

معرف UUID لمجموعة وحدات تخزين APFS (vuid)

- **النوع:** OctetString (16)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** يُشير `vuid` إلى مجموعة وحدات التخزين التي يجب أن يستخدمها kernel كجذر. هذا الحقل معلوماتي بشكل أساسي، ولا يُستخدم لقيود الأمن. ويتم تعيين `vuid` هذا من قِبل المستخدم ضمنيًا عند إنشاء تثبيت جديد لنظام التشغيل.

معرف UUID للمجموعة لمفتاح تشفير المفاتيح (kuid) (KEK)

- **النوع:** OctetString (16)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** يُشير `kuid` إلى وحدة التخزين التي تم تمهيدها. كان يتم استخدام مفتاح تشفير المفاتيح عادةً لحماية البيانات. لكل LocalPolicy، يتم استخدامه لحماية مفتاح توقيع سياسة LocalPolicy. ويتم تعيين `kuid` من قِبل المستخدم ضمنيًا عند إنشاء تثبيت جديد لنظام التشغيل.

قياس سياسة التمهيد الموثوقة لـ recoveryOS المقترن (prot)

- **النوع:** OctetString (48)
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** قياس سياسة الإقلاع الموثوق بها لـ recoveryOS المقترن (TBPM) عبارة عن حساب تجزئة SHA384 تكرارية خاصة عبر ملف بيانات Image4 الخاص بسياسة LocalPolicy، باستثناء القيم غير القابلة لإعادة التشغيل، لتحديد قياس ثابت مع مرور الوقت (نظرًا لتحديث القيم غير القابلة لإعادة التشغيل مثل `lpnh` بشكل متكرر). ويوجد حقل `prot` لكل سياسة LocalPolicy في macOS، ويوفر إقرانًا للإشارة إلى سياسة LocalPolicy لـ recoveryOS التي تتوافق مع سياسة LocalPolicy لـ macOS.

يحتوي على سياسة محلية لـ recoveryOS موقّعة بواسطة Secure Enclave (hrlp)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** يشير `hrlp` إلى ما إذا كانت قيمة `prot` (أعلاه) هي قياس سياسة LocalPolicy لـ recoveryOS موقّعة بواسطة Secure Enclave أم لا. فإذا لم يكن الأمر كذلك، يتم توقيع LocalPolicy لـ recoveryOS بواسطة خادم التوقيع على الإنترنت من Apple، والذي يقوم بتوقيع أشياء مثل ملفات macOS Image4.

إصدار نظام التشغيل المحلي (love)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR و recoveryOS و macOS
- **الوصف:** يشير `love` إلى إصدار OS الذي تم إنشاء LocalPolicy لأجله. يتم الحصول على الإصدار من بيان الحالة الآتي أثناء إنشاء LocalPolicy ويتم استخدامه لفرض قيود اقتران recoveryOS.

تمهيد متعدد آمن (smb0)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR و recoveryOS
- **الوصف:** إذا كان `smb0` موجودًا وصحيحًا، يسمح LLB بالتوقيع على ملف بيانات Image4 الخاص بالمرحلة التالية عالميًا، بدلاً من طلب توقيع مخصص. ويمكن للمستخدمين تغيير هذا الحقل باستخدام أداة أمن بدء التشغيل أو `bputil` لإرجاع مستوى الأمن إلى تأمين منخفض.

تمهيد متعدد آمن (smb1)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR
- **الوصف:** إذا كان `smb1` موجودًا وصحيحًا، يسمح iBoot للكائنات مثل مجموعة kernel مخصصة بأن تكون مُوقّعة من قِبل Secure Enclave باستخدام المفتاح نفسه الموجود في LocalPolicy. ويعد وجود `smb0` شرطًا أساسيًا لوجود `smb1`. ويمكن للمستخدمين تغيير هذا الحقل باستخدام أدوات سطر الأوامر مثل `csrutil` أو `bputil` لإرجاع مستوى الأمن إلى تأمين أقل تقييدًا.

تمهيد متعدد آمن (smb2)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR
- **الوصف:** إذا كان `smb2` موجودًا وصحيحًا، فإن iBoot يسمح لمجموعة Kernel المساعدة بأن تكون موقعة بواسطة Secure Enclave بنفس مفتاح LocalPolicy. ويعد وجود `smb0` شرطًا أساسيًا لوجود `smb2`. ويمكن للمستخدمين تغيير هذا الحقل باستخدام أداة أمن بدء التشغيل أو `bputil` لإرجاع مستوى الأمان إلى تأمين منخفض وتمكين kexts التابعة لجهات خارجية.

تمهيد متعدد آمن (smb3)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR
- **الوصف:** إذا كان `smb3` موجودًا وصحيحًا، فقد اختار المستخدم على الجهاز السماح لحل إدارة جهاز الجوال MDM بالتحكم في نظامه. يؤدي وجود هذا الحقل إلى جعل سياسة LocalPolicy المتحكمة في تطبيق معالج Secure Enclave تقبل مصادقة MDM بدلاً من طلب مصادقة المستخدم المحلي. ويمكن للمستخدمين تغيير هذا الحقل باستخدام أداة أمن بدء التشغيل أو `bputil` لتمكين التحكم المُدار في kexts التابعة لجهات خارجية وتحديثات البرامج. (في macOS 11.2 أو أحدث، يستطيع MDM أيضًا بدء تحديث إلى أحدث إصدار من macOS إذا كان نمط الأمن الحالي هو التأمين الكامل).

تمهيد متعدد آمن (smb4)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** macOS
- **الوصف:** إذا كانت قيمة `smb4` موجودة وصحيحة، فقد اختار الجهاز السماح لـ MDM بالتحكم في نظام التشغيل باستخدام Apple School Manager أو Apple Business ManagerApple Business Essentials. يؤدي وجود هذا الحقل إلى جعل سياسة LocalPolicy المتحكمة في تطبيق Secure Enclave تقبل مصادقة MDM بدلاً من طلب مصادقة المستخدم المحلي. يتم تغيير هذا الحقل بواسطة حل MDM عندما يكتشف ظهور الرقم التسلسلي للجهاز في أي من هذه الخدمات الثلاث.

حماية تكامل النظام (sip0)

- **النوع:** عدد صحيح غير مُوقَّع من 64 بت
- **البيئات المتغيرة:** 1TR
- **الوصف:** تحتوي `sip0` على وحدات بت سياسة حماية تكامل النظام (SIP) الموجودة والتي تم تخزينها سابقًا في NVRAM. تُضاف وحدات بت سياسة SIP الجديدة هنا (بدلاً من استخدام حقول LocalPolicy مثلما هو موضح أدناه)، إذا كانت تُستخدم في macOS فقط، ولا تُستخدم بواسطة LLB. ويمكن للمستخدمين تغيير هذا الحقل باستخدام `csrutil` من 1TR لتعطيل SIP وإرجاع مستوى الأمان إلى تأمين أقل تقييدًا.

حماية تكامل النظام (sip1)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR
- **الوصف:** إذا كانت قيمة `sip1` موجودة وصحيحة، يسمح iBoot بحالات الفشل في التحقق من تجزئة جذر وحدة تخزين SSV. ويمكن للمستخدمين تغيير هذا الحقل باستخدام `csrutil` أو `bputil` من 1TR.

حماية تكامل النظام (sip2)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR
- **الوصف:** إذا كانت قيمة sip2 موجودة وصحيحة، فلن يقوم iBoot بقفل سجل أجهزة **منطقة القراءة فقط للنص القابل للتكوين (CTRR)** التي تحدد ذاكرة kernel على أنها غير قابلة للكتابة. ويمكن للمستخدمين تغيير هذا الحقل باستخدام `csrutil` أو `bputil` من 1TR.

حماية تكامل النظام (sip3)

- **النوع:** قيمة منطقية
- **البيئات المتغيرة:** 1TR
- **الوصف:** إذا كانت قيمة `sip3` موجودة وصحيحة، لن يفرض iBoot قائمة السماح المضمنة الخاصة به لمتغير boot-args NVRAM، والذي قد يؤدي إلى تصفية الخيارات التي يتم تمريرها إلى kernel. ويمكن للمستخدمين تغيير هذا الحقل باستخدام `csrutil` أو `bputil` من 1TR.

الشهادات و RemotePolicy

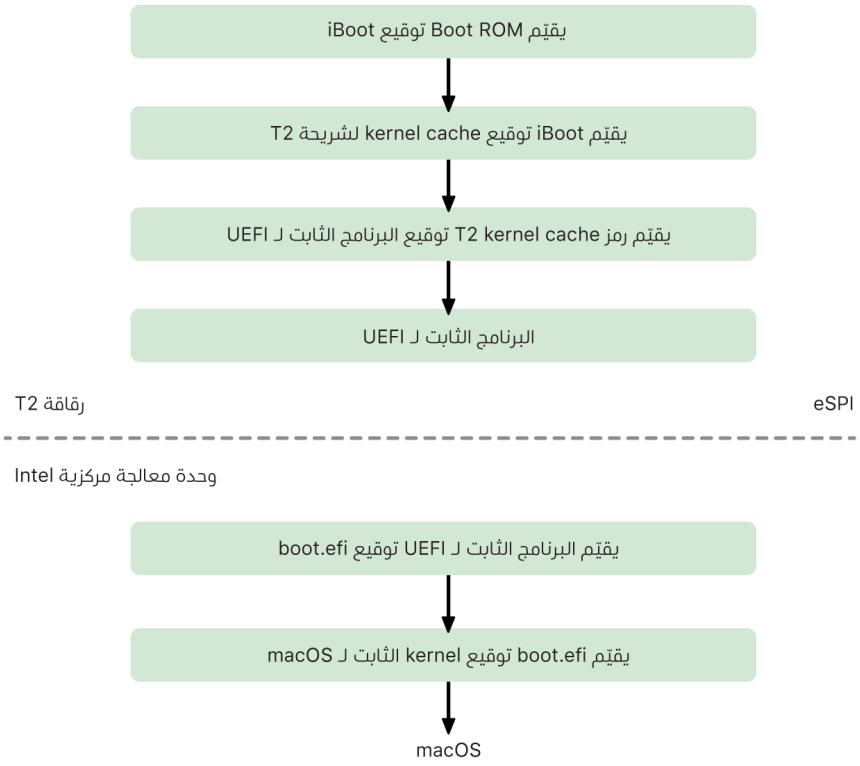
كما هو موضح في إنشاء مفتاح توقيع LocalPolicy وإدارته، تحتوي LocalPolicy Image4 أيضًا على شهادة هوية المالك (OIC) و RemotePolicy المضمنة.

أجهزة كمبيوتر Mac المستندة إلى Intel

عملية التمهيد على Mac مستند إلى Intel

Mac المستند إلى Intel المزود بشريحة Apple T2 أمنية

عند تشغيل كمبيوتر Mac مستند إلى Intel مزود بشريحة Apple T2 الأمنية، تنفّذ الشريحة عملية تمهيد آمن من Boot ROM الخاص بها بالطريقة ذاتها كما في الـ iPhone والـ iPad وأجهزة كمبيوتر Mac المزودة بسيليكون Apple. وهذا يتحقق من مُحمّل إقلاع iBoot ويُعدّ الخطوة الأولى في سلسلة الثقة. كما يتحقق iBoot من kernel والتعليمات البرمجية لملحق kernel على شريحة T2، والتي تتحقق لاحقًا من برنامج Intel UEFI الثابت. يتوفر برنامج UEFI الثابت والتوقيع المقترن به مبدئيًا على شريحة T2 فقط.



بعد التحقق، يتم تعيين صورة برنامج UEFI الثابت في جزء من ذاكرة شريحة T2. يتم توفير هذه الذاكرة لوحدة معالجة Intel المركزية من خلال الواجهة الطرفية التسلسلية المحسّنة (eSPI). عندما تقوم وحدة معالجة Intel المركزية بالتمهيد لأول مرة، فإنه يقوم بإحضار برنامج UEFI الثابت عبر eSPI من نسخة تم التحقق من سلامتها وتعيينها إلى الذاكرة للبرنامج الثابت الموجود على شريحة T2.

يستمر تقييم سلسلة الثقة على وحدة معالجة Intel المركزية، مع قيام برنامج UEFI الثابت بتقييم توقيع boot.efi، وهو محمّل إقلاع macOS. يتم تخزين توقيعات التمهيد الآمن في macOS المتواجد في Intel بنفس تنسيق Image4 المستخدم في التمهيد الآمن في iOS و iPadOS وشريحة T2، والتعليمات البرمجية التي تحلل ملفات Image4 هي نفس التعليمات البرمجية المحصّنة من عملية تطبيق التمهيد الآمن في iOS و iPadOS الحالي. يتحقق Boot.efi بدوره من توقيع ملف جديد، يسمى immutablekernel. عند تمكين التمهيد الآمن، يمثل ملف immutablekernel المجموعة الكاملة من ملحقات Apple kernel المطلوبة لتشغيل macOS. تنتهي سياسة التمهيد الآمن عند التسليم إلى immutablekernel، وبعد ذلك، تصبح سياسات الأمن في macOS (مثل حماية تكامل النظام وملحقات kernel الموقّعة) سارية المفعول.

في حالة وجود أي أخطاء أو إخفاقات في هذه العملية، يدخل الـ Mac في وضع الاسترداد أو وضع استرداد شريحة Apple T2 الأمنية أو وضع ترقية البرنامج الثابت للجهاز (DFU) في شريحة Apple T2 الأمنية.

Microsoft Windows على Mac مستند إلى Intel مزود بشريحة T2

بشكل افتراضي، لا تثق أجهزة كمبيوتر Mac المستندة إلى Intel التي تدعم التمهيد الآمن إلا بالمحتوى الموقّع من Apple. ومع ذلك، لتحسين أمن عمليات تثبيت Boot Camp، تدعم Apple أيضًا التمهيد الآمن لـ Windows. يتضمن البرنامج الثابت لواجهة البرامج الثابتة القابلة للتوسعة الموحدة (UEFI) نسخة من شهادة Microsoft Windows Production CA 2011 تُستخدم لمصادقة مُحمّلات إقلاع Microsoft.

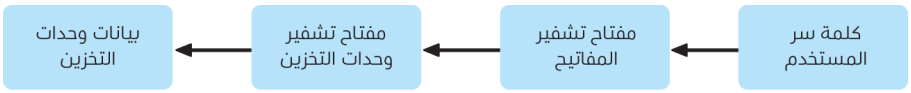
ملاحظة: لا توجد حاليًا أي ثقة تم توفيرها لـ Microsoft Corporation UEFI CA 2011، والتي قد تسمح بالتحقق من التعليمات البرمجية الموقَّعة من قِبل شركاء Microsoft. يُستخدم UEFI CA هذا بشكل شائع للتحقق من أصالة مُحمّلات الإقلاع لأنظمة التشغيل الأخرى، مثل متغيرات Linux.

لا يتم تمكين دعم التمهيد الآمن لنظام Windows بشكل افتراضي؛ بدلاً من ذلك، يتم تمكينه باستخدام مساعد منظم الإقلاع (BCA). عندما يقوم أحد المستخدمين بتشغيل BCA، تتم إعادة تكوين macOS للوثوق في التعليمات البرمجية المُوقّعة من الطرف الأول في Microsoft أثناء التمهيد. بعد اكتمال BCA، في حالة فشل macOS في اجتياز تقييم ثقة الطرف الأول من Apple أثناء التمهيد الآمن، يحاول برنامج UEFI الثابت تقييم ثقة الكائن وفقًا لتنسيق التمهيد الآمن في UEFI. إذا نجح تقييم الثقة، يستمر الـ Mac في العمل ويقوم بتمهيد Windows. وإذا لم ينجح، يدخل الـ Mac في وضع recoveryOS ويُبلغ المستخدم بفشل تقييم الثقة.

أجهزة كمبيوتر Mac المستندة إلى Intel غير المزودة بشريحة T2

أجهزة كمبيوتر Mac المستندة إلى Intel غير المزودة بشريحة T2 لا تدعم التمهيد الآمن. لذا، يقوم البرنامج الثابت لواجهة البرامج الثابتة القابلة للتوسعة الموحدة (UEFI) بتحميل برنامج إقلاع macOS (boot.efi) من نظام الملفات دون التحقق، ويقوم برنامج الإقلاع بتحميل kernel (prelinkedkernel) من نظام الملفات دون التحقق. لحماية تكامل سلسلة التمهيد، يجب على المستخدمين تمكين جميع آليات الأمن التالية:

- **حماية تكامل النظام (SIP):** يتم تمكينها افتراضيًا، مما يحمي جهاز الإقلاع و kernel من عمليات الكتابة الضارة من داخل macOS الجاري تشغيله.
- **خزنة الملفات:** يمكن تمكينها بطريقتين: بواسطة المستخدم أو بواسطة مسؤول إدارة جهاز الجوال (MDM). وهذا يحمي ضد المهاجم الموجود فعليًا الذي يستخدم نمط القرص المستهدف لاستبدال برنامج الإقلاع.
- **كلمة سر البرنامج الثابت:** يمكن تمكينها بطريقتين: بواسطة المستخدم أو بواسطة مسؤول MDM. يساعد هذا على الحماية ضد المهاجم الموجود فعليًا الذي يحاول تشغيل أنماط الإقلاع البديلة مثل recoveryOS أو نمط المستخدم الواحد أو نمط القرص المستهدف التي يمكن من خلالها استبدال برنامج الإقلاع. كما يساعد أيضًا على منع التمهيد من الوسائط البديلة التي يمكن للمهاجم من خلالها تشغيل تعليمات برمجية لاستبدال برنامج الإقلاع.



أنماط التمهيد على Mac مستند إلى Intel مزود بشريحة Apple T2 أمنية

تحتوي أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة Apple T2 أمنية على مجموعة متنوعة من أنماط التمهيد التي يمكن دخولها في وقت التمهيد عن طريق الضغط على مجموعات مفاتيح، والتي يتم التعرف عليها بواسطة برنامج UEFI الثابت أو برنامج الإقلاع. لن تعمل بعض أوضاع التمهيد، مثل نمط المستخدم الواحد، ما لم يتم تغيير سياسة الأمن إلى "بلا تأمين" في أداة أمن بدء التشغيل.

الوضع	مجموعة المفاتيح	الوصف
تمهيد macOS	لا شيء	يقوم برنامج UEFI الثابت بالتسليم إلى برنامج إقلاع macOS (تطبيق UEFI)، الذي بدوره يقوم بالتسليم إلى macOS kernel. عند التمهيد القياسي لـ Mac مع تمكين خزنة الملفات، يعرض برنامج إقلاع macOS واجهة نافذة تسجيل الدخول التي تأخذ كلمة السر لفك تشفير التخزين.
مدير بدء التشغيل	الخيارات (⌥)	يقوم برنامج UEFI الثابت بتشغيل تطبيق UEFI المضمن الذي يعرض للمستخدم واجهة تحديد جهاز التمهيد.
نمط القرص المستهدف (TDM)	T	يقوم برنامج UEFI الثابت بتشغيل تطبيق UEFI المضمن الذي يعرض جهاز التخزين الداخلي كجهاز تخزين أولي مستند إلى الكتلة عبر Fire Wire أو ثندربولت أو USB أو أي مجموعة من الثلاثة (حسب طراز Mac).
نمط المستخدم الواحد	الأوامر S-(⌘)	يمرر macOS kernel علامة `-s` في متجه وسيطة launchd، ثم ينشئ launchd مكون shell للمستخدم الفردي في tty الخاص بتطبيق وحدة التحكم. **ملاحظة:** في حالة خروج المستخدم من shell، يستمر macOS في التمهيد إلى نافذة تسجيل الدخول.
recoveryOS	الأوامر R-(⌘)	يقوم برنامج UEFI الثابت بتحميل الحد الأدنى من macOS من ملف صورة القرص الموقّعة (.dmg) على جهاز التخزين الداخلي.
recoveryOS على الإنترنت	الخيارات رماوألا-(⌥) R-(⌘)	يتم تنزيل صورة القرص الموقّعة من الإنترنت باستخدام HTTP.
التشخيصات	D	يقوم برنامج UEFI الثابت بتحميل الحد الأدنى لبيئة تشخيصات UEFI من ملف صورة القرص الموقّعة على جهاز التخزين الداخلي.
تشخيصات الإنترنت	الخيارات D-(⌥)	يتم تنزيل صورة القرص الموقّعة من الإنترنت باستخدام HTTP.
تمهيد Windows	لا شيء	إذا تم تثبيت Windows باستخدام منظم الإقلاع، فإن برنامج UEFI الثابت يقوم بالتسليم إلى برنامج إقلاع Windows الذي يقوم بالتسليم إلى Windows kernel.

أداة أمن بدء التشغيل على Mac مزود بشريحة Apple T2 أمنية

نظرة عامة

على أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة Apple T2 أمنية، تتعامل أداة أمن بدء التشغيل مع عدد من إعدادات سياسة الأمن. يمكن الوصول إلى الأداة عن طريق التمهيد في recoveryOS وتحديد أداة أمن بدء التشغيل من قائمة الأدوات المساعدة، وتحمي إعدادات الأمن المدعومة من التلاعب السهل من قِبل أي مهاجم.

تتطلب تغييرات السياسة الجوهرية وجود مصادقة، حتى في وضع الاسترداد. عند فتح أداة أمن بدء التشغيل لأول مرة، فإنها تطالب المستخدم بإدخال كلمة سر المسؤول من تثبيت macOS الأساسي المرتبط بـ recoveryOS الذي يتم تمهيده حاليًا. في حالة عدم وجود مسؤول، يجب إنشاء واحد قبل تغيير السياسة. تتطلب شريحة T2 تمهيد كمبيوتر Mac حاليًا في recoveryOS وأن تتم المصادقة مع بيانات اعتماد مدعومة من Secure Enclave قبل إجراء مثل هذا التغيير في السياسة. تحتوي تغييرات سياسة الأمن على متطلبين ضمنيين. يجب على recoveryOS:

- أن يتم تمهيده من جهاز تخزين متصل مباشرةً بشريحة T2، لأن الأقسام الموجودة على الأجهزة الأخرى لا تحتوي على بيانات اعتماد مدعومة من Secure Enclave مرتبطة بجهاز التخزين الداخلي.
- أن يكون موجودًا على وحدة تخزين تستند إلى APFS، نظرًا لعدم وجود دعم إلا لتخزين بيانات اعتماد المصادقة في الاسترداد المرسلة إلى Secure Enclave على وحدة تخزين APFS "ما قبل التمهيد" بمحرك الأقراص. لا يمكن لوحدات التخزين بتنسيق HFS plus استخدام التمهيد الآمن.

لا يتم عرض هذه السياسة إلا في أداة أمن بدء التشغيل على Mac مستند إلى Intel مزود بشريحة T2. على الرغم من أن معظم حالات الاستخدام يجب ألا تتطلب تغييرات في سياسة التمهيد الآمن، إلا أن المستخدمين يتحكمون في النهاية في إعدادات أجهزتهم، وقد يختارون، حسب احتياجاتهم، تعطيل وظيفة التمهيد الآمن على الـ Mac الخاص بهم أو إرجاعها إلى إصدار قديم.

لا تنطبق تغييرات سياسة التمهيد الآمن التي تم إجراؤها من داخل هذا التطبيق إلا على تقييم سلسلة الثقة التي يتم التحقق منها على معالج Intel. ويكون خيار "التمهيد الآمن لشريحة T2" ساري المفعول دائمًا.

يمكن تكوين سياسة التمهيد الآمن إلى أحد الإعدادات الثلاثة: تأمين كامل وتأمين متوسط وبلا تأمين. "بلا تأمين" يعطّل تقييم التمهيد الآمن تمامًا على معالج Intel ويسمح للمستخدم بتمهيد كل ما يريد.

سياسة تمهيد التأمين الكامل

سياسة التأمين الكامل هي سياسة التمهيد الافتراضية، وتتصرف بشكل مشابه لـ iOS و iPadOS أو التأمين الكامل على Mac مزود برقاقات Apple. في الوقت الذي يتم فيه تخفيض مستوى أمن البرنامج وتحضيره للتثبيت، يتم تخصيصه بتوقيع يتضمن معرف الشريحة الحصري (ECID) -وهو معرف فريد خاص بشريحة T2 في هذه الحالة - كجزء من طلب التوقيع. ويكون التوقيع الذي يرجع من خادم التوقيع فريدًا وقابلاً للاستخدام فقط بواسطة شريحة T2 المعينة هذه. تم تصميم البرنامج الثابت لواجهة البرامج الثابتة القابلة للتوسعة الموحدة (UEFI) لضمان أنه عندما تكون سياسة التأمين الكامل سارية المفعول، لا يكون التوقيع المحدد موقعًا من قِبل Apple فحسب، بل تم توقيعه لهذا الـ Mac بالتحديد، ويربط هذا الإصدار من macOS بشكل أساسي بهذا الـ Mac. وهذا يساعد في منع هجمات التراجع كما هو موضح في سياسة التأمين الكامل على Mac مزود بسيليكون Apple.

سياسة تمهيد التأمين المتوسط

تشبه سياسة تمهيد التأمين المتوسط إلى حد ما سياسة تمهيد UEFI الآمن التقليدية، حيث يقوم المورّد (الذي تمثله Apple في هذه الحالة) بإنشاء توقيع رقمي للتعليمات البرمجية لتأكيد أن مصدرها هو المورّد. وبهذه الطريقة، يتم منع المهاجمين من إدراج تعليمات برمجية غير موقّعة. ونُشير إلى هذا التوقيع على أنه توقيع "عام"، لأنه يمكن استخدامه على أي Mac، لأي فترة زمنية، لأجهزة كمبيوتر Mac التي تم تعيين سياسة التأمين المتوسط بها حاليًا. لا يدعم iOS أو iPadOS أو شريحة T2 ذاتها التوقيعات العامة. ولا يحاول هذا الإعداد منع هجمات التراجع.

سياسة تمهيد الوسائط

لا توجد سياسة تمهيد الوسائط إلا على أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة T2 وهي مستقلة عن سياسة التمهيد الآمن. حتى إذا عطّل المستخدم التمهيد الآمن، فإن هذا لا يغير السلوك الافتراضي المتمثل في منع تمهيد الـ Mac من أي شيء آخر غير جهاز التخزين المتصل مباشرة بشريحة T2. (سياسة إقلاع الوسائط غير مطلوبة على Mac مزود برقاقات Apple. لمزيد من المعلومات، انظر التحكم في سياسة أمن قرص بدء التشغيل).

حماية كلمة سر البرنامج الثابت في Mac مستند إلى Intel

يدعم macOS على أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة Apple T2 أمنية استخدام كلمة سر البرنامج الثابت للمساعدة على منع التعديلات غير المقصودة على إعدادات البرنامج الثابت على Mac معين. صُمِّمت كلمة السر للبرنامج الثابت لمنع تحديد أنماط الإقلاع البديلة مثل الإقلاع في نمط recoveryOS أو نمط المستخدم الواحد أو الإقلاع من وحدة تخزين غير مصرح بها، أو الإقلاع في نمط القرص المستهدف.

ملاحظة: كلمة سر البرنامج الثابت غير مطلوبة على أجهزة كمبيوتر Mac المزودة بسيليكون Apple، لأن وظيفة البرنامج الثابت المهمة التي تعمل على تقييدها قد تم نقلها إلى recoveryOS، ثم (عند تمكين خزنة الملفات) يتطلب recoveryOS مصادقة المستخدم قبل تمكين الوصول إلى وظائفه المهمة.

يمكن الوصول إلى النمط الأساسي لكلمة سر البرنامج الثابت من أداة كلمة سر البرنامج الثابت في recoveryOS على أجهزة كمبيوتر Mac المستندة إلى Intel **غير المزودة** بشريحة T2، ومن أداة أمن بدء التشغيل على أجهزة كمبيوتر Mac المستندة إلى Intel **المزودة** بشريحة T2. وتتوفر الخيارات المتقدمة (مثل إمكانية المطالبة بكلمة السر في كل عملية تمهيد) من أداة سطر الأوامر `firmwarepasswd` في macOS.

يعد تعيين كلمة سر للبرنامج الثابت أمرًا مهمًا بشكل خاص للحد من مخاطر الهجمات على أجهزة كمبيوتر Mac المستندة إلى Intel غير المزودة بشريحة T2 من مهاجم له وجود مادي في المكان. تستطيع كلمة سر البرنامج الثابت أن تساعد في منع المهاجم من التمهيد إلى نمط recoveryOS الذي يمكن من خلاله تعطيل حماية تكامل النظام (SIP). وبتقييد تمهيد الوسائط البديلة، لا يستطيع المهاجم تنفيذ التعليمات البرمجية المميزة من نظام تشغيل آخر لمهاجمة البرامج الثابتة الطرفية.

توجد آلية لإعادة تعيين كلمة سر البرنامج الثابت لمساعدة المستخدم الذي ينسى كلمة السر الخاصة به. يضغط المستخدم على مجموعة مفاتيح عند بدء التشغيل، ويتم تزويده بسلسلة خاصة بالطراز لتقديمها إلى AppleCare. تُوقّع AppleCare رقميًا على مَوْرد يتم التحقق من التوقيع عليه بواسطة معرف الموارد المنتظم (URI). وإذا كان التوقيع صالحًا والمحتوى خاصًا بالـ Mac المحدد، يزيل برنامج UEFI الثابت كلمة سر البرنامج الثابت.

بالنسبة للمستخدم الذي لا يريد لأحد غيره إزالة كلمة سر البرنامج الثابت الخاصة به عن طريق البرامج، تمت إضافة خيار `-disable-reset-capability` إلى أداة سطر الأوامر `firmwarepasswd` في macOS 10.15. وقبل تعيين هذا الخيار، يجب على المستخدم الإقرار بأنه في حالة نسيان كلمة السر والحاجة إلى إزالتها، يجب أن يتحمل المستخدم تكلفة استبدال اللوحة المنطقية اللازمة لتحقيق ذلك. يجب على المؤسسات التي تريد حماية أجهزة كمبيوتر Mac الخاصة بها من المهاجمين الخارجيين ومن الموظفين تعيين كلمة سر للبرنامج الثابت على الأنظمة المملوكة للمؤسسة. يمكن إتمام ذلك على الجهاز بأي من الطرق التالية:

- في وقت التوفير، باستخدام أداة سطر الأوامر `firmwarepasswd` يدويًا
- باستخدام أدوات إدارة الجهات الخارجية التي تستخدم أداة سطر الأوامر `firmwarepasswd`
- باستخدام إدارة جهاز الجوال (MDM)

recoveryOS وبيئات التشخيص على Mac مستند إلى Intel

recoveryOS

يكون recoveryOS منفصلاً تمامًا عن macOS الرئيسي، ويتم تخزين المحتويات بالكامل في ملف صورة قرص يسمى BaseSystem.dmg. توجد أيضًا BaseSystem.chunklist مقترنة تُستخدم للتحقق من تكامل BaseSystem.dmg. chunklist عبارة عن سلسلة من علامات التجزئة لشرائح من BaseSystem.dmg بحجم 10 ميغابايت. يقيّم البرنامج الثابت لواجهة البرامج الثابتة القابلة للتوسعة الموحدة (UEFI) توقيع ملف chunklist، ثم يقيّم التجزئة لشريحة واحدة في المرة الواحدة من BaseSystem.dmg. وهذا يساعد على ضمان مطابقتها للمحتوى الموقّع الموجود في chunklist. في حالة عدم تطابق أي من علامات التجزئة هذه، يتم إلغاء التمهيد من recoveryOS، ويحاول برنامج UEFI الثابت التمهيد من recoveryOS على الإنترنت بدلاً من ذلك.

في حالة اكتمال عملية التحقق بنجاح، يقوم برنامج UEFI الثابت بتحميل BaseSystem.dmg باعتباره قرص RAM ويقوم بتشغيل ملف boot.efi الموجود فيه. لا توجد حاجة إلى برنامج UEFI الثابت من أجل إجراء فحص معين لـ boot.efi، ولا إلى boot.efi من أجل فحص kernel، لأن محتويات نظام التشغيل المكتملة (التي لا تشكل هذه العناصر منها سوى مجموعة فرعية) قد تم بالفعل التحقق من تكاملها.

تشخيصات Apple

إن إجراء تمهيد بيئة التشخيص المحلية هو في الغالب نفس إجراء تشغيل recoveryOS. تُستخدم ملفات AppleDiagnostics.dmg وكذلك AppleDiagnostics.chunklist منفصلة، لكن يتم التحقق منهما بنفس طريقة ملفات BaseSystem. بدلاً من تشغيل boot.efi، يشغّل برنامج UEFI الثابت ملفًا داخل صورة القرص (ملف .dmg) باسم diags.efi، يكون بدوره مسؤولاً عن استدعاء مجموعة متنوعة من برامج تشغيل UEFI الأخرى التي يمكنها التفاعل مع المكونات المادية والتحقق من وجود أخطاء بها.

recoveryOS على الإنترنت وبيئات التشخيص

إذا حدث خطأ في تشغيل الاسترداد المحلي أو بيئات التشخيص، يحاول برنامج UEFI الثابت تنزيل الصور من الإنترنت بدلاً من ذلك. (يمكن للمستخدم أيضًا أن يطلب جلب الصور من الإنترنت بشكل خاص باستخدام تسلسلات المفاتيح الخاصة المحفوظة عند التمهيد.) يتم إجراء التحقق من تكامل صور القرص وقوائم chunklists التي يتم تنزيلها من خادم استرداد نظام التشغيل بنفس الطريقة المتبعة مع الصور المُستردة من جهاز تخزين.

على الرغم من أن الاتصال بخادم استرداد نظام التشغيل يتم باستخدام HTTP، إلا أن المحتويات الكاملة التي يتم تنزيلها تظل خاضعة لعملية التحقق من تكاملها كما هو موضح سابقًا، وبالتالي تكون محمية ضد تلاعب أي مهاجم يتحكم في الشبكة. في حالة فشل جزء فردي في تخطي التحقق من التكامل، يُطلب مرة أخرى من خادم استرداد نظام التشغيل 11 مرة، قبل التخلي عنه وعرض الخطأ.

عندما تمت إضافة أنماط الاسترداد على الإنترنت والتشخيص إلى أجهزة كمبيوتر Mac في عام 2011، تقرر أنه من الأفضل استخدام عملية نقل أبسط عبر HTTP ومعالجة مصادقة المحتوى باستخدام آلية chunklist، بدلاً من تنفيذ وظيفة HTTPS الأكثر تعقيدًا في برنامج UEFI الثابت وبالتالي زيادة أجزاء البرنامج الثابت المعرضة للهجوم.

أمن وحدة تخزين النظام

بالنسبة إلى macOS 10.15، قدمت Apple وحدة تخزين نظام للقراءة فقط، وهي وحدة تخزين مخصصة ومعزولة لمحتوى النظام. يضيف macOS 11 أو أحدث حماية تشفير قوية إلى محتوى النظام باستخدام **وحدة تخزين نظام مُوقّعة (SSV)**. يتميز SSV بآلية kernel تتحقق من تكامل محتوى النظام في وقت التشغيل، وترفض أي بيانات -سواءً كانت تعليمات برمجية أو غيرها- بدون توقيع تشفير صالح من Apple. بدءًا من iOS 15 و iPadOS 15، تحصل أيضًا وحدة تخزين النظام على iPhone أو iPad على حماية تشفير لوحدة تخزين النظام الموقَّعة.

يساعد SSV في منع العبث بأي برنامج من برامج Apple يمثل جزءًا من نظام التشغيل، ويجعل أيضًا تحديث برامج macOS أكثر موثوقية وأكثر أمانًا. ولأن SSV يستخدم لقطات APFS (نظام ملفات Apple)، يمكن استعادة إصدار النظام القديم دون إعادة التثبيت إذا تعذر إجراء تحديث.

منذ طرح APFS، عمل على توفير تكامل بيانات تعريف نظام الملفات باستخدام مجاميع اختبارية غير مشفرة على جهاز التخزين الداخلي. يعزز SSV آلية التكامل عن طريق إضافة تجزئات التشفير، ومن ثم توسيعها لتشمل كل بايت من بيانات الملف. تتم تجزئة البيانات من جهاز التخزين الداخلي (بما في ذلك بيانات تعريف نظام الملفات) بشكل مشفر في مسار القراءة، ثم تتم مقارنة التجزئة بقيمة متوقعة في بيانات تعريف نظام الملفات. في حالة عدم التطابق، يفترض النظام أن البيانات قد تم التلاعب بها، ولن يُعيدها إلى البرنامج الذي يطلبها.

يتم تخزين كل تجزئة SSV SHA256 في شجرة بيانات تعريف نظام الملفات الرئيسي، والتي تكون مجزأةً بحد ذاتها. ولأن كل عقدة في الشجرة تتحقق بشكل متكرر من تكامل تجزئات فروعها—على غرار شجرة التجزئة الثنائية (Merkle)—فإن قيمة تجزئة عقدة الجذر، تسمى **الختم**، تشمل كل بايت من البيانات في SSV، ما يعني أن التوقيع المشفر يغطي وحدة تخزين النظام بالكامل.

أثناء تثبيت macOS وتحديثه، تتم إعادة حوسبة الختم من نظام الملفات على الجهاز ويتم التحقق من هذا القياس مقابل القياس الموقَّع من Apple. على أجهزة كمبيوتر Mac المزودة بسيليكون Apple، يتحقق مُحمّل التمهيد من الختم قبل نقل التحكم إلى kernel. على أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة Apple T2 أمنية، يقوم مُحمّل التمهيد بإعادة توجيه القياس والتوقيع إلى kernel، والذي يتحقق بعد ذلك من الختم مباشرةً قبل تثبيت نظام الملفات الجذر. في كلتا الحالتين، إذا فشل التحقق، ستتوقف عملية بدء التشغيل، وسيُطلب من المستخدم إعادة تثبيت macOS. يتكرر هذا الإجراء في كل عملية تمهيد إلا إذا اختار المستخدم الدخول في وضع تأمين أقل من حيث المستوى وقرّر بشكل منفصل تعطيل وحدة تخزين النظام المُوقّعة.

أثناء تحديثات برامج iOS و iPadOS، يتم إعداد وحدة تخزين النظام وإعادة حوسبتها بطريقة مماثلة. تتحقق مُحمّلات إقلاع iOS و iPadOS من سلامة الختم وكونه مطابقًا لقيمة موقَّعة من Apple قبل السماح للجهاز ببدء تشغيل kernel. تدفع حالات عدم التطابق أثناء التمهيد المستخدم لتحديث برنامج النظام على الجهاز. لا يُسمح للمستخدمين بتعطيل حماية وحدة تخزين نظام موقَّعة على iOS و iPadOS.

SSV وتوقيع التعليمات البرمجية

ما يزال توقيع التعليمات البرمجية موجودًا ويتم فرضه بواسطة kernel. تقوم وحدة تخزين النظام المُوقّعة بتوفير الحماية عند قراءة أي بايت على الإطلاق من جهاز التخزين الداخلي. بينما يوفر توقيع التعليمات البرمجية الحماية عندما يتم تعيين كائنات Mach في الذاكرة على أنها قابلة للتنفيذ. يعمل كل من SSV وتوقيع التعليمات البرمجية على حماية التعليمات البرمجية القابلة للتنفيذ على جميع مسارات القراءة والتنفيذ.

SSV وخزنة الملفات

في macOS 11 أو أحدث، يوفر SSV حماية مكافئة لمحتوى النظام أثناء عدم النشاط، وبالتالي لم تعد وحدة تخزين النظام بحاجة إلى أن تكون مشفرة. سيكتشف نظام الملفات أي تعديلات يتم إجراؤها على نظام الملفات أثناء عدم نشاطه عند قراءتها. إذا شغَّل المستخدم خزنة الملفات، فإن محتوى المستخدم في وحدة تخزين البيانات يظل مشفرًا بسر يوفره المستخدم.

إذا اختار المستخدم تعطيل SSV، يصبح النظام عرضة للعبث أثناء عدم نشاطه، ويمكن لهذا التلاعب أن يُمكّن المهاجم من استخراج بيانات المستخدم المُشفّرة عند بدء تشغيل النظام التالي. لذلك، لن يسمح النظام للمستخدم بتعطيل SSV إذا كانت خزنة الملفات قيد التشغيل. ويجب تمكين الحماية أثناء عدم النشاط أو تعطيلها لكلتا وحدتي التخزين بطريقة متسقة.

في macOS 10.15 أو أقدم، يحمي خزنة الملفات برامج نظام التشغيل أثناء عدم نشاطها عن طريق تشفير محتوى المستخدم والنظام بمفتاح محمي بواسطة سر يحدده المستخدم. وهذا يحمي من المهاجم الذي لديه وصول مادي إلى الجهاز من الوصول إلى نظام الملفات الذي يحتوي على برامج النظام أو تعديله بشكل فعال.

SSV و Mac مزودة بشريحة Apple T2 أمنية

على أجهزة كمبيوتر Mac المزودة بشريحة Apple T2 أمنية، لا يحمي SSV سوى macOS نفسه فقط. بينما البرنامج الذي يتم تشغيله على شريحة T2 ويتحقق من macOS يكون محميًا بواسطة التمهيد الآمن.

تحديثات البرامج الآمنة

الأمن مجرد عملية؛ ولا يكفي التمهيد الموثوق لإصدار نظام التشغيل المُثبّت في المصنع، بل يجب أيضًا وجود آلية للحصول على آخر تحديثات الأمن بسرعة وأمان. تصدر Apple تحديثات البرامج بانتظام لمعالجة الدواعي الأمنية الناشئة. يتلقى مستخدمو أجهزة iPhone و iPad إشعارات التحديث على الجهاز. يجد مستخدمو Mac التحديثات المتوفرة في إعدادات النظام (macOS 13 أو أحدث) أو تفضيلات النظام (macOS 12 أو أقدم). يتم تسليم التحديثات لاسلكيًا من أجل الاعتماد السريع لأحدث الإصلاحات الأمنية.

أمن عملية التحديث

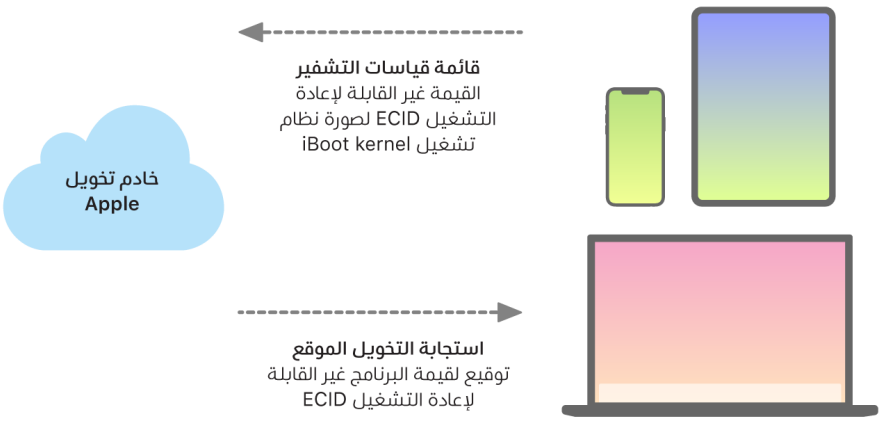
تستخدم عملية التحديث نفس جذر الثقة المستند إلى المكونات المادية الذي يستخدمه التمهيد الآمن المصمم لتثبيت التعليمات البرمجية الموقعة من Apple فقط. تستخدم عملية التحديث أيضًا تخويل برامج النظام للتحقق من عدم تثبيت سوى نُسخ إصدارات نظام التشغيل التي يتم توقيعها بفعالية من قِبل Apple على أجهزة iPhone و iPad أو أجهزة كمبيوتر Mac التي تم تكوين إعداد التأمين الكامل عليها كسياسة للتمهيد الآمن في أداة أمن بدء التشغيل. مع وجود هذه العمليات الآمنة في مكانها الصحيح، تستطيع Apple منع التوقيع على إصدارات أقدم من أنظمة التشغيل ذات ثغرات معروفة، وبالتالي المساعدة في منع هجمات الإرجاع إلى إصدار أقدم.

للحصول على مزيد من الأمن لتحديث البرامج، عندما يكون الجهاز المطلوب ترقيته متصلاً فعليًا بالـ Mac، يتم تنزيل نسخة كاملة من iOS أو iPadOS وتثبيتها. ولكن بالنسبة لتحديثات البرامج عبر الأثير (OTA)، **لا يتم تنزيل إلا المكونات المطلوبة لإكمال التحديث فقط**، مما يؤدي إلى تحسين كفاءة الشبكة من خلال عدم تنزيل نظام التشغيل بالكامل. يمكن تخزين تحديثات البرامج مؤقتًا على أي Mac مثبت عليه macOS 10.13 أو أحدث مع تشغيل ميزة التخزين المؤقت للمحتوى، بحيث لا تحتاج أجهزة iPhone و iPad إلى إعادة تنزيل التحديث الضروري عبر الإنترنت. (يظل لزامًا عليها الاتصال بخوادم Apple لإكمال عملية التحديث.)

عملية التحديث المخصصة

أثناء الترقيات والتحديثات، يتم توفير بعض المعلومات لخادم تخويل تثبيت Apple الذي يتضمن قائمة من قياسات التشفير لكل جزء من حزمة التثبيت المطلوب تثبيتها (على سبيل المثال، iBoot و kernel وصورة نظام التشغيل) وقيمة عشوائية غير قابلة لإعادة التشغيل ومعرف الشريحة الحصري (ECID) الفريد للجهاز.

يتحقق خادم التخويل من قائمة القياسات المقدَّمة مقابل الإصدارات التي يُسمح لها بقبول التثبيت، ويضيف ECID إلى القياس ويوقّع النتيجة إذا وجد مطابقة. ويمرر الخادم مجموعة كاملة من البيانات الموقَّعة إلى الجهاز كجزء من عملية الترقية. تؤدي إضافة ECID إلى "تخصيص" تخويل الجهاز الطالب. من خلال التخويل والتوقيع للقياسات المعروفة فقط، يضمن الخادم أن يتم التحديث تمامًا كما قدمته Apple.



يتحقق تقييم سلسلة الثقة في وقت التمهيد من أن التوقيع يأتي من Apple وأن قياس العنصر الذي يتم تحميله من جهاز التخزين، مُدمجًا مع ECID الخاص بالجهاز، يطابق ما يُغطيه التوقيع. تم تصميم هذه الخطوات لتضمن أنه على الأجهزة التي تدعم التخصيص، يكون التخويل لجهاز معين وأن نظام تشغيل أقدم من إصدار البرنامج الثابت من جهاز ما لا يمكن نسخه إلى جهاز آخر. تساعد القيمة غير القابلة لإعادة التشغيل على منع المهاجم من حفظ استجابة الخادم واستخدامها للعبث بجهاز أو تغيير برامج النظام بطريقة أخرى.

إن عملية التخصيص هي السبب وراء ضرورة اتصال الشبكة بشركة Apple دائمًا لتحديث أي جهاز مزود بسيليكون Apple، بما في ذلك أجهزة كمبيوتر Mac المستندة إلى Intel المزودة بشريحة Apple T2 الأمنية.

على الأجهزة التي تتضمن Secure Enclave، يستخدم هذا المكون المادي تخويل برامج النظام بطريقة مماثلة للتحقق من تكامل برامجه والمساعدة على منع عمليات تثبيت إصدار أقدم.

تكامل نظام التشغيل

تم تصميم برامج أنظمة التشغيل في Apple مع توفير الأمان في صميمها. يتضمن هذا التصميم جذرًا للثقة في المكونات المادية - تم تعزيزه لتمكين التمهيد الآمن - وعملية تحديث برامج آمنة تتميز بالسرعة والأمان. تستخدم أنظمة التشغيل في Apple أيضًا إمكانات المكونات المادية المزودة بالسيليكون المصممة لهذا الغرض للمساعدة في منع الاستغلال أثناء تشغيل النظام. تعمل ميزات وقت التشغيل هذه على حماية سلامة التعليمات البرمجية الموثوق بها أثناء التنفيذ. وباختصار، فإن برامج أنظمة التشغيل في Apple تساعد في الحد من الهجمات وتقنيات الاستغلال سواء كانت ناشئة عن تطبيق ضار أو من الويب أو من خلال أي قناة أخرى. تتوفر وسائل الحماية المذكورة هنا على الأجهزة التي تحتوي على أنظمة SoC المصمم بواسطة Apple المدعوم، بما في ذلك iOS و iPadOS و tvOS و watchOS والآن macOS على Mac مزود برقاقات Apple.

الميزة	A10	A11, S3	A12 و A13 و A14 و S4 إلى S9	A15 و A16 و A17	M1 و M2 و M3
حماية تكامل Kernel	✓	✓	✓	✓	✓
قيود الأذونات السريعة	✗	✓	✓	✓	✓
حماية تكامل المعالج الثانوي للنظام	✗	✗	✓	✓	✓
رموز مصادقة المؤشر	✗	✗	✓	✓	✓
طبقة حماية الصفحة	✗	✓	✓	✓	✗ راجع الملاحظة 1 أدناه.
Secure Page Table Monitor	✗	✗	✗	✓ راجع الملاحظة 2 أدناه.	✗

الملاحظة 1: تتطلب طبقة حماية الصفحة (PPL) تنفيذ النظام الأساسي للتعليمات البرمجية المُوقّعة والموثوق بها **فقط**، وهذا نموذج أمن لا ينطبق على macOS.

الملاحظة 2: Secure Page Table Monitor (SPTM) مدعوم على A15 و A16 و A17 ويُستخدَم بدلًا من طبقة حماية الصفحة على الأنظمة الأساسية المدعومة.

حماية تكامل Kernel

بعد اكتمال تهيئة مكونات kernel في نظام التشغيل، يتم تمكين حماية تكامل Kernel (KIP) للمساعدة على منع تعديلات kernel والتعليمات البرمجية لبرنامج التشغيل. توفر وحدة تحكم الذاكرة منطقة ذاكرة فعلية محمية يستخدمها iBoot لتحميل kernel وملحقات kernel. بعد اكتمال بدء التشغيل، ترفض وحدة تحكم الذاكرة الكتابة إلى منطقة الذاكرة الفعلية المحمية. ويتم تكوين وحدة إدارة الذاكرة (MMU) الخاصة بمعالج التطبيقات للمساعدة على منع تعيين التعليمات البرمجية المميزة من الذاكرة الفعلية خارج منطقة الذاكرة المحمية وللمساعدة على منع تعيينات الذاكرة الفعلية القابلة للكتابة داخل منطقة ذاكرة kernel.

لمنع إعادة التكوين، يتم قفل المكونات المادية المستخدمة لتمكين KIP بعد اكتمال عملية التمهيد.

قيود الأذونات السريعة

بدءًا من شريحة بايونك A11 من Apple و S3 SoCs، تم تقديم مجموعة أولية جديدة للمكونات المادية. تتضمن قيود الأذونات السريعة الأولية هذه سجل وحدة معالجة مركزية يقيّد الأذونات لكل سلسلة بسرعة. باستخدام قيود الأذونات السريعة (المعروفة أيضًا باسم سجلات APRR)، يمكن لأنظمة التشغيل المدعومة إزالة أذونات التنفيذ من الذاكرة دون تكلفة إضافية لاستدعاء النظام وتمرير صفحة من الجدول أو محاذاتها. توفر هذه السجلات مستوى إضافيًا للحد من الهجمات من الويب، خاصةً بالنسبة إلى التعليمات البرمجية التي يتم تجميعها في وقت التشغيل (يتم تجميعها في الوقت المحدد تمامًا) - لأن الذاكرة لا يمكن تنفيذها بفاعلية في الوقت نفسه الذي تجري فيه القراءة منها والكتابة إليها.

حماية تكامل المعالج الثانوي للنظام

يتعامل البرنامج الثابت الخاص بالمعالج الثانوي مع العديد من مهام النظام الهامة — على سبيل المثال، Secure Enclave ومعالج مستشعر الصور ومعالج الحركة الثانوي. وبالتالي يعد أمنه جزءًا أساسيًا من أمن النظام ككل. لمنع تعديل البرامج الثابتة للمعالج الثانوي، تستخدم Apple آلية تسمى **حماية تكامل المعالج الثانوي للنظام (SCIP)**.

تعمل SCIP بطريقة تشبه كثيرًا حماية تكامل Kernel (KIP): في وقت التمهيد، يقوم iBoot بتحميل البرنامج الثابت لكل معالج ثانوي في منطقة ذاكرة محمية، وهي منطقة محجوزة ومنفصلة عن منطقة KIP. ثم يقوم iBoot بتكوين وحدة ذاكرة كل معالج ثانوي للمساعدة على منع:

- التعيينات القابلة للتنفيذ خارج الجزء الخاص به من منطقة الذاكرة المحمية
- التعيينات القابلة للكتابة داخل الجزء الخاص به من منطقة الذاكرة المحمية

أيضًا في وقت التمهيد، لتكوين SCIP لـ Secure Enclave، يتم استخدام نظام تشغيل Secure Enclave. بعد اكتمال عملية التمهيد، يتم قفل المكونات المادية المستخدمة لتمكين SCIP. وقد تم تصميم ذلك لمنع إعادة التكوين.

رموز مصادقة المؤشر

تُستخدم رموز مصادقة المؤشر (PACs) للحماية من استغلال أخطاء تلف الذاكرة. وتستخدم برامج النظام والتطبيقات المضمنة PAC للمساعدة على منع تعديل مؤشرات الوظائف وعناوين الإرجاع (مؤشرات التعليمات البرمجية). يستخدم PAC خمس قيم 128 بت سرية للتوقيع على تعليمات وبيانات kernel، وتوجد لكل عملية في مساحة المستخدم مفاتيح B الخاصة بها. وتكون العناصر عشوائية وموقَّعة كما هو موضح أدناه.

العنصر	المفتاح	القيمة العشوائية
Function Return Address	IB	عنوان التخزين
Function Pointers	IA	0
Block Invocation Function	IA	عنوان التخزين
Objective-C Method Cache	IB	عنوان التخزين + الفئة + المحدِّد
C++ V-Table Entries	IA	عنوان التخزين + التجزئة (اسم أسلوب مشوّه)
Computed Goto Label	IA	التجزئة (اسم الوظيفة)
Kernel Thread State	GA	٠
User Thread State Registers	IA	عنوان التخزين
C++ V-Table Pointers	DA	0

يتم تخزين قيمة التوقيع في وحدات بت المساحة المتروكة غير المستخدمة في الجزء العلوي من مؤشر 64 بت. ويتم التحقق من التوقيع قبل الاستخدام، وتتم استعادة المساحة المتروكة للمساعدة على ضمان الحصول على عنوان مؤشر يعمل بكفاءة. ويؤدي عدم نجاح التحقّق إلى إحباط العملية. يزيد هذا التحقق من الصعوبة التي تواجه العديد من الهجمات، مثل هجوم البرمجة الموجهة للإرجاع (ROP)، الذي يحاول خداع الجهاز لتنفيذ التعليمات البرمجية الموجودة بشكل ضار من خلال معالجة عناوين إرجاع الوظائف المخزنة على المكدس.

طبقة حماية الصفحة

تم تصميم طبقة حماية الصفحة (PPL) في iOS و iPadOS و watchOS لمنع تعديل التعليمات البرمجية لمساحة المستخدم بعد اكتمال التحقق من توقيع التعليمات البرمجية. وبناءً على حماية تكامل Kernel وقيود الأذونات السريعة، تُدير PPL تجاوزات أذونات جداول الصفحات للتأكد من أن PPL وحدها يمكنها تغيير الصفحات المحمية التي تحتوي على تعليمات المستخدم البرمجية وجداول الصفحات. يوفر النظام انخفاضًا كبيرًا في عدد الأجزاء المعرضة للهجوم من خلال دعم فرض تكامل التعليمات البرمجية على مستوى النظام، حتى في مواجهة kernel مخترقة. لا تتوفر هذه الحماية في macOS لأن PPL تنطبق فقط على الأنظمة التي يجب أن يتم فيها توقيع جميع التعليمات البرمجية المنفذة.

Secure Page Table Monitor و Trusted Execution Monitor

صُمِّم كلٌّ من Secure Page Table Monitor (SPTM) و Trusted Execution Monitor (TXM) للعمل معًا للمساعدة في منع إجراء تعديل على جداول الصفحات لعمليات كلٍّ من المستخدم و kernel، حتى عندما يكون لدى المهاجمين إمكانات الكتابة في kernel ويمكنهم تجاوز حماية تدفق التحكم. ينفِّذ SPTM ذلك عن طريق استخدام مستوى امتياز أعلى من kernel، واستخدام TXM بمستوى امتياز أقل لإنفاذ السياسات التي تحكم تنفيذ التعليمات البرمجية فعليًا. صُمِّم هذا النظام بحيث لا تتحول تسوية TXM تلقائيًا إلى تجاوز SPTM بسبب فصل الامتيازات وإدارة الثقة بينهما. في أنظمة SOC لدى A15 و A16 و A17، يُستخدم SPTM (مع TXM) بدلاً من PPL، ما يعمل على تقليل الأجزاء المعرضة للهجوم ومن دون الاعتماد على ثقة kernel، حتى خلال تمهيد مبكر. يعتمد SPTM أيضًا على أوليات الرقاقات الجديدة التي تمثل تطورًا لقيود الأذونات السريعة التي تستخدمها PPL.

تنشيط اتصالات البيانات بشكل آمن

على أجهزة iPhone و iPad وأجهزة كمبيوتر Mac، في حالة عدم إنشاء اتصال بيانات مؤخرًا، يجب على المستخدمين استخدام بصمة الوجه أو بصمة الإصبع أو رمز دخول لتنشيط اتصالات البيانات عبر واجهة ثندربولت أو USB أو لايتننغ أو USB أو الموصل الذكي، أو — في macOS 13.3 أو أحدث — البطاقات الرقمية ذات السعة الموسعة "SDXC". ويعمل هذا على تقييد الأجزاء المعرضة للهجوم في الأجهزة المتصلة فعليًا مثل أجهزة الشحن الضارة مع الاستمرار في تمكين استخدام الملحقات الأخرى ضمن قيود زمنية معقولة. إذا مر مدة تزيد عن ساعة منذ قفل iPhone أو iPad منذ انتهاء اتصال بيانات الملحق، فلن يسمح الجهاز بإنشاء أي اتصالات بيانات جديدة حتى يتم فتح قفل الجهاز. وخلال فترة الساعة هذه، لن يتم السماح إلا باتصالات البيانات من الملحقات التي تم توصيلها سابقًا بالجهاز أثناء وجوده في حالة فتح القفل. يتم تذكر هذه الملحقات لمدة 30 يومًا بعد آخر مرة من اتصالها. ستؤدي المحاولات التي يجريها ملحق غير معروف لفتح اتصال بيانات خلال هذه الفترة إلى تعطيل جميع اتصالات بيانات الملحقات عبر هذه الاتصالات إلى أن يتم فتح قفل الجهاز مرة أخرى. فترة الساعة هذه:

- تساعد على ضمان ألا يضطر المستخدمون الذين يترددون على الاتصال بأي Mac أو PC أو ملحقات أو الربط سلكيًا بكاربلاي إلى إدخال رموز الدخول الخاصة بهم في كل مرة يقومون فيها بربط أجهزتهم
- تعد ضرورية لأن النظام البيئي الملحق لا يوفر طريقة موثوقة للتشفير لتحديد هوية الملحقات قبل إنشاء اتصال بيانات

بالإضافة إلى ذلك، إذا كان قد مر أكثر من 3 أيام منذ إنشاء اتصال بيانات بالملحق، فإن الجهاز لن يسمح باتصالات البيانات الجديدة بعد قفله. وهذا لزيادة الحماية للمستخدمين الذين لا يستخدمون مثل هذه الملحقات في كثير من الأحيان. يتم أيضًا تعطيل اتصالات البيانات هذه عندما يكون الجهاز في حالة يتطلب فيها رمز دخول لإعادة تمكين المصادقة البيومترية.

يمكن للمستخدم اختيار إعادة تمكين اتصالات البيانات دائمة التشغيل في الإعدادات (إعداد بعض الأجهزة المساعدة يقوم بذلك تلقائيًا).

التحقق من الملحقات في iPhone و iPad

يوفر برنامج ترخيص Made for iPhone و iPad (MFi)لجهات تصنيع الملحقات المعتمدة إمكانية الوصول إلى بروتوكول ملحقات iPod (iAP) والمكونات المادية الداعمة اللازمة.

عندما يتصل ملحق Made for iPhone (MFi) بـ iPhone أو iPad، يجب أن يثبت الملحق لشركة Apple أنه معتمد. (يحدث اتصال الجهاز الملحق باستخدام ثندربولت أو لايتننغ أو Bluetooth أو—لأجهزة محددة—USB-C.) باعتبارها دليلاً على المصادقة، يرسل الملحق شهادة مقدمة من Apple إلى الجهاز، ثم يتحقق الجهاز منها بعد ذلك. ثم يُرسل الجهاز تحديًا يجب أن يجيب عليه الملحق باستجابة موقَّعة. وتتم معالجة هذه العملية بالكامل بواسطة دائرة متكاملة (IC) مخصصة توفرها Apple لجهات تصنيع الملحقات المعتمدة وتكون شفافة بالنسبة للملحق نفسه.

يمكن أن تطلب ملحقات MFi تم التحقق منها إمكانية الوصول إلى طرق النقل والوظائف المختلفة؛ على سبيل المثال، الوصول إلى تدفقات الصوت الرقمية عبر كبل ثندربولت أو معلومات الموقع المتوفرة عبر Bluetooth. تم تصميم الدائرة المتكاملة للمصادقة للمساعدة على ضمان عدم منح حق الوصول الكامل إلى الجهاز إلا لملحقات MFi المعتمدة فقط. وإذا كان الملحق لا يدعم المصادقة، فإن وصوله يقتصر على الصوت التناظري ومجموعة فرعية صغيرة من عناصر التحكم في تشغيل الصوت التسلسلي (UART).

تستخدم البث السريع أيضًا الدائرة المتكاملة للمصادقة بغرض التحقق من اعتماد Apple لأجهزة الاستقبال. تستخدم تدفقات صوت البث السريع وفيديو كاربلاي بروتوكول MFi-SAP (بروتوكول الارتباط الآمن)، الذي يشفر الاتصال بين الملحق والجهاز باستخدام AES128 في نمط العداد (CTR). ويتم تبادل المفاتيح سريعة الزوال باستخدام تبادل مفاتيح ECDH (Curve25519) وتوقيعها باستخدام مفتاح RSA سعة 1024 بت الخاص بالدائرة المتكاملة للمصادقة كجزء من بروتوكول محطة إلى محطة (STS).

BlastDoor للرسائل والمعرفات

تتضمن أنظمة iOS و iPadOS و macOS و watchOS ميزة أمنية تسمى **BlastDoor**، تم تقديمها للمرة الأولى في iOS 14 والإصدارات ذات الصلة. الهدف من BlastDoor هو المساعدة على حماية النظام عن طريق تقييد المهاجمين—ما يزيد من تعقيد جهودهم في استغلال الرسائل وخدمة الهوية من Apple (IDS). تعمل BlastDoor على عزل البيانات غير الموثوق بها التي تصل إلى الرسائل و IDS والمتجهات الأخرى وتحليلها وتحويل ترميزها والتحقق من صحتها للمساعدة على منع الهجمات.

وتقوم BlastDoor بذلك عن طريق توظيف قيود وضع الحماية والتحقق الآمن من مخرجات الذاكرة، ما يصنع عقبات كبيرة أمام المهاجمين للتغلب عليها قبل الوصول إلى أجزاء أخرى من نظام التشغيل. وهي مصممة لتحسين حماية المستخدم من الهجمات بشكل كبير، خصوصًا الهجمات "من دون نقرات"—تلك التي لا تتطلب تفاعل المستخدم.

وأخيرًا، يعامل تطبيق الرسائل حركة المرور من "المرسلين المعروفين" بشكل مختلف عن "المرسلين غير المعروفين"، ما يوفر مجموعة مختلفة من الوظائف لكل مجموعة وتقسيم البيانات "المعروفة" مقابل "غير المعروفة" إلى مثيلات BlastDoor فريدة.

أمن نمط المنع على أجهزة Apple

نمط المنع عبارة عن حماية اختيارية بدرجة كبيرة تم تصميمها لعدد قليل جدًا من الأفراد الذين قد تستهدفهم بعض التهديدات الرقمية الأكثر تطورًا مثل برامج التجسس المأجورة بشكل شخصي، بسبب هويتهم أو أعمالهم. لا تستهدف الهجمات من هذا النوع معظم الأشخاص أبدًا.

عند تشغيل نمط المنع، لا يعمل الجهاز بالطريقة المعتادة. لتقليل الأجزاء المعرضة للهجوم التي من الممكن استغلالها، تُفرض قيود صارمة على بعض التطبيقات والمواقع الإلكترونية والميزات لأسباب أمنية، وقد لا تتوفر بعض التجارب على الإطلاق.

يتوفر نمط المنع على iOS 16 و iPadOS 16 و macOS 13 و watchOS 10 أو أحدث. تتوفر وسائل حماية إضافية على iOS 17 و iPadOS 17 و macOS 14 والتحديثات في watchOS 10.1 أو أحدث. للاستفادة من الميزات الإضافية لنمط المنع، يجب تحديث الأجهزة إلى أحدث نظام تشغيل. لمزيد من المعلومات، انظر مقال دعم Apple نبذة عن نمط المنع.

يجري نمط المنع مقايضات لتوفير أمن أفضل على حساب الوظيفة أو الأداء أو كليهما. تؤثر هذه المقايضات في الآتي:

- خدمات الخلفية
- الاتصال
- إدارة الجهاز
- فيس تايم
- GameCenter
- البريد
- الرسائل
- الصور
- سفاري
- إعدادات النظام
- WebKit

الإمكانات الإضافية لأمن الأنظمة في macOS

الإمكانات الإضافية لأمن الأنظمة في macOS

يعمل macOS على مجموعة أوسع من المكونات المادية (على سبيل المثال، وحدات المعالجة المركزية المستندة إلى Intel، ووحدات المعالجة المركزية المستندة إلى Intel والمزودة بشريحة Apple T2 الأمنية، ووحدات SoC المزودة بسيليكون Apple)، كما يدعم مجموعة من حالات استخدام الحوسبة ذات الأغراض العامة. بينما يكتفي بعض المستخدمين باستخدام التطبيقات الأساسية المُثبتة مسبقًا فقط أو تلك المتوفرة من App Store، يمثّل الآخرون المتسللين إلى kernel الذين يحتاجون إلى تعطيل جميع وسائل حماية النظام الأساسي بصورة أساسية حتى يتمكنوا من تشغيل واختبار التعليمات البرمجية الخاصة بهم أثناء تنفيذها بأعلى مستويات الثقة. ويقع معظمهم في مكان ما في الوسط، بينما العديد منهم لديهم أجهزة طرفية وبرامج تتطلب مستويات مختلفة من الوصول. صممت Apple نظام macOS الأساسي من خلال منهج متكامل للمكونات المادية والبرامج والخدمات - نظام أساسي يوفر الأمن حسب التصميم ويسهّل التكوين والنشر والإدارة، مع الحفاظ على قابلية التكوين التي يتوقعها المستخدمون. ويتضمن macOS أيضًا تقنيات الأمن الرئيسية التي يحتاجها متخصصو تقنية المعلومات للمساعدة في حماية بيانات الشركة والاندماج في بيئات الشبكات المؤسسية الآمنة.

توفر الإمكانات التالية الدعم والمساعدة لتأمين الاحتياجات المتنوعة لمستخدمي macOS. وتتضمن:

- أمن وحدة تخزين النظام
- حماية تكامل النظام
- ذاكرات التخزين المؤقتة الموثوق بها
- حماية الأجهزة الطرفية
- دعم وأمن Rosetta 2 (الترجمة التلقائية) لأجهزة كمبيوتر Mac المزودة بسيليكون Apple
- دعم DMA ووسائل الحماية
- دعم وأمن ملحقات Kernel (kext)
- دعم وأمن ROM الاختياري
- أمن البرنامج الثابت لـ UEFI على أجهزة كمبيوتر Mac المستندة إلى Intel

حماية تكامل النظام

يستخدم macOS أذونات kernel للحد من إمكانية الكتابة في ملفات النظام المهمة باستخدام ميزة تسمى **حماية تكامل النظام (SIP)**. وتكون تلك الميزة منفصلة وبجانب ميزة حماية تكامل Kernel (KIP) المستندة إلى المكونات المادية المتوفرة على أجهزة كمبيوتر Mac المزودة بسيليكون Apple ، والتي تحمي تعديل kernel في الذاكرة. تتم الاستفادة من تقنية التحكم في الوصول الإلزامي لتوفير ذلك بالإضافة إلى عدد من وسائل الحماية الأخرى على مستوى kernel، بما في ذلك وضع الحماية ومخزن البيانات.

عناصر التحكم في الوصول الإلزامية

يستخدم macOS عناصر التحكم في الوصول الإلزامية—وهي سياسات تضع قيودًا أمنية، يتم إنشاؤها بواسطة المطور، ولا يمكن تجاوزها. ويختلف هذا النهج عن عناصر التحكم في الوصول الاختيارية، التي تتيح للمستخدمين تجاوز سياسات الأمن وفقًا لتفضيلاتهم.

لا تكون عناصر التحكم في الوصول الإلزامية مرئية للمستخدمين، لكنها تمثل التقنية الأساسية التي تساعد على تمكين العديد من الميزات المهمة، بما في ذلك وضع الحماية والإشراف العائلي والتفضيلات المُدارة والملحقات وحماية تكامل النظام.

حماية تكامل النظام

تعمل **حماية تكامل النظام** على تقييد المكونات لتكون للقراءة فقط في مواقع محددة مهمة في نظام الملفات للمساعدة على منع التعليمات البرمجية الضارة من تعديلها. حماية تكامل النظام عبارة عن إعداد خاص بالكمبيوتر يكون قيد التشغيل بشكل افتراضي عندما يقوم المستخدم بالترقية إلى OS X 10.11 أو أحدث. على Mac المستند إلى Intel، يؤدي تعطيله إلى إزالة الحماية لجميع الأقسام الموجودة على جهاز التخزين الفعلي. ويطبق macOS سياسة الأمن هذه على كل عملية يتم تشغيلها على النظام، بغض النظر عما إذا كان يتم تشغيلها في وضع الحماية أم بامتيازات إدارية.

ذاكرات التخزين المؤقتة الموثوق بها

تُعدّ ذاكرة التخزين المؤقت الموثوق بها الثابتة أحد الكائنات المضمنة في سلسلة التمهيد الآمن، وهي عبارة عن سجل موثوق به يضم جميع ثنائيات Mach-O التي يتم التحكم فيها في وحدة تخزين النظام المُوقَّعة. ويتم تمثيل كل Mach-O بتجزئة دليل تعليمات برمجية. للبحث الفعال، يتم فرز هذه التجزئات قبل إدراجها في ذاكرة التخزين المؤقت للثقة. دليل التعليمات البرمجية عبارة عن نتيجة عملية التوقيع التي يتم تنفيذها بواسطة `codesign(1)`. لفرض ذاكرة التخزين المؤقت للثقة، يجب أن يظل SIP ممكّنًا. لتعطيل فرض ذاكرة التخزين المؤقت للثقة على Mac مزود بسيليكون Apple، يجب تكوين التمهيد الآمن إلى التأمين الأقل تقييدًا.

عند تنفيذ ملف ثنائي (سواء كجزء من إنتاج عملية جديدة أو تعيين تعليمة برمجية قابلة للتنفيذ في عملية موجودة)، يتم استخراج دليل التعليمات البرمجية الخاص به وتجزئته. إذا تم العثور على التجزئة الناتجة في ذاكرة التخزين المؤقت الموثوق بها، فسيتم منح التعيينات القابلة للتنفيذ التي تم إنشاؤها للملف الثنائي امتيازات النظام الأساسي، أي أنها قد تمتلك أي استحقاق ويتم تنفيذها دون إجراء مزيد من التحقق من صحة التوقيع. وهذا على النقيض من أجهزة كمبيوتر Mac المستندة إلى Intel، حيث يتم نقل امتيازات النظام الأساسي إلى محتوى نظام التشغيل بواسطة شهادة Apple التي توقّع على الملفات الثنائية. (لا تُقيّد هذه الشهادة أي استحقاقات قد يمتلكها الملف الثنائي.)

يجب أن تحتوي الملفات الثنائية غير المرتبطة بالنظام الأساسي (على سبيل المثال، التعليمات البرمجية التابعة لجهات خارجية موثوقة) على سلاسل شهادات صالحة لتنفيذها، كما أن الاستحقاقات التي قد تمتلكها تكون مُقيّدة بملف تعريف التوقيع الصادر عن برنامج Apple Developer Program إلى المطور.

يتم توقيع كل الملفات الثنائية الواردة مع macOS باستخدام **معرّف نظام أساسي**. في Mac المزود برقاقات Apple، يُستخدم هذا المعرّف للإشارة إلى أنه على الرغم من توقيع Apple على الملف الثنائي، إلا أن تجزئة دليل التعليمات البرمجية يجب أن تكون موجودة في ذاكرة التخزين المؤقت الموثوقة لتنفيذها. وفي أجهزة كمبيوتر Mac المستندة إلى Intel، يُستخدم معرّف النظام الأساسي لتنفيذ عملية إبطال مستهدفة لثنائيات من إصدار أقدم من macOS؛ ويساعد هذا الإلغاء المستهدف على منع تنفيذ هذه الثنائيات على الإصدارات الأحدث.

تقوم ذاكرة التخزين المؤقت الموثوق بها الثابتة بقفل مجموعة من الثنائيات بشكل كامل إلى إصدار معين من macOS. ويساعد هذا السلوك على منع إدخال الثنائيات المُوقَّعة من قِبَل Apple بشكل شرعي من أنظمة التشغيل القديمة إلى أنظمة تشغيل أحدث لتمكين المهاجم من اكتساب المزايا.

تعليمات النظام الأساسي البرمجية الواردة من خارج نظام التشغيل

تُجري Apple تثبيتًا مسبقًا لبعض الثنائيات التي يتم توقيعها بمعرّف نظام أساسي — على سبيل المثال، Xcode ومجموعة أدوات التطوير. وحتى مع ذلك، ما يزال مسموحًا بتنفيذها مع وجود امتيازات النظام الأساسي على أجهزة Mac المزودة برقاقات Apple وتلك المزودة بشريحة T2. نظرًا لأنه يتم تثبيت برنامج النظام الأساسي هذا مسبقًا بشكل مستقل عن macOS، فإنه لا يخضع لسلوكيات الإلغاء التي تفرضها ذاكرة التخزين المؤقت الموثوق بها الثابتة.

ذاكرات التخزين المؤقتة الموثوق بها القابلة للتحميل

تُجري Apple تثبيتًا مسبقًا لحِزم برامج معينة مع **ذاكرات تخزين مؤقتة موثوق بها قابلة للتحميل**. وتحتوي ذاكرات التخزين المؤقتة هذه على نفس بنية البيانات الموجودة لدى ذاكرة التخزين المؤقتة الموثوق بها الثابتة. ولكن على الرغم من وجود ذاكرة تخزين مؤقتة موثوق بها ثابتة واحدة، ويتم ضمان قفل محتوياتها دائمًا في نطاقات للقراءة فقط بعد اكتمال التهيئة المبكرة لملحق kernel، تُضاف ذاكرات التخزين المؤقتة الموثوق بها القابلة للتحميل إلى النظام في وقت التشغيل.

تتم مصادقة ذاكرات التخزين المؤقتة الموثوق بها هذه إما من خلال نفس الآلية التي تصادق على البرامج الثابتة للتمهيد (التخصيص باستخدام خدمة التوقيع الموثوق به من Apple) أو كائنات مُوقَّعة عالميًا (لا تربطها توقيعاتها بجهاز معين).

مثال على ذاكرة التخزين المؤقتة الموثوق بها المخصصة هي ذاكرة التخزين المؤقتة المثبتة مسبقًا مع صورة القرص المستخدمة لإجراء تشخيصات ميدانية على أجهزة كمبيوتر Mac المزودة بسيليكون Apple. يتم تخصيص ذاكرة التخزين المؤقت الموثوق بها هذه، إلى جانب صورة القرص، ويتم تحميلها إلى kernel الخاص بكمبيوتر Mac المحدد أثناء تمهيده في وضع التشخيص. وتتيح ذاكرة التخزين المؤقتة الموثوق بها تشغيل البرامج داخل صورة القرص في وجود امتياز النظام الأساسي.

يتم توفير مثال لذاكرة التخزين المؤقتة الموثوق بها المُوقَّعة عالميًا مع تحديثات برامج macOS. تسمح ذاكرة التخزين المؤقتة الموثوق بها هذه بتشغيل جزء من التعليمات البرمجية ضمن تحديث البرامج—**مذ التحديث**—في وجود امتياز النظام الأساسي. يقوم مذ التحديث بإجراء أي عمل لتنظيم مراحل تحديث البرامج لأن النظام المضيف يفتقر إلى القدرة على الأداء بطريقة متسقة عبر الإصدارات.

أمن معالج الجهاز الطرفي في أجهزة كمبيوتر Mac

تحتوي جميع أنظمة الحوسبة الحديثة على العديد من معالجات الأجهزة الطرفية المضمنة المخصصة لمهام مثل الشبكات والرسومات وإدارة الطاقة والمزيد. غالبًا ما تكون معالجات الأجهزة الطرفية هذه أحادية الغرض وتكون أقل قوة بكثير من وحدة المعالجة المركزية الأساسية. وتصبح الأجهزة الطرفية المضمنة التي لا تنفّذ أمنًا كافيًا هدفًا سهلاً للمهاجمين الذين يسعون إلى أهداف أسهل لاستغلالها ثم إصابة نظام التشغيل إصابةً دائمةً. بعد إصابة البرنامج الثابت لأحد المعالجات الطرفية، يمكن للمهاجم استهداف البرامج على وحدة المعالجة المركزية الأساسية، أو التقاط البيانات الحساسة مباشرةً (على سبيل المثال، يمكن لجهاز إيثرنت رؤية محتويات الحِزم غير المشفرة).

تعمل Apple على تقليل عدد المعالجات الطرفية اللازمة وعلى تجنب التصميمات التي تتطلب برامج ثابتة، كلما أمكن ذلك. ولكن عندما تكون المعالجات المنفصلة مع برامجها الثابت مطلوبة، تُبذل الجهود للمساعدة على ضمان عدم قدرة المهاجم على إصابة هذا المعالج إصابةً دائمةً. يمكن أن يتم ذلك عن طريق التحقق من المعالج بإحدى طريقتين:

- تشغيل المعالج بحيث يقوم بتنزيل البرامج الثابتة التي يتم التحقق منها من وحدة المعالجة المركزية الأساسية عند بدء التشغيل
- ضمان قيام المعالج الطرفي بتنفيذ سلسلة التمهيد الآمن الخاصة به، للتحقق من البرنامج الثابت للمعالج الطرفي في كل مرة يبدأ فيها تشغيل الـ Mac

تعمل Apple مع الموردين لمراجعة عمليات التنفيذ لديهم، وتحسين تصميماتهم لتشمل الخصائص المطلوبة مثل:

- ضمان الحد الأدنى من نقاط قوة التشفير
- ضمان الإبطال الفعّال للبرامج الثابتة الضارة المعروفة
- تعطيل واجهات تصحيح الأخطاء
- توقيع البرنامج الثابت باستخدام مفاتيح التشفير المخزّنة في وحدات أمن المكونات المادية (HSMs) التي تتحكم فيها Apple

في السنوات الأخيرة، عملت Apple مع بعض الموردين الخارجيين لاعتماد نفس بُنى البيانات "Image4" ورمز التحقق والبنية الأساسية للتوقيع المستخدمة بواسطة سيليكون Apple.

عندما لا تكون عملية التشغيل الخالية من التخزين أو التخزين بالإضافة إلى التمهيد الآمن خيارًا، فإن التصميم يفرض أن يتم توقيع تحديثات البرامج الثابتة بشكل مشفر والتحقق منها قبل تحديث التخزين الثابت.

Rosetta 2 على Mac مزود بسيليكون Apple

يمكن لأجهزة كمبيوتر Mac المزودة بسيليكون Apple تشغيل التعليمات البرمجية التي يتم تجميعها لمجموعة التعليمات x86_64 باستخدام آلية ترجمة تسمى **Rosetta 2**. هناك نوعان من الترجمة المعروضة: في الوقت المناسب، وقبل الموعد.

الترجمة في الوقت المناسب

في قناة الترجمة في الوقت المناسب (JIT)، يتم تحديد كائن Mach x86_64 مبكرًا في مسار تنفيذ الصورة. عند مواجهة هذه الصور، ينقل kernel التحكم إلى كعب روتين ترجمة Rosetta خاصة بدلاً من محرر الروابط الديناميكي (`dyld(1)`. يقوم كعب روتين الترجمة بعد ذلك بترجمة صفحات x86_64 أثناء تنفيذ الصورة. تحدث هذه الترجمة بالكامل داخل العملية. ويظل kernel يتحقق من تجزئات التعليمات البرمجية لكل صفحة x86_64 مقابل توقيع التعليمات البرمجية المرفق بالملف الثنائي كما هو خاطئ. في حالة عدم تطابق التجزئة، يفرض kernel سياسة الإصلاح المناسبة لتلك العملية.

الترجمة قبل الموعد

في مسار الترجمة قبل الموعد (AOT)، تتم قراءة ثنائيات x86_64 من وحدة التخزين في الأوقات التي يراها النظام مثالية للاستجابة بالنسبة لتلك التعليمات البرمجية. تتم كتابة الأعمال المُترجمة إلى وحدة التخزين كنوع خاص من ملف كائنات Mach. ويشبه هذا الملف صورة قابلة للتنفيذ، ولكن يتم تمييزها للإشارة إلى أنها المنتج المُترجَم لصورة أخرى.

في هذا النموذج، تستمد أعمال AOT جميع معلومات الهوية الخاصة بها من صورة x86_64 الأصلية القابلة للتنفيذ. لفرض هذا الارتباط، يقوم كيان ذو امتيازات خاص بمساحة المستخدم بالتوقيع على أعمال الترجمة باستخدام مفتاح خاص بالجهاز تتم إدارته بواسطة Secure Enclave. لا يتم تحرير هذا المفتاح إلا إلى الكيان ذي الامتيازات الخاص بمساحة المستخدم، والذي يتم تعريفه على أنه يستخدم استحقاقات مُقيّدة. يتضمن دليل التعليمات البرمجية الذي تم إنشاؤه لأعمال الترجمة تجزئة دليل التعليمات البرمجية لصورة x86_64 الأصلية القابلة للتنفيذ. يُعرف التوقيع على أعمال الترجمة نفسها باسم **التوقيع التكميلي**.

تبدأ قناة AOT بشكل مشابه لقناة JIT، حيث تنقل kernel التحكم إلى Rosetta وقت التشغيل بدلاً من محرر الروابط الديناميكية `dyld(1)`. ولكن Rosetta وقت التشغيل يُرسل بعد ذلك استعلام التواصل بين العمليات (IPC) إلى خدمة نظام Rosetta، والذي يسأل عما إذا كانت هناك ترجمة AOT متاحة للصورة الحالية القابلة للتنفيذ أم لا. وفي حالة العثور عليها، توفر خدمة Rosetta مؤشرًا لهذه الترجمة، ويتم تعيينها في العملية وتنفيذها. أثناء التنفيذ، يفرض kernel تجزئات دليل التعليمات البرمجية لأعمال الترجمة التي تمت مصادقتها من خلال التوقيع المتجذر في مفتاح التوقيع الخاص بالجهاز. ولا يتم تضمين تجزئات دليل التعليمات البرمجية الخاصة بصورة x86_64 الأصلية في هذه العملية.

يتم تخزين الأعمال المترجمة في مخزن بيانات لا يمكن لأي كيان الوصول إليه في وقت التشغيل باستثناء خدمة Rosetta. وتدير خدمة Rosetta الوصول إلى ذاكرة التخزين المؤقت الخاصة بها عن طريق توزيع واصفات ملفات للقراءة فقط على أعمال الترجمة الفردية؛ وهذا يحد من الوصول إلى ذاكرة التخزين المؤقت لأعمال AOT. يتم عن عمد تضييق نطاق التواصل بين العمليات الخاص بهذه الخدمة وكذلك البصمة التابعة لها بغرض تقليل أجزائها المعرضة للهجوم.

إذا كانت تجزئة دليل التعليمات البرمجية لصورة x86_64 الأصلية لا تتطابق مع نظيرتها المشفرة في توقيع أعمال ترجمة AOT، فإن هذه النتيجة تعتبر مكافئة لتوقيع تعليمات برمجية غير صالح، ويتم اتخاذ إجراء الإنفاذ المناسب.

إذا قامت عملية عن بُعد بالاستعلام عن kernel للاستحقاقات أو خصائص هوية تعليمات برمجية أخرى لملف AOT تنفيذي مُترجَم، يتم إرجاع خصائص الهوية لصورة x86_64 الأصلية إليها.

محتوى ذاكرة التخزين المؤقتة الموثوق بها الثابتة

يأتي macOS 11 أو أحدث مزودًا بثنائيات Mach "fat" تحتوي على شرائح من التعليمات البرمجية للكمبيوتر x86_64 و arm64. على أجهزة كمبيوتر Mac المزودة بسيليكون Apple، قد يقرر المستخدم تنفيذ شريحة x86_64 لملف نظام ثنائي من خلال قناة Rosetta، على سبيل المثال لتحميل مكون إضافي لا يحتوي على متغير arm64 أصلي. ولدعم هذا الأسلوب، تحتوي ذاكرة التخزين المؤقتة الموثوق بها الثابتة التي تأتي مع macOS، بشكل عام، على ثلاث تجزئات دليل تعليمات برمجية لكل ملف من ملفات كائنات Mach:

- تجزئة دليل تعليمات برمجية لشريحة arm64
- تجزئة دليل تعليمات برمجية لشريحة x86_64
- تجزئة دليل تعليمات برمجية لترجمة AOT لشريحة x86_64

يعتبر إجراء ترجمة Rosetta AOT حتميًا إذ يعيد إنتاج مخرجات متطابقة لأي إدخال معين، بغض النظر عن وقت إجراء الترجمة أو نوع الجهاز الذي يتم إجراؤها عليه.

أثناء إنشاء macOS، يتم تشغيل كل ملف من ملفات كائنات Mach من خلال قناة ترجمة Rosetta AOT المرتبطة بإصدار macOS الجاري إنشاؤه، ويتم تسجيل تجزئة دليل التعليمات البرمجية الناتجة في ذاكرة التخزين المؤقتة الموثوق بها. لتحقيق الكفاءة، لا يتم توفير المنتجات المترجمة الفعلية مع نظام التشغيل ويتم إعادة تكوينها عند الطلب عندما يطلبها المستخدم.

عند تنفيذ صورة x86_64 على كمبيوتر Mac مزود بسيليكون Apple، إذا كانت تجزئة دليل التعليمات البرمجية لهذه الصورة موجودة في ذاكرة التخزين المؤقتة الموثوق بها الثابتة، فمن المتوقع **أيضًا** أن تكون تجزئة دليل التعليمات البرمجية لأعمال AOT الناتجة موجودة في ذاكرة التخزين المؤقتة الموثوق بها الثابتة. ولا يتم توقيع مثل هذه المنتجات بواسطة المفتاح الخاص بالجهاز، لأن سلطة التوقيع تكون متجذرة في سلسلة التمهيد الآمن في Apple.

تعليمات x86_64 البرمجية غير المُوقَّعة

لا تسمح أجهزة كمبيوتر Mac المزودة بسيليكون Apple بتنفيذ تعليمات arm64 البرمجية الأصلية بدون إرفاق توقيع تعليمات برمجية صالح. يمكن أن يكون هذا التوقيع بسيطًا مثل التوقيع الذي يُسمى بتوقيع التعليمات البرمجية "المخصص" (cf. `codesign(1)`) الذي لا يحمل أي هوية فعلية من النصف السري لزوج مفاتيح غير متماثل (إنه ببساطة قياس غير مصادق عليه للملف الثنائي).

يُسمح بتنفيذ تعليمات x86_64 البرمجية المترجمة من خلال Rosetta بدون معلومات توقيع، لأسباب تتعلق بتوافق الملف الثنائي. لا يتم نقل أي هوية محددة إلى هذه التعليمات البرمجية من خلال إجراء توقيع Secure Enclave الخاص بالجهاز، ويتم تنفيذه بدقة بالقيود ذاتها التي تنفذها التعليمات البرمجية الأصلية غير المُوقَّعة على أجهزة كمبيوتر Mac المستندة إلى Intel.

وسائل حماية الوصول إلى الذاكرة المباشرة في أجهزة كمبيوتر Mac

لتحقيق إنتاجية عالية على الواجهات عالية السرعة مثل PCIe و FireWire وثندربولت و USB، يجب أن تدعم أجهزة الكمبيوتر الوصول المباشر للذاكرة (DMA) من الأجهزة الطرفية. وهذا يعني أنه يجب أن يكون بإمكانها القراءة والكتابة إلى RAM دون مشاركة مستمرة من وحدة المعالجة المركزية. منذ 2012، طبقت أجهزة كمبيوتر Mac تقنيات عديدة لحماية DMA، مما أدى إلى الوصول إلى أفضل وأشمل مجموعة من وسائل حماية DMA على أي كمبيوتر.

وسائل حماية الوصول إلى الذاكرة المباشرة على أجهزة كمبيوتر Mac المزودة بسيليكون Apple

تحتوي الأنظمة على شرائح من Apple على وحدة إدارة ذاكرة إدخال/إخراج (IOMMU) لكل وكيل DMA في النظام، بما في ذلك منافذ PCIe وثندربولت. ولأن لكل IOMMU مجموعتها الخاصة من جداول ترجمة العناوين لترجمة طلبات DMA، فلا يمكن للأجهزة الطرفية المتصلة بواسطة PCIe أو ثندربولت الوصول إلا إلى الذاكرة التي تم تعيينها صراحةً لاستخدامها. لا يمكن للأجهزة الطرفية الوصول إلى الذاكرة التي تنتمي إلى أجزاء أخرى من النظام—مثل kernel أو البرامج الثابتة—أو الذاكرة المخصصة للأجهزة الطرفية الأخرى. إذا اكتشفت IOMMU محاولةً من جهاز طرفي للوصول إلى ذاكرة لم يتم تعيينها لاستخدام هذا الجهاز الطرفي، فإنها تعمل على تشغيل حالة خطأ في kernel.

وسائل حماية الوصول إلى الذاكرة المباشرة على Mac مستند إلى Intel

تعمل أجهزة كمبيوتر Mac المستندة إلى Intel مع تقنية Intel Virtualization Technology for Directed I/O (VT-d) على تهيئة IOMMU، مما يتيح إعادة تعيين DMA وإعادة تعيين المقاطعة، في وقت مبكر جدًا من عملية التمهيد للتخفيف من فئات مختلفة من الثغرات الأمنية. يبدأ مكون IOMMU المادي من Apple في العمل بسياسة رفض افتراضي، لذا فإنه فور تشغيل النظام، يبدأ تلقائيًا بحظر طلبات DMA من الأجهزة الطرفية. بعد التهيئة بواسطة البرنامج، تبدأ وحدات IOMMU في السماح بطلبات DMA من الأجهزة الطرفية إلى مناطق الذاكرة التي تم تعيينها بشكل صريح لاستخدامها.

ملاحظة: إعادة تعيين المقاطعة لـ PCIe ليست ضرورية على أجهزة كمبيوتر Mac المزودة بسيليكون Apple حيث تتعامل كل IOMMU مع وحدات MSI للأجهزة الطرفية الخاصة بها.

بدءًا من macOS 11، تقوم جميع أجهزة كمبيوتر Mac المزودة بشريحة Apple T2 الأمنية بتشغيل برامج تشغيل UEFI التي تسهل الوصول المباشر للذاكرة DMA في بيئة الحلقة 3 المقيدة عندما يتم إقران برامج التشغيل هذه بأجهزة خارجية. تساعد هذه الخاصية في التخفيف من الثغرات الأمنية التي قد تحدث عندما يتفاعل جهاز ضار مع برنامج تشغيل UEFI بطريقة غير متوقعة في وقت التمهيد. على وجه الخصوص، يقلل من تأثير الثغرات الأمنية في برامج التشغيل التي تتعامل مع مخازن DMA المؤقتة.

توسيع ملحق kernel بشكل آمن في macOS

بدءًا من macOS 11، إذا تم تمكين ملحقات kernel التابعة لجهات خارجية (kexts)، فلا يمكن تحميلها في kernel عند الطلب. بدلاً من ذلك، يتم دمجها في **مجموعة kernel المساعدة (AuxKC)**، والتي يتم تحميلها أثناء عملية التمهيد. بالنسبة لأجهزة كمبيوتر Mac المزودة بسيليكون Apple، يتم تسجيل قياس AuxKC في LocalPolicy (بينما في الأجهزة السابقة، يوجد AuxKC على وحدة تخزين البيانات). وتتطلب إعادة بناء AuxKC موافقة المستخدم وإعادة تشغيل macOS لتحميل التغييرات إلى kernel، كما تتطلب تكوين التمهيد الآمن على مستوى التأمين المنخفض.

هام: لم يعد من المستحسن تشغيل Kexts لـ macOS. تُخاطر Kexts بتكامل وموثوقية نظام التشغيل، وتنصح Apple المستخدمين بتحديد الحلول التي لا تتطلب توسيع kernel.

ملحقات Kernel في أجهزة كمبيوتر Mac المزودة بسيليكون Apple

يجب تمكين Kexts بشكل صريح لأجهزة كمبيوتر Mac المزودة بسيليكون Appleعن طريق الضغط على زر الطاقة عند بدء التشغيل للدخول في نمط One True Recovery (1TR)، ثم الرجوع إلى التأمين المنخفض وتحديد المربع لتمكين ملحقات kernel. يتطلب هذا الإجراء أيضًا إدخال كلمة سر المسؤول لتفويض الرجوع إلى إصدار أقدم. يجعل الجمع بين متطلبات 1TR وكلمة السر من الصعب على المهاجمين الذين يستخدمون البرامج فقط بدءًا من داخل macOS إدخال kexts في macOS، والتي يمكنهم استغلالها بعد ذلك للحصول على امتيازات kernel.

بعد أن يأذن المستخدم بتحميل kexts، يتم استخدام تحميل ملحقات Kernel المعتمدة من المستخدم أعلاه للسماح بتثبيت kexts. يستخدم التفويض المستخدم للتدفق أعلاه أيضًا لالتقاط تجزئة SHA384 لقائمة kext المعتمدة من المستخدم (UAKL) في LocalPolicy. يعد برنامج إدارة kernel (`kmd`) مسؤولاً عن التحقق من صحة kexts الموجودة في UAKL لتضمينها في AuxKC.

- إذا تم تمكين حماية تكامل النظام (SIP)، يتم التحقق من توقيع كل kext قبل تضمينه في AuxKC.
- إذا تم تعطيل SIP، فلا يتم فرض توقيع kext.

يسمح هذا الأسلوب بتدفقات التأمين الأقل تقييدًا للمطورين أو المستخدمين الذين ليسوا جزءًا من برنامج مطوري Apple باختبار kexts قبل التوقيع عليها.

بعد إنشاء AuxKC، يتم إرسال القياس إلى Secure Enclave ليتم توقيعه وإدراجه في بنية بيانات Image4 والتي يمكن تقييمها بواسطة iBoot عند بدء التشغيل. وكجزء من إنشاء AuxKC، يتم أيضًا إنشاء إيصال kext. يحتوي هذا الإيصال على قائمة kexts التي تم تضمينها بالفعل في AuxKC، لأن المجموعة يمكن أن تكون مجموعة فرعية من UAKL إذا حدثت kexts محظورة. يتم تضمين تجزئة SHA384 لهيكل بيانات AuxKC Image4 وإيصال kext في LocalPolicy. يتم استخدام تجزئة AuxKC Image4 للتحقق الإضافي بواسطة iBoot عند بدء التشغيل للمساعدة على التأكد من أنه لا يمكن بدء تشغيل ملف AuxKC Image4 أقدم مُوقّع من قِبل Secure Enclave باستخدام LocalPolicy أحدث. يتم استخدام إيصال kext بواسطة أنظمة فرعية مثل Apple Pay لتحديد ما إذا كان هناك أي kexts تم تحميلها حاليًا والتي يمكن أن تتداخل مع مصداقية macOS. وفي حالة وجودها، يمكن بعد ذلك تعطيل إمكانات Apple Pay.

ملحقات النظام

يتيح macOS 10.15 للمطورين توسيع إمكانات macOS عن طريق تثبيت وإدارة ملحقات النظام التي تعمل في مساحة المستخدم بدلاً من العمل على مستوى kernel. من خلال التشغيل في مساحة المستخدم، تزيد ملحقات النظام من استقرار وأمن macOS. وبالرغم من تمتع kexts بطبيعتها بالوصول الكامل إلى نظام التشغيل بأكمله، فإن الملحقات التي تعمل في مساحة المستخدم لا تُمنح إلا الامتيازات اللازمة لتنفيذ وظيفتها المحددة.

يمكن للمطورين استخدام إطارات العمل بما في ذلك DriverKit و EndpointSecurity و NetworkExtension لكتابة برامج تشغيل USB والواجهات البشرية وأدوات أمن نقطة النهاية (مثل منع فقدان البيانات أو وكلاء نقطة النهاية الآخرين) و VPN وأدوات الشبكة، كل ذلك دون الحاجة إلى كتابة kexts. ولا ينبغي استخدام وكلاء الأمن التابعين لجهات خارجية إلا إذا استخدموا واجهات API هذه أو كانت لديهم خريطة طريق قوية للانتقال إليها وبعيدًا عن ملحقات kernel.

تحميل ملحقات Kernel المعتمدة من المستخدم

لتحسين الأمن، يجب موافقة المستخدم على تحميل ملحقات kernel المثبتة مع تثبيت macOS 10.13 أو بعده. وتُعرف هذه العملية باسم **تحميل ملحق Kernel الذي يوافق عليه المستخدم**. يلزم الحصول على تخويل من المسؤول للموافقة على ملحق kernel. لا تتطلب ملحقات Kernel تخويلاً في الحالات التالية:

- عند تثبيتها على Mac مثبت عليه macOS 10.12 أو أقدم
- إذا كانت بديلاً لملحقات معتمدة سابقًا
- إذا كان مسموحًا لها بالتحميل دون موافقة المستخدم باستخدام أداة سطر الأوامر `spctl` المتاحة عند تمهيد Mac من recoveryOS
- إذا كان مسموحًا لها بالتحميل باستخدام تكوين إدارة جهاز الجوال (MDM)

  بدءًا من macOS 10.13.2، يمكن للمستخدمين استخدام MDM لتحديد قائمة ملحقات kernel التي يتم تحميلها دون موافقة المستخدم. يتطلب هذا الخيار جهاز Mac يعمل بـ macOS 10.13.2 مسجل في MDM—من خلال Apple School Manager، أو Apple Business Manager أو تسجيل MDM معتمد من قِبل المستخدم.

أمن ROM الاختياري في macOS

ملاحظة: وحدات ROM الاختيارية غير مدعومة حاليًا في أجهزة كمبيوتر Mac المزودة بسيليكون Apple.

أمن ROM الاختياري على Mac مزود بشريحة Apple T2 الأمنية

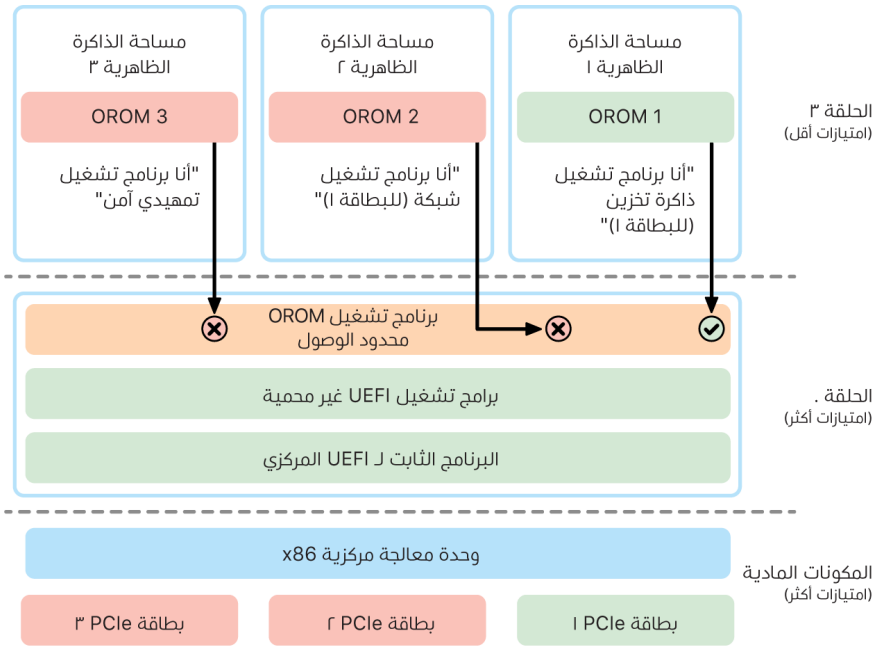
يمكن أن تحتوي أجهزة ثندربولت و PCIe على "Option ROM" أو (OROM) متصل فعليًا بالجهاز. (لا يعد هذا عادةً ROM حقيقيًا، ولكنه بدلاً من ذلك شريحة قابلة لإعادة الكتابة تُخزّن البرامج الثابتة.) في الأنظمة المستندة إلى UEFI، يكون هذا البرنامج الثابت عادةً برنامج تشغيل UEFI الذي تتم قراءته بواسطة برنامج UEFI الثابت ثم تنفيذه. من المفترض أن تقوم التعليمة البرمجية التي تم تنفيذها بتهيئة وتكوين المكونات المادية التي تم استردادها منها، بحيث يمكن جعل المكونات المادية قابلة للاستخدام بواسطة باقي البرامج الثابتة. وهذه الإمكانية مطلوبة حتى تتمكن المكونات المادية المتخصصة التابعة لجهات خارجية من التحميل والتشغيل خلال مراحل بدء التشغيل الأولى—على سبيل المثال، لبدء التشغيل من صفائف RAID الخارجية.

لكن نظرًا لأن OROMs قابلة لإعادة الكتابة عمومًا، إذا استبدل أحد المهاجمين OROM الخاص بجهاز طرفي شرعي، فقد يتم تنفيذ تعليمات المهاجم البرمجية في وقت مبكر من عملية التمهيد ويكون بإمكانه العبث في بيئة التنفيذ وانتهاك سلامة البرامج التي يتم تحميلها لاحقًا. وبالمثل، إذا قدّم المهاجم أجهزته الضارة إلى النظام، فسيكون بإمكانه أيضًا تنفيذ تعليمات برمجية ضارة.

في macOS 10.12.3، تم تغيير سلوك أجهزة كمبيوتر Mac المباعة بعد 2011 إلى عدم تنفيذ OROMs افتراضيًا في الوقت الذي يتم فيه تمهيد الـ Mac، ما لم يتم الضغط على مجموعة مفاتيح خاصة. وتكون مجموعة المفاتيح هذه محمية ضد OROMs الضارة التي يتم إدخالها عن غير قصد في تسلسل تمهيد macOS. تم تغيير السلوك الافتراضي لأداة كلمة سر البرنامج الثابت أيضًا، بحيث عندما يقوم المستخدم بتعيين كلمة سر للبرنامج الثابت، لا يمكن تنفيذ OROMs حتى إذا تم الضغط على مجموعة المفاتيح. وذلك يؤدي إلى الحماية ضد أي مهاجم بحوزته الجهاز ماديًا يحاول عن قصد إدخال OROM ضار. بالنسبة للمستخدمين الذين ما زالوا بحاجة إلى تشغيل OROMs بينما لديهم مجموعة كلمات سر للبرامج الثابتة، يمكن تكوين خيار غير افتراضي باستخدام أداة سطر الأوامر `firmwarepasswd` في macOS.

أمن OROM محدود الوصول

في macOS 10.15، تم تحديث برنامج UEFI الثابت بحيث يحتوي على آلية لإدخال OROMs في وضع الحماية ولتجريدها من امتيازاتها. عادةً ما ينفذ برنامج UEFI الثابت جميع التعليمات البرمجية، بما في ذلك OROMs، على مستوى الامتياز الأقصى لوحدة المعالجة المركزية، يُدعى الحلقة 0، ومساحة ذاكرة ظاهرية مشتركة واحدة لجميع التعليمات البرمجية والبيانات. تمثل الحلقة 0 مستوى الامتياز الذي يتم تشغيل kernel في macOS عليه، في حين أن مستوى الامتياز الأدنى، الحلقة 3، هو مكان تشغيل التطبيقات. إن وضع حماية OROM يجرّد OROMs من امتيازاتها عن طريق الاستفادة من فصل الذاكرة الظاهرية مثلما يفعل kernel، ثم تشغيل OROMs في الحلقة 3.



يعمل وضع الحماية أيضًا على إضافة مزيد من القيود المشددة على كل من الواجهات التي تستطيع OROMs الاتصال بها (فيما يشبه تصفية اتصالات النظام في kernels)، ونوع الجهاز الذي يستطيع OROM التسجيل باسمه (فيما يشبه وضع اعتماد التطبيقات). تكمن فائدة هذا التصميم في أن OROMs الضارة لم تعد قادرة على الكتابة مباشرةً في أي مكان داخل ذاكرة الحلقة 0. وبدلاً من ذلك تقتصر على واجهة وضع الحماية الضيقة جدًا والمحددة جيدًا. وتعمل هذه الواجهة المحدودة على تقليل الأجزاء المعرضة للهجوم بشكل كبير وتُجبر المهاجمين على الخروج أولاً من وضع الحماية وتصعيد الامتياز.

أمن البرنامج الثابت لـ UEFI في Mac مستند إلى Intel

يُقدّم Mac المستند إلى Intel المزود برقاقة Apple T2 أمنية وسائل تأمين باستخدام البرنامج الثابت UEFI (Intel).

نظرة عامة

منذ 2006، تستخدم أجهزة كمبيوتر Mac المزودة بوحدة معالجة مركزية تستند إلى Intel برنامجًا ثابتًا من Intel يستند إلى الإصدار 1 أو الإصدار 2 من مجموعة أدوات التطوير (EDK) لواجهة البرامج الثابتة القابلة للتوسعة (EFI). تتوافق التعليمات البرمجية التي تستند إلى EDK2 مع مواصفات واجهة البرامج الثابتة القابلة للتوسعة الموحدة (UEFI). ويشير هذا القسم إلى برنامج Intel الثابت باعتباره **برنامج UEFI الثابت**. كان برنامج UEFI الثابت أول تعليمة برمجية يتم تنفيذها على شريحة Intel.

بالنسبة لأجهزة كمبيوتر Mac المستندة إلى Intel التي لا تحتوي على شريحة Apple T2 الأمنية، يكون جذر الثقة لبرنامج UEFI الثابت الشريحة المخزّن عليها البرنامج الثابت. وتوقّع Apple تحديثات برنامج UEFI الثابت رقميًا ويتحقق منها البرنامج الثابت قبل تحديث وحدة التخزين. للمساعدة على منع هجمات التراجع، يجب أن تحتوي التحديثات دائمًا على إصدار أحدث من الإصدار الموجود. ومع ذلك، من المحتمل أن يتمكن للمهاجم الذي لديه وصول مادي إلى الـ Mac استخدام المكونات المادية لتوصيل شريحة تخزين البرامج الثابتة وتحديث الشريحة لوضع محتوى ضار. وبالمثل، إذا تم العثور على ثغرات أمنية في عملية التمهيد المبكرة لبرنامج UEFI الثابت (قبل أن تقيّد الكتابة على شريحة التخزين)، فقد يؤدي ذلك أيضًا إلى إصابة دائمة في برنامج UEFI الثابت. وهذا عبارة عن قيد بنيوي في المكونات المادية شائع في معظم أجهزة الكمبيوتر المستندة إلى Intel وموجود في جميع أجهزة كمبيوتر Mac المستندة إلى Intel التي بدون شريحة T2.

للمساعدة في منع الهجمات المادية التي تُفسد برنامج UEFI الثابت، وضعنا تصميمًا جديدًا لأجهزة كمبيوتر Mac لغرس جذور الثقة في برنامج UEFI الثابت في شريحة T2. على أجهزة كمبيوتر Mac هذه، يكون جذر الثقة لبرنامج UEFI الثابت هو برنامج T2 الثابت على وجه الخصوص، كما هو موضح في قسم عملية التمهيد على Mac مستند إلى Intel.

المكون الفرعي لمحرك إدارة Intel (ME)

يعد البرنامج الثابت **لمحرك إدارة Intel (ME)** أحد المكونات الفرعية المخزنة داخل برنامج UEFI الثابت. ويُستخدم ME—وهو معالج منفصل ونظام فرعي في شرائح Intel—بشكل أساسي لحماية حقوق النشر الخاصة بالصوت والفيديو على Mac يحتوي على رسومات تستند إلى Intel فقط. لتقليل الأجزاء المعرضة للهجوم في هذا المكون الفرعي، تقوم أجهزة كمبيوتر Mac المستندة إلى Intel بتشغيل برنامج ME ثابت مخصص تمت إزالة معظم المكونات منه. نظرًا لأن برنامج ME الثابت على الـ Mac الناتج أصغر من الحد الأدنى الافتراضي للبنية التي توفرها Intel، فإن العديد من المكونات التي تعرضت لهجمات عامة من قبل الباحثين الأمنيين في الماضي لم تعد موجودة.

نمط إدارة النظام (SMM)

لدى معالجات Intel نمط تنفيذ خاص متميز عن التشغيل العادي. ذلك النمط، الذي يُسمى **نمط إدارة النظام (SMM)**، تم تقديمه في الأصل للتعامل مع العمليات الحساسة للوقت مثل إدارة الطاقة. لكن لتنفيذ مثل هذه الإجراءات، كانت أجهزة كمبيوتر Mac قديمًا تستخدم وحدة تحكم دقيقة منفصلة تسمى **وحدة تحكم إدارة النظام (SMC)**. لم تعد SMC وحدة تحكم دقيقة منفصلة، فقد تم دمجها في شريحة T2.

أمن الأنظمة لـ watchOS

تستخدم Apple Watch العديد من إمكانات أمن النظام الأساسي القائمة على المكونات المادية نفسها التي يستخدمها iOS. على سبيل المثال، Apple Watch:

- تنفّذ التمهيد الآمن وتحديثات البرامج الآمنة
- تحافظ على تكامل نظام التشغيل
- تساعد في حماية البيانات - سواء على الجهاز أو عند الاتصال بهاتف iPhone مقترن أو بالإنترنت

وتتضمن التقنيات المدعومة تلك التقنيات المدرجة في أمن الأنظمة (على سبيل المثال، KIP و SKP و SCIP) بالإضافة إلى حماية البيانات وسلسلة المفاتيح وتقنيات الشبكة.

تحديث watchOS

يمكن تكوين watchOS ليتم تحديثه خلال ساعات الليل. لمزيد من المعلومات حول كيفية تخزين رمز دخول Apple Watch واستخدامه أثناء التحديث، انظر حاويات المفاتيح.

اكتشاف المعصم

إذا تم تمكين اكتشاف المعصم، يتم قفل الجهاز تلقائيًا بعد فترة وجيزة من إزالته من معصم المستخدم. وإذا تم تعطيل اكتشاف المعصم، يوفر مركز التحكم خيارًا لقفل Apple Watch. عند قفل Apple Watch، لا يمكن استخدام Apple Pay إلا عن طريق إدخال رمز الدخول على Apple Watch. ويتم إيقاف اكتشاف المعصم باستخدام تطبيق Apple Watch على الـ iPhone. يمكن أيضًا فرض هذا الإعداد باستخدام حل إدارة جهاز الجوال (MDM).

قفل التنشيط

عند تشغيل تحديد الموقع على iPhone، تستطيع Apple Watch المقترنة به استخدام ميزة قفل التنشيط. ويُصعّب قفل التنشيط على أي شخص استخدام أو بيع Apple Watch التي تعرضت للفقدان أو السرقة. يتطلب قفل التنشيط Apple ID وكلمة السر الخاصين بالمستخدم لإلغاء إقران Apple Watch أو مسحها أو إعادة تنشيطها.

الإقران الآمن مع الـ iPhone

يمكن إقران Apple Watch بجهاز iPhone واحد فقط في المرة الواحدة. عندما تكون Apple Watch غير مقترنة، يقوم الـ iPhone بإرسال التعليمات لمسح كل المحتوى والبيانات من الساعة.

يتم تأمين اقتران Apple Watch مع الـ iPhone باستخدام عملية خارج النطاق لتبادل المفاتيح العامة، متبوعة بالسر المشترك لرابط ®Bluetooth منخفض الطاقة (BLE). تعرض Apple Watch نمطًا متحركًا يتم التقاطه بواسطة الكاميرا على الـ iPhone. ويحتوي النمط على سر مشفر يُستخدم في اقتران BLE 4.1 خارج النطاق. يستخدم إدخال مفتاح مرور BLE القياسي كطريقة اقتران احتياطية، إذا لزم الأمر.

بعد إنشاء جلسة BLE وتشفيرها باستخدام أعلى بروتوكول أمني متاح في مواصفات Bluetooth الأساسية، ومفاتيح تبادل iPhone و Apple Watch باستخدام أي مما يلي:

- عملية مقتبسة من خدمة الهوية من Apple (IDS) كما هو موضح في نظرة عامة على أمن iMessage.
- تبادل المفاتيح باستخدام IKEv2/IPsec. تتم مصادقة تبادل المفاتيح الأولي باستخدام إما مفتاح جلسة Bluetooth (لسيناريوهات الاقتران) أو مفاتيح IDS (لسيناريوهات تحديث نظام التشغيل). ينشئ كل جهاز زوج مفاتيح Ed25519 خاص-عام عشوائي سعة 256 بت وخلال عملية تبادل المفاتيح الأولية، يتم تبادل المفاتيح العامة. عند إقران Apple Watch بـ watchOS 10 أو أحدث للمرة الأولى، يرجع جذر المفاتيح الخاصة إلى Secure Enclave.

  على iPhone الذي يعمل بنظام iOS 17 أو أحدث، لا يرجع جذر المفاتيح الخاصة إلى Secure Enclave، لأن المستخدم الذي يستعيد نسخة iCloud الاحتياطية إلى iPhone نفسه يحافظ على اقتران Apple Watch الحالي دون الحاجة إلى إجراء نقل.

ملاحظة: تختلف الآلية المستخدمة لتبادل المفاتيح والتشفير، وذلك بناءً على إصدارات نظام التشغيل على iPhone و Apple Watch. وتستخدم أجهزة iPhone المثبت عليها iOS 13 أو أحدث عند إقرانها بـ Apple Watch مثبت عليها watchOS 6 أو أحدث IKEv2/IPsec فقط لتبادل المفاتيح والتشفير.

بعد استبدال المفاتيح:

- يتم تجاهل مفتاح جلسة Bluetooth ويتم تشفير جميع الاتصالات بين iPhone و Apple Watch باستخدام إحدى الطرق المذكورة أعلاه — مع Bluetooth المشفرة و Wi-Fi والروابط الخلوية التي توفر طبقة تشفير ثانوية.
- (IKEv2/IPsec فقط) يتم تخزين المفاتيح في سلسلة مفاتيح النظام واستخدامها لمصادقة جلسات IKEv2/IPsec المستقبلية بين الأجهزة. يتم تشفير الاتصال الإضافي بين هذه الأجهزة وحماية تكاملها باستخدام AES-256-GCM على أجهزة iPhone المثبّت عليها iOS 15 أو أحدث مقترنة بـ Apple Watch Series 4 أو أحدث مثبّت عليها watchOS 8 أو أحدث. (يتم استخدام ChaCha20-Poly1305 بمفاتيح 256 بت على الأجهزة الأقدم أو الأجهزة المثبت عليها إصدارات أنظمة التشغيل الأقدم).

يتم تدوير عنوان جهاز Bluetooth منخفض الطاقة على فترات زمنية مدتها 15 دقيقة لتقليل مخاطر تعقب الجهاز محليًا إذا لجأ شخص ما إلى بث معرّف دائم.

لدعم التطبيقات التي تحتاج إلى تدفق البيانات، يتم توفير التشفير باستخدام الطرق الموضحة في أمن فيس تايم، وذلك باستخدام إما خدمة الهوية من Apple (IDS) التي يوفرها iPhone المقترن أو اتصال إنترنت مباشر.

تنفذ Apple Watch تخزينًا مشفرًا بالمكونات المادية وحماية على أساس الفئة للملفات وعناصر سلسلة المفاتيح. كما يتم استخدام حاويات المفاتيح التي يتم التحكم في الوصول إليها لعناصر سلسلة المفاتيح. يتم أيضًا تأمين المفاتيح المستخدمة للاتصال بين الـ Apple Watch والـ iPhone باستخدام الحماية المستندة إلى الفئة. لمزيد من المعلومات، انظر حافظات المفاتيح لحماية البيانات.

فتح القفل التلقائي و Apple Watch

لمزيد من الراحة عند استخدام أجهزة Apple متعددة، يمكن لبعض الأجهزة فتح قفل الأجهزة الأخرى تلقائيًا في مواقف معينة. يدعم فتح القفل التلقائي ثلاثة استخدامات:

- يمكن فتح قفل Apple Watch بواسطة iPhone.
- يمكن فتح قفل Mac بواسطة Apple Watch.
- يمكن فتح قفل iPhone بواسطة Apple Watch عندما يتم اكتشاف المستخدم أثناء تغطية أنفه وفمه.

جميع حالات الاستخدام الثلاثة مبنية على الأساس الرئيسي نفسه: بروتوكول محطة إلى محطة (STS) مُصادَق عليه بشكل متبادل، مع مفاتيح طويلة الأجل يتم تبادلها في وقت تمكين الميزة ومفاتيح جلسة مؤقتة فريدة يتم التفاوض عليها لكل طلب. بغض النظر عن قناة الاتصال الأساسية، يتم التفاوض على معبر STS مباشرة بين Secure Enclaves في كلا الجهازين، ويتم الاحتفاظ بجميع مواد التشفير داخل هذا النطاق الآمن (باستثناء أجهزة كمبيوتر Mac التي لا تحتوي على Secure Enclave، والتي تنهي معبر STS في ملحق kernel).

فتح القفل

يمكن تقسيم تسلسل فتح القفل الكامل إلى مرحلتين. أولاً، يقوم الجهاز الذي يتم فتح قفله ("الهدف") بإنشاء سر فتح قفل مشفر وإرساله إلى الجهاز الذي ينفّذ فتح القفل ("البادئ"). بعد ذلك، يقوم البادئ بفتح القفل باستخدام السر الذي تم إنشاؤه سابقًا.

لتأمين فتح القفل التلقائي، يتصل الجهازان ببعضها باستخدام اتصال BLE. ثم يتم إرسال سر فتح قفل مكون من 32 بايت تم إنشاؤه عشوائيًا بواسطة الجهاز المستهدف إلى البادئ عبر معبر STS. أثناء عملية فتح القفل التالية باستخدام المقاييس الحيوية أو رمز الدخول، يعمل الجهاز المستهدف على تغليف المفتاح المشتق من رمز الدخول (PDK) الخاص به بسر فتح القفل ويتجاهل سر فتح القفل من ذاكرته.

لتنفيذ فتح القفل، يقوم الجهازان ببدء اتصال BLE جديد ثم استخدام شبكة Wi-Fi من نظير إلى نظير لتقريب المسافة بينهما بشكل آمن. إذا كان الجهازان ضمن النطاق المحدد وتم استيفاء سياسات الأمن المطلوبة، يرسل البادئ سر فتح القفل الخاص به إلى المستهدف عبر معبر STS. يقوم المستهدف بعد ذلك بإنشاء سر جديد لفتح القفل مكون من 32 بايت وإعادته إلى البادئ. إذا نجح سر فتح القفل الحالي الذي أرسله البادئ في فك تشفير سجل فتح القفل، فسيتم فتح قفل الجهاز المستهدف وإعادة تغليف PDK بسر جديد لفتح القفل. أخيرًا، يتم بعد ذلك تجاهل سر فتح القفل الجديد و PDK من ذاكرة الجهاز المستهدف.

سياسات أمن فتح القفل التلقائي على Apple Watch

لمزيد من الراحة، يمكن فتح قفل Apple Watch بواسطة iPhone مباشرةً بعد بدء التشغيل الأولي دون مطالبة المستخدم أولاً بإدخال رمز المرور على Apple Watch نفسها. لتحقيق ذلك، يتم استخدام سر فتح القفل العشوائي (الذي تم إنشاؤه أثناء تسلسل فتح القفل الأول بعد تمكين الميزة) لإنشاء سجل ضمان طويل الأجل، يتم تخزينه في حاوية مفاتيح Apple Watch. يتم تخزين سر سجل الضمان في سلسلة مفاتيح iPhone ويتم استخدامه لبدء جلسة جديدة بعد كل إعادة تشغيل على Apple Watch.

سياسات أمن فتح القفل التلقائي على iPhone

تنطبق سياسات الأمن الإضافية على فتح القفل التلقائي على iPhone باستخدام Apple Watch. لا يمكن استخدام Apple Watch بدلاً من بصمة الوجه على iPhone في عمليات أخرى، مثل Apple Pay أو تفويضات التطبيق. عندما تنجح Apple Watch في فتح قفل iPhone مقترن، تعرض الساعة إشعارًا وتقوم بتشغيل إشعار حسي مرتبط. إذا ضغط المستخدم على زر قفل iPhone في الإشعار، ترسل الساعة إلى iPhone أمر قفل عبر BLE. عندما يتلقى iPhone أمر القفل، فإنه يقفل ويعطل كلاً من بصمة الوجه وفتح القفل باستخدام Apple Watch. يجب إجراء فتح قفل iPhone التالي باستخدام رمز دخول iPhone.

يتطلب فتح قفل iPhone مقترن بنجاح من Apple Watch (عند التمكين) استيفاء المعايير التالية:

- يجب أن يكون iPhone قد تم فتح قفله باستخدام طريقة أخرى مرة واحدة على الأقل بعد وضع Apple Watch المرتبطة على المعصم وفتح قفلها.
- يجب أن تكون المستشعرات قادرة على اكتشاف تغطية الأنف والفم.
- يجب أن تكون المسافة المقاسة من مترين إلى ثلاثة أمتار أو أقل
- يجب ألا تكون Apple Watch في نمط وقت النوم.
- يجب أن يكون قد تم فتح قفل Apple Watch أو iPhone مؤخرًا، أو يجب أن تكون Apple Watch قد تعرضت لحركة جسدية تشير إلى أن مرتديها نشط (على سبيل المثال، ليس نائمًا).
- يجب أن يكون iPhone قد تم فتح قفله مرة واحدة على الأقل خلال آخر 6,5 ساعات.
- يجب أن يكون iPhone في حالة يُسمح فيها لميزة بصمة الوجه بفتح قفل الجهاز. (لمزيد من المعلومات، انظر بصمة الوجه وبصمة الإصبع ورموز المرور وكلمات السر).

الموافقة في macOS باستخدام Apple Watch

عند تمكين فتح القفل التلقائي باستخدام Apple Watch، يمكن استخدام Apple Watch في مكانها أو مع بصمة الإصبع للموافقة على مطالبات التخويل والمصادقة من:

- تطبيقات macOS و Apple التي تطلب التخويل
- تطبيقات الجهات الخارجية التي تطلب المصادقة
- كلمة سر سفاري المحفوظة
- الملاحظات الآمنة

الاستخدام الآمن لـ Wi-Fi والبيانات الخلوية و iCloud و Gmail

عندما لا تكون Apple Watch ضمن نطاق Bluetooth، يمكن استخدام Wi-Fi أو الشبكة الخلوية بدلاً من ذلك. تنضم Apple Watch تلقائيًا إلى شبكات Wi-Fi التي تم الانضمام إليها بالفعل على الـ iPhone المقترن والتي تمت مزامنة بيانات اعتمادها مع Apple Watch أثناء وجود كلا الجهازين في النطاق. يمكن بعد ذلك تكوين سلوك الانضمام التلقائي على أساس كل-شبكة في قسم Wi-Fi في تطبيق إعدادات Apple Watch. ويمكن ربط شبكات Wi-Fi التي لم يتم الانضمام إليها من قبل على أي من الجهازين يدويًا في قسم Wi-Fi في تطبيق إعدادات Apple Watch.

عندما تكون Apple Watch والـ iPhone خارج النطاق، تتصل Apple Watch مباشرة بخوادم iCloud و Gmail لجلب البريد، بدلاً من مزامنة بيانات البريد مع الـ iPhone المقترن عبر الإنترنت. بالنسبة لحسابات Gmail، يجب على المستخدم المصادقة مع Google في قسم البريد في تطبيق Watch على الـ iPhone. يُرسل رمز OAuth الذي تم استلامه من Google إلى Apple Watch بتنسيق مشفر عبر خدمة الهوية من Apple (IDS) حتى يمكن استخدامه لجلب البريد. ولا يُستخدم رمز OAuth هذا مطلقًا للاتصال بخادم Gmail من الـ iPhone المقترن.

الإنشاء العشوائي للأرقام

تعد مولدات الأرقام العشوائية الزائفة المشفرة (CPRNG) لبنة مهمة للبرامج الآمنة. تحقيقًا لهذه الغاية، توفر Apple برنامجًا موثوقًا به CPRNG يعمل في kernels الخاصة بكل من iOS و iPadOS و macOS و tvOS و watchOS. ويكون مسؤولاً عن تجميع الإنتروبيا الأولية من النظام وتوفير أرقام عشوائية آمنة للمستهلكين في كل من kernel ومساحة المستخدم.

مصادر الإنتروبيا

يتم نشر kernel CPRNG من مصادر إنتروبيا متعددة أثناء التمهيد وعلى مدى عمر الجهاز. وهذا يتضمن (يتوقف على مدى التوفر):

- مكون TRNG المادي في Secure Enclave
- التشوهات القائمة على التوقيت المجمّعة أثناء التمهيد
- الإنتروبيا المجمعة من مقاطعات المكونات المادية
- ملفًا أصليًا يُستخدم للتخزين الدائم للإنتروبيا عبر عمليات التمهيد
- تعليمات Intel البرمجية العشوائية، على سبيل المثال، RDSEED و RDRAND (على Mac مستند إلى Intel فقط)

Kernel CPRNG

kernel CPRNG عبارة عن تصميم مشتق من Fortuna يستهدف مستوى أمن 256 بت. يوفر أرقامًا عشوائية عالية الجودة للمستهلكين في مساحة المستخدم باستخدام واجهات API التالية:

- استدعاء نظام `getentropy`(2)
- الجهاز العشوائي (/dev/random)

يقبل kernel CPRNG إنتروبيا يتم توفيرها بواسطة المستخدم من خلال عمليات الكتابة على الجهاز العشوائي.

جهاز الأبحاث الأمنية من Apple

جهاز الأبحاث الأمنية من Apple عبارة عن iPhone مدمج بشكل خاص للسماح للباحثين في مجال الأمن بإجراء أبحاث على iOS من دون الحاجة إلى إلغاء أو تعطيل ميزات أمن النظام الأساسي للـ iPhone. باستخدام هذا الجهاز، يمكن للباحث تحميل المحتوى الجانبي الذي يعمل بأذونات مكافئة للنظام الأساسي، وبالتالي إجراء بحث على نظام أساسي يقوم بنمذجة أجهزة الإنتاج بشكل أوثق.

للمساعدة على ضمان عدم تأثر أجهزة المستخدم بسياسة تنفيذ جهاز الأبحاث الأمنية، يتم تنفيذ تغييرات السياسة في متغير من iBoot وفي مجموعة Boot Kernel. وتفشل هذه العناصر في التمهيد على مكونات المستخدم المادية. يتحقق iBoot البحثي من وجود حالة اندماج جديدة ويدخل في حلقة مشكلة إذا تم تشغيله على مكونات مادية مدمجة غير بحثية.

يتيح النظام الفرعي للتشفير للباحث تحميل ذاكرة تخزين مؤقت موثوق بها مخصصة وصورة قرص تحتوي على المحتوى المطابق. وقد تم اتخاذ عدد من التدابير الدفاعية المتعمقة للمساعدة على ضمان عدم سماح هذا النظام الفرعي بالتنفيذ على أجهزة المستخدم:

- لا يُحمل `launchd` قائمة خصائص launchd على `cryptexd` إذا اكتشف جهاز عميل عادي.
- يتم إلغاء `cryptexd` إذا اكتشف جهاز عميل عادي.
- لا تعمل `AppleImage4` على توريد القيمة غير القابلة لإعادة التشغيل التي تُستخدم للتحقق من وحدة تشفير البحث على جهاز عميل عادي.
- يرفض خادم التوقيع تخصيص صورة قرص تشفير لجهاز ليس في قائمة السماح الصريحة.

لاحترام خصوصية الباحث الأمني، لا يتم إرسال سوى قياسات (مثل التجزئات) للعناصر التنفيذية أو ذاكرة التخزين المؤقت لـ kernel ومعرفات جهاز الأبحاث الأمنية إلى Apple أثناء التخصيص. ولا تتلقى Apple محتوى التشفير الذي يتم تحميله على الجهاز.

لتجنب محاولة جهة ضارة التنكُّر بجهاز بحث في هيئة جهاز مستخدم لخداع هدف لاستخدامه بغرض الاستخدام اليومي، يحتوي جهاز الأبحاث الأمنية على الاختلافات التالية:

- يبدأ تشغيل جهاز الأبحاث الأمنية أثناء الشحن فقط. ويمكن أن يكون هذا باستخدام كبل لايتننغ أو شاحن Qi متوافق. إذا لم يكن الجهاز في وضع الشحن أثناء بدء التشغيل، يدخل الجهاز في نمط الاسترداد. إذا بدأ المستخدم الشحن وأعاد تشغيل الجهاز، يتم بدء تشغيله كالمعتاد. بمجرد بدء تشغيل XNU، لا يحتاج الجهاز إلى الشحن لمواصلة التشغيل.
- يتم عرض الكلمات **Security Research Device** أو "جهاز أبحاث أمنية" أسفل شعار Apple أثناء بدء تشغيل iBoot.
- يتم تمهيد ملحق XNU kernel في وضع verbose.
- يظهر اسم الجهاز على الجانب في رسالة "ملكية Apple". سري وخاضع للملكية. اتصل بالرقم "+1 877 595 1125".

فيما يلي إجراءات إضافية يتم تنفيذها في البرنامج الذي يظهر بعد التمهيد:

- يتم عرض النص **Security Research Device** أو "جهاز أبحاث أمنية" أثناء إعداد الجهاز.
- يتم عرض الكلمات **Security Research Device** على شاشة القفل وفي تطبيق الإعدادات.

يوفر جهاز الأبحاث الأمنية للباحثين الإمكانات التالية التي لا يوفرها جهاز المستخدم. يمكن للباحثين:

- تحميل تعليمات برمجية قابلة للتنفيذ بشكل جانبي على الجهاز مع استحقاقات عشوائية على مستوى الإذن نفسه، مثل مكونات نظام تشغيل Apple
- بدء الخدمات عند بدء التشغيل
- الإبقاء على المحتوى عبر عمليات إعادة التشغيل
- استخدام استحقاق `research.com.Apple.license-to-operate` للسماح بعملية لتصحيح أي عملية أخرى على النظام، بما في ذلك عمليات النظام.

  يتم احترام مساحة اسم `.research` فقط من خلال متغير RESEARCH الخاص بامتداد AppleMobileFileIntegrity kernel؛ كما يتم إنهاء أي عملية بهذا الاستحقاق على جهاز العميل أثناء التحقق من صحة التوقيع.
- تخصيص ذاكرة التخزين المؤقت المخصصة لـ kernel واستعادتها

التشفير وحماية البيانات

نظرة عامة على التشفير وحماية البيانات

تساعد إمكانات سلسلة التمهيد الآمن وأمن الأنظمة وأمن التطبيقات على التحقّق من عدم تشغيل سوى التعليمات البرمجية والتطبيقات الموثوق بها على الجهاز. تحتوي أجهزة Apple على ميزات تشفير إضافية لحماية بيانات المستخدم، حتى في حالة تعرض أجزاء أخرى من البنية الأساسية الأمنية للاختراق (على سبيل المثال، في حالة فقدان الجهاز أو تشغيل تعليمات برمجية غير موثوق بها). كل هذه الميزات تعود بالنفع على كل من المستخدمين ومسؤولي تقنية المعلومات في حماية المعلومات الشخصية والمؤسسية وتوفير طرق للمسح عن بُعد الفوري والكامل في حالة سرقة الجهاز أو فقدانه.

تستخدم أجهزة iPhone و iPad منهجية لتشفير الملفات تسمى **حماية البيانات**، في حين أن البيانات الموجودة على أجهزة كمبيوتر Mac المستندة إلى Intel تكون محمية بتقنية لتشفير وحدات التخزين تسمى **خزنة الملفات**. يستخدم الـ Mac المزود بسيليكون Apple نموذجًا هجينًا يدعم حماية البيانات، مع وضع الأمرين التاليين في الاعتبار: مستوى الحماية الأدنى (الفئة D) غير مدعوم، والمستوى الافتراضي (الفئة C) يستخدم مفتاح وحدة تخزين ويعمل تمامًا مثل خزنة الملفات على Mac مستند إلى Intel. في كل الحالات، تمتد جذور التسلسلات الهرمية لإدارة المفاتيح إلى السليكون المخصص لـ Secure Enclave، ويدعم محرك AES مخصص التشفير بسرعة الخط ويساعد في ضمان عدم تعرض مفاتيح التشفير طويلة الأجل إلى نظام تشغيل kernel أو وحدة المعالجة المركزية (حيث قد تتعرض للخطر). (لا يستخدم أي Mac مستند إلى Intel مزود بشريحة T1 أو لا يحتوي على Secure Enclave السيليكون المخصص لحماية مفاتيح تشفير خزنة الملفات الخاصة به.)

إلى جانب استخدام حماية البيانات وخزنة الملفات للمساعدة على منع الوصول غير المصرح به إلى البيانات، تستخدم Apple **ملحقات kernel في نظام تشغيل** لفرض الحماية والأمن. يستخدم kernel عناصر التحكم في الوصول لوضع التطبيقات في وضع الحماية (الذي يقيد البيانات التي يمكن للتطبيق الوصول إليها) وآلية تسمى **مخزن البيانات** (التي تقيد الوصول إلى بيانات التطبيق من جميع التطبيقات الأخرى التي تطلبها، بدلاً من تقييد عمليات الاستدعاء التي يمكن أن يقوم بها التطبيق).

رموز الدخول وكلمات السر

لحماية بيانات المستخدم من الهجمات الضارة، تستخدم Apple رموز المرور على الـ iOS و iPadOS وكلمات السر على الـ macOS. كلما زاد طول رموز المرور وكلمات السر، زادت قوتهما—وأصبح من السهل مكافحة هجمات القوة الغاشمة. لزيادة مكافحة الهجمات، تفرض Apple تأخيرًا زمنيًا (لـ iOS و iPadOS) وعددًا محدودًا من محاولات كلمة المرور (لـ Mac).

على iOS و iPadOS، يقوم المستخدم بتمكين حماية البيانات تلقائيًا عند إعداد رمز المرور أو كلمة السر. ويتم تمكين حماية البيانات كذلك على الأجهزة الأخرى التي تدعم نظام Apple على شريحة (SoC)—مثل الـ Mac المزود برقاقات Apple و Apple TV و Apple Watch. على macOS، تستخدم Apple برنامج تشفير وحدة التخزين المضمن لـ **خزنة الملفات**.

كيف تعمل رموز المرور وكلمات السر القوية على زيادة الأمن

يدعم iOS و iPadOS رموز المرور الأبجدية المكونة من ست خانات وأربع خانات والطويلة بشكل عشوائي. بالإضافة إلى فتح قفل الجهاز، يوفر رمز الدخول أو كلمة السر إنتروبيا لبعض مفاتيح التشفير. وهذا يعني أن المهاجم الذي بحوزته الجهاز لا يمكنه الوصول إلى البيانات في فئات حماية محددة دون رمز الدخول.

يكون رمز الدخول أو كلمة السر متشابكًا مع معرف UID الخاص بالجهاز، لذلك يجب تنفيذ محاولات القوة الغاشمة على الجهاز الذي يتعرض للهجوم. ويتم استخدام عدد تكرار كبير لجعل كل محاولة أبطأ. كما تتم معايرة عدد التكرار بحيث تستغرق المحاولة الواحدة حوالي 80 مللي ثانية. في الواقع، قد يستغرق أكثر من خمس سنوات ونصف لتجربة جميع مجموعات رموز الدخول الأبجدية الرقمية المكونة من ستة أحرف وبها أحرف وأرقام صغيرة.

كلما كان رمز دخول المستخدم أقوى، يصبح مفتاح التشفير أقوى. وباستخدام بصمة الوجه وبصمة الإصبع، يمكن للمستخدم إنشاء رمز دخول أقوى بكثير من وصفه بأنه عملي. يؤدي رمز الدخول القوي إلى زيادة مقدار الإنتروبيا الفعّال الذي يحمي مفاتيح التشفير المستخدمة لحماية البيانات، دون التأثير سلبًا على تجربة المستخدم في فتح قفل الجهاز عدة مرات على مدار اليوم.

إذا تم إدخال كلمة سر طويلة تحتوي على أرقام فقط، يتم عرض لوحة مفاتيح رقمية في شاشة القفل بدلاً من لوحة المفاتيح الكاملة. قد يكون إدخال رمز دخول رقمي أطول أسهل من إدخال رمز دخول أبجدي رقمي أقصر، مع توفير مستوى أمني مماثل.

يمكن للمستخدمين تحديد رمز دخول أبجدي رقمي أطول عن طريق تحديد رمز أبجدي رقمي مخصص في خيارات رمز الدخول في الإعدادات > بصمة الإصبع ورمز الدخول أو بصمة الوجه ورمز الدخول.

كيف تعمل التأخيرات الزمنية المتصاعدة على مكافحة هجمات القوة الغاشمة

على iOS و iPadOS و macOS، لمزيد من مكافحة هجمات القوة الغاشمة على رمز الدخول، ثمة تأخيرات زمنية متصاعدة بعد إدخال رمز دخول أو كلمة سر أو رمز PIN غير صالح (حسب الجهاز وحالته)، كما هو موضح في الجدول أدناه.

المحاولات	3	4	5	6	7	8	9	10 أو أكثر
شاشة قفل iOS و iPadOS	لا شيء	دقيقة واحدة	5 دقائق	15 دقيقة	ساعة واحدة	3 ساعات	8 ساعات	الجهاز مُعطّل ويجب توصيله بـ Mac أو كمبيوتر شخصي
شاشة قفل watchOS	لا شيء	دقيقة واحدة	5 دقائق	15 دقيقة	ساعة واحدة	3 ساعات	8 ساعات	الجهاز مُعطّل ويجب توصيله بـ iPhone
شاشة القفل ونافذة تسجيل الدخول في macOS	لا شيء	دقيقة واحدة	5 دقائق	15 دقيقة	ساعة واحدة	3 ساعات	8 ساعات	8 ساعات
وضع الاسترداد في macOS	لا شيء	دقيقة واحدة	5 دقائق	15 دقيقة	ساعة واحدة	3 ساعات	8 ساعات	انظر "كيف تعمل التأخيرات الزمنية المتصاعدة على مكافحة هجمات القوة الغاشمة في macOS" أدناه
خزنة ملفات مزودة بمفتاح استرداد (شخصي أو مؤسسي أو iCloud)	لا شيء	دقيقة واحدة	5 دقائق	15 دقيقة	ساعة واحدة	3 ساعات	8 ساعات	انظر "كيف تعمل التأخيرات الزمنية المتصاعدة على مكافحة هجمات القوة الغاشمة في macOS" أدناه
رمز PIN للقفل عن بُعد في macOS	دقيقة واحدة	5 دقائق	15 دقيقة	30 دقيقة	ساعة واحدة	ساعة واحدة	ساعة واحدة	ساعة واحدة

إذا تم تشغيل خيار مسح البيانات لـ iPhone أو iPad (في الإعدادات > [بصمة الوجه] أو [بصمة الإصبع] ورمز الدخول)، تتم إزالة جميع المحتويات والإعدادات من جهاز التخزين بعد 10 محاولات غير صحيحة متتابعة لإدخال رمز الدخول. ولا يتم حساب المحاولات المتتالية لنفس رمز الدخول غير الصحيح في حدود هذا الحد. يتوفر هذا الإعداد أيضًا كسياسة إدارية من خلال حل إدارة الأجهزة المحمولة (MDM) الذي يدعم هذه الميزة وعبر Microsoft Exchange ActiveSync، ويمكن تعيينه على حد أقل.

على الأجهزة التي تحتوي على Secure Enclave، يتم فرض التأخير بواسطة Secure Enclave. وإذا تمت إعادة تشغيل الجهاز أثناء تأخير زمني، يظل التأخير ساري النفاذ، مع بدء المؤقت من جديد للفترة الحالية.

كيف تعمل التأخيرات الزمنية المتصاعدة على مكافحة هجمات القوة الغاشمة في macOS

للمساعدة على منع هجمات القوة الغاشمة، عند بدء تشغيل Mac، لا يُسمح بأكثر من 10 محاولة لإدخال كلمة السر في نافذة تسجيل، ويتم فرض تأخيرات زمنية متصاعدة بعد عدد معين من المحاولات غير الصحيحة. يتم فرض التأخيرات بواسطة Secure Enclave. وإذا تمت إعادة تشغيل الـ Mac أثناء تأخير زمني، يظل التأخير ساري النفاذ، مع بدء المؤقت من جديد للفترة الحالية.

للمساعدة على منع البرامج الضارة من التسبب في فقدان دائم للبيانات من خلال محاولة مهاجمة كلمة سر المستخدم، لا تُفرض هذه الحدود بعد أن يسجل المستخدم الدخول إلى Mac بنجاح، ولكن يُعاد فرضها بعد إعادة التشغيل. إذا تم استنفاد المحاولات العشرة، تكون هناك 10 محاولات أخرى متاحة بعد إعادة التشغيل في recoveryOS. وإذا تم استنفاد تلك المحاولات أيضًا، تكون هناك 10 محاولة إضافية متاحة لكل آلية استرداد خزنة الملفات (استرداد iCloud ومفتاح استرداد خزنة الملفات والمفتاح المؤسسي)، بحد أقصى 30 محاولة إضافية. بعد استنفاد تلك المحاولات الإضافية، تصبح Secure Enclave غير قادرة على معالجة أي طلبات لفك تشفير وحدة التخزين أو التحقق من كلمة السر، وتصبح البيانات الموجودة على محرك الأقراص غير قابلة للاسترداد.

للمساعدة على حماية البيانات في بيئة مؤسسية، يجب على قسم تكنولوجيا المعلومات (IT) تحديد سياسات تكوين خزنة الملفات وفرضها باستخدام حل MDM. ويتوفر لدى المؤسسات العديد من الخيارات لإدارة وحدات التخزين المشفرة، بما في ذلك مفاتيح الاسترداد المؤسسية أو مفاتيح الاسترداد الشخصية (التي يمكن تخزينها اختياريًا باستخدام MDM للضمان) أو مزيج من الاثنين. يمكن أيضًا تعيين تدوير المفاتيح كسياسة في MDM.

على Mac المزود بشريحة Apple T2 الأمنية، تؤدي كلمة السر وظيفة مماثلة، باستثناء أن المفتاح المنشأ يُستخدم لتشفير خزنة الملفات بدلاً من حماية البيانات. كما يوفر macOS خيارات إضافية لاسترداد كلمة السر:

- استرداد iCloud
- استرداد خزنة الملفات
- مفتاح خزنة الملفات المؤسسي

حماية البيانات

نظرة عامة على حماية البيانات

تستخدم Apple تقنية تسمى حماية البيانات لحماية البيانات المخزنة في وحدة تخزين فلاش على الأجهزة التي تدعم Apple SoC—مثل الـ iPhone والـ iPad والـ Apple Watch والـ Apple TV والـ Mac المزود برقاقات Apple. باستخدام حماية البيانات، يمكن لأي جهاز الاستجابة للأحداث الشائعة، مثل المكالمات الهاتفية الواردة، مع توفير مستوى عالٍ من التشفير لبيانات المستخدم في الوقت نفسه. تقوم بعض تطبيقات النظام (مثل الرسائل والبريد والتقويم وجهات الاتصال والصور) وقيم بيانات الصحة باستخدام حماية البيانات بشكل افتراضي. تتلقى تطبيقات الجهات الخارجية هذه الحماية تلقائيًا.

التنفيذ

يتم تنفيذ حماية البيانات من خلال إنشاء وإدارة تسلسل هرمي للمفاتيح، وتعتمد على تقنيات تشفير المكونات المادية المضمنة في أجهزة Apple. ويتم التحكم في حماية البيانات على أساس كل ملف عن طريق تعيين كل ملف إلى فئة؛ ويتم تحديد إمكانية الوصول وفقًا لما إذا كان قد تم فتح قفل مفاتيح الفئات أم لا. يسمح نظام ملفات Apple (APFS) لنظام الملفات بإمكانية تقسيم المفاتيح إلى أساس لكل مدى (حيث يمكن وجود مفاتيح مختلفة لأجزاء من الملف).

في كل مرة يتم فيها إنشاء ملف على وحدة تخزين البيانات، تنشئ حماية البيانات مفتاح 256 بت جديدًا (**مفتاح لكل ملف**) وترسله إلى محرك AES المادي الذي يستخدم المفتاح لتشفير الملف في أثناء كتابته إلى وحدة تخزين الفلاش. على أجهزة A14 إلى A17 و M1 إلى M3، يستخدم التشفير AES-256 في نمط XTS حيث يمر المفتاح لكل ملف 256 بت من خلال وظيفة اشتقاق المفاتيح (إصدار NIST الخاص 108 -800) لاشتقاق قرص 256 بت ومفتاح تشفير 256 بت. على أجهزة A9 إلى A13 و S5 إلى S9، يستخدم التشفير AES-128 في نمط XTS، حيث يتم تقسيم المفتاح لكل ملف 256 بت لتوفير قرص 128 بت ومفتاح تشفير 128 بت.

على Mac المزود برقاقات Apple، يتم تعيين حماية البيانات بشكل افتراضي على الفئة C (انظر فئات حماية البيانات)، ولكنها تستخدم مفتاح وحدة تخزين بدلاً من مفتاح لكل نطاق أو لكل ملف—وهذا يعمل على إعادة إنشاء نموذج أمن خزنة الملفات لبيانات المستخدم بفعالية. يجب على المستخدمين مواصلة الاشتراك في خزنة الملفات لتلقي الحماية الكاملة لتشابك التسلسل الهرمي لمفاتيح التشفير مع كلمة السر الخاصة بهم. ويستطيع المطورون أيضًا الاشتراك في فئة حماية أعلى تستخدم مفتاحًا لكل ملف أو لكل نطاق.

حماية البيانات في أجهزة Apple

على أجهزة Apple المزودة بحماية البيانات، يكون كل ملف محميًا بمفتاح فريد لكل ملف (أو لكل نطاق). والمفتاح، الذي تم تغليفه باستخدام خوارزمية تغليف مفاتيح NIST AED، يتم تغليفه أيضًا بأحد مفاتيح الفئات المتعددة، اعتمادًا على تحديد كيفية الوصول إلى الملف. بعد ذلك يتم تخزين المفتاح لكل ملف المغلّف في بيانات التعريف الخاصة بالملف.

قد تدعم الأجهزة التي بتنسيق APFS استنساخ الملفات (نُسخ ذات تكلفة صفرية تستخدم تقنية النسخ عند الكتابة). إذا تم استنساخ ملف، يحصل كل نصف من النسخة المستنسخة على مفتاح جديد لقبول عمليات الكتابة الواردة حتى تتم كتابة البيانات الجديدة على الوسائط باستخدام مفتاح جديد. بمرور الوقت، قد يصبح الملف مركبًا من نطاقات متعددة (أو أجزاء)، يتم تعيين كل منها إلى مفاتيح مختلفة. ومع ذلك، تتم حماية كل النطاقات التي تُكوّن الملف بواسطة نفس مفتاح الفئة.

عند فتح ملف ما، يتم فك تشفير بيانات التعريف الخاصة به باستخدام مفتاح نظام الملفات، مع الكشف عن المفتاح لكل ملف المغلّف بجانب تعليق حول الفئة التي تحميه. يتم فك تغليف المفتاح لكل ملف (أو لكل مدى) باستخدام مفتاح الفئة، ثم يتم توفيره لمحرك AES المادي، الذي يفك تشفير الملف أثناء قراءته من مساحة تخزين الفلاش. تحدث معالجة جميع مفاتيح الملفات المغلفة في Secure Enclave؛ لا يتم كشف مفتاح الملف مباشرةً لمعالج التطبيقات أبدًا. عند بدء التشغيل، يتفاوض Secure Enclave على مفتاح مؤقت مع محرك AES. عندما يفك Secure Enclave تغليف مفاتيح الملف، تتم إعادة تغليفه بالمفتاح المؤقت ويتم إرساله مرة أخرى إلى معالج التطبيقات.

يتم تشفير بيانات التعريف لجميع الملفات في نظام ملفات وحدة تخزين البيانات باستخدام مفتاح وحدة تخزين عشوائي يتم إنشاؤه عند تثبيت نظام التشغيل لأول مرة أو عند مسح المستخدم للجهاز. يتم تشفير هذا المفتاح وتغليفه بواسطة مفتاح تغليف مفاتيح لا تعرفه سوى Secure Enclave من أجل التخزين طويل الأجل. يتغير مفتاح تغليف المفاتيح مع كل مرة يمسح فيها المستخدم جهازه. في SoCs على A9 (وأحدث)، تعتمد Secure Enclave على إنتروبيا، مدعومة بأنظمة غير قابلة لإعادة التشغيل، لتحقيق قابلية المسح ولحماية مفتاح تغليف المفاتيح الخاص بها، من بين الأصول الأخرى. لمزيد من المعلومات، انظر التخزين غير المتطاير الآمن.

تمامًا مثل المفاتيح لكل ملف أو لكل مدى، فإن مفتاح بيانات التعريف الخاص بوحدة تخزين البيانات لا يُكشف أبدًا لمعالج التطبيقات بشكل مباشر؛ توفر Secure Enclave إصدارًا سريع الزوال لكل تمهيد بدلاً من ذلك. عند التخزين، يتم تغليف مفتاح نظام الملفات المُشفّر أيضًا بواسطة "مفتاح قابل للمسح" مخزن في التخزين القابل للمسح أو باستخدام مفتاح تغليف مفتاح الوسائط، ومحمي بآلية Secure Enclave غير القابلة لإعادة التشغيل. ولا يوفر هذا المفتاح سرية إضافية للبيانات. بدلاً من ذلك، تم تصميمه ليتم مسحه سريعًا عند الطلب (بواسطة المستخدم عبر خيار "مسح جميع المحتويات والإعدادات" أو عن طريق مستخدم أو مسؤول يُصدر أمر مسح عن بُعد من أحد حلول إدارة جهاز الجوال (MDM) أو Microsoft Exchange ActiveSync أو iCloud). ويؤدي مسح المفتاح بهذه الطريقة إلى جعل جميع الملفات غير قابلة للوصول إليها بطريقة مشفرة.

قد يتم تشفير محتويات الملف باستخدام مفتاح واحد أو أكثر من المفاتيح لكل ملف (أو لكل مدى) يتم تغليفها بمفتاح فئة وتخزينه في بيانات التعريف الخاصة بالملف، والذي بدوره يتم تشفيره باستخدام مفتاح نظام الملفات. ويكون مفتاح الفئة محميًا بواسطة معرف UID للمكونات المادية، ورمز دخول المستخدم بالنسبة لبعض الفئات. يوفر هذا التسلسل الهرمي المرونة والأداء. على سبيل المثال، لا يتطلب تغيير فئة الملف إلا إعادة تغليف المفتاح لكل ملف الخاص به، ويؤدي تغيير رمز الدخول فقط إلى إعادة تغليف مفتاح الفئة.

فئات حماية البيانات

عند إنشاء ملف جديد على الأجهزة التي تدعم حماية البيانات، يتم تعيينه إلى فئة بواسطة التطبيق الذي يقوم بإنشائه. وتستخدم كل فئة سياسات مختلفة لتحديد متى يمكن الوصول إلى البيانات. يتوفر وصف للفئات والسياسات الأساسية في الأقسام التالية. علمًا بأن أجهزة كمبيوتر Mac المزودة برقاقات Apple لا تدعم الفئة D: لا توجد حماية، ويتم تحديد حد أمني حول تسجيل الدخول والخروج (لا يتم القفل أو فتح القفل كما هو الحال على iPhone و iPad).

الفئة	نوع الحماية
الفئة A: الحماية الكاملة	NSFileProtectionComplete
الفئة B: محمية ما لم تُفتح	NSFileProtectionCompleteUnlessOpen
الفئة C: محمية حتى أول مصادقة من المستخدم **ملاحظة:** يستخدم macOS مفتاح وحدة تخزين لإعادة إنشاء خصائص حماية خزنة الملفات.	NSFileProtectionCompleteUntilFirstUserAuthentication
الفئة D: بلا حماية **ملاحظة:** غير مدعومة على macOS.	NSFileProtectionNone

الحماية الكاملة

NSFileProtectionComplete: يكون مفتاح الفئة محميًا بمفتاح مشتق من رمز دخول أو كلمة سر المستخدم ومعرف UID للجهاز. وبعد فترة وجيزة من قفل المستخدم للجهاز (10 ثوانٍ، إذا كان إعداد "يلزم إدخال كلمة السر" هو "فورًا")، يتم تجاهل مفتاح الفئة الذي تم فك تشفيره، ما يجعل الوصول إلى جميع البيانات في هذه الفئة غير ممكن حتى يُدخل المستخدم رمز الدخول مرة أخرى أو يفتح قفل الجهاز (يسجل الدخول إليه) باستخدام بصمة الوجه أو بصمة الإصبع.

في macOS، بعد تسجيل خروج المستخدم الأخير بفترة وجيزة، يتم تجاهل مفتاح الفئة الذي تم فك تشفيره، مما يجعل الوصول إلى كل البيانات في هذه الفئة غير ممكن حتى يُدخِل أي مستخدم رمز الدخول مرة أخرى أو يسجّل الدخول إلى الجهاز باستخدام بصمة الإصبع.

محمية ما لم تُفتح

NSFileProtectionCompleteUnlessOpen: قد تكون هناك حاجة إلى كتابة بعض الملفات أثناء قفل الجهاز أو عند تسجيل خروج المستخدم. من الأمثلة الجيدة على ذلك تنزيل مرفق بريد في الخلفية. يتم تحقيق هذا السلوك باستخدام تشفير منحنى القطع الناقص غير المتماثل (ECDH عبر Curve25519). ويكون المفتاح لكل ملف المعتاد محميًا بواسطة مفتاح مشتق باستخدام اتفاقية مفتاح One-Pass Diffie-Hellman كما هو موضح في NIST SP 800-56A.

يتم تخزين المفتاح العام سريع الزوال للاتفاقية إلى جانب المفتاح لكل ملف المغلّف. إن KDF هي وظيفة اشتقاق مفتاح التسلسل (البديل المعتمد 1) كما هو موضح في البند 5.8.1 من NIST SP 800-56A. تم إهمال AlgorithmID. PartyUInfo و PartyVInfo هما المفتاحان العامان سريع الزوال والثابت، على التوالي. ويتم استخدام SHA256 كدالة تجزئة. بمجرد إغلاق الملف، يتم مسح المفتاح لكل ملف من الذاكرة. لفتح الملف مرة أخرى، تتم إعادة إنشاء السر المشترك باستخدام المفتاح الخاص للفئة "محمية ما لم تُفتح" والمفتاح العام سريع الزوال للملف، اللذين يتم استخدامهما لفك تغليف المفتاح لكل ملف الذي يتم استخدامه بعد ذلك لفك تشفير الملف.

في macOS، يمكن الوصول إلى الجزء الخاص بـ NSFileProtectionCompleteUnlessOpen طالما تم تسجيل دخول أي مستخدم على النظام أو تمت المصادقة عليه.

محمية حتى أول مصادقة من المستخدم

NSFileProtectionCompleteUntilFirstUserAuthentication: تتصرف هذه الفئة بنفس طريقة "الحماية الكاملة"، باستثناء أن مفتاح الفئة الذي تم فك تشفيره لا تتم إزالته من الذاكرة عند قفل الجهاز أو تسجيل خروج المستخدم. وتتمتع الحماية في هذه الفئة بخصائص مشابهة لتشفير وحدة التخزين الكاملة لسطح المكتب، وتحمي البيانات من الهجمات التي تنطوي على إعادة تشغيل. هذه هي الفئة الافتراضية لجميع بيانات تطبيقات الجهات الخارجية التي لم يتم تخصيصها بأي طريقة إلى فئة من فئات حماية البيانات.

في macOS، تستخدم هذه الفئة مفتاح وحدة تخزين يمكن الوصول إليه طالما تم تركيب وحدة التخزين، وتعمل تمامًا مثل خزنة الملفات.

بلا حماية

NSFileProtectionNone: يكون مفتاح الفئة هذا محميًا بمعرف UID فقط، ويتم الاحتفاظ به في التخزين القابل للمسح. نظرًا لأن جميع المفاتيح اللازمة لفك تشفير الملفات في هذه الفئة مخزنة على الجهاز، فإن التشفير لا يتيح إلا ميزة المسح السريع عن بُعد. إذا لم يتم تعيين الملف إلى فئة من فئات حماية البيانات، يظل مُخزنًا في شكل مشفر (كما هو الحال مع جميع البيانات الموجودة على جهاز iOS و iPadOS).

وهذا غير مدعوم في macOS.

ملاحظة: في macOS، بالنسبة لوحدات التخزين التي لا تتوافق مع نظام التشغيل الذي تم تمهيده، يمكن الوصول إلى كل فئات حماية البيانات طالما تم تثبيت وحدة التخزين. وتعد الفئة NSFileProtectionComple teUntilFirstUserAuthentication فئة حماية البيانات الافتراضية. تتوفر وظيفة المفتاح لكل مدى لكل من Rosetta 2 والتطبيقات الأصلية.

حافظات المفاتيح لحماية البيانات

تُجمَّع المفاتيح الخاصة بكل من فئات حماية البيانات في الملفات وسلسلة المفاتيح في حافظات المفاتيح وتُدار على iOS و iPadOS و tvOS و watchOS. تستخدم أنظمة التشغيل حافظات المفاتيح التالية: المستخدم والجهاز والنسخ الاحتياطي والضمان ونسخ iCloud الاحتياطي.

حافظة مفاتيح المستخدم

حافظة مفاتيح المستخدم هي المكان الذي يتم فيه تخزين مفاتيح الفئات المغلفة المستخدمة في التشغيل العادي للجهاز. على سبيل المثال، عند إدخال رمز دخول، يتم تحميل **NSFileProtectionComplete** من حافظة مفاتيح المستخدم ويتم تغليفها. إنه ملف قائمة خصائص ثنائية (.plist) مخزّن في الفئة "بلا حماية".

بالنسبة للأجهزة التي تحتوي على SoCs أقدم من A9، يتم تشفير محتويات ملف .plist بمفتاح محفوظ في التخزين القابل للمسح. لتوفير الأمن لحافظات المفاتيح، يتم مسح هذا المفتاح ومنحه من جديد في كل مرة يغيّر فيها المستخدم رمز الدخول الخاص به.

بالنسبة إلى الأجهزة المزودة بـ SoCs من فئة A9 أو أحدث، يتضمن ملف .plist مفتاحًا يشير إلى تخزين حافظة المفاتيح في خزانة محمية بواسطة قيمة غير قابلة لإعادة التشغيل – تتحكم فيها Secure Enclave.

تدير Secure Enclave حافظة مفاتيح المستخدم ويمكن الاستعلام عنها فيما يتعلق بحالة قفل الجهاز. وتشير إلى أنه لم يتم فتح قفل الجهاز إلا إذا كان يمكن الوصول إلى جميع مفاتيح الفئات الموجودة في حافظة مفاتيح المستخدم وتم فك تغليفها بنجاح.

حافظة مفاتيح الجهاز

تُستخدم حافظة مفاتيح الجهاز لتخزين مفاتيح الفئات المُغلفة المستخدمة في العمليات التي تتضمن بيانات خاصة بالجهاز. وتحتاج أجهزة iPadOS التي تم تكوينها للاستخدام المشترك في بعض الأحيان إلى الوصول إلى بيانات الاعتماد قبل قيام أي مستخدم بتسجيل الدخول؛ ولذلك، يلزم وجود حافظة مفاتيح غير محمية برمز دخول المستخدم.

لا يدعم iOS و iPadOS الفصل المشفر لمحتوى نظام الملفات لكل مستخدم، مما يعني أن النظام يستخدم مفاتيح الفئات من حافظة مفاتيح الجهاز لتغليف المفاتيح لكل ملف. ومع ذلك، فإن سلسلة المفاتيح تستخدم مفاتيح الفئات من حافظة مفاتيح المستخدم لحماية العناصر الموجودة في سلسلة مفاتيح المستخدم. في أجهزة iPhone و iPad التي تم تكوينها للاستخدام من قِبل مستخدم واحد (التكوين الافتراضي)، تصبح حافظة مفاتيح الجهاز وحافظة مفاتيح المستخدم واحدة ومتماثلة ومحمية بواسطة رمز دخول المستخدم.

حافظة مفاتيح النسخ الاحتياطي

يتم إنشاء حافظة مفاتيح النسخ الاحتياطي عند عمل نسخة احتياطية مشفرة بواسطة iTunes (في macOS 10.15 أو أقدم) أو فايندر (في macOS 10.14 أو أحدث) وتخزينها على الكمبيوتر الذي تم عمل نسخة احتياطية من الجهاز عليه. ويتم إنشاء حافظة مفاتيح جديدة بها مجموعة جديدة من المفاتيح، وتتم إعادة تشفير البيانات المنسوخة احتياطيًا لهذه المفاتيح الجديدة. كما هو موضح سابقًا، تظل عناصر سلسلة المفاتيح غير المرتحلة مغلّفةً بالمفتاح المشتق من UID، مما يسمح باستعادتها إلى الجهاز الذي تم نسخها احتياطيًا منه في الأصل ولكن يتم جعلها غير قابلة للوصول إليها على جهاز مختلف.

يتم تشغيل حافظة المفاتيح - المحمية بمجموعة كلمات السر - من خلال 10 ملايين تكرار من وظيفة اشتقاق المفتاح PBKDF2. وعلى الرغم من هذا العدد الكبير من التكرارات، لا يوجد رابط بجهاز معين، وبالتالي يمكن نظريًا شن هجوم القوة الغاشمة بشكل متوازٍ عبر العديد من أجهزة الكمبيوتر على حافظة المفاتيح المنسوخة احتياطيًا. يمكن التخفيف من شدة هذا التهديد بكلمة سر قوية بما فيه الكفاية.

إذا اختار المستخدم عدم تشفير النسخة الاحتياطية، فلا يتم تشفير الملفات بغض النظر عن فئة حماية البيانات الخاصة بها ولكن تبقى سلسلة المفاتيح محمية بمفتاح مشتق من UID. وهذا هو السبب في أن عناصر سلسلة المفاتيح لا تنتقل إلى جهاز جديد إلا إذا تم تعيين كلمة سر للنسخة الاحتياطية.

حافظة مفاتيح الضمان

يتم استخدام حافظة مفاتيح الضمان للمزامنة مع فايندر (في macOS 10.15 أو أحدث) أو iTunes (في macOS 10.14 أو أقدم) عبر USB وإدارة جهاز الجوال (MDM). وتتيح حافظة المفاتيح هذه لكل من فايندر أو iTunes إجراء النسخ الاحتياطي والمزامنة دون مطالبة المستخدم بإدخال رمز دخول، كما تتيح لحل MDM مسح رمز دخول المستخدم عن بُعد. ويتم تخزينها على الكمبيوتر الذي يُستخدم للمزامنة مع فايندر أو iTunes أو على حل MDM الذي يدير الجهاز عن بُعد.

تعمل حافظة مفاتيح الضمان على تحسين تجربة المستخدم أثناء مزامنة الجهاز، مما قد يتطلب الوصول إلى جميع فئات البيانات. عند توصيل جهاز مقفل برمز الدخول بفايندر أو iTunes لأول مرة، تتم مطالبة المستخدم بإدخال رمز دخول. ويُنشئ الجهاز بعد ذلك حافظة مفاتيح ضمان تحتوي على نفس مفاتيح الفئات المستخدمة على الجهاز، وتكون محمية بمفتاح تم إنشاؤه حديثًا. يتم تقسيم حافظة مفاتيح الضمان والمفتاح الذي يحميها بين الجهاز والمضيف أو الخادم، مع تخزين البيانات على الجهاز في الفئة "محمية حتى أول مصادقة من المستخدم". لهذا السبب يجب إدخال رمز دخول الجهاز قبل قيام المستخدم بالنسخ الاحتياطي باستخدام فايندر أو iTunes لأول مرة بعد إعادة التمهيد.

في حالة تحديث البرامج عبر الأثير (OTA)، تتم مطالبة المستخدم برمز الدخول عند بدء التحديث. ويُستخدم ذلك لإنشاء رمز فتح القفل لمرة واحدة بشكل آمن، والذي يفتح قفل حافظة مفاتيح المستخدم بعد التحديث. لا يمكن إنشاء هذا الرمز دون إدخال رمز دخول المستخدم، ويتم إبطال أي رمز تم إنشاؤه سابقًا في حالة تغيير رمز دخول المستخدم.

إن رموز فتح القفل لمرة واحدة مخصصة إما للتثبيت المراقب أو غير المراقب لتحديث البرامج. ويتم تشفيرها باستخدام مفتاح مشتق من القيمة الحالية لعدّاد رتيب في Secure Enclave ومعرف UUID الخاص بحافظة المفاتيح ومعرف UID الخاص بـ Secure Enclave.

على SoCs في A9 (أو أحدث)، لم يعد رمز فتح القفل لمرة واحدة يعتمد على العدّادات أو التخزين القابل للمسح. بدلاً من ذلك، يكون محميًا بواسطة قيمة غير قابلة لإعادة التشغيل تتحكم فيها Secure Enclave.

تنتهي صلاحية رمز فتح القفل لمرة واحدة لتحديثات البرامج المراقبة بعد 20 دقيقة. في iOS 13 و iPadOS 13.1 أو أحدث، يُخزَّن الرمز في خزانة محمية بواسطة Secure Enclave. قبل iOS 13، كان يتم تصدير هذا الرمز من Secure Enclave وتتم كتابته على التخزين القابل للمسح أو يكون محميًا بواسطة آلية Secure Enclave غير القابلة لإعادة التشغيل. ويزيد مؤقت السياسة من قيمة العداد في حالة عدم إعادة تمهيد الجهاز في غضون 20 دقيقة.

تجري تحديثات البرامج غير المراقبة عندما يكتشف النظام وجود تحديث متوفر وعندما يكون أي مما يلي صحيحًا:

- تكوين تحديثات تلقائية في iOS 12 أو أحدث.
- اختيار المستخدم "تثبيت لاحقًا" عند إخطاره بالتحديث.

بعد أن يُدخل المستخدم رمز الدخول، يتم إنشاء رمز فتح القفل لمرة واحدة ويمكن أن يظل صالحًا في Secure Enclave لمدة تصل إلى 8 ساعات. إذا لم يكن قد تم التحديث بعد، يتم إتلاف رمز فتح القفل لمرة واحدة مع كل قفل ويُعاد إنشاؤه مع كل فتح قفل لاحق. ومع كل فتح قفل يبدأ الإطار الزمني الذي مدته 8 ساعات من جديد. بعد 8 ساعات، يقوم مؤقت السياسة بإبطال رمز فتح القفل لمرة واحدة.

حافظة مفاتيح نسخ iCloud الاحتياطي

تشبه حافظة مفاتيح نسخ iCloud الاحتياطي حافظة مفاتيح النسخ الاحتياطي. تكون جميع مفاتيح الفئات في حافظة المفاتيح هذه غير متماثلة (باستخدام Curve25519، مثل فئة حماية البيانات "محمية ما لم تُفتح"). تُستخدَم حافظة المفاتيح غير المتماثلة كذلك لحماية سلسلة المفاتيح المنسوخة احتياطيًا لاسترداد سلسلة مفاتيح iCloud.

حماية المفاتيح في أنماط التمهيد البديلة

تم تصميم حماية البيانات لتوفير الوصول إلى بيانات المستخدم بعد المصادقة الناجحة فقط، وللمستخدم المُعتمَد فقط. وتم تصميم فئات حماية البيانات لدعم مجموعة متنوعة من حالات الاستخدام، مثل القدرة على قراءة بعض البيانات وكتابتها حتى عندما يكون الجهاز مقفلاً (ولكن بعد إلغاء القفل لأول مرة). يتم اتخاذ خطوات إضافية لحماية الوصول إلى بيانات المستخدم أثناء أنماط التمهيد البديلة مثل تلك التي يتم استخدامها في نمط تحديث البرنامج الثابت للجهاز (DFU) أو نمط الاسترداد أو تشخيصات Apple أو حتى أثناء تحديث البرامج. وتستند هذه الإمكانات إلى مزيج من ميزات المكونات المادية والبرامج، وقد تم توسيعها مع تطور السيليكون الذي صممته Apple.

الميزة	A10	A11 إلى A17 S3 إلى S9 M1 و M2 و M3
الاسترداد: محمي بكل فئات حماية البيانات	✓	✓
أنماط التمهيد البديلة لكل من نمط DFU والاسترداد وتحديثات البرامج: حماية البيانات من الفئة A و B و C	✗	✓

تم تزويد محرك Secure Enclave AES بوحدات بت جذرية برمجية قابلة للقفل. عند إنشاء المفاتيح من UID، يتم تضمين وحدات البت الجذرية هذه في دالة اشتقاق المفتاح لإنشاء تسلسلات هرمية إضافية للمفاتيح. تختلف طريقة استخدام البت الجذري وفقًا للنظام الموجود على الشريحة:

- بدءًا من SoCs من فئة Apple A10 و S3، تم تخصيص بت جذري لتمييز المفاتيح المحمية برمز دخول المستخدم. يتم تعيين البت الجذري للمفاتيح التي تتطلب رمز دخول المستخدم (بما في ذلك مفاتيح الفئة A والفئة B والفئة C لحماية البيانات)، ومسحه للمفاتيح التي لا تتطلب رمز دخول المستخدم (بما في ذلك مفتاح بيانات تعريف نظام الملفات ومفاتيح الفئة D).

- في iOS 13 أو أحدث و iPadOS 13.1 أو أحدث على الأجهزة التي تحتوي على A10 أو أحدث، يتم جعل جميع بيانات المستخدم غير قابلة للوصول إليها بطريقة مشفرة عند تمهيد الأجهزة في نمط التشخيصات. ويتم تحقيق ذلك من خلال إدخال بت جذري إضافي يتحكم إعداده في القدرة على الوصول إلى مفتاح الوسائط، وهو ضروري بحد ذاته للوصول إلى بيانات التعريف (وبالتالي المحتويات الخاصة بجميع الملفات) الموجودة على وحدة تخزين البيانات المشفرة باستخدام حماية البيانات. تشمل هذه الحماية الملفات المحمية في جميع الفئات (A و B و C و D)، وليس فقط تلك التي تتطلب رمز دخول المستخدم.
- في A12 SoCs، تقوم Boot ROM في Secure Enclave بقفل البت الجذري لرمز الدخول إذا كان معالج التطبيقات قد دخل في نمط ترقية البرنامج الثابت للجهاز (DFU) أو وضع الاسترداد. عند قفل البت الجذري لرمز الدخول، لا يُسمح بإجراء أي عملية لتغييره. وهذا يمنع الوصول إلى البيانات المحمية برمز دخول المستخدم.

تؤدي استعادة الجهاز بعد دخوله إلى وضع DFU إلى إعادته إلى حالة جيدة معروفة مع التأكد من وجود رمز موقع من قبل Apple غير معدّل فقط. يمكن الدخول في وضع DFU يدويًا.

راجع مقالات دعم Apple التالية حول كيفية وضع جهاز في وضع DFU:

الجهاز	مقال دعم Apple
iPhone و iPad	إذا نسيت رمز مرور iPhone
Apple TV	إذا ظهر لك رمز تحذير على Apple TV
Mac مزود بسيليكون Apple	كيفية إنعاش أو استعادة البرنامج الثابت لـ Mac

حماية بيانات المستخدم في مواجهة الهجوم

غالبًا ما يحاول المهاجمون الذين يحاولون استخراج بيانات المستخدم استخدام عدد من التقنيات: استخراج البيانات المُشفَّرة إلى وسيطة أخرى بهدف شن هجوم بقوة غاشمة أو التلاعب بإصدار نظام التشغيل أو تغيير سياسة الأمن للجهاز أو إضعافها لتسهيل الهجوم. غالبًا ما تتطلب مهاجمة البيانات الموجودة على الجهاز الاتصال بالجهاز باستخدام واجهات مادية مثل ثندربولت أو لايتننغ أو USB-C. وتشتمل أجهزة Apple على ميزات للمساعدة في منع مثل هذه الهجمات.

تدعم أجهزة Apple تقنية تسمى **حماية المفاتيح المؤمنة (SKP)** مصممة لضمان عدم توفر مواد التشفير خارج الجهاز، أو يتم استخدامها إذا تم إجراء عمليات تلاعب في إصدارات نظام التشغيل أو إعدادات الأمن دون الحصول على تصريح مناسب من المستخدم. **لا** تتوفر هذه الميزة بواسطة Secure Enclave، بل تدعمها سجلات المكونات المادية الموجودة في الطبقة السفلية لتوفير طبقة إضافية من الحماية للمفاتيح الضرورية لتشفير بيانات المستخدم المستقلة عن Secure Enclave.

ملاحظة: لا يتوفر SKP إلا على الأجهزة التي تحتوي على SoC المصمم من Apple.

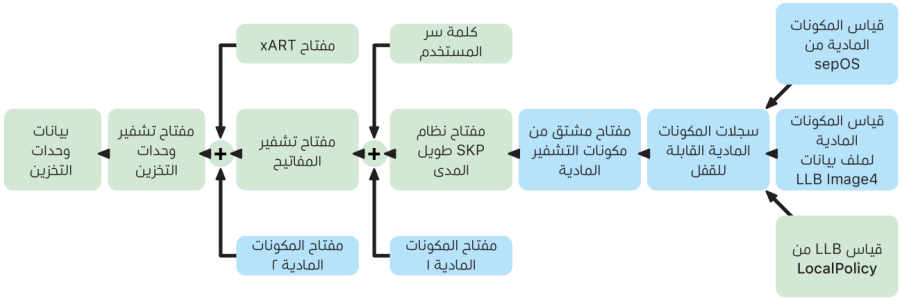
الميزة	A11 إلى A17 S3 إلى S9 M1 و M2 و M3
حماية المفاتيح المؤمنة	✓

يمكن أيضًا تكوين أجهزة iPhone و iPad لتنشيط اتصالات البيانات فقط في الحالات التي من المرجح أن تشير إلى أن الجهاز لا يزال تحت التحكم المادي للمالك المعتمد.

حماية المفاتيح المؤمنة (SKP)

في أجهزة Apple التي تدعم حماية البيانات، تتم حماية (أو تأمين) مفتاح تشفير المفاتيح (KEK) باستخدام قياسات البرامج على النظام، بالإضافة إلى ربطه بمعرف UID المتوفر فقط من Secure Enclave. على أجهزة كمبيوتر Apple المزودة بسيليكون Apple، يتم تعزيز حماية KEK من خلال دمج معلومات حول سياسة الأمن على النظام، لأن macOS يدعم تغييرات سياسة الأمن المهمة (على سبيل المثال، تعطيل التمهيد الآمن أو SIP) غير المدعومة على أنظمة أساسية أخرى. على أجهزة كمبيوتر Mac المزودة بسيليكون Apple، تتضمن هذه الحماية مفاتيح خزنة الملفات، لأنه يتم تنفيذ خزنة الملفات باستخدام ميزة حماية البيانات (الفئة C).

يُطلق على المفتاح الناتج عن تشابك كلمة سر المستخدم ومفتاح SKP طويل الأجل ومفتاح الجهاز 1 (معرف UID من Secure Enclave) **المفتاح المشتق من كلمة السر**. يُستخدم هذا المفتاح لحماية حاوية مفاتيح المستخدم (على جميع الأنظمة الأساسية المدعومة) و KEK (على macOS فقط)، ثم تمكين فتح القفل بالمقاييس الحيوية أو فتح القفل التلقائي باستخدام الأجهزة الأخرى مثل Apple Watch.



يلتقط مراقب التمهيد في Secure Enclave قياس نظام تشغيل Secure Enclave الذي يتم تحميله. عندما تقيس Boot ROM الخاصة بمعالج التطبيقات ملف بيانات Image4 المرفق بـ LLB، يحتوي ملف البيانات هذا على قياس لكل البرامج الثابتة الأخرى المقترنة بالنظام والتي يتم تحميلها أيضًا. تحتوي LocalPolicy على التكوينات الأمنية الأساسية لـ macOS التي يتم تحميلها. وتحتوي LocalPolicy أيضًا على الحقل `nsih` وهو تجزئة لملف بيانات Image4 على macOS. يحتوي ملف بيانات Image4 في macOS على قياسات لكل البرامج الثابتة المقترنة بـ macOS وكائنات تمهيد macOS الأساسية مثل مجموعة Boot Kernel أو تجزئة جذر وحدة تخزين النظام الموقَّعة (SSV).

إذا تمكّن المهاجم من تغيير أي من البرامج الثابتة أو البرامج أو مكونات التكوين الأمني المقيسة الواردة أعلاه بشكل غير متوقع، فإنه يقوم بتعديل القياسات المُخزّنة في سجلات المكونات المادية. يتسبب تعديل القياسات في اشتقاق **مفتاح جذر قياس النظام (SMRK)** المشتق من مكونات التشفير المادية إلى قيمة مختلفة، كسر الختم بشكل فعال على التسلسل الهرمي للمفاتيح. وهذا يؤدي إلى انعدام إمكانية الوصول إلى **مفتاح جهاز قياس النظام (SMDK)**، مما يتسبب بدوره في جعل KEK، ومن ثمَّ البيانات، منيعةً ضد الوصول إليها.

ومع ذلك، يجب أن يستوعب النظام الذي لا يتعرض للهجوم تحديثات البرامج الشرعية التي تغيّر قياسات البرامج الثابتة والحقل `nsih` في LocalPolicy للإشارة إلى قياسات macOS الجديدة. في الأنظمة الأخرى التي تحاول تضمين قياسات البرامج الثابتة، ولكن ليس لها مصدر معروف لتقصي الحقائق، يُطلب من المستخدم تعطيل الأمن وتحديث البرنامج الثابت ثم إعادة تمكينهما بحيث يمكن التقاط أساس جديد للقياس. وهذا يزيد بشكل كبير من خطر عبث المهاجم بالبرامج الثابتة أثناء تحديث البرامج. وتُساعد النظامَ حقيقةُ أن ملف بيانات Image4 يحتوي على جميع القياسات المطلوبة. كما يمكن للمكونات المادية التي تفك تشفير SMDK باستخدام SMRK عندما تتطابق القياسات أثناء التمهيد العادي، تشفير SMDK إلى أحدث مقترح SMRK. من خلال تحديد القياسات المتوقعة بعد تحديث البرنامج، يمكن للمكونات المادية تشفير SMDK الذي يمكن الوصول إليه في نظام التشغيل الحالي، بحيث يظل قابلاً للوصول إليه في نظام التشغيل الأحدث. وبالمثل، عندما يقوم العميل بتغيير إعدادات الأمن بشكل مشروع في LocalPolicy، يجب تشفير SMDK إلى SMRK الأحدث استنادًا إلى قياس LocalPolicy التي سيقوم LLB بحسابها عند إعادة التشغيل التالية.

دور نظام ملفات Apple

نظام ملفات Apple (APFS) هو نظام ملفات خاص تم تصميمه مع وضع التشفير في الاعتبار. ويعمل APFS عبر جميع أنظمة Apple الأساسية؛ لكل من iPhone و iPad و Mac و Apple TV و Apple Watch. وبجانب تحسينه لتخزين الفلاشSSD/، يتميز بتشفير قوي وبيانات تعريف النسخ عند الكتابة ومشاركة المساحة واستنساخ الملفات والدلائل واللقطات والتحجيم السريع للدلائل وأولويات ذات حفظ آمن ذرّي وأساسيات لنظام الملفات محسّنة بالإضافة إلى تصميم فريد للنسخ عند الكتابة يستخدم إدماج الإدخال/الإخراج لتقديم أقصى أداء مع ضمان موثوقية البيانات.

مشاركة مساحة التخزين

يخصص APFS مساحة التخزين عند الطلب. عندما تحتوي حاوية APFS واحدة على وحدات تخزين متعددة، تتم مشاركة المساحة الخالية في الحاوية ويمكن تخصيصها لأي من وحدات التخزين الفردية حسب الحاجة. تستخدم كل وحدة تخزين جزءًا واحدًا فقط من الحاوية الكلية، وبالتالي فإن المساحة المتاحة هي الحجم الكلي للحاوية مطروحًا منها المساحة المستخدمة في جميع وحدات التخزين في الحاوية.

وحدات التخزين المتعددة

في macOS 10.15 أو أحدث، يجب أن تحتوي حاوية APFS المستخدمة لبدء تشغيل الـ Mac على خمس وحدات تخزين على الأقل، يتم إخفاء أول ثلاث وحدات تخزين منها عن المستخدم:

- **وحدة تخزين التمهيد المسبق:** تُعد وحدة التخزين غير مشفرة كما تتضمن البيانات اللازمة لتمهيد كل وحدة تخزين للنظام في الحاوية.
- **وحدة تخزين VM:** تُعد وحدة التخزين غير مشفرة كما تُستخدم بواسطة macOS لتخزين ملفات المبادلة المشفرة.
- **وحدة تخزين الاسترداد:** تُعد وحدة التخزين هذه غير مشفرة، كما يتعين توافرها دون فتح قفل وحدة تخزين النظام للبدء في recoveryOS.
- **وحدة تخزين النظام:** تحتوي على التالي:
  - جميع الملفات اللازمة لبدء الـ Mac
  - جميع التطبيقات المثبّتة في الأساس بواسطة macOS (التطبيقات التي تُستخدم للبقاء في مجلد Applications/ تبقى الآن في System/Applications/)

  ملاحظة: بشكل افتراضي، لا تستطيع أي عملية الكتابة إلى وحدة تخزين النظام، حتى عمليات النظام من Apple.
- **وحدة تخزين البيانات:** تحتوي على بيانات قابلة للتغيير، مثل:
  - أي بيانات داخل مجلد المستخدم، بما في ذلك الصور والموسيقى والفيديوهات والمستندات
  - التطبيقات التي ثبّتها المستخدم، بما في ذلك تطبيقات AppleScript والمؤتمت
  - إطارات العمل المخصصة والبرامج الخفية المثبّتة من قِبل المستخدم أو المؤسسة أو تطبيقات الجهات الخارجية
  - المواقع الأخرى المملوكة والقابلة للكتابة بواسطة المستخدم، مثل Applications/ و Library/ و / Users و Volumes/ و usr/local/ و private/ و var/ و tmp/

يتم إنشاء وحدة تخزين بيانات لكل وحدة تخزين نظام إضافية. وتتم مشاركة جميع وحدات تخزين التمهيد المسبق و VM والاسترداد ولا يتم تكرارها.

على الـ macOS 11 أو أحدث، يتم التقاط لقطة لوحدة تخزين النظام. يقوم نظام التشغيل بالتمهيد من لقطة لوحدة تخزين النظام، وليس مجرد من تحميل للقراءة فقط لوحدة تخزين النظام القابلة للتغيير.

في iOS و iPadOS، يتم تقسيم مساحة التخزين إلى مجلدي APFS على الأقل:

- وحدة تخزين النظام
- وحدة تخزين البيانات

حماية بيانات سلسلة المفاتيح

تحتاج العديد من التطبيقات إلى التعامل مع كلمات السر وغيرها من أجزاء البيانات القصيرة والحساسة في الوقت ذاته، مثل المفاتيح ورموز تسجيل الدخول. توفر سلسلة المفاتيح طريقة آمنة لتخزين هذه العناصر. تستخدم أنظمة تشغيل Apple المختلفة آليات مختلفة لفرض الضمانات المرتبطة بفئات حماية سلسلة المفاتيح المختلفة. في macOS (بما في ذلك أجهزة كمبيوتر Mac المزودة برقاقات Apple)، لا تُستخدَم حماية البيانات مباشرة لفرض هذه الضمانات.

نظرة عامة

يتم تشفير عناصر سلسلة المفاتيح باستخدام مفتاحي AES-256-GCM مختلفين: مفتاح جدول (بيانات تعريف) ومفتاح لكل صف (مفتاح سري). يتم تشفير بيانات تعريف سلسلة المفاتيح (جميع السمات الأخرى بخلاف kSecValue) باستخدام مفتاح بيانات التعريف لإجراء عمليات بحث سريعة، ويتم تشفير القيمة السرية (kSecValueData) باستخدام المفتاح السري. وتتم حماية مفتاح بيانات التعريف بواسطة Secure Enclave، ولكن يتم تخزينه مؤقتًا في معالج التطبيقات للسماح بالاستعلامات السريعة لسلسلة المفاتيح. يتطلب المفتاح السري دائمًا رحلة ذهاب وإياب من خلال Secure Enclave.

يتم تطبيق سلسلة المفاتيح كقاعدة بيانات SQLite مخزنة على نظام الملفات. لا توجد سوى قاعدة بيانات واحدة، ويحدد برنامج `securityd` الخفي عناصر سلسلة المفاتيح التي يمكن لكل عملية أو تطبيق الوصول إليها. تؤدي واجهات API الخاصة بالوصول إلى سلسلة المفاتيح إلى إجراء اتصالات بالبرنامج الخفي الذي يستعلم عن استحقاقات "keychain-access-groups" و "application-identifier" و "application-group" الخاصة بالتطبيق. بدلاً من تقييد الوصول إلى عملية واحدة، تسمح مجموعات الوصول بمشاركة عناصر سلسلة المفاتيح بين التطبيقات.

لا يمكن مشاركة عناصر سلسلة المفاتيح إلا بين التطبيقات التي من نفس المطور. لمشاركة عناصر سلسلة المفاتيح، تستخدم تطبيقات الجهات الخارجية مجموعات الوصول مع بادئة مخصصة لها من خلال Apple Developer Program عبر مجموعات التطبيقات. يتم تطبيق متطلبات البادئة وتفرد مجموعة التطبيقات من خلال توقيع التعليمات البرمجية وملفات تعريف التموين وبرنامج Apple Developer Program.

تتم حماية بيانات سلسلة المفاتيح باستخدام بنية فئة مماثلة لتلك المستخدمة في حماية بيانات الملفات. تحتوي هذه الفئات على سلوكيات مكافئة لفئات حماية البيانات، ولكنها تستخدم مفاتيح ووظائف مميزة.

التوفر	حماية بيانات الملفات	حماية بيانات سلسلة المفاتيح
عند فتح القفل	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
أثناء القفل	NSFileProtectionComplete UnlessOpen	✕
بعد فتح القفل الأول	NSFileProtectionComplete UntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
دائمًا	NSFileProtectionNone	kSecAttrAccessibleAlways
تمكين رمز الدخول	✕	kSecAttrAccessibleWhen PasscodeSetThisDeviceOnly

يمكن للتطبيقات التي تستخدم خدمات تحديث الخلفية استخدام **kSecAttrAccessibleAfterFirstUnlock** لعناصر سلسلة المفاتيح التي يجب الوصول إليها أثناء تحديثات الخلفية.

تتصرف الفئة **kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly** مثل **kSecAttrAccessibleWhenUnlocked**؛ لكنها لا تكون متوفرة إلا عند تكوين الجهاز برمز دخول. ولا تكون هذه الفئة موجودة إلا في حافظة مفاتيح النظام؛ وهي:

- لا تتم مزامنتها مع سلسلة مفاتيح iCloud
- لا يتم نسخها احتياطيًا
- لا يتم تضمينها في حافظات المفاتيح المودعة في الضمان

إذا تمت إزالة رمز الدخول أو إعادة تعيينه، تصبح العناصر عديمة الفائدة من خلال تجاهل مفاتيح الفئات.

تشتمل فئات سلسلة المفاتيح الأخرى على نظير "هذا الجهاز فقط"، والذي يكون دائمًا محميًا بمعرف UID عند نسخه من الجهاز في أثناء النسخ الاحتياطي، ما يجعله عديم الفائدة إذا تمت استعادته إلى جهاز مختلف. حققت Apple التوازن بين الأمن وقابلية الاستخدام بعناية عن طريق اختيار فئات سلسلة المفاتيح التي تختلف وفقًا لنوع المعلومات التي يتم تأمينها وعند الحاجة إليها من قبل iOS و iPadOS.

وسائل حماية فئة بيانات سلسلة المفاتيح

يتم فرض وسائل حماية الفئات الواردة أدناه لعناصر سلسلة المفاتيح.

العنصر	يمكن الوصول إليه
كلمات سر Wi-Fi	بعد فتح القفل الأول
حسابات البريد	بعد فتح القفل الأول
حسابات Microsoft Exchange ActiveSync	بعد فتح القفل الأول
كلمات سر VPN	بعد فتح القفل الأول
LDAP, CalDAV, CardDAV	بعد فتح القفل الأول
رموز حسابات شبكات التواصل الاجتماعي	بعد فتح القفل الأول
مفاتيح تشفير إعلانات التسليم	بعد فتح القفل الأول
رمز iCloud	بعد فتح القفل الأول
مفاتيح iMessage	بعد فتح القفل الأول
كلمة سر المشاركة المنزلية	عند فتح القفل
كلمات سر سفاري	عند فتح القفل
إشارات سفاري المرجعية	عند فتح القفل
فايندر/نسخ iTunes الاحتياطي	عند فتح القفل، غير مرتحل
شهادات VPN	بعد فتح القفل الأول، غير مرتحل
مفاتيح Bluetooth®	دائمًا، غير مرتحل
رمز خدمة الإشعارات اللحظية من Apple (APNs)	دائمًا، غير مرتحل
شهادات iCloud والمفتاح الخاص	دائمًا، غير مرتحل
SIM PIN	دائمًا، غير مرتحل
رمز تحديد الموقع	دائمًا
البريد الصوتي	دائمًا

على macOS، جميع عناصر سلسلة المفاتيح المثبتة بواسطة ملفات تعريف التكوين متاحة **دائمًا**. على iOS و iPadOS، تكون لعناصر سلسلة المفاتيح المثبتة بواسطة ملف تعريف تكوين إمكانية وصول مختلفة استنادًا إلى أنواعها وطريقة الإشارة إليها ووقت تثبيتها. بشكل افتراضي، تكون عناصر سلسلة المفاتيح المثبتة باستخدام ملفات تعريف التكوين **متاحة بعد فتح القفل الأول وغير مرتحلة**. ومع ذلك، يكون عنصر سلسلة المفاتيح المثبت بواسطة ملف تعريف التكوين متاحًا **دائمًا** إذا كان:

- مثبتًا قبل الترقية إلى iOS 15 أو iPadOS 15 أو أحدث
- شهادة (ليس هوية)
- إنها هوية يشير إليها `IdentityCertificateUUID` في حمولة `com.Apple.mdm`

التحكم في الوصول إلى سلسلة المفاتيح

يمكن أن تستخدم سلاسل المفاتيح قوائم التحكم في الوصول (ACLs) لتعيين سياسات لمتطلبات إمكانية الوصول والمصادقة. يمكن للعناصر وضع الشروط التي تتطلب وجود المستخدم عن طريق تحديد عدم إمكانية الوصول إليها ما لم تتم المصادقة باستخدام بصمة الوجه أو بصمة الإصبع أو عن طريق إدخال رمز الدخول أو كلمة السر الخاصة بالجهاز. يمكن كذلك تقييد الوصول إلى العناصر عن طريق تحديد أن تسجيل بصمة الوجه أو بصمة الإصبع لم يتغير منذ إضافة العنصر. يساعد هذا القيد في منع المهاجم من إضافة بصمة إصبعه الخاصة للوصول إلى عنصر من عناصر سلسلة المفاتيح. يتم تقييم قوائم ACL داخل Secure Enclave ولا يتم إصدارها إلى kernel إلا في حالة استيفاء قيودها المحددة.

بنية سلسلة المفاتيح في macOS

يقدم macOS أيضًا وصولاً إلى سلسلة المفاتيح لتخزين أسماء المستخدمين وكلمات السر بكل سهولة وأمان، بما في ذلك الهويات الرقمية ومفاتيح التشفير والملاحظات الآمنة. ويمكن الوصول إليه عن طريق فتح تطبيق الوصول إلى سلسلة المفاتيح في /Applications/Utilities/. ويُلغي استخدام سلسلة المفاتيح الحاجة إلى إدخال — أو حتى تذكر — بيانات الاعتماد لكل مورد. يتم إنشاء سلسلة مفاتيح افتراضية أولية لكل مستخدم Mac، على الرغم من أنه يمكن للمستخدمين إنشاء سلاسل مفاتيح أخرى لأغراض محددة.

بالإضافة إلى الاعتماد على سلاسل مفاتيح المستخدم، يعتمد macOS على عدد من سلاسل المفاتيح على مستوى النظام تحافظ على أصول المصادقة التي لا تخص المستخدم، مثل بيانات اعتماد الشبكة وهويات البنية الأساسية للمفتاح العام (PKI). إحدى سلاسل المفاتيح هذه، وهي جذور النظام، غير قابلة للتغيير وتخزّن شهادات الجهة الموثقة (CA) الجذرية لـ PKI على الإنترنت لتسهيل المهام الشائعة مثل الخدمات المصرفية عبر الإنترنت والتجارة الإلكترونية. يمكن للمستخدم كذلك نشر شهادات الجهة الموثقة التي يتم توفيرها داخليًا لأجهزة كمبيوتر Mac المُدارة للمساعدة في التحقق من صحة المواقع والخدمات الداخلية.

خزنة الملفات

تشفير وحدة التخزين باستخدام خزنة الملفات في macOS

توفر أجهزة كمبيوتر Mac ميزة خزنة الملفات، وهي إمكانية تشفير مضمنة لتأمين جميع البيانات غير النشطة. يستخدم خزنة الملفات خوارزمية تشفير البيانات AES-XTS لحماية وحدات التخزين الكاملة على أجهزة التخزين الداخلية والقابلة للإزالة.

يتم تنفيذ خزنة الملفات على أجهزة كمبيوتر Mac المزودة بسيليكون Apple باستخدام حماية البيانات من الفئة C مع مفتاح وحدة تخزين. على Mac مزود برقاقات Apple وشريحة Apple T2 الأمنية، تعمل أجهزة التخزين الداخلية المشفرة المتصلة مباشرةً بـ Secure Enclave على الاستفادة من الإمكانات الأمنية في المكونات المادية وكذلك الخاصة بمحرك AES. بعد قيام المستخدم بتشغيل خزنة الملفات على Mac، تكون بيانات الاعتماد الخاصة به مطلوبة أثناء عملية التمهيد.

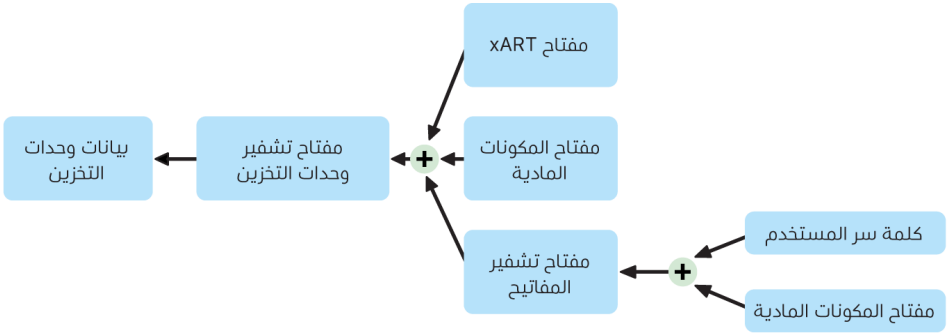
ملاحظة: بالنسبة إلى أجهزة كمبيوتر Mac (1) **قبل تلك المزودة بشريحة T2** أو (2) مزودة مساحة تخزين داخلية **لم يتم توفيرها في الأصل مع Mac** أو (3) مزودة بمساحة تخزين خارجية: بعد تشغيل خزانة الملفات، تُشفَّر جميع الملفات الموجودة وأي بيانات أخرى مكتوبة. لا تُشفَّر البيانات التي تمت إضافتها ثم حذفها قبل تشغيل خزانة الملفات وقد تكون قابلة للاسترداد باستخدام أدوات استرداد البيانات الجنائية.

تشغيل التخزين الداخلي باستخدام خزنة الملفات

بدون بيانات اعتماد تسجيل دخول صالحة أو مفتاح استرداد تشفير، تظل وحدات تخزين APFS الداخلية مشفرة ومحمية من الوصول غير المصرح به حتى إذا تمت إزالة جهاز التخزين الفعلي وتوصيله بكمبيوتر آخر. في macOS 10.15، يتضمن ذلك كلاً من وحدة تخزين النظام ووحدة تخزين البيانات. بدءًا من macOS 11، تتم حماية وحدة تخزين النظام بوحدة تخزين النظام المُوقّعة (SSV)، ولكن تظل وحدة تخزين البيانات محمية بالتشفير. يتم تنفيذ تشفير وحدة التخزين الداخلية على أجهزة كمبيوتر Mac المزودة بسيليكون Apple وكذلك المزودة بشريحة T2 من خلال إنشاء وإدارة تسلسل هرمي للمفاتيح، والبناء على تقنيات تشفير المكونات المادية المضمنة في الشريحة. تم تصميم هذا التسلسل الهرمي للمفاتيح لتحقيق أربعة أهداف في وقت واحد:

- طلب كلمة سر المستخدم لفك التشفير
- حماية النظام من الهجوم بقوة غاشمة مباشرةً مقابل وسائط التخزين التي تمت إزالتها من الـ Mac
- توفير طريقة سريعة وآمنة لمسح المحتوى عن طريق حذف مواد التشفير اللازمة

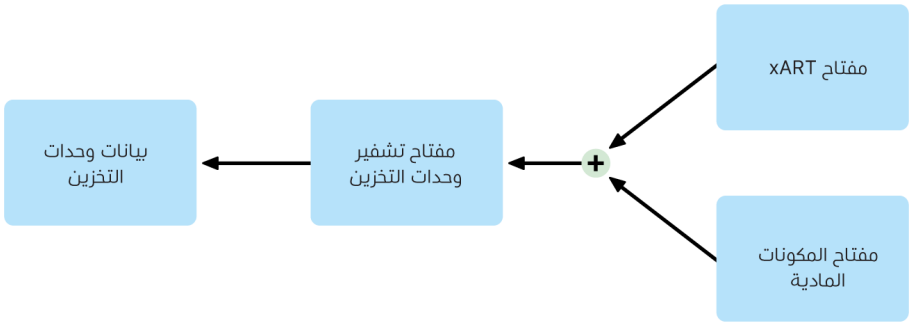
تمكين المستخدمين من تغيير كلمات السر الخاصة بهم (وبدورها مفاتيح التشفير المستخدمة لحماية ملفاتهم) دون الحاجة إلى إعادة تشفير وحدة التخزين بأكملها



على أجهزة Mac المزودة برقاقات Apple وتلك المزودة بشريحة T2، تحدث جميع عمليات معالجة مفاتيح خزنة الملفات في Secure Enclave؛ لا تُكشف أبدًا مفاتيح التشفير لوحدة معالجة Intel المركزية مباشرة. بشكل افتراضي، يتم إنشاء جميع وحدات تخزين APFS باستخدام مفتاح تشفير وحدة تخزين. يتم تشفير محتويات وحدة التخزين وبيانات التعريف باستخدام مفتاح تشفير وحدة التخزين هذا، الذي يتم تغليفه بمفتاح تشفير المفاتيح (KEK). وتتم حماية مفتاح تشفير المفاتيح (KEK) بتركيبة من كلمة سر المستخدم ومعرف UID للمكونات المادية عند تشغيل خزنة الملفات.

إيقاف التخزين الداخلي باستخدام خزنة الملفات

إذا لم يكن خزنة الملفات قيد التشغيل على Mac مزود بسيليكون Apple أو Mac مزود بشريحة T2 أثناء عملية مساعد الإعداد الأولية، تظل وحدة التخزين مشفرةً ولكن مفتاح تشفير وحدة التخزين لا يكون محميًا إلا بواسطة معرف UID للمكونات المادية في Secure Enclave.



إذا تم تشغيل خزنة الملفات لاحقًا—وهي عملية تكون فورية لأنه قد تم تشفير البيانات بالفعل—فإن آلية مكافحة إعادة التشغيل تساعد على منع استخدام المفتاح القديم (استنادًا إلى معرف UID للمكونات المادية فقط) لفك تشفير وحدة التخزين. ومن ثم تتم حماية وحدة التخزين بتركيبة من كلمة سر المستخدم ومعرف UID للمكونات المادية كما هو موضح سابقًا.

حذف وحدات تخزين خزنة الملفات

عند حذف وحدة تخزين، يتم حذف مفتاح تشفير وحدة التخزين الخاص بها بشكل آمن بواسطة Secure Enclave. وهذا يساعد على منع الوصول في المستقبل باستخدام هذا المفتاح حتى بواسطة Secure Enclave. بالإضافة إلى ذلك، يتم تغليف جميع مفاتيح تشفير وحدات التخزين بمفتاح وسائط. لا يوفر مفتاح الوسائط سرية إضافية للبيانات، ولكنه بدلاً من ذلك تم تصميمه لتمكين الحذف السريع والآمن للبيانات لأنه بدونه يكون فك التشفير مستحيلاً.

على أجهزة Mac المزودة برقاقات Apple وتلك المزودة بشريحة T2، يكون مسح مفتاح الوسائط بواسطة تقنية Secure Enclave المدعومة أمرًا مضمونًا، على سبيل المثال بواسطة أوامر MDM عن بُعد. ويؤدي مسح مفتاح الوسائط بهذه الطريقة إلى جعل وحدة التخزين غير قابلة للوصول إليها بطريقة مشفرة.

أجهزة التخزين القابلة للإزالة

لا يستخدم تشفير أجهزة التخزين القابلة للإزالة الإمكانات الأمنية في Secure Enclave، ويتم تنفيذ تشفيرها بنفس الطريقة المستخدمة في أجهزة كمبيوتر Mac المستندة إلى Intel غير المزودة بشريحة T2.

إدارة خزنة الملفات في macOS

في macOS، يمكن للمؤسسات إدارة خزنة الملفات باستخدام SecureToken أو رمز Bootstrap.

استخدام الرمز الآمن

يغير نظام ملفات Apple (APFS) في macOS 10.13 أو أحدث كيفية إنشاء مفاتيح تشفير خزنة الملفات. في الإصدارات السابقة من macOS على وحدات تخزين CoreStorage، كان يتم إنشاء المفاتيح المستخدمة في عملية تشفير خزنة الملفات عند قيام المستخدم أو المؤسسة بتشغيل خزنة الملفات على Mac. في macOS على وحدات تخزين APFS، يتم إنشاء المفاتيح إما أثناء إنشاء المستخدم، أو تعيين كلمة سر المستخدم الأول، أو أثناء تسجيل الدخول الأول بواسطة مستخدم الـ Mac. يعد هذا التطبيق لمفاتيح التشفير، عند إنشائها، وكيفية تخزينها جزءًا من ميزة تُعرف باسم **الرمز الآمن**. وعلى وجه التحديد، فإن الرمز الآمن هو إصدار مغلف من مفتاح تشفير المفاتيح (KEK) محمي بكلمة سر المستخدم.

عند نشر خزنة الملفات على APFS، يمكن للمستخدم متابعة التالي:

- استخدام الأدوات والعمليات الموجودة، مثل مفتاح الاسترداد الشخصي (PRK) الذي يمكن تخزينه باستخدام حل إدارة جهاز الجوال (MDM) للضمان
- تأجيل تمكين خزنة الملفات حتى يقوم المستخدم بتسجيل الدخول إلى Mac أو الخروج منه
- إنشاء مفتاح استرداد مؤسسي (IRK) واستخدامه

في macOS 11، يؤدي تعيين كلمة السر الأولية للمستخدم الأول على الـ Mac إلى منح هذا المستخدم رمزًا آمنًا. في بعض عمليات سير العمل، قد لا يكون هذا هو السلوك المطلوب، كما في السابق، فمنح أول رمز آمن يتطلب من حساب المستخدم تسجيل الدخول. لمنع حدوث ذلك، أضف `;DisabledTags;SecureToken` إلى سمة المستخدم التي تم إنشاؤها برمجيًا `AuthenticationAuthority` قبل تعيين كلمة سر المستخدم كما هو موضح أدناه:

```
sudo dscl . append /Users/<user name> AuthenticationAuthority
";DisabledTags;SecureToken"
```

استخدام رمز Bootstrap

قدَّم macOS 10.15 ميزة جديدة—**رمز Bootstrap**—للمساعدة على منح رمز آمن لكل من حسابات الجوال وحساب المسؤول الذي أنشأه تسجيل الجهاز الاختياري ("المسؤول المُدار"). على الـ macOS 11، يمكن لرمز Bootstrap منح رمز آمن لأي مستخدم يقوم بتسجيل الدخول إلى كمبيوتر Mac، بما في ذلك حسابات المستخدمين المحليين. يتطلب استخدام ميزة رمز Bootstrap في macOS 10.15 أو أحدث ما يلي:

- تسجيل الـ Mac في MDM باستخدام Apple School Manager أو Apple Business Manager، مما يجعل الـ Mac خاضعًا للإشراف
- دعم مورد MDM

على الـ macOS 10.15.4 أو أحدث، يتم إنشاء رمز Bootstrap وإيداعه في الضمان لدى MDM مع تسجيل الدخول الأول من قِبل أي مستخدم تم تمكين الرمز الآمن لديه–إذا كان حل MDM يدعم تلك الميزة. يمكن أيضًا إنشاء رمز Bootstrap وإيداعه في الضمان لدى حل MDM باستخدام أداة سطر الأوامر `profiles`، إذا لزم الأمر.

على الـ macOS 11 يمكن كذلك استخدام رمز Bootstrap لأكثر من مجرد منح رمز آمن لحسابات المستخدمين. على الـ Mac المزود برقاقات Apple، يمكن استخدام رمز Bootstrap، إذا كان متوفرًا، للسماح بتثبيت كل من ملحقات Kernel وتحديثات البرامج عند إدارتهما باستخدام MDM.

مفاتيح الاسترداد المؤسسية مقابل مفاتيح الاسترداد الشخصية

تدعم خزنة الملفات على كل من وحدات التخزين CoreStorage و APFS استخدام مفتاح استرداد مؤسسي (IRK، يُعرف سابقًا باسم **الهوية الرئيسية لخزنة الملفات**) لفتح قفل وحدة التخزين. بالرغم من أن مفتاح الاسترداد المؤسسي (IRK) مفيد لعمليات سطر الأوامر لفتح قفل وحدة تخزين أو إيقاف خزنة الملفات كليًا، فإن فائدته بالنسبة إلى المؤسسات محدودة، خصوصًا عند استخدام الإصدارات الحديثة من macOS. وعلى Mac مزود برقاقات Apple، لا توفر مفاتيح IRK قيمة وظيفية، وذلك لسببين رئيسيين: أولًا، لا يمكن استخدام مفاتيح IRK للوصول إلى recoveryOS، وثانيًا، لأن نمط القرص المستهدف لم يعد مدعومًا، لا يمكن فتح قفل وحدة التخزين عن طريق توصيلها بـ Mac آخر. لهذين السببين وأكثر، **لم يعد يوصى باستخدام IRK للإدارة المؤسسية لخزنة الملفات على أجهزة كمبيوتر Mac**. بدلًا من ذلك، ينبغي استخدام مفتاح استرداد شخصي (PRK).

كيفية حماية Apple لبيانات المستخدمين الشخصية

حماية وصول التطبيقات إلى بيانات المستخدم

بالإضافة إلى تشفير البيانات غير النشطة، تساعد أجهزة Apple في منع التطبيقات من الوصول إلى معلومات المستخدم الشخصية دون إذن باستخدام تقنيات متنوعة مثل مخزن البيانات. في الإعدادات في iOS و iPadOS وفي إعدادات النظام في macOS (macOS 13 أو أحدث) أو تفضيلات النظام (macOS 12 أو أقدم)، يمكن للمستخدم معرفة التطبيقات التي سمح لها بالوصول إلى معلومات معينة، وكذلك منح أو إبطال أي وصول في المستقبل. يتم فرض الوصول في الحالات الآتية:

- **iOS و iPadOS و macOS:** التقويمات والكاميرا وجهات الاتصال والميكروفون والصور والتذكيرات والتعرف على الكلام
- **iOS و iPadOS:** Bluetooth والمنزل والوسائط وتطبيقات الوسائط و Apple Music والحركة واللياقة
- **iOS و watchOS:** صحتي
- **macOS:** مراقبة الإدخال (على سبيل المثال، النقرات على لوحة المفاتيح) والمطالبة وتسجيل الشاشة (على سبيل المثال، لقطات الشاشة الثابتة والفيديو) وإعدادات النظام (macOS 13 أو أحدث) أو تفضيلات النظام (macOS 12 أو أقدم)

في iOS 13.4 أو أحدث و iPadOS 13.4 أو أحدث، تتم حماية بيانات جميع التطبيقات التابعة لجهات خارجية تلقائيًا في مخزن بيانات. يساعد مخزن البيانات على الحماية من الوصول غير المصرح به إلى البيانات، حتى من العمليات التي ليست في وضع الحماية في حد ذاتها. الفئات الإضافية على الـ iOS 15 أو أحدث، بما في ذلك الشبكة المحلية والتفاعلات القريبة ومستشعر البحث وبيانات الاستخدام والتركيز.

إذا سجل المستخدم الدخول إلى iCloud، يتم منح التطبيقات في iOS و iPadOS الوصول بشكل افتراضي إلى iCloud Drive. يمكن للمستخدمين التحكم في وصول كل تطبيق ضمن iCloud في الإعدادات. ويوفر iOS و iPadOS أيضًا قيودًا تمنع حركة البيانات بين التطبيقات والحسابات المثبتة بواسطة أحد حلول إدارة جهاز الجوال (MDM) وتلك التي قام المستخدم بتثبيتها.

حماية الوصول إلى البيانات الصحية للمستخدم

توفر HealthKit مستودعًا مركزيًا لبيانات الصحة واللياقة البدنية على الـ iPhone والـ Apple Watch. وتعمل HealthKit أيضًا بشكل مباشر مع أجهزة الصحة واللياقة، مثل أجهزة مراقبة معدل ضربات القلب المتوافقة التي تعمل بتقنية Bluetooth منخفض الطاقة (BLE) ومعالج الحركة الثانوي المضمن في العديد من أجهزة iOS. تتطلب جميع تفاعلات HealthKit مع تطبيقات الصحة واللياقة ومؤسسات الرعاية الصحية وأجهزة الصحة واللياقة إذنًا من المستخدم. ويتم تخزين هذه البيانات في فئة حماية البيانات "محمية ما لم تُفتح". يتم التخلي عن الوصول إلى البيانات بعد 10 دقائق من قفل الجهاز، وتصبح البيانات قابلة للوصول في المرة التالية التي يُدخل فيها المستخدم رمز الدخول أو يستخدم بصمة الوجه أو بصمة الإصبع لفتح قفل الجهاز.

تجميع بيانات الصحة واللياقة البدنية وتخزينها

تقوم HealthKit أيضًا بتجميع وتخزين بيانات الإدارة، مثل أذونات الوصول للتطبيقات وأسماء الأجهزة المتصلة بـ HealthKit وجدولة المعلومات المستخدمة لتشغيل التطبيقات عند توفر بيانات جديدة. يتم تخزين هذه البيانات في فئة حماية البيانات "محمية حتى أول مصادقة من المستخدم". وتخزن ملفات دفتر اليومية المؤقتة السجلات الصحية التي يتم إنشاؤها عندما يكون الجهاز مغلقًا، مثلما يحدث عند ممارسة المستخدم التمارين الرياضية. ويتم تخزين هذه البيانات في فئة حماية البيانات "محمية ما لم تُفتح". وعند فتح قفل الجهاز، يتم استيراد ملفات دفتر اليومية المؤقتة إلى قواعد بيانات الصحة الأساسية، ثم يتم حذفها عند اكتمال الدمج.

يمكن تخزين بيانات تطبيق صحتي في iCloud. يتطلب التشفير الكامل لبيانات تطبيق صحتي تثبيت iOS 12 أو أحدث والمصادقة بخطوتين. بخلاف ذلك، تظل بيانات المستخدم مشفرة في التخزين والنقل لكنها غير مشفرة تشفيرًا كاملاً. بعد أن يقوم المستخدم بتشغيل المصادقة بخطوتين والتحديث إلى iOS 12 أو أحدث، يتم ترحيل بيانات صحة المستخدم إلى التشفير الكامل.

إذا عمل المستخدم نسخة احتياطية من جهازه باستخدام فايندر (في macOS 10.15 أو أحدث) أو iTunes (في macOS 10.14 أو أقدم)، فلا يتم تخزين بيانات الصحة إلا إذا تم تشفير النسخة الاحتياطية.

سجلات الصحة السريرية

يمكن للمستخدمين تسجيل الدخول إلى أنظمة الصحة المدعومة في تطبيق صحتي للحصول على نسخة من سجلات الصحة السريرية الخاصة بهم. عند اتصال المستخدم بأحد أنظمة الصحة، يقوم المستخدم بالمصادقة باستخدام بيانات اعتماد عميل OAuth 2. بعد الاتصال، يتم تنزيل بيانات سجل الصحة السريرية مباشرةً من مؤسسة الرعاية الصحية باستخدام اتصال TLS 1.3 محمي. بمجرد التنزيل، يتم تخزين سجلات الصحة السريرية بشكل آمن إلى جانب بيانات الصحة الأخرى.

أصالة بيانات تطبيق صحتي

تشتمل البيانات المخزَّنة في قاعدة البيانات على بيانات تعريف لتتبع مصدر كل سجل بيانات. وتتضمن بيانات التعريف هذه معرف تطبيق يحدد التطبيق الذي قام بتخزين السجل. بالإضافة إلى ذلك، يمكن أن يحتوي عنصر بيانات تعريف اختياري على نسخة من السجل موقَّعة رقميًا. ويهدف هذا إلى توفير أصالة البيانات للسجلات التي تم إنشاؤها بواسطة جهاز موثوق به. التنسيق المستخدم للتوقيع الرقمي هو صياغة رسالة الترميز (CMS) المحدد في RFC 5652.

وصول التطبيقات الخارجية إلى بيانات تطبيق صحتي

يتم التحكم في الوصول إلى HealthKit API من خلال الاستحقاقات، ويجب أن تتوافق التطبيقات مع القيود المفروضة على كيفية استخدام البيانات. على سبيل المثال، لا يُسمح للتطبيقات باستخدام بيانات الصحة للإعلان. وتكون التطبيقات أيضًا مطالبة بتزويد المستخدمين بسياسة خصوصية توضح استخدامها لبيانات الصحة.

يتم التحكم في وصول التطبيقات إلى بيانات الصحة من خلال إعدادات الخصوصية لدى المستخدم. يُطلب من المستخدمين منح حق الوصول عندما تطلب التطبيقات الوصول إلى بيانات الصحة، على غرار جهات الاتصال والصور ومصادر بيانات iOS الأخرى. ولكن، مع بيانات الصحة، تُمنح التطبيقات وصولاً منفصلاً لقراءة البيانات وكتابتها، بالإضافة إلى وصول منفصل لكل نوع من أنواع بيانات الصحة. يمكن للمستخدمين عرض وإلغاء الأذونات التي منحوها للوصول إلى بيانات الصحة ضمن الإعدادات > صحتي > الوصول إلى البيانات والأجهزة.

إذا تم منح الإذن لكتابة البيانات، يمكن للتطبيقات أيضًا قراءة البيانات التي تكتبها. وفي حالة منح الإذن لقراءة البيانات، يمكن للتطبيقات قراءة البيانات التي تكتبها جميع المصادر. ومع ذلك، لا يمكن للتطبيقات تحديد الوصول الممنوح للتطبيقات الأخرى. بالإضافة إلى ذلك، لا يمكن للتطبيقات أن تحدد بشكل قاطع ما إذا كانت قد مُنحت حق الوصول لقراءة بيانات الصحة أم لا. عندما لا يمتلك أحد التطبيقات حق الوصول للقراءة، لا تنتج أي بيانات من جميع الاستعلامات—تنتج نفس الاستجابة كقاعدة بيانات فارغة. وقد تم التصميم بتلك الطريقة لمنع التطبيقات من استنتاج الحالة الصحية للمستخدم من خلال معرفة أنواع البيانات التي يتتبعها المستخدم.

الهوية الطبية للمستخدمين

يوفر تطبيق صحتي للمستخدمين خيار ملء نموذج الهوية الطبية بمعلومات قد تكون مهمة أثناء المشكلات الطبية الطارئة. ويتم إدخال المعلومات أو تحديثها يدويًا ولا تتم مزامنتها مع المعلومات الموجودة في قواعد بيانات الصحة.

يتم عرض معلومات الهوية الطبية عن طريق الضغط على زر الطوارئ على شاشة القفل. ويتم تخزين المعلومات في الجهاز باستخدام فئة حماية البيانات "بلا حماية" بحيث يمكن الوصول إليها دون الحاجة إلى إدخال رمز دخول الجهاز. الهوية الطبية هي ميزة اختيارية تمكّن المستخدمين من تحديد كيفية تحقيق التوازن بين اهتمامات السلامة والخصوصية على حد سواء. يتم نسخ هذه البيانات احتياطيًا في نسخة iCloud الاحتياطية في iOS 13 أو أقدم. في iOS 14، تتم مزامنة الهوية الطبية بين الأجهزة باستخدام CloudKit ويكون له نفس خصائص التشفير مثل بقية البيانات الصحية.

مشاركة البيانات الصحية

على الـ iOS 15 يمنح تطبيق "صحتي" المستخدمين خيار مشاركة البيانات الصحية الخاصة بهم مع مستخدمين آخرين. تتم مشاركة البيانات الصحية بين المستخدمين باستخدام تشفير iCloud الكامل ولا يمكن لـ Apple الوصول إلى البيانات التي يتم إرسالها عبر مشاركة البيانات الصحية. لاستخدام هذه الميزة، يجب أن يعمل كل من المستخدمين المرسلين والمستقبلين على الـ iOS 15 أو أحدث وأن تكون لديهم مصادقة ثنائية ممكّنة.

يمكن للمستخدمين كذلك اختيار مشاركة بياناتهم الصحية مع مقدم الرعاية الصحية لديهم باستخدام ميزة المشاركة مع الموفر على تطبيق "صحتي". البيانات التي تتم مشاركتها باستخدام هذه الميزة متاحة فقط للمؤسسات الصحية التي يختارها المستخدم باستخدام التشفير الكامل ولا تحتفظ Apple بمفاتيح التشفير ولا تكون لديها إمكانية الوصول إليها لفك تشفير البيانات الصحية التي تمت مشاركتها أو عرضها أو الوصول إليها بأي طريقة أخرى من خلال ميزة المشاركة مع الموفر. يمكن العثور على مزيد من التفاصيل حول كيفية حماية تصميم هذه الخدمة للبيانات الصحية للمستخدمين في قسم الأمان والخصوصية في دليل تسجيل Apple لمؤسسات.

التوقيع الرقمي والتشفير

قوائم التحكم في الوصول

يتم تقسيم بيانات سلسلة المفاتيح وحمايتها باستخدام قوائم التحكم في الوصول (ACLs). ونتيجةً لذلك، لا يمكن الوصول إلى بيانات الاعتماد التي تخزّنها تطبيقات الجهات الخارجية بواسطة تطبيقات ذات هويات مختلفة ما لم يوافق عليها المستخدم صراحةً. توفّر هذه الحماية الآلية اللازمة لتأمين بيانات اعتماد المصادقة في أجهزة Apple عبر نطاق واسع من التطبيقات والخدمات داخل المؤسسة.

البريد

في تطبيق البريد، يمكن للمستخدمين إرسال رسائل موقعة رقميًا ومشفرة. يكتشف تطبيق البريد تلقائيًا موضوع عنوان البريد الإلكتروني الحساس لحالة الأحرف RFC 5322 الملائم أو الأسماء البديلة للموضوع في شهادات التوقيع الرقمي والتشفير على رموز مصادقة رقم التعريف الشخصي المرفقة (PIV) في البطاقات الذكية المتوافقة. إذا تطابق حساب بريد إلكتروني تم تكوينه مع عنوان بريد إلكتروني على شهادة توقيع رقمي أو تشفير على رمز PIV مرفق، يعرض تطبيق البريد تلقائيًا زر التوقيع في شريط الأدوات في نافذة رسالة جديدة. وإذا كان تطبيق البريد لديه شهادة تشفير البريد الإلكتروني للمستلم أو يمكنه اكتشافها في قائمة العناوين العامة (GAL) في Microsoft Exchange، تظهر أيقونة غير مقفلة في شريط أدوات الرسائل الجديد. تشير أيقونة القفل المُقفل إلى أنه سيتم إرسال الرسالة مشفرةً باستخدام المفتاح العام للمستلم.

S/MIME لكل رسالة

يدعم iOS و iPadOS و macOS ميزة S/MIME لكل رسالة. وهذا يعني أنه يمكن لمستخدمي S/MIME اختيار توقيع الرسائل وتشفيرها دائمًا بشكل افتراضي أو توقيع وتشفير رسائل فردية بشكل انتقائي.

يمكن تسليم الهويات المستخدمة مع S/MIME إلى أجهزة Apple باستخدام أحد ملفات تعريف التكوين أو حلول إدارة جهاز الجوال (MDM) أو بروتوكول التسجيل البسيط للشهادات (SCEP) أو الجهة الموثقة لـ Microsoft Active Directory.

البطاقات الذكية

يتضمن macOS 10.12 أو أحدث دعمًا أصليًا لبطاقات PIV. وتُستخدم هذه البطاقات على نطاق واسع في المؤسسات التجارية والحكومية لكل من المصادقة بخطوتين والتوقيع الرقمي والتشفير.

تتضمن البطاقات الذكية هوية رقمية واحدة أو أكثر تحتوي على زوج من المفاتيح العامة والخاصة وشهادة مقترنة. ويوفر فتح قفل البطاقة الذكية برقم التعريف الشخصي (PIN) الوصول إلى المفاتيح الخاصة المستخدمة في عمليات المصادقة والتشفير والتوقيع. تحدد الشهادة ما يمكن استخدام المفتاح له وما السمات المرتبطة به وما إذا كان قد تم التحقق من صحته (توقيعه) من قِبل شهادة الجهة الموثقة (CA) أم لا.

يمكن استخدام البطاقات الذكية للمصادقة بخطوتين. العاملان المطلوبان لفتح قفل البطاقة هما "شيء يمتلكه المستخدم" (البطاقة) و"شيء يعرفه المستخدم" (رمز PIN). يشتمل macOS 10.12 أو أحدث على دعم أصلي لمصادقة نافذة تسجيل الدخول الخاصة بالبطاقة الذكية ومصادقة شهادة العميل لمواقع الويب على سفاري. ويدعم أيضًا مصادقة Kerberos باستخدام أزواج المفاتيح (PKINIT) لتسجيل الدخول الموحد إلى الخدمات المدعومة من Kerberos. لمعرفة المزيد حول البطاقات الذكية و macOS، انظر مقدمة عن تكامل البطاقات الذكية في **نشر أنظمة Apple الأساسية**.

صور الأقراص المشفرة

في macOS، تعمل صور الأقراص المشفرة بمثابة حاويات آمنة يمكن للمستخدمين من خلالها تخزين أو نقل المستندات الحساسة والملفات الأخرى. ويتم إنشاء صور الأقراص المشفرة باستخدام أداة القرص، الموجودة في /Applications/Utilities/. يمكن تشفير صور القرص باستخدام تشفير AES سعة 128 بت أو 256 بت. نظرًا لأن صورة القرص المحمّلة تُعامل على أنها وحدة تخزين محلية متصلة بالـ Mac، يمكن للمستخدمين نسخ الملفات والمجلدات المخزَّنة فيها ونقلها وفتحها. كما هو الحال مع خزنة الملفات، يتم تشفير محتويات صورة القرص وفك تشفيرها في الوقت الفعلي. باستخدام صور الأقراص المشفرة، يمكن للمستخدمين تبادل المستندات والملفات والمجلدات بأمان عن طريق حفظ صورة قرص مشفرة إلى وسائط قابلة للإزالة أو إرسالها كمرفق برسالة بريد أو تخزينها على خادم بعيد. لمزيد من المعلومات حول صور الأقراص المشفرة، انظر دليل مستخدم أداة القرص.

أمن التطبيقات

نظرة عامة على أمن التطبيقات

تعتبر التطبيقات اليوم من بين العناصر الأكثر أهمية في بنية الأمن. وعلى الرغم من أن التطبيقات توفر فوائد إنتاجية مذهلة للمستخدمين، إلا أنها تتمتع أيضًا بإمكانية التأثير سلبًا على أمن النظام واستقراره وبيانات المستخدم إذا لم يتم التعامل معها بشكل صحيح.

لذلك، توفر Apple طبقات من الحماية للمساعدة في ضمان خلو التطبيقات من البرامج الضارة المعروفة وعدم العبث بها. هذا بالإضافة إلى وسائل حماية تفرض مراعاة الحرص عند الوصول من التطبيقات إلى بيانات المستخدم. توفر عناصر التحكم في الأمن هذه نظامًا أساسيًا مستقرًا وآمنًا للتطبيقات، مما يمكّن آلاف المطورين من تقديم مئات الآلاف من التطبيقات لكل من iOS و iPadOS و macOS — كل ذلك دون التأثير على سلامة النظام. ويمكن للمستخدمين الوصول إلى هذه التطبيقات على أجهزة Apple الخاصة بهم دون خوف لا مبرر له من الفيروسات أو البرامج الضارة أو الهجمات غير المصرح بها.

على iPhone و iPad، يتم الحصول على جميع التطبيقات من App Store — وجميع التطبيقات تكون في وضع الحماية — لتوفير أكثر عناصر التحكم تشددًا.

على الـ Mac، يتم الحصول على العديد من التطبيقات من App Store، لكن مستخدمي الـ Mac يقومون أيضًا بتنزيل التطبيقات واستخدامها من الإنترنت. لدعم التنزيل من الإنترنت بأمان، يضع macOS طبقات من عناصر التحكم الإضافية. أولاً، بشكل افتراضي في macOS 10.15 أو أحدث، يجب توثيق جميع تطبيقات الـ Mac بواسطة Apple لبدء تشغيلها. ويساعد هذا المتطلب على ضمان خلو هذه التطبيقات من البرامج الضارة المعروفة، دون اشتراط توفير التطبيقات من خلال App Store. ثانيًا، يتضمن macOS أحدث حماية من الفيروسات لحظر البرامج الضارة وإزالتها إذا لزم الأمر.

كعنصر تحكم إضافي عبر الأنظمة الأساسية، يساعد وضع الحماية في حماية بيانات المستخدم من وصول التطبيقات غير المصرح به. وفي macOS، تكون البيانات الموجودة في المناطق الحرجة محمية بحد ذاتها، مما يساعد في ضمان استمرار سيطرة المستخدمين على الوصول إلى الملفات في سطح المكتب والمستندات والتنزيلات والمناطق الأخرى من جميع التطبيقات، سواء كانت التطبيقات التي تحاول الوصول موجودة في وضع الحماية بحد ذاتها أم لا.

الإمكانية الأصلية	المكافئ الخارجي
قائمة المكونات الإضافية غير المعتمدة، قائمة ملحقات سفاري غير المعتمدة	تعريفات الفيروسات/البرامج الضارة
عزل الملف	تعريفات الفيروسات/البرامج الضارة
توقيعات XProtect/Yara	تعريفات الفيروسات/البرامج الضارة؛ حماية نقطة النهاية
الحارس الرقمي	حماية نقطة النهاية؛ تفرض توقيع التعليمات البرمجية على التطبيقات للمساعدة على ضمان تشغيل البرامج الموثوق فيها فقط.
eficheck (ضرورية لأجهزة كمبيوتر Mac التي لا تحتوي على شريحة Apple T2 أمنية)	حماية نقطة النهاية؛ اكتشاف rootkit
جدار حماية التطبيقات	حماية نقطة النهاية؛ تفعيل جدار الحماية
فلتر الحزم (pf)	حلول جدار الحماية
حماية تكامل النظام	مضمنة في macOS
عناصر التحكم في الوصول الإلزامية	مضمنة في macOS
قائمة استبعاد Kext	مضمنة في macOS
توقيع التعليمات البرمجية للتطبيقات الإلزامي	مضمنة في macOS
توثيق التطبيق	مضمنة في macOS

أمن التطبيقات في iOS و iPadOS

مقدمة عن أمن التطبيقات في iOS و iPadOS

بخلاف الأنظمة الأساسية للأجهزة المحمولة الأخرى، لا يسمح iOS و iPadOS للمستخدمين بتثبيت التطبيقات غير الموقعة التي قد تكون ضارة من مواقع الويب أو تشغيل تطبيقات غير موثوق بها. بدلاً من ذلك، (خارج الاتحاد الأوروبي) يجب تنزيل جميع التطبيقات من App Store، حيث تأتي جميع التطبيقات من مطورين مُعرَّفين ويجب اجتيازها مراجعة مؤتمتة وبشرية. في وقت التشغيل، يتم إجراء عمليات فحص توقيع التعليمات البرمجية لجميع صفحات الذاكرة القابلة للتنفيذ أثناء تحميل الصفحات للمساعدة على التأكد من أنه لم يتم تعديل التطبيق منذ تثبيته أو آخر تحديث له.

بعد التحقق من أن التطبيق وارد من مصدر معتمد، يفرض iOS و iPadOS تدابير أمنية مصممة لمنعه من اختراق التطبيقات الأخرى أو بقية النظام.

معلومات عن أمن App Store

App Store مكان موثوق به حيث يمكن للمستخدمين استكشاف التطبيقات وتنزيلها بأمان. على App Store، تأتي التطبيقات من مطورين مُعرَّفين وافقوا على اتباع إرشادات Apple، ويتم توزيعها إلى المستخدمين بضمانات تشفير ضد التعديل. تتم مراجعة كل تطبيق وكل تحديث لكل تطبيق لتقييم ما إذا كان يطابق المتطلبات المتعلقة بالخصوصية والأمن والسلامة. هذه العملية التي يتم تحسينها باستمرار مصممة لحماية المستخدمين عن طريق إبعاد البرامج الضارة والمجرمين السيبرانيين والمحتالين عن App Store. إضافة إلى ذلك، يجب على التطبيقات المصممة للأطفال اتباع إرشادات صارمة تتعلق بجمع البيانات والأمن ومصممة لإبقاء الأطفال سالمين، ويجب أن تتكامل مع ميزات الإشراف العائلي في iOS و iPadOS بشكل وثيق.

تتضمن وسائل حماية أمن App Store الآتي:

- **عمليات المسح المؤتمتة للبرامج الضارة المعروفة:** للمساعدة على منعها من دخول App Store بتاتًا، ومن ثَم عدم وصولها إلى المستخدمين أو الإضرار بهم.
- **مراجعة بشرية بواسطة فريق من الخبراء:** لمراجعة وصف التطبيق— بما في ذلك النص التسويقي ولقطات الشاشة—لتحري الدقة. ينشئ ذلك حاجزًا كبيرًا ضد عمليات الاحتيال الأكثر شيوعًا والمستخدمة في توزيع البرامج الضارة: حيث يتم تقديم البرنامج الضار على أنه تطبيق مشهور أو ادعاء توفير ميزات رائعة ليست مقدمة فعليًا.
- **عمليات التحقق اليدوية:** للتحقق من أن التطبيق لا يطلب وصولاً غير ضروري لبيانات حساسة ولإجراء تقييم إضافي للتطبيقات التي تستهدف الأطفال للمساعدة على ضمان امتثالها للقواعد الأكثر صرامةً المتعلقة بجمع البيانات والسلامة.
- **مراجعات موثوق بها ومركزية من المستخدمين:** للمساعدة على توضيح المشكلات والتقليل من احتمالية تضليل المهاجم للكثير من المستخدمين بشكل كبير. حتى في حال تمكن تطبيق ضار من إخفاء سلوكه تمامًا خلال عملية المراجعة، يقوم مستخدمو التطبيق الذين يواجهون المشكلات ويبلغون بها بتنبيه الآخرين — و Apple — ومن ثَم توفير سبيل آخر للكشف عنه. يكافح App Store بشدة المراجعات الاحتيالية لتحسين قيمة هذه الإشارة.
- **عمليات التصحيح والإزالة:** في حال حدوث مشكلات. في حال دخول تطبيق إلى App Store لكن يتم اكتشاف انتهاكه للإرشادات لاحقًا، تعمل Apple مع المطور لحل المشكلة بسرعة. في حالات خطرة تتضمن الاحتيال والأنشطة الضارة، تتم إزالة التطبيق من App Store فورًا ويمكن إخطار المستخدمين اللذين نزلوا التطبيقات بسلوك التطبيق الضار.

يعتمد أمن التطبيقات في iOS و iPadOS على مزيج من كل الطبقات—مراجعة قوية للتطبيقات للمساعدة على منع تثبيت التطبيقات الضارة وعوامل حماية قوية للمنصة للحد من الضرر الذي قد تحدثه التطبيقات الضارة. يوفر الأمن المصمم في iOS و iPadOS للمستخدمين عوامل حماية قوية هي الأفضل مقارنةً بأي جهاز استهلاكي آخر، لكن عوامل الحماية تلك ليست مصممة للحماية من الاختيارات التي قد يتم خداع المستخدم لاتخاذها. تفرض مراجعة التطبيقات سياسات App Store المصممة لحماية المستخدمين من التطبيقات التي قد تحاول الإضرار بهم أو خداعهم ليمنحوا الوصول إلى البيانات الحساسة. وتصعِّب مراجعة التطبيقات، في الحالات الخطرة جدًا التي تحاول فيها التطبيقات الضارة تجاوز عوامل الحماية الموجودة في الجهاز، على التطبيقات الضارة الوصول إلى أجهزة المستخدمين أساسًا.

وعلى الرغم من ذلك، لا تكون تدابير App Store الأمنية وحدها مثالية دائمًا، فهي تعمل كجزء من إستراتيجية دفاعية عميقة عن أمن المنصة، حيث تسهم في جعل الهجمات واسعة الانتشار التي ضد مستخدمي iOS و iPadOS غير عملية وغير اقتصادية للمهاجمين ذوي الدوافع المالية. تحمي Apple أمن النظام البيئي وتوفر راحة البال للعملاء عن طريق مراجعة كل تطبيق قبل توفره على App Store للمساعدة على ضمان خلوّه من البرامج الضارة وجاهزيته للمستخدمين، وعن طريق إزالة التطبيقات من التوزيع بسلاسة إذا اتضح أنها ضارة والحد من انتشار متغيرات مستقبلية.

عملية توقيع التعليمات البرمجية للتطبيقات في iOS و iPadOS

في iOS و iPadOS، توفر Apple أمن التطبيقات من خلال أشياء مثل توقيع التعليمات البرمجية الإلزامي وتسجيل الدخول الصارم للمطور والمزيد.

توقيع التعليمات البرمجية الإلزامي

بعد بدء تشغيل kernel في iOS أو iPadOS، يتحكم في عمليات المستخدم وتطبيقاته التي يمكن تشغيلها. للمساعدة على ضمان أن ترد جميع التطبيقات من مصدر معروف ومعتمد وعدم العبث بها، يتطلب iOS و iPadOS توقيع جميع التعليمات البرمجية القابلة للتنفيذ باستخدام شهادة صادرة من Apple. يتم توقيع التطبيقات المتوفرة مع الجهاز، مثل البريد وسفاري، بواسطة Apple. يجب أيضًا التحقق من صحة تطبيقات الجهات الخارجية وتوقيعها باستخدام شهادة صادرة من Apple. ويعمل توقيع التعليمات البرمجية الإلزامي على توسيع مفهوم سلسلة الثقة من نظام التشغيل إلى التطبيقات، ويساعد على منع تطبيقات الجهات الخارجية من تحميل موارد التعليمات البرمجية غير الموقّعة أو استخدام تعليمات برمجية ذاتية التعديل.

كيفية توقيع المطورين تطبيقاتهم

يمكن للمطورين توقيع تطبيقاتهم من خلال التحقق من صحة الشهادة (من خلال برنامج Apple Developer Program). ويمكنهم أيضًا تضمين إطارات العمل داخل تطبيقاتهم والتحقق من صحة هذه التعليمة البرمجية من خلال شهادة صادرة من) Appleمن خلال سلسلة معرّف الفريق).

- **التحقق من صحة الشهادة:** لتطوير وتثبيت التطبيقات في أجهزة iPhone أو iPad، يجب على المطورين التسجيل لدى Apple والانضمام إلى برنامج Apple Developer Program. تتحقق Apple من الهوية الفعلية لكل مطور، سواء كان فردًا أم شركة، قبل إصدار الشهادة. وتتيح هذه الشهادة للمطورين توقيع التطبيقات وإرسالها إلى App Store للتوزيع. نتيجةً لذلك، تم تقديم جميع التطبيقات في App Store من قِبل شخص أو مؤسسة بهوية معروفة، مما يعمل كمانع لإنشاء تطبيقات ضارة. وتمت مراجعتها أيضًا من قِبل Apple للمساعدة على التأكد من أنها تعمل بشكل عام كما هو موضح ولا تحتوي على أخطاء واضحة أو غيرها من المشكلات البارزة. بالإضافة إلى التقنية التي تمت مناقشتها بالفعل، تمنح عملية التمحيص هذه المستخدمين الثقة في جودة التطبيقات التي يشترونها.
- **التحقق من صحة توقيع التعليمة البرمجية:** يسمح iOS و iPadOS للمطورين بدمج إطارات العمل داخل تطبيقاتهم، ومن ثم يمكن استخدامها من خلال التطبيق نفسه أو من خلال الملحقات المدمجة داخل التطبيق. لحماية النظام والتطبيقات الأخرى من تحميل تعليمات برمجية تابعة لجهات خارجية داخل مساحة العنوان، يقوم النظام بإجراء تحقق من صحة توقيع التعليمات البرمجية لجميع المكتبات الديناميكية التي ترتبط بها عملية ما وقت بدء التشغيل. ويتم إتمام عملية التحقق من الصحة هذه من خلال معرف الفريق الذي يتم استخراجه من الشهادة الصادرة من Apple. معرف الفريق عبارة عن سلسلة أبجدية رقمية مكونة من 10 أحرف، مثل 1A2B3C4D5F. قد يرتبط البرنامج مع أي مكتبة للنظام الأساسي تتوفر مع النظام أو أي مكتبة تحمل معرف الفريق ذاته في توقيع التعليمات البرمجية الخاص بها باعتباره العنصر الرئيسي القابل للتنفيذ. ولأن العناصر القابلة للتنفيذ التي تتوفر كجزء من النظام لا تحمل معرف فريق، لا يمكنها الارتباط إلا بالمكتبات التي تتوفر مع النظام نفسه.

التحقق من ملكية التطبيقات الداخلية

تمتلك الشركات المؤهلة إمكانية كتابة تطبيقات داخلية مملوكة للاستخدام داخل أروقتها وتوزيعها على موظفيها. وتستطيع الشركات والمؤسسات التقدم إلى برنامج Apple Developer Enterprise Program (ADEP). لمزيد من المعلومات ولمراجعة متطلبات الأهلية، انظر موقع برنامج Apple Developer Enterprise Program الإلكتروني. بعد أن تصبح المؤسسة عضوًا في برنامج ADEP، يمكنها التسجيل للحصول على ملف تعريف تموين يسمح للتطبيقات الداخلية المملوكة بالعمل على الأجهزة التي تُصرّح لها.

يجب أن يكون لدى المستخدمين ملف تعريف التموين مثبّت لتشغيل تلك التطبيقات. وهذا يساعد على ضمان عدم تمكُّن غير المستخدمين المقصودين في المؤسسة من تحميل التطبيقات على iPhone أو iPad. وتكون التطبيقات المُثبّتة من خلال إدارة جهاز الجوال (MDM) موثوقًا بها ضمنيًا لأن العلاقة بين المؤسسة والجهاز قد تم تأسيسها بالفعل. بخلاف ذلك، يتعين على المستخدم الموافقة على ملف تعريف التموين الخاص بالتطبيق في الإعدادات. يمكن للمؤسسات كذلك تقييد موافقة المستخدمين على التطبيقات من مطورين غير معروفين. عند التشغيل الأول لأي تطبيق داخلي مملوك، يجب أن يتلقى الجهاز تأكيدًا إيجابيًا من Apple بأنه مسموح بتشغيل التطبيق.

أمن المعالجة وقت التشغيل في iOS و iPadOS

يساعد iOS و iPadOS على ضمان أمن وقت التشغيل باستخدام "وضع الحماية" والاستحقاقات المعلنة وعشوائية تخطيط مساحة العنوان (ASLR).

وضع الحماية

تكون جميع تطبيقات الجهات الخارجية في "وضع الحماية"، لذا فهي ممنوعة من الوصول إلى الملفات المخزنة بواسطة تطبيقات أخرى أو من إجراء تغييرات على الجهاز. وقد تم تصميم وضع الحماية لحماية التطبيقات من جمع أو تعديل المعلومات المخزنة بواسطة التطبيقات الأخرى. يحتوي كل تطبيق على دليل رئيسي فريد يضم ملفاته، ويتم تعيينه عشوائيًا عند تثبيت التطبيق. إذا احتاج تطبيق جهة خارجية إلى الوصول إلى معلومات أخرى غير معلوماته الخاصة، فإنه لا يفعل ذلك إلا باستخدام الخدمات الحصرية التي يوفرها iOS و iPadOS.

ملفات النظام وموارده محمية أيضًا من تطبيقات المستخدم. تعمل غالبية ملفات وموارد iOS و iPadOS مثل "جوال" مستخدم لا يتمتع بامتيازات، كما تفعل جميع تطبيقات الجهات الخارجية. ويتم تحميل قسم نظام التشغيل بالكامل للقراءة فقط. بينما الأدوات غير الضرورية، مثل خدمات تسجيل الدخول عن بُعد، لا يتم تضمينها في برامج النظام؛ وواجهات API لا تسمح للتطبيقات بتصعيد امتيازاتها الخاصة لتعديل التطبيقات الأخرى أو iOS و iPadOS.

استخدام الاستحقاقات

تتحكم الاستحقاقات المعلنة في إمكانية الوصول من خلال تطبيقات الجهات الخارجية إلى معلومات المستخدم وإلى الميزات مثل iCloud وإمكانية التوسعة. الاستحقاقات عبارة عن أزواج قيم أساسية يتم تسجيل دخولها إلى أحد التطبيقات وتسمح بالمصادقة بما يتجاوز عوامل وقت التشغيل، مثل معرف مستخدم UNIX. نظرًا لأن الاستحقاقات يتم توقيعها رقميًا، لا يمكن تغييرها. وتُستخدم الاستحقاقات على نطاق واسع بواسطة تطبيقات النظام والبرامج الخفية لتنفيذ عمليات ذات امتيازات خاصة قد تتطلب تشغيل العملية كجذر. وهذا يقلل بشكل كبير من احتمال تصعيد الامتياز بواسطة تطبيق نظام مُخترق أو برنامج خفي.

بالإضافة إلى ذلك، لا يمكن للتطبيقات إجراء معالجة في الخلفية إلا من خلال واجهات API التي يوفرها النظام. يتيح ذلك للتطبيقات الاستمرار في العمل دون تدهور في الأداء أو التأثير بشكل كبير في عمر البطارية.

عشوائية تخطيط مساحة العنوان

إن عشوائية تخطيط مساحة العنوان (ASLR) تساعد على الحماية من استغلال أخطاء فساد الذاكرة. وتستخدم التطبيقات المضمنة تقنية ASLR للمساعدة على ضمان عشوائية جميع مناطق الذاكرة عند التشغيل. بالإضافة إلى العمل عند التشغيل، تقوم ASLR بالترتيب العشوائي لعناوين الذاكرة الخاصة بالتعليمات البرمجية القابلة للتنفيذ ومكتبات النظام ووحدات البناء البرمجية ذات الصلة، ما يقلل احتمال وقوع العديد من الهجمات. على سبيل المثال، يحاول هجوم return-to-libc خداع الجهاز لتنفيذ تعليمات برمجية ضارة من خلال التلاعب بعناوين الذاكرة الخاصة بمكتبات المكدس والنظام. ومن ثم فإن عشوائية تعيين موضع هذه المكتبات يجعل تنفيذ الهجوم أكثر صعوبة، خاصة عبر أجهزة متعددة. تقوم Xcode وبيئات تطوير iOS أو iPadOS، بتجميع برامج الجهات الخارجية تلقائيًا مع تشغيل دعم ASLR.

ميزة عدم التنفيذ

يوفر iOS و iPadOS مزيدًا من الحماية باستخدام ميزة عدم التنفيذ مطلقًا (XN) في ARM، والتي تميّز صفحات الذاكرة على أنها غير قابلة للتنفيذ. ولا يمكن استخدام صفحات الذاكرة التي تم تمييزها على أنها قابلة للكتابة وقابلة للتنفيذ إلا بواسطة التطبيقات تحت ظروف محكمة للغاية: يتحقق kernel من وجود استحقاق توقيع التعليمات البرمجية الديناميكي من Apple فقط. وحتى ذلك الحين، يمكن إجراء اتصال `mmap` واحد فقط لطلب صفحة قابلة للتنفيذ وقابلة للكتابة يتم منحها عنوانًا عشوائيًا. يستخدم سفاري هذه الوظيفة لبرنامج التحويل البرمجي JavaScript Just-in-Time (JIT) الخاص به.

دعم الملحقات في iOS و iPadOS و macOS

يسمح iOS و iPadOS و macOS للتطبيقات بتوفير وظائف للتطبيقات الأخرى من خلال توفير الملحقات. الملحقات عبارة عن ثنائيات قابلة للتنفيذ موقَّعة لأغراض خاصة، يتم تعبئتها داخل التطبيق. أثناء التثبيت، يكتشف النظام تلقائيًا الملحقات ويجعلها متاحة للتطبيقات الأخرى باستخدام نظام مطابقة.

نقاط الملحقات

تسمى منطقة النظام التي تدعم الملحقات **نقطة الملحق**. وتوفر كل نقطة ملحق واجهات API وتفرض سياسات لهذه المنطقة. يحدد النظام الملحقات التي تكون متاحة بناءً على قواعد المطابقة الخاصة بنقطة الملحق. ويُشغِّل النظام تلقائيًا عمليات الملحقات حسب الحاجة ويتحكم في مدة تشغيلها. يمكن استخدام الاستحقاقات لتقييد إتاحة الملحق لتطبيقات نظام معينة. على سبيل المثال، لا تظهر أداة عرض اليوم إلا في مركز الإشعارات، ولا يتوفر ملحق المشاركة إلا من جزء المشاركة. من أمثلة نقاط الملحقات، أدوات اليوم والمشاركة والإجراءات وتحرير الصور وموفر الملفات ولوحة المفاتيح المخصصة.

طريقة تواصل الملحقات

تعمل الملحقات في مساحة العنوان الخاصة بها. إن التواصل بين الملحق والتطبيق الذي تم تنشيطه منه يستخدم الاتصالات بين العمليات بوساطة إطار عمل النظام. ولا تكون لديها إمكانية الوصول إلى ملفات بعضهم بعضًا أو مساحات الذاكرة لكل منها. فقد صُممت الملحقات بحيث تكون معزولة عن بعضها بعضًا، وعن التطبيقات التي تحتويها، وعن التطبيقات التي تستخدمها. وتكون في وضع الحماية مثل أي تطبيق آخر تابع لجهة خارجية ولها حاوية منفصلة عن حاوية التطبيق الذي يحتويها. ومع ذلك، فإنها تشترك في نفس إمكانية الوصول إلى ضوابط الخصوصية التي يتمتع بها التطبيق الحاوي. لذلك إذا منح المستخدم جهات الاتصال حق الوصول إلى أحد التطبيقات، يتم تمديد هذه المنحة لتشمل الملحقات المضمنة في التطبيق ولكن ليس الملحقات التي يتم تنشيطها بواسطة التطبيق.

طريقة استخدام لوحات المفاتيح المخصصة

تعد لوحات المفاتيح المخصصة نوعًا خاصًا من الملحقات، يُمكّنها المستخدم للنظام بأكمله. بعد تمكين ملحق لوحة المفاتيح، يُستخدم لأي حقل من حقول النص باستثناء إدخال رمز الدخول وأي طريقة عرض آمنة للنصوص. لتقييد نقل بيانات المستخدم، يتم تشغيل لوحات المفاتيح المخصصة بشكل افتراضي في وضع حماية مقيّد للغاية يمنع الوصول إلى الشبكة وإلى والخدمات التي تنفذ عمليات الشبكة نيابة عن عملية ما وإلى واجهات API التي قد تتيح للملحق تسريب بيانات الكتابة. ويمكن لمطوري لوحات المفاتيح المخصصة المطالبة بأن تكون ملحقاتهم ذات وصول مفتوح، مما يتيح للنظام تشغيل الملحق في وضع الحماية الافتراضي بعد الحصول على موافقة من المستخدم.

MDM والملحقات

بالنسبة للأجهزة المسجلة في حل إدارة جهاز الجوال (MDM)، تلتزم ملحقات المستندات ولوحة المفاتيح بقواعد (إدارة "فتح في"). على سبيل المثال، يمكن أن يساعد حل MDM على منع المستخدمين من تصدير مستند من تطبيق مُدار إلى مزود مستندات غير مُدار، أو يساعد على منعها من استخدام لوحة مفاتيح غير مُدارة مع تطبيق مُدار. بالإضافة إلى ذلك، يمكن لمطوري التطبيقات منع استخدام ملحقات لوحات المفاتيح التابعة لجهات خارجية داخل تطبيقاتهم.

حماية التطبيقات ومجموعات التطبيقات في iOS و iPadOS

في iOS و iPadOS، يمكن للمؤسسات حماية التطبيقات بأمان باستخدام IOS SDK والانضمام إلى مجموعة التطبيقات في Apple Developer Portal.

اعتماد حماية البيانات في التطبيقات

تقدّم (SDK) مجموعة أدوات تطوير برامج iOS لكل من iOS و iPadOS مجموعة كاملة من واجهات API تسهّل على مطوري الجهات الخارجية والمطورين الداخليين اعتماد حماية البيانات والمساعدة في ضمان أعلى مستوى من الحماية في تطبيقاتهم. وتتوفر حماية البيانات لواجهات API للملفات وقواعد البيانات، بما في ذلك NSFileManager و CoreData و NSData و SQLite.

يتم أيضًا تخزين قاعدة بيانات تطبيق البريد (بما في ذلك المرفقات) والكتب المُدارة وإشارات سفاري المرجعية وصور تشغيل التطبيق وبيانات الموقع من خلال التشفير، مع مفاتيح محمية برمز دخول المستخدم على جهازه. ويطبّق التقويم (باستثناء المرفقات) وجهات الاتصال والتذكيرات والملاحظات والرسائل والصور استحقاق `Data Protection` **محمية حتى أول مصادقة من المستخدم**.

التطبيقات التي يُثبّتها المستخدم ولا تكون ضمن فئة حماية بيانات محددة تندرج ضمن الفئة "محمية حتى أول مصادقة من المستخدم" بشكل افتراضي.

الانضمام إلى مجموعة تطبيقات

يمكن للتطبيقات والملحقات التي يملكها حساب مطور معين مشاركة المحتوى عند تكوينه ليكون جزءًا من مجموعة تطبيقات. ويقرر المطور ما إذا كان يريد إنشاء المجموعات المناسبة على Apple Developer Portal وتضمين المجموعة المطلوبة من التطبيقات والملحقات أم لا. بمجرد تكوين التطبيقات لتكون جزءًا من مجموعة تطبيقات، يمكنها الوصول إلى التالي:

- حاوية مشتركة على وحدة التخزين مخصصة للتخزين وتبقى على الجهاز طالما تم تثبيت تطبيق واحد على الأقل من المجموعة
- التفضيلات المشتركة
- عناصر سلسلة المفاتيح المشتركة

يساعد Apple Developer Portal على ضمان أن تكون معرّفات مجموعة التطبيقات (GID) فريدة عبر النظام البيئي للتطبيق.

أمن التطبيقات في macOS

مقدمة عن أمن التطبيقات في macOS

يتكون أمن التطبيقات في macOS من عدد من الطبقات المتداخلة؛ أولها خيار تشغيل التطبيقات الموقَّعة والموثوق بها فقط من App Store. بالإضافة إلى ذلك، يضع macOS طبقات من الحماية للمساعدة على ضمان أن تكون التطبيقات التي يتم تنزيلها من الإنترنت خالية من البرامج الضارة المعروفة. ويوفر macOS تقنيات لاكتشاف البرامج الضارة وإزالتها، بجانب وسائل حماية إضافية مصممة لمنع التطبيقات غير الموثوق بها من الوصول إلى بيانات المستخدم. تم تصميم خدمات Apple مثل التوثيق وتحديثات XProtect للمساعدة على منع تثبيت البرامج الضارة. عند الضرورة، تحدد هذه الخدمات مواقع البرامج الضارة التي ربما تكون قد تجنبت الكشف عنها في البداية ثم تزيلها بسرعة وكفاءة. وفي النهاية، يتمتع مستخدم macOS بحرية العمل في إطار النموذج الأمني الذي يكون منطقيًا بالنسبة له — بما في ذلك تشغيل التعليمات البرمجية غير الموقَّعة وغير الموثوق بها تمامًا.

عملية توقيع التعليمات البرمجية للتطبيقات في macOS

توقّع Apple على كل التطبيقات المتوفرة من App Store. وقد تم تصميم هذا التوقيع لضمان عدم العبث بها أو تبديلها. كما توقّع Apple على أي تطبيقات تتوفر مع أجهزة Apple.

في macOS 10.15، يجب أن يوقّع المطور جميع التطبيقات الموزَّعة خارج App Store باستخدام شهادة معرّف المطور الصادرة من) Appleمدمجة مع مفتاح خاص) وأن يتم توثيقها من قِبل Apple كي تعمل وفقًا لإعدادات الحارس الرقمي الافتراضية. يجب أيضًا توقيع التطبيقات التي تم تطويرها داخليًا باستخدام معرف المطور الصادر من Apple بحيث يستطيع المستخدمون التحقق من سلامتها.

في macOS، يعمل توقيع التعليمات البرمجية والتوثيق بشكل مستقل — ويمكن تنفيذهما بواسطة جهات فاعلة مختلفة — لتحقيق أهداف مختلفة. ويتم تنفيذ توقيع التعليمات البرمجية بواسطة المطور باستخدام شهادة معرف المطور الخاصة به (صادرة بواسطة Apple). ويُثبِت التحقق من هذا التوقيع للمستخدم أن برامج المطور لم يتم العبث بها منذ إنشاء المطور إياها وتوقيعها. ويمكن تنفيذ التوثيق بواسطة أي شخص في سلسلة توزيع البرامج ويُثبت أنه قد تم تزويد Apple بنسخة من التعليمات البرمجية للتحقق من وجود برامج ضارة ولم يتم العثور على برامج ضارة معروفة. ناتج التوثيق عبارة عن تذكرة يتم تخزينها على خوادم Apple ويمكن تدبيسها اختياريًا بالتطبيق (من قِبل أي شخص) دون إبطال توقيع المطور.

تتطلب عناصر التحكم في الوصول الإلزامية (MACs) توقيع التعليمات البرمجية لتمكين الاستحقاقات المحمية بواسطة النظام. على سبيل المثال، يجب أن تكون التطبيقات التي تتطلب الوصول عبر جدار الحماية ذات تعليمات برمجية موقَّعة باستخدام استحقاق MAC المناسب.

الحارس الرقمي وحماية وقت التشغيل في macOS

يوفر macOS تقنية الحارس الرقمي وحماية وقت التشغيل للمساعدة على ضمان تشغيل البرامج الموثوقة فقط على Mac الخاص بالمستخدم.

الحارس الرقمي

يتضمن macOS تقنية أمن تسمى **الحارس الرقمي**، المصممة لتساعد على ضمان تشغيل البرامج الموثوقة فقط على Mac الخاص بالمستخدم. عندما يقوم المستخدم بتنزيل وفتح تطبيق أو مكون إضافي أو حزمة مُثبّت من خارج App Store، يتحقق الحارس الرقمي من أن البرنامج من مطور معلوم الهوية، وأنه تم توثيقه بواسطة Apple على أنه خالٍ من المحتوى الضار المعروف، ولم يتم تغييره. تطلب الحارس الرقمي أيضًا موافقة المستخدم قبل فتح البرنامج الذي تم تنزيله لأول مرة للتأكد من عدم خداع المستخدم لتشغيل تعليمات برمجية قابلة للتنفيذ يعتقد أنها مجرد ملف بيانات. يتتبع الحارس الرقمي أيضًا مصدر الملفات المكتوبة بواسطة البرنامج الذي تم تنزيله.

بشكل افتراضي، تساعد الحارس الرقمي على ضمان أن تكون جميع البرامج التي يتم تنزيلها موقَّعة بواسطة App Store أو موقَّعة بواسطة مطور مسجَّل وموثَّقة من قِبل Apple. تم تصميم كلٌ من عملية مراجعة App Store وقناة التوثيق لضمان خلو التطبيقات من البرامج الضارة المعروفة. لذا فإنه بشكل افتراضي، **يتم فحص جميع البرامج الموجودة في macOS بحثًا عن المحتويات الضارة المعروفة عند فتحها لأول مرة، بغض النظر عن كيفية وصولها إلى الـ Mac**.

يتوفر لدى المستخدمين والمؤسسات خيار السماح بالبرامج المثبتة من App Store فقط. بدلاً من ذلك، يمكن للمستخدمين تجاوز سياسات الحارس الرقمي لفتح أي برنامج، ما لم يكن مقيّدًا بواسطة أحد حلول إدارة جهاز الجوال (MDM). وبإمكان المؤسسات استخدام MDM لتكوين إعدادات الحارس الرقمي، بما في ذلك السماح بالبرامج الموقَّعة بهويات بديلة. ومن الممكن أيضًا تعطيل الحارس الرقمي بالكامل، إذا لزم الأمر.

توفر الحارس الرقمي أيضًا حماية ضد توزيع المكونات الإضافية الضارة مع التطبيقات غير الضارة. إذ يؤدي استخدام التطبيق إلى تحميل مكون إضافي ضار دون علم المستخدم. وعند الضرورة، تفتح الحارس الرقمي التطبيقات من مواقع عشوائية في وضع القراءة فقط. وقد تم تصميم ذلك لمنع التحميل التلقائي للمكونات الإضافية الموزَّعة مع التطبيق.

حماية وقت التشغيل

تكون ملفات النظام وموارده و kernel الخاصة به محمية من مساحة التطبيقات الخاصة بالمستخدم. وتُوضع كل التطبيقات المتوفرة من App Store في وضع الحماية لتقييد الوصول إلى البيانات المخزنة بواسطة التطبيقات الأخرى. إذا احتاج تطبيق وارد من App Store إلى الوصول إلى بيانات من تطبيق آخر، فلا يمكنه القيام بذلك إلا باستخدام واجهات API والخدمات التي يوفرها macOS.

الحماية ضد البرامج الضارة في macOS

تُشغّل Apple عملية تحليل التهديدات لتحديد البرامج الضارة وحظرها بسرعة.

ثلاث طبقات للحماية

ويتم تنظيم وسائل الحماية من البرامج الضارة في ثلاث طبقات:

1. **منع تشغيل البرامج الضارة أو تنفيذها:** App Store أو الحارس الرقمي إلى جانب التوثيق
2. **حظر تشغيل البرامج الضارة على أنظمة العملاء:** الحارس الرقمي والتوثيق و XProtect
3. **معالجة البرامج الضارة التي تم تنفيذها:** XProtect

تم تصميم الطبقة الأولى من الحماية لإعاقة توزيع البرامج الضارة ومنع بدء تشغيلها حتى ولو لمرة واحدة—يُعد هذا هدف App Store والحارس الرقمي إلى جانب وظيفة التوثيق.

تهدف طبقة الحماية التالية إلى المساعدة على ضمان أنه في حال ظهور برامج ضارة على أي Mac، يتم التعرّف عليها وحظرها بسرعة، وذلك لإيقاف الانتشار وإصلاح أنظمة Mac التي نجحت في التسلل إليها بالفعل. تتم إضافة XProtect إلى طبقة الحماية هذه، إلى جانب الحارس الرقمي والتوثيق.

وأخيرًا، تعمل XProtect على معالجة البرامج الضارة التي نجحت في التسلل إلى النظام.

تجتمع وسائل الحماية هذه، التي تم تناولها بالتفصيل أدناه، لدعم أفضل ممارسات الحماية من الفيروسات والبرامج الضارة. وتوجد وسائل حماية إضافية، خاصةً على أجهزة كمبيوتر Mac المزودة بسيليكون Apple للحد من الضرر المحتمل للبرامج الضارة التي تنجح في التسلل إلى النظام. انظر حماية وصول التطبيقات إلى بيانات المستخدم للاطلاع على الطرق التي يمكن أن يساعد بها macOS في حماية بيانات المستخدم من البرامج الضارة، وكذلك تكامل نظام التشغيل لمعرفة الطرق التي يستطيع بها macOS الحد من الإجراءات التي يمكن أن تُجريها البرامج الضارة على النظام.

التوثيق

التوثيق عبارة عن خدمة للبحث عن البرامج الضارة تقدمها Apple. يقوم المطورون الذين يرغبون في توزيع تطبيقات macOS خارج App Store بإرسال تطبيقاتهم لإجراء الفحص كجزء من عملية التوزيع. تفحص Apple هذا البرنامج بحثًا عن برامج ضارة معروفة، وإذا لم يتم العثور على أي منها، فإنها تُصدر تذكرة توثيق. ويقوم المطورون عادةً بإرفاق هذه التذكرة في تطبيقاتهم حتى يتمكن الحارس الرقمي من التحقق من التطبيق وبدء تشغيله، حتى دون اتصال بالإنترنت.

بإمكان Apple أيضًا إصدار تذكرة إلغاء للتطبيقات المعروفة بأنها ضارة، حتى لو كانت قد تم توثيقها سابقًا. ويقوم macOS بانتظام بالتحقق من وجود تذاكر إلغاء جديدة بحيث يكون لدى الحارس الرقمي أحدث المعلومات ويمكنه حظر تشغيل مثل هذه الملفات. يمكن لهذه العملية حظر التطبيقات الضارة بسرعة كبيرة لأن التحديثات تجري في الخلفية بشكل أكثر تكرارًا من تحديثات الخلفية التي تدفع توقيعات XProtect الجديدة. بالإضافة إلى ذلك، يمكن تطبيق هذه الحماية على التطبيقات التي تم توثيقها سابقًا، والتي لم يتم توثيقها.

XProtect

يتضمن macOS تقنية حماية من الفيروسات مضمنة تسمى **XProtect** للكشف عن البرامج الضارة وإزالتها استنادًا إلى التوقيع. يستخدم النظام تواقيع Yara، وهي أداة تُستخدم لإجراء الكشف عن البرامج الضارة استنادًا إلى التوقيعات، والتي تحرص Apple على تحديثها بشكل منتظم. تراقب Apple حالات العدوى والإصابة بالبرامج الضارة الجديدة وتُحدّث التوقيعات تلقائيًا — بشكل مستقل عن تحديثات النظام — للمساعدة في حماية أجهزة كمبيوتر Mac ضد الإصابات بالبرامج الضارة. ويقوم XProtect تلقائيًا باكتشاف البرامج الضارة المعروفة ومنع تنفيذها. في macOS 10.15 أو أحدث، يتحقق XProtect من المحتوى الضار المعروف عند:

- تشغيل تطبيق لأول مرة
- تغيير تطبيق (في نظام الملفات)
- تحديث توقيعات XProtect

عندما يكتشف XProtect برامج ضارة معروفة، يتم حظر البرنامج وإعلام المستخدم ومنحه خيار نقل البرنامج إلى سلة المهملات.

ملاحظة: تكون عملية التوثيق فعالة ضد الملفات المعروفة (أو تجزئات الملفات) ويمكن استخدامها على التطبيقات التي تم تشغيلها سابقًا. وتُعدّ قواعد XProtect المستندة إلى التوقيعات أكثر عمومية من تجزئة ملف معين حيث يمكنها العثور على متغيرات لم تعرفها Apple. تفحص XProtect التطبيقات التي تم تغييرها أو التطبيقات عند تشغيلها لأول مرة فقط.

في حال وصول برنامج ضار إلى أي Mac، فإن XProtect تتضمن كذلك تقنية لمعالجة حالات الإصابة. على سبيل المثال، تتضمن محركًا يعمل على معالجة الإصابات بالبرامج الضارة بناءً على التحديثات التي يتم توفيرها تلقائيًا من) Appleكجزء من التحديثات التلقائية لملفات بيانات النظام وتحديثات الأمن). يزيل هذا النظام البرامج الضارة عند تلقي معلومات مُحدَّثة، ويستمر في البحث بشكل دوري عن الإصابات بالبرامج الضارة؛ ومع ذلك، لا يعيد XProtect تشغيل Mac تلقائيًا. بالإضافة إلى ذلك، يحتوي XProtect على محرك متقدم لاكتشاف البرامج الضارة غير المعروفة بناءً على التحليل السلوكي. تُستخدَم المعلومات حول البرامج الضارة التي اكتشفها هذا المحرك، بما في ذلك البرنامج المسؤول في النهاية عن تنزيلها، لتحسين توقيعات XProtect وأمن macOS.

التحديثات الأمنية التلقائية لـ XProtect

تُصدر Apple تحديثات لـ XProtect تلقائيًا استنادًا إلى أحدث معلومات متوفرة عن التهديدات. وبشكل افتراضي، يتحقق macOS من هذه التحديثات يوميًا. تكون تحديثات التوثيق التي يتم توزيعها باستخدام مزامنة CloudKit أكثر تكرارًا.

كيف تستجيب Apple عند اكتشاف برامج ضارة جديدة

عند اكتشاف برامج ضارة جديدة، يمكن تنفيذ عدد من الخطوات:

- يتم إلغاء أي شهادات مرتبطة بمعرّف المطور.
- يتم إصدار تذاكر إلغاء التوثيق لكل الملفات (التطبيقات والملفات ذات الصلة).
- يتم تطوير توقيعات XProtect وإصدارها.

  يتم تطبيق هذه التوقيعات أيضًا بأثر رجعي على البرامج التي تم توثيقها سابقًا، ويمكن أن تؤدي أي اكتشافات جديدة إلى حدوث إجراء أو أكثر من الإجراءات السابقة.

في النهاية، تُطلق عملية الكشف عن البرامج الضارة سلسلة من الخطوات على مدار الثواني والساعات والأيام التالية لنشر أفضل وسائل حماية ممكنة لمستخدمي الـ Mac.

التحكم في وصول التطبيقات إلى الملفات في macOS

تؤمن Apple بأنه من حق المستخدمين امتلاك الشفافية الكاملة وحرية الموافقة والرفض والتحكم في ما تفعله التطبيقات ببياناتهم. في macOS 10.15، يفرض النظام هذا النموذج للمساعدة على ضمان اشتراط حصول جميع التطبيقات على موافقة المستخدم قبل الوصول إلى الملفات الموجودة في المستندات والتنزيلات وسطح المكتب و iCloud Drive ووحدات التخزين على الشبكة. في macOS 10.13 أو أحدث، التطبيقات التي تتطلب الوصول إلى جهاز التخزين بالكامل تجب إضافتها بشكل صريح في إعدادات النظام (macOS 13 أو أحدث) أو تفضيلات النظام (macOS 12 أو أقدم). بالإضافة إلى ذلك، تتطلب إمكانيات الوصول والأتمتة إذن المستخدم للمساعدة على ضمان عدم التحايل على وسائل الحماية الأخرى. استنادًا إلى سياسة الوصول، قد يُطلب من المستخدمين، أو يُشترط عليهم، تغيير الإعداد في:

- في macOS 13 أو أحدث: إعدادات النظام > الخصوصية والأمن > الخصوصية
- في macOS 12 أو أقدم: تفضيلات النظام > الأمن والخصوصية > الخصوصية

العنصر	مطالبة المستخدم حسب التطبيق	وجوب تحرير إعدادات خصوصية النظام بواسطة المستخدم
إمكانية الوصول	✗	✓
الوصول الكامل إلى التخزين الداخلي	✗	✓
الملفات والمجلدات **ملاحظة:** تتضمن سطح المكتب والمستندات والتنزيلات ووحدات التخزين على الشبكة ووحدات التخزين القابلة للإزالة	✓	✗
الأتمتة (أحداث Apple)	✓	✗

يُطلب من المستخدم الذي يقوم بتشغيل خزنة الملفات على الـ Mac توفير بيانات اعتماد صالحة قبل متابعة عملية التمهيد واكتساب حق الوصول إلى أوضاع بدء التشغيل المتخصصة. بدون بيانات اعتماد تسجيل دخول صالحة أو مفتاح استرداد، تظل وحدة التخزين بأكملها مشفرة ومحمية من الوصول غير المصرح به، حتى إذا تمت إزالة جهاز التخزين الفعلي وتوصيله بكمبيوتر آخر.

لحماية البيانات في بيئة مؤسسية، يجب على قسم تقنية المعلومات تحديد وفرض سياسات تكوين خزنة الملفات باستخدام إدارة الأجهزة المحمولة (MDM). ويتوفر لدى المؤسسات العديد من الخيارات لإدارة وحدات التخزين المشفرة، بما في ذلك مفاتيح الاسترداد المؤسسية أو مفاتيح الاسترداد الشخصية (التي يمكن تخزينها اختياريًا باستخدام MDM للضمان) أو مزيج من الاثنين. يمكن أيضًا تعيين تدوير المفاتيح كسياسة في MDM.

الميزات الآمنة في تطبيق الملاحظات

يتضمن تطبيق الملاحظات ميزة الملاحظات الآمنة—على الـ iPhone والـ iPad والـ Mac وموقع iCloud الإلكتروني—التي تتيح للمستخدمين حماية محتويات ملاحظات محددة. يمكن للمستخدمين كذلك مشاركة ملاحظات مع الآخرين بشكل آمن.

الملاحظات الآمنة

يتم تشفير الملاحظات الآمنة تشفيرًا كاملاً باستخدام عبارة دخول يقدمها المستخدم تكون مطلوبة لعرض الملاحظات على أجهزة iOS و iPadOS و macOS وموقع ويب iCloud. يمكن أن يكون لكل حساب iCloud (بما في ذلك حسابات "على الجهاز الخاص بي") عبارة دخول منفصلة.

عندما يُؤمّن المستخدم الملاحظة، يتم اشتقاق مفتاح 16 بايت من عبارة دخول المستخدم باستخدام PBKDF2 و SHA256. ويتم تشفير الملاحظة وجميع مرفقاتها باستخدام AES مع Galois/Counter Mode (AES-GCM). كما يتم إنشاء سجلات جديدة في Core Data و CloudKit لتخزين الملاحظة المشفرة والمرفقات والعلامات ومتجه التهيئة. بعد إنشاء السجلات الجديدة، تُحذف البيانات الأصلية غير المشفرة. وتشمل المرفقات التي تدعم التشفير الصور والرسومات والجداول والخرائط ومواقع الويب. لا يمكن تشفير الملاحظات التي تحتوي على أنواع أخرى من المرفقات، ولا يمكن إضافة المرفقات غير المدعومة إلى الملاحظات الآمنة.

لعرض ملاحظة آمنة، يتعين على المستخدم إدخال عبارة الدخول أو المصادقة باستخدام بصمة الوجه أو بصمة الإصبع. بعد مصادقة المستخدم بنجاح، سواء لعرض أو إنشاء ملاحظة آمنة، يفتح تطبيق الملاحظات جلسة آمنة. أثناء فتح الجلسة الآمنة، يمكن للمستخدم عرض أو تأمين الملاحظات الأخرى دون مصادقة إضافية. لكن لا تنطبق الجلسة الآمنة إلا على الملاحظات المحمية بعبارة الدخول المقدمة. ويظل لزامًا على المستخدم مصادقة الملاحظات المحمية بعبارة دخول مختلفة. تُغلق الجلسة الآمنة في الحالات التالية:

- عند ضغط المستخدم على زر القفل الآن في تطبيق الملاحظات
- عند تبديل تطبيق الملاحظات إلى الخلفية لأكثر من 3 دقائق (8 دقائق في macOS)
- عند قفل جهاز iOS أو iPadOS

لتغيير عبارة الدخول في ملاحظة آمنة، يجب على المستخدم إدخال عبارة الدخول الحالية، نظرًا إلى عدم توفر بصمة الوجه وبصمة الإصبع عند تغيير عبارة الدخول. بعد اختيار عبارة دخول جديدة، يُعيد تطبيق الملاحظات، في نفس الحساب، صياغة مفاتيح جميع الملاحظات الموجودة المشفرة بعبارة عبارة الدخول السابقة.

إذا أخطأ المستخدم في كتابة عبارة الدخول ثلاث مرات متتالية، يعرض تطبيق الملاحظات تلميحًا مقدمًا من المستخدم، إذا كان المستخدم قد قام بتوفير واحد عند الإعداد. وإذا ظلّ المستخدم لا يتذكر عبارة الدخول، يمكنه إعادة تعيينها في إعدادات تطبيق الملاحظات. تتيح هذه الميزة للمستخدمين إنشاء ملاحظات آمنة جديدة باستخدام عبارة دخول جديدة، ولكنها لن تسمح لهم بعرض الملاحظات التي تم تأمينها سابقًا. ويظل من الممكن عرض الملاحظات التي تم تأمينها سابقًا في حالة تذكر عبارة الدخول القديمة. تتطلب إعادة تعيين عبارة الدخول وجود عبارة دخول حساب المستخدم على iCloud.

الملاحظات المشتركة

يمكن أن تشارك مع الآخرين الملاحظات التي لا تكون مشفرة تشفيرًا كاملاً باستخدام عبارة دخول. وتظل الملاحظات المشتركة تستخدم نوع البيانات المشفرة في CloudKit لأي نص أو مرفقات يضعها المستخدم في الملاحظة. ويتم تشفير الأصول دائمًا باستخدام مفتاح يتم تشفيره في CKRecord. ولا يتم تشفير بيانات التعريف، مثل تواريخ الإنشاء والتعديل. تدير CloudKit العملية التي يمكن للمشاركين من خلالها تشفير وفك تشفير بيانات بعضهم بعضًا.

الميزات الآمنة في تطبيق الاختصارات

في تطبيق الاختصارات، تتم مزامنة الاختصارات اختياريًا عبر أجهزة Apple باستخدام iCloud. يمكن أيضًا مشاركة الاختصارات مع مستخدمين آخرين عبر iCloud. ويتم تخزين الاختصارات محليًا بتنسيق مشفر.

الاختصارات المخصصة متعددة الاستخدامات — فهي تشبه البرامج النصية أو البرامج. عند تنزيل الاختصارات من الإنترنت، يتم تحذير المستخدم من أن Apple لم تراجع الاختصار ويُمنح الفرصة لفحص الاختصار. للحماية من الاختصارات الضارة، يتم تنزيل تعريفات البرامج الضارة المحدَّثة لتحديد الاختصارات الضارة في وقت التشغيل.

يمكن للاختصارات المخصصة أيضًا تشغيل JavaScript محدد من قِبل المستخدم على مواقع الويب في سفاري عند الاستدعاء من صفحة المشاركة. للحماية ضد JavaScript الضارة التي، على سبيل المثال، تخدع المستخدم لتشغيل برنامج نصي على موقع ويب خاص بالوسائط الاجتماعية يجمع بياناته، يتم التحقق من صحة JavaScript وفقًا لتعريفات البرامج الضارة سالفة الذكر. في المرة الأولى التي يُشغّل فيها أحد المستخدمين JavaScript على أحد المجالات، يُطلب من المستخدم السماح بتشغيل الاختصارات التي تحتوي على JavaScript في صفحة الويب الحالية لهذا المجال.

أمن الخدمات

نظرة عامة على أمن الخدمات

صممت Apple مجموعة قوية من الخدمات لمساعدة المستخدمين في تحقيق أقصى قدر من الاستفادة والإنتاجية على أجهزتهم. توفر هذه الخدمات إمكانات قوية للتخزين السحابي والمزامنة وتخزين كلمات السر والمصادقة والدفع والمراسلة والاتصالات وغير ذلك، وكل ذلك مع حماية خصوصية المستخدمين وأمن بياناتهم.

يتناول هذا الفصل تقنيات الأمن المستخدمة في iCloud وتسجيل الدخول باستخدام Apple وApple Pay و iMessage ومراسلة الشركات من Apple وفيس تايم وتحديد الموقع والاستمرارية.

ملاحظة: لا تتوفر بعض خدمات ومحتويات Apple في بعض البلدان أو المناطق.

Apple ID و Apple ID المُدار

نظرة عامة على أمن Apple ID

Apple ID هو الحساب المستخدم في تسجيل الدخول إلى خدمات Apple. من المهم للمستخدمين إبقاء حسابات Apple ID الخاصة بهم آمنة لمنع الوصول غير المصرح به إلى حساباتهم. وللمساعدة في ذلك، تتطلب حسابات Apple ID كلمات سر قوية تتوفر بها الشروط التالية:

- يجب ألا يقل طولها عن ثمانية أحرف
- يجب أن تحتوي على حروف وأرقام
- يجب ألا يحتوي على ثلاثة أحرف متطابقة متتالية أو أكثر
- لا يمكن أن تكون كلمة سر شائعة الاستخدام

من المستحسن أن يتجاوز المستخدمون هذه الإرشادات بإضافة المزيد من الأحرف وعلامات الترقيم لجعل كلمات السر أشد قوة.

تقوم Apple كذلك بإبلاغ المستخدمين بالبريد الإلكتروني أو الإشعارات الموجهة أو كليهما عند إجراء تغييرات مهمة على حساباتهم—على سبيل المثال، إذا تم تغيير كلمة السر أو معلومات الفوترة أو في حالة استخدام Apple ID لتسجيل الدخول على جهاز جديد. وإذا بدا أي شيء غير مألوف، يُطلب من المستخدم تغيير كلمة سر Apple ID الخاص به على الفور.

بالإضافة إلى ذلك، تستعين Apple بمجموعة متنوعة من السياسات والتدابير المصممة لحماية حسابات المستخدمين. وذلك يتضمن تقييد عدد محاولات تسجيل الدخول وإعادة تعيين كلمة السر الفاشلة، والمراقبة النشطة لعمليات الاحتيال للمساعدة في اكتشاف الهجمات فور حدوثها، والمراجعة المنتظمة للسياسات مما يتيح لشركة Apple التكيف مع أي معلومات جديدة قد تؤثر على أمن المستخدم.

ملاحظة: تُعيَّن سياسة كلمة سر Apple ID المُدار بواسطة أحد المسؤولين في Apple School Manager أو Apple Business Manager.

المصادقة بخطوتين

لمساعدة المستخدمين على تأمين حساباتهم بشكل أكبر، تستخدم Apple بشكل افتراضي **المصادقة بخطوتين**—طبقة إضافية من الأمن لحسابات Apple ID. s% مصممة لضمان عدم وصول أي شخص غير مالك الحساب إلى الحساب، حتى لو كان شخصًا آخر يعرف كلمة السر. باستخدام المصادقة بخطوتين، لا يمكن الوصول إلى حساب المستخدم إلا على الأجهزة الموثوق بها فقط، مثل iPhone أو iPad أو Mac الخاص بالمستخدم، أو على أجهزة أخرى بعد إكمال عملية تحقق عبر أحد هذه الأجهزة الموثوق بها أو رقم هاتف موثوق به. لتسجيل الدخول لأول مرة على أي جهاز جديد، يلزم توفر معلومتين — كلمة سر Apple ID ورمز تحقق مكون من ستة أرقام يكون معروضًا على أجهزة المستخدم الموثوق بها أو مرسلاً إلى رقم هاتف موثوق به. بإدخال الرمز، يؤكد المستخدم أنه يثق بالجهاز الجديد وأنه آمن لتسجيل الدخول. ونظرًا لأن كلمة السر وحدها لم تعد كافية للوصول إلى حساب المستخدم، فإن المصادقة بخطوتين تعمل على تحسين أمن Apple ID الخاص بالمستخدم وجميع معلوماته الشخصية التي يُخزّنها لدى Apple. ويتم دمجها مباشرةً في iOS و iPadOS و macOS و tvOS و watchOS وأنظمة المصادقة المستخدمة من قِبل مواقع Apple على الويب.

عندما يسجّل المستخدم الدخول إلى موقع من مواقع Apple على الويب عبر متصفح ويب، يتم إرسال طلب خطوة ثانية إلى جميع الأجهزة الموثوق بها المرتبطة بحساب المستخدم على iCloud، لطلب الموافقة على جلسة الويب. وفي الحالات التي يسجل فيها المستخدم الدخول إلى موقع من مواقع Apple على الويب من متصفح على جهاز موثوق به، يرى رمز التحقق معروضًا محليًا على الجهاز الذي يستخدمه. عندما يُدخل المستخدم الرمز على ذلك الجهاز، تتم الموافقة على جلسة الويب.

إعادة تعيين كلمة السر واستعادة الحساب

في حال نسيان كلمة سر حساب Apple ID، يمكن للمستخدم إعادة تعيينها على جهاز موثوق به. في حالة عدم توفر جهاز موثوق به مع معرفة كلمة السر، يمكن للمستخدم استخدام رقم هاتف موثوق به للمصادقة من خلال التحقق عبر خدمة الرسائل القصيرة. بالإضافة إلى ذلك، لتوفير الاسترداد الفوري لحساب Apple ID، يمكن استخدام رمز دخول مستخدم سابقًا لإعادة التعيين بالتزامن مع الرسائل القصيرة. إذا لم تكن هذه الخيارات ممكنة، يجب اتباع عملية استرداد الحساب. لمزيد من المعلومات، انظر مقال دعم Apple كيفية استخدام استراد الحساب عندما لا تستطيع إعادة تعيين كلمة سر Apple ID.

أمن Apple ID المُدار

تعمل حسابات Apple ID المُدارة بطريقة مماثلة إلى حد كبير لحساب Apple ID، لكنها تملكها وتتحكم فيها مؤسسة أو منشآت تعليمية. ويمكن لهذه المؤسسات إعادة تعيين كلمات السر وإيقاف الاتصالات مثل فيس تايم و iMessage وإعداد أذونات تستند إلى الأدوار للموظفين وأعضاء الفريق والمدرسين والطلاب.

بالنسبة لحسابات Apple ID المُدارة، تُعطَّل بعض الخدمات (على سبيل المثال، App Store و HomeKit وتحديد الموقع).

إدارة الوصول إلى حسابات Apple ID المُدارة

يمكن أن تستخدم المؤسسات ميزة إدارة الوصول المتوفرة في Apple Business Manager و Apple School Manager و Apple Business Essentials لتحديد المكان الذي يمكن فيه استخدام حسابات Apple ID المُدارة والخدمات المتوفرة لها.

بفضل استخدام إدارة الوصول، يمكنك تحديد ما إذا كان بإمكان المستخدمين تسجيل الدخول باستخدام حسابات Apple ID المُدارة على أي جهاز، أو على الأجهزة المُدارة فقط، أو على الأجهزة المُدارة والخاضعة للإشراف فقط. كما يتمكن المسؤولون أيضًا من تكوين ما إذا كان يُسمح للمستخدمين بتسجيل الدخول إلى iCloud على الويب أم لا. يسمح ذلك للمؤسسات باستخدام حالة إدارة الجهاز كعامل لتحديد ما إذا كان ينبغي منح الوصول إلى البيانات التنظيمية أم لا.

وبالإضافة إلى ذلك، يمكن أن يحدد المسؤولون خدمات iCloud التي تتوفر لمستخدميهم. يتضمن ذلك تحديد الوصول إلى برامج Apple Developer، والإصدار التجريبي من برنامج AppleSeed for IT، وتحديد ما إذا كان يُسمَح للمستخدمين بالوصول إلى بوابة خصوصية Apple على الموقع Privacy.Apple.com.

تدعم حسابات Apple ID المُدارة أيضًا التعاون في المستندات باستخدام Keynote و Numbers و Pages والتذكيرات والملاحظات، بالإضافة إلى الاتصال باستخدام فيس تايم و iMessage. بالنسبة إلى هذه الخدمات، يمكن أن تحدد المؤسسات ما إذا كان بإمكان المستخدمين التعاون مع أي شخص أو مع الحسابات التي تم إنشاؤها فقط داخل مؤسسة Apple School Manager أو Apple Business Manager أو Apple Business Essential نفسها.

في حالة تغيُّر قواعد إدارة الوصول، فإنها تُطبَّق على الأجهزة التي سجَّل المستخدم الدخول إليها باستخدام حساب Apple ID المُدار. في حالة تغيُّر متطلبات حالة إدارة الجهاز، يتم تسجيل الخروج من حساب Apple ID المُدار تلقائيًا من الجهاز إذا كانت حالة الجهاز لا تتوافق مع المتطلبات الجديدة.

فحص حسابات Apple ID المُدارة

تدعم حسابات Apple ID المدارة التي تم إنشاؤها في Apple School Manager **الفحص** أيضًا، مما يتيح للمؤسسات الامتثال للوائح القانونية ولوائح الخصوصية. يتمكن المستخدم الذي يحصل على دور مسؤول أو مدير موقع أو مدير موظفين أو مدرس من فحص حسابات Apple ID المُدارة المحددة.

يستطيع المراقبون مراقبة الحسابات التي تحتهم فقط في التسلسل الهرمي للمؤسسة. على سبيل المثال، يمكن للمدرسين مراقبة الطلاب، ويستطيع المديرون فحص حسابات المدرسين والطلاب، وبإمكان المسؤولين فحص حسابات المديرين والمدرسين والطلاب.

عند طلب فحص بيانات الاعتماد باستخدام Apple School Manager، يتم إصدار حساب خاص يمتلك حق الوصول إلى Apple ID المُدار الذي تم طلب الفحص له فقط. ويمكن للمراقب بعد ذلك قراءة وتعديل محتوى المستخدم المخزّن في iCloud أو في التطبيقات التي تدعم CloudKit. يتم تسجيل كل طلب للوصول إلى التدقيق في Apple School Manager. وتوضح السجلات هوية المراقب وحساب Apple ID المُدار الذي طلب المراقب الوصول إليه ووقت الطلب وما إذا تم إجراء الفحص أم لا.

iCloud

نظرة عامة على أمن iCloud

يُخزّن iCloud جهات الاتصال والتقويمات والصور والمستندات وغيرها من العناصر الخاصة بالمستخدم، ويواصل تحديث المعلومات أولاً بأول عبر جميع أجهزته تلقائيًا. ويمكن أيضًا استخدام iCloud بواسطة تطبيقات الجهات الخارجية لتخزين ومزامنة المستندات والقيم الرئيسية لبيانات التطبيقات كما هو محدد بواسطة المطوّر. يقوم المستخدم بإعداد iCloud من خلال تسجيل الدخول باستخدام Apple ID واختيار الخدمات التي يرغب في استخدامها. يستطيع مسؤولو تقنية المعلومات تعطيل بعض ميزات iCloud مثل iCloud Drive ونسخ iCloud الاحتياطي باستخدام ملفات تعريف تكوين برنامج إدارة الأجهزة المحمولة (MDM).

يستخدم iCloud أساليب أمان قوية ويطبق سياسات صارمة لحماية بيانات المستخدم. يتم تشفير معظم بيانات iCloud على جهاز المستخدم أولاً، باستخدام مفاتيح iCloud التي يُنشئها الجهاز، قبل تحميلها على خوادم iCloud. بالنسبة إلى البيانات غير المشفرة تشفيرًا كاملاً، يُحمّل جهاز المستخدم مفاتيح iCloud هذه بأمان إلى وحدات أمن المكونات المادية الخاصة بـ iCloud في مراكز بيانات Apple. يتيح ذلك لـ Apple مساعدة المستخدم على استعادة البيانات وفك تشفيرها نيابة عن المستخدم متى احتاج إليها (على سبيل المثال، عند تسجيل الدخول على جهاز جديد أو الاستعادة من نسخة احتياطية أو الوصول إلى بيانات iCloud على الويب). يتم تشفير البيانات المنقولة بين أجهزة المستخدم وخوادم iCloud بشكل منفصل أثناء نقلها باستخدام أمن طبقة النقل (TLS) وتُخزن خوادم iCloud بيانات المستخدم بطبقة إضافية من التشفير غير نشطة.

يتم تأمين مفاتيح التشفير، عند توفرها لـ Apple، في مراكز بيانات Apple. عند معالجة البيانات المخزنة في مركز بيانات تابع لجهة خارجية، لا يتم الوصول إلى مفاتيح التشفير هذه إلا من خلال برنامج Apple الذي يعمل على خوادم آمنة وأثناء إجراء المعالجة الضرورية فقط. لمزيد من الخصوصية والأمن، تستخدم العديد من خدمات Apple تشفيرًا كاملاً، ما يعني أنه لا يمكن الوصول إلى بيانات iCloud الخاصة بالمستخدم إلا من قِبل المستخدمين أنفسهم ومن الأجهزة الموثوق بها فقط التي سجلوا الدخول إليها باستخدام Apple ID.

تقدم Apple إلى المستخدمين خيارين لتشفير البيانات المخزنة في iCloud وحمايتها:

- **الحماية القياسية للبيانات (الإعداد الافتراضي):** يتم تشفير بيانات iCloud الخاصة بالمستخدم، ويتم تأمين مفاتيح التشفير في مراكز بيانات Apple، ويمكن لـ Apple المساعدة على استعادة البيانات والحساب. يتم تشفير بيانات iCloud معينة فقط—14 فئة من البيانات، بما في ذلك بيانات الصحة وكلمات السر في سلسلة مفاتيح iCloud—تشفيرًا كاملًا.
- **الحماية المتقدمة للبيانات لـ iCloud:** هي إعداد اختياري يقدم أعلى مستوى من أمن بيانات السحابة من Apple. إذا اختار المستخدم تشغيل الحماية المتقدمة للبيانات، فإن أجهزته الموثوق بها تحتفظ وحدها بالوصول إلى مفاتيح التشفير لأغلبية بيانات iCloud، ومن ثم حمايتها باستخدام التشفير الكامل. عندما يشغِّل المستخدمون الحماية المتقدمة للبيانات، يزداد عدد فئات البيانات التي تستخدم التشفير الكامل إلى 23 فئة ويتضمن نسخ iCloud الاحتياطي والصور والملاحظات والمزيد.

إن الفئات المحددة لبيانات iCloud المحمية بالتشفير الكامل مدرجة في مقال دعم Apple نظرة عامة على أمان بيانات iCloud.

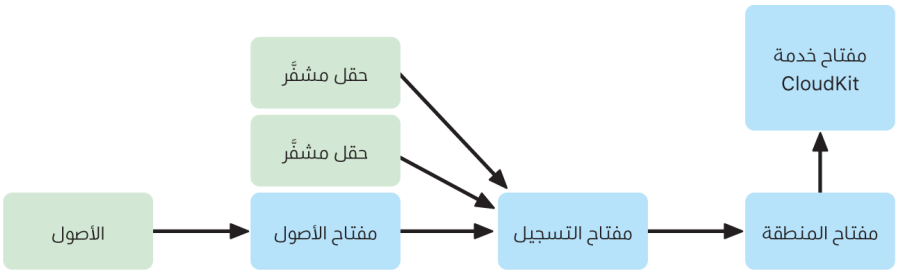
تشفير iCloud

يرتبط تشفير البيانات في iCloud ارتباطًا وثيقًا بنموذج تخزين البيانات، بدءًا من أطر عمل CloudKit وواجهات برمجة التطبيقات (APIs) التي تسمح للتطبيقات وبرامج النظام بتخزين البيانات في iCloud نيابة عن المستخدم وإبقاء كل شيء محدثًا عبر الأجهزة وعلى الويب.

تشفير CloudKit

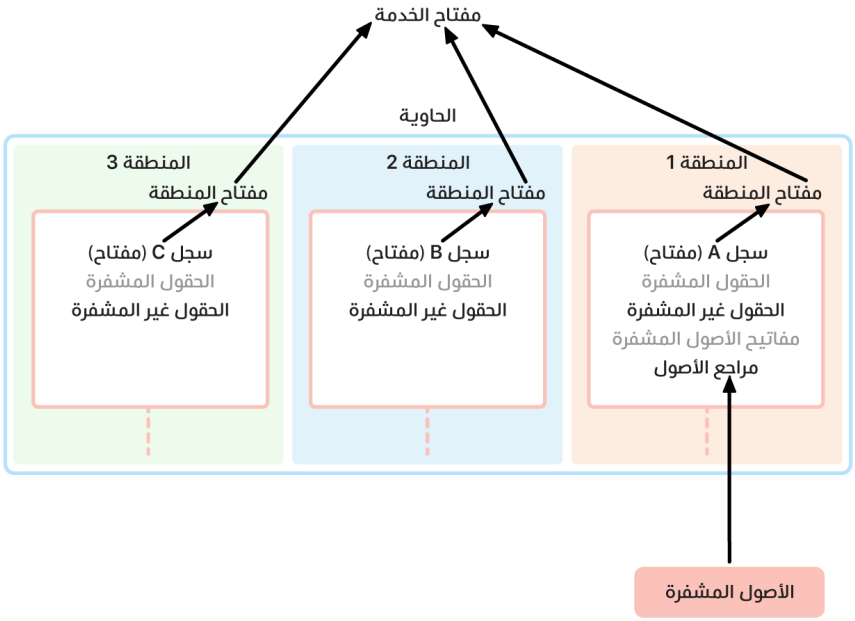
CloudKit هي إطار عمل يتيح لمطوري التطبيقات تخزين بيانات القيمة الأساسية والبيانات المهيكلة والأصول (البيانات الكبيرة المخزنة بشكل منفصل عن قاعدة البيانات، مثل الصور والفيديوهات) في iCloud. تدعم CloudKit كلًا من قواعد البيانات العامة والخاصة، المجمعة في حاويات. قواعد البيانات العامة مشتركة عالميًا، وعادة ما تُستخدم للأصول العامة، ولا يتم تشفيرها. وتُخزن قواعد البيانات الخاصة بيانات iCloud الخاصة بكل مستخدم.

تستخدم CloudKit تسلسلًا هرميًا للمفاتيح يتطابق مع بنية البيانات. وتعد قاعدة البيانات الخاصة بكل حاوية محمية بتسلسل هرمي للمفاتيح، متجذر في مفتاح غير متماثل يُسمى **مفتاح خدمة CloudKit**. هذه المفاتيح فريدة لكل مستخدم iCloud وتُنشأ على أجهزته الموثوق بها. عند كتابة البيانات في CloudKit، تُنشأ جميع مفاتيح السجلات على جهاز المستخدم الموثوق به وتُغلف بالتسلسل الهرمي المناسب للمفاتيح قبل تحميل أي بيانات.



تستخدم العديد من خدمات Apple، المدرجة في مقال دعم Apple نظرة عامة على أمان بيانات iCloud، التشفير الكامل باستخدام مفتاح خدمة CloudKit محمي بالطريقة نفسها التي تتم مزامنة سلسلة مفاتيح iCloud بها. بالنسبة لحاويات CloudKit هذه، لا تتوفر مفاتيح الخدمة إلا على أجهزة المستخدم الموثوقة فقط ولا يمكن لشركة Apple أو أي جهة خارجية الوصول إليها. تتم مزامنة هذه المفاتيح بين أجهزة المستخدم حتى إذا اختار المستخدم عدم استخدام سلسلة مفاتيح iCloud لمزامنة كلمات السر ومفاتيح المرور وبيانات المستخدم الأخرى. في حالة فقدان الجهاز، يمكن للمستخدمين استرداد بيانات سلسلة مفاتيح iCloud باستخدام أمن استرداد سلسلة مفاتيح iCloud أو جهات اتصال استرداد الحساب أو مفتاح استرداد الحساب.

إدارة مفتاح التشفير



يعتمد أمن البيانات المشفرة في CloudKit على أمن مفاتيح التشفير المطابقة. تنقسم مفاتيح خدمة CloudKit إلى فئتين: مشفرة بالكامل ومتوفرة بعد المصادقة.

- **مفاتيح الخدمة المشفرة بالكامل:** بالنسبة إلى خدمات iCloud المشفرة بالكامل، لا يتم توفير المفاتيح الخاصة لخدمة CloudKit ذات الصلة لخوادم Apple أبدًا. تُنشأ أزواج مفاتيح الخدمة، بما في ذلك المفاتيح الخاصة، محليًا على جهاز المستخدم الموثوق به وتُنقل إلى أجهزة المستخدم الأخرى باستخدام أمن سلسلة مفاتيح iCloud. على الرغم من أن عمليات استرداد سلسلة مفاتيح iCloud وتدفقات المزامنة تتم بواسطة خوادم Apple، يتم منع هذه الخوادم بشكل مشفر من الوصول إلى أي من بيانات سلسلة المفاتيح الخاصة بالمستخدم. في أسوأ حالة لفقدان الوصول إلى سلسلة مفاتيح iCloud وجميع آليات الاسترداد الخاصة بها، تُفقد البيانات المشفرة بالكامل في CloudKit. لا تستطيع Apple المساعدة على استرداد هذه البيانات.
- **مفاتيح الخدمة المتوفرة بعد المصادقة:** بالنسبة إلى الخدمات الأخرى، مثل الصور و iCloud Drive، تُخزن مفاتيح الخدمة في وحدات أمن المكونات المادية الخاصة بـ iCloud في مراكز بيانات Apple، ويمكن أن تصل إليها بعض خدمات Apple. عندما يسجّل المستخدم الدخول إلى iCloud على جهاز جديد ويقوم بمصادقة Apple ID، يمكن أن تصل خوادم Apple إلى هذه المفاتيح من دون تدخل أو إدخال إضافي من المستخدم. على سبيل المثال، بعد تسجيل الدخول إلى iCloud.com، يمكن للمستخدم عرض صوره على الإنترنت على الفور. مفاتيح الخدمة هذه هي المفاتيح **المتوفرة بعد المصادقة**.

الحماية المتقدمة للبيانات لـ iCloud

الحماية المتقدمة للبيانات لـ iCloud هي إعداد اختياري يقدم أعلى مستوى من أمن بيانات السحابة من Apple. عندما يشغل المستخدم الحماية المتقدمة للبيانات، فإن أجهزته الموثوق بها تحتفظ وحدها بالوصول إلى مفاتيح التشفير لأغلبية بيانات iCloud، ومن ثم حمايتها باستخدام **التشفير الكامل**. بالنسبة إلى المستخدمين الذين يشغِّلون الحماية المتقدمة للبيانات، يزداد العدد الإجمالي لفئات البيانات المحمية باستخدام التشفير الكامل من 14 إلى 23 فئة ويتضمن نسخ iCloud الاحتياطي والصور والملاحظات والمزيد.

ملاحظة: قد لا تكون هذه الميزة متوفرة في جميع البلدان أو المناطق.

نظريًا، تُعد الحماية المتقدمة للبيانات أمرًا بسيطًا: تُحذَف جميع مفاتيح خدمة CloudKit التي تم إنشاؤها على الجهاز وتم تحميلها لاحقًا إلى وحدات أمن المكونات المادية (HSM) الخاصة بـ iCloud **المتوفرة بعد المصادقة** في مراكز بيانات Apple من وحدات أمن المكونات المادية (HSM) هذه وبدلًا من ذلك يتم الاحتفاظ بها بالكامل ضمن نطاق حماية سلسلة مفاتيح iCloud للحساب. ويتم التعامل معها مثل مفاتيح الخدمة الحالية **المشفرة بالكامل**، ما يعني أنه لم يعد بإمكان Apple قراءة هذه المفاتيح أو الوصول إليها.

تحمي الحماية المتقدمة للبيانات كذلك حقول CloudKit تلقائيًا التي يختار مطورو الجهات الخارجية وضع علامة عليها كمشفرة وجميع أصول CloudKit.

تمكين الحماية المتقدمة للبيانات

عندما يشغل المستخدم الحماية المتقدمة للبيانات، ينفذ الجهاز الموثوق به إجراءين: أولًا، ينقل غرض المستخدم لتشغيل الحماية المتقدمة للبيانات إلى أجهزته الأخرى التي تشارك في التشفير الكامل. ويقوم بذلك عن طريق كتابة قيمة جديدة، تم توقيعها بواسطة المفاتيح المحلية للجهاز، في بيانات تعريف جهاز سلسلة مفاتيح iCloud. لا يمكن لخوادم Apple إزالة هذه المصادقة أو تعديلها بينما تتم مزامنتها مع أجهزة المستخدم الأخرى.

ثانيًا، يبدأ الجهاز في إزالة مفاتيح الخدمة **المتوفرة بعد المصادقة** من مراكز بيانات Apple. نظرًا إلى أن هذه المفاتيح محمية بواسطة وحدات أمن المكونات المادية (HSMs) الخاصة بـ iCloud، فإن هذا الحذف فوري ودائم وغير قابل للإلغاء. بعد حذف المفاتيح، لم يعد بإمكان Apple الوصول إلى **أي** من البيانات المحمية بواسطة مفاتيح خدمة المستخدم. في هذا الوقت، يبدأ الجهاز عملية تدوير المفتاح غير المتزامن التي تُنشئ مفتاح خدمة جديدًا لكل خدمة كان مفتاحها متوفرًا سابقًا لخوادم Apple. إذا فشل تدوير المفتاح، بسبب انقطاع الشبكة أو أي خطأ آخر، فإن الجهاز يعيد محاولة تدوير المفتاح حتى ينجح.

بعد نجاح تدوير مفتاح الخدمة، لا يمكن فك تشفير البيانات الجديدة المكتوبة إلى الخدمة باستخدام مفتاح الخدمة القديم. فهي محمية بالمفتاح الجديد الذي تتحكم فيه أجهزة المستخدم الموثوق بها فقط ولم يكن متوفرًا أبدًا لـ Apple.

الحماية المتقدمة للبيانات والوصول إلى موقع الويب iCloud.com

عندما يشغّل المستخدم الحماية المتقدمة للبيانات لأول مرة، يتم إيقاف الوصول إلى بياناته على موقع الويب iCloud.com تلقائيًا. وذلك لأن خوادم iCloud على الويب لم يعد بإمكانها الوصول إلى المفاتيح المطلوبة لفك تشفير بيانات المستخدم وعرضها. يمكن للمستخدم اختيار تشغيل الوصول إلى الويب مرة أخرى واستخدام مشاركة أجهزته الموثوق بها للوصول إلى بيانات iCloud المشفرة على الويب.

بعد تشغيل الوصول إلى الويب، يجب على المستخدم تخويل تسجيل الدخول إلى الويب على أحد أجهزته الموثوق بها في كل مرة يزور فيها iCloud.com. التخويل "يدعم" الجهاز للوصول إلى الويب. خلال الساعة التالية، يقبل هذا الجهاز الطلبات من خوادم Apple محددة لتحميل مفاتيح الخدمة الفردية، لكن تلك المطابقة لقائمة الخدمات المسموح بها التي يمكن الوصول إليها عادةً على iCloud.com فقط. بعبارة أخرى، حتى بعد تخويل المستخدم تسجيل الدخول إلى الويب، يتعذر على طلب الخادم حث جهاز المستخدم على تحميل مفاتيح الخدمة للبيانات التي لم يكن مقصود عرضها على iCloud.com، (مثل بيانات الصحة أو كلمات السر في سلسلة مفاتيح iCloud) لا تطلب خوادم Apple إلا مفاتيح الخدمة اللازمة لفك تشفير البيانات المحددة التي يطلب المستخدم الوصول إليها على الويب. في كل مرة يتم فيها تحميل مفتاح الخدمة، يتم تشفيره باستخدام مفتاح مؤقت مرتبط بجلسة الويب التي خولها المستخدم ويتم عرض إشعار على جهاز المستخدم، يظهر خدمة iCloud التي يتم توفير بياناتها مؤقتًا لخوادم Apple.

الاحتفاظ باختيارات المستخدم

لا يمكن تعديل إعدادات الحماية المتقدمة للبيانات والوصول إلى موقع الويب iCloud.com إلا من قِبل المستخدم. تُخزَّن هذه القيم في بيانات تعريف جهاز سلسلة مفاتيح iCloud الخاصة بالمستخدم ولا يمكن تغييرها إلا من أحد أجهزة المستخدم الموثوق بها. لا يمكن لخوادم Apple تعديل هذه الإعدادات نيابة عن المستخدم، ولا يمكن إرجاعها إلى التكوين السابق.

العواقب الأمنية للمشاركة والتعاون

في معظم الحالات، عندما يشارك المستخدمون المحتوى للتعاون مع بعضهم—على سبيل المثال، من خلال الملاحظات المشتركة أو التذكيرات المشتركة أو المجلدات المشتركة في iCloud Drive أو مكتبة الصور المشتركة على iCloud—ويتم تشغيل الحماية المتقدمة للبيانات لدى جميع المستخدمين، يتم استخدام خوادم Apple فقط لإنشاء المشاركة لكن ليس لديها حق الوصول إلى مفاتيح التشفير للبيانات المشتركة. يظل المحتوى مشفرًا بالكامل ولا يمكن الوصول إليه إلا على أجهزة المشاركين الموثوق بها. بالنسبة إلى كل عملية مشاركة، قد تُخزن Apple عنوانًا وصورة مصغرة تمثيلية مع الحماية القياسية للبيانات لإظهار معاينة للمستخدمين المستلمين.

تحديد خيار "أي شخص لديه رابط" عند تمكين التعاون سيجعل المحتوى متوفرًا على خوادم Apple بموجب الحماية القياسية للبيانات، حيث يجب أن تكون الخوادم قادرة على توفير الوصول إلى أي شخص يفتح عنوان URL.

لا يدعم تعاون iWork وميزة الألبومات المشتركة في تطبيق الصور الحماية المتقدمة للبيانات. عند تعاون المستخدمين على مستند iWork أو فتح مستند iWork من مجلد مشترك في iCloud Drive، يتم تحميل مفاتيح تشفير المستند بأمان إلى خوادم iWork في مراكز بيانات Apple. هذا لأن التعاون في الوقت الفعلي في iWork يتطلب وساطة من جانب الخادم لتنسيق تغييرات المستند بين المشاركين. ويتم تخزين الصور المضافة إلى الألبومات المشتركة بالحماية القياسية للبيانات، حيث تسمح الميزة بمشاركة الألبومات بشكل عام على الويب.

تعطيل الحماية المتقدمة للبيانات

يمكن للمستخدم إيقاف الحماية المتقدمة للبيانات في أي وقت. إذا قرر فعل ذلك:

1. يسجل جهاز المستخدم أولًا اختياره الجديد في بيانات تعريف مشاركة سلسلة مفاتيح iCloud وتتم مزامنة هذا الإعداد بأمان مع جميع أجهزته.

2. يُحمّل جهاز المستخدم مفاتيح الخدمة بأمان لجميع الخدمات **المتوفرة بعد المصادقة** إلى وحدات أمن المكونات المادية (HSMs) الخاصة بـ iCloud في مراكز بيانات Apple. لا يتضمن هذا أبدًا مفاتيح الخدمات المشفرة بالكامل بموجب الحماية القياسية للبيانات، مثل سلسلة مفاتيح iCloud والصحة.

يُحمّل الجهاز كلًا من مفاتيح الخدمة الأصلية التي تم إنشاؤها قبل تشغيل الحماية المتقدمة للبيانات، ومفاتيح الخدمة الجديدة التي تم إنشاؤها بعد قيام المستخدم بتشغيل الميزة. هذا يجعل جميع البيانات في هذه الخدمات يمكن الوصول إليها بعد المصادقة ويرجع الحساب إلى الحماية القياسية للبيانات، حيث يمكن لـ Apple مرة أخرى مساعدة المستخدم على استرداد معظم بياناته إذا فقد الوصول إلى حسابه.

لا تغطي الحماية المتقدمة للبيانات بيانات iCloud

بسبب الحاجة إلى العمل البيني مع أنظمة البريد الإلكتروني وجهات الاتصال والتقويم العالمية، لا يتم تشفير البريد وجهات الاتصال والتقويم الخاصة بـ iCloud تشفيرًا كاملاً.

يخزن iCloud بعض البيانات من دون حماية مفاتيح خدمة CloudKit الخاصة بالمستخدم، حتى عند تشغيل الحماية المتقدمة للبيانات. يجب إعلان حقول سجلات CloudKit بشكل صريح على أنها "مشفرة" في مخطط الحاوية لحمايتها وتتطلب قراءة الحقول المشفرة وكتابتها استخدام واجهات برمجة التطبيقات (APIs) مخصصة. تُستخدم التواريخ والأوقات التي تم فيها تعديل ملف أو كائن لفرز معلومات المستخدم وتُستخدم المجموعات الاختبارية لبيانات الملفات والصور لمساعدة Apple على إلغاء تكرار تخزين iCloud وتخزين الجهاز الخاص بالمستخدم وتحسينهما—كل ذلك من دون الوصول إلى الملفات والصور نفسها. تتوفر تفاصيل حول كيفية استخدام التشفير لفئات بيانات محددة في مقال دعم Apple نظرة عامة على أمان بيانات iCloud.

كانت القرارات مثل استخدام المجموعات الاختبارية لإلغاء تكرار البيانات—وهي تقنية مشهورة تسمى **التشفير المتقارب**—جزءًا من التصميم الأصلي لخدمات iCloud عند إطلاقها. يتم دائمًا تشفير بيانات التعريف هذه، لكن يتم تخزين مفاتيح التشفير من قِبل Apple بموجب الحماية القياسية للبيانات. لمواصلة تعزيز عمليات الحماية الأمنية لجميع المستخدمين، تلتزم Apple بضمان تشفير المزيد من البيانات، بما في ذلك هذا النوع من بيانات التعريف، تشفيرًا كاملاً عند تشغيل الحماية المتقدمة للبيانات.

متطلبات الحماية المتقدمة للبيانات

تتضمن متطلبات تشغيل الحماية المتقدمة للبيانات لـ iCloud ما يأتي:

- يجب أن يدعم حساب المستخدم التشفير الكامل. يتطلب التشفير الكامل مصادقة ثنائية لـ Apple ID ورمز مرور أو كلمة سر معينة على أجهزة المستخدم الموثوق بها. لمزيد من المعلومات، انظر مقال دعم Apple المصادقة بخطوتين لـ Apple ID.
- يجب تحديث الأجهزة التي سجل المستخدم الدخول إليها باستخدام Apple ID إلى iOS 16.2 و iPadOS 16.2 و macOS 13.1 و tvOS 16.2 و watchOS 9.2 أو أحدث وأحدث إصدار من iCloud لـ Windows. يمنع هذا المطلب إصدارًا سابقًا من iOS أو iPadOS أو macOS أو tvOS أو watchOS من إساءة معالجة مفاتيح الخدمة المنشأة حديثًا عن طريق إعادة تحميلها إلى وحدات أمن المكونات المادية (HSMs) **المتوفرة بعد المصادقة** في محاولة مضللة لإصلاح حالة الحساب.
- يجب على المستخدم إعداد طريقة استرداد بديلة واحدة على الأقل—جهة اتصال واحدة أو أكثر للاسترداد أو مفتاح للاسترداد—يمكن استخدامها لاسترداد بيانات iCloud الخاصة به إذا فقد الوصول إلى حسابه.

إذا فشلت طرق الاسترداد، مثل إذا كانت معلومات جهة اتصال الاسترداد غير محدثة أو نسيها المستخدم، فلن تستطيع Apple المساعدة على استرداد بيانات iCloud المشفرة بالكامل الخاصة بالمستخدم.

يمكن تشغيل الحماية المتقدمة للبيانات لـ iCloud لحسابات Apple ID فقط. حسابات Apple ID المُدارة وحسابات الأطفال (تختلف حسب البلد أو المنطقة) ليست مدعومة.

أمن نسخ iCloud الاحتياطي

ينسخ iCloud المعلومات احتياطيًا — بما في ذلك إعدادات الجهاز وبيانات التطبيقات والصور ومقاطع الفيديو في ألبوم الكاميرا والمحادثات في تطبيق الرسائل — يوميًا عبر Wi-Fi. ولا يحدث نسخ iCloud الاحتياطي إلا عند قفل الجهاز وتوصيله بمصدر طاقة وإمكانية الوصول إلى الإنترنت عبر Wi-Fi. نظرًا إلى تشفير التخزين المستخدم في iOS و iPadOS، تم تصميم نسخ iCloud الاحتياطي للحفاظ على البيانات آمنة مع السماح بحدوث النسخ الاحتياطي والاستعادة تدريجيًا من دون مراقبة. بشكل افتراضي، يتم نسخ مفتاح خدمة نسخ iCloud الاحتياطي احتياطيًا بأمان إلى وحدات أمن المكونات المادية الخاصة بـ iCloud في مراكز بيانات Apple وهو جزء من فئة البيانات المتوفرة بعد المصادقة. بالنسبة إلى المستخدمين الذين يشغّلون الحماية المتقدمة للبيانات لـ iCloud، فإن مفتاح خدمة نسخ iCloud الاحتياطي محمي من خلال التشفير الكامل ومتوفر للمستخدمين على أجهزتهم الموثوق بها فقط.

عند إنشاء ملفات في فئات حماية البيانات التي لا يمكن الوصول إليها عندما يكون الجهاز مقفلاً، يتم تشفير مفاتيح كل ملف، باستخدام مفاتيح الفئات من حافظة مفاتيح نسخ iCloud الاحتياطي ونسخ الملفات احتياطيًا إلى iCloud في حالتها الأصلية المشفرة. يتم تشفير جميع الملفات في أثناء نقلها وعند تخزينها، وتُشفر باستخدام مفاتيح مستندة إلى الحساب، كما هو موضح في تشفير CloudKit.

تحتوي حافظة مفاتيح نسخ iCloud الاحتياطي على مفاتيح (Curve25519) غير متماثلة لفئات حماية البيانات التي لا يمكن الوصول إليها عندما يكون الجهاز مقفلاً. ويتم تخزين مجموعة النسخ الاحتياطي في حساب iCloud الخاص بالمستخدم وتتكون من نسخة من ملفات المستخدم وحافظة مفاتيح نسخ iCloud الاحتياطي. تتم حماية حافظة مفاتيح نسخ iCloud الاحتياطي بمفتاح عشوائي يتم تخزينه كذلك مع مجموعة النسخ الاحتياطي. ولا يتم استخدام كلمة سر iCloud الخاصة بالمستخدم للتشفير، لذلك فلن يؤدي تغيير كلمة سر iCloud إلى إبطال النُسخ الاحتياطية الحالية.

عند الاستعادة، يتم استرداد الملفات المنسوخة احتياطيًا وحافظة مفاتيح نسخ iCloud الاحتياطي ومفتاح حافظة المفاتيح من حساب iCloud الخاص بالمستخدم. ويتم فك تشفير حافظة مفاتيح نسخ iCloud الاحتياطي باستخدام مفتاحها، ثم تُستخدم المفاتيح لكل ملف في حافظة المفاتيح لفك تشفير الملفات الموجودة في مجموعة النسخ الاحتياطي التي تتم كتابتها كملفات جديدة في نظام الملفات، ومن ثم يُعاد تشفيرها وفقًا لفئة حماية البيانات الخاصة بها.

يتم نسخ المحتوى الآتي احتياطيًا باستخدام نسخ iCloud الاحتياطي:

- سجلات الموسيقى والأفلام وبرامج التلفاز والتطبيقات والكتب المشتراة. يتضمن نسخ iCloud الاحتياطي الخاص بالمستخدم معلومات حول المحتوى الذي تم شراؤه الموجود على جهاز المستخدم، ولكن ليس المحتوى الذي تم شراؤه بعينه. عندما يستعيد المستخدم المحتوى من نسخ iCloud الاحتياطي، يتم تنزيل المحتوى الذي تم شراؤه تلقائيًا من iTunes Store أو App Store أو تطبيق Apple TV أو Apple Books. لا يتم تنزيل بعض أنواع المحتوى تلقائيًا في جميع البلدان أو المناطق وقد لا تتوفر عمليات الشراء السابقة إذا تم استرداد مبلغها أو إذا لم تعد متوفرة في المتجر الخاص بها. يرتبط سجل الشراء الكامل بـ Apple ID الخاص بالمستخدم.
- الصور والفيديوهات على أجهزة المستخدم. لاحظ أنه إذا شغّل المستخدم صور iCloud في iOS 8.1 أو iPadOS 13.1 أو OS X 10.10.3 أو أحدث، فهذا يعني أن الصور والفيديوهات مُخزَّنة بالفعل في iCloud، ومن ثم لا يتم تضمينها في نسخ iCloud الاحتياطي الخاص بالمستخدم.
- جهات الاتصال وأحداث التقويم والتذكيرات والملاحظات
- إعدادات الجهاز
- بيانات التطبيقات
- الشاشة الرئيسية وتنظيم التطبيقات
- تكوين HomeKit
- بيانات الهوية الطبية
- كلمة سر مذكرات الصوت (إذا لزم الأمر، تتطلب بطاقة SIM الفعلية التي كانت قيد الاستخدام في أثناء النسخ الاحتياطي)
- الرسائل ومراسلة الشركات من Apple والرسائل النصية (SMS) ورسائل خدمة رسائل الوسائط المتعددة (MMS) (إذا لزم الأمر، تتطلب بطاقة SIM الفعلية التي كانت قيد الاستخدام في أثناء النسخ الاحتياطي)

يتم استخدام نسخ iCloud الاحتياطي كذلك لنسخ سلسلة مفاتيح الجهاز المحلي احتياطيًا، المشفرة بمفتاح مشتق من مفتاح التشفير الجذري للمعرف الفريد (UID) لـ Secure Enclave الخاص بالجهاز. هذا المفتاح خاص بالجهاز وليس معروفًا من قِبل Apple. وهذا يسمح بعدم استعادة قاعدة البيانات إلا إلى الجهاز ذاته الذي نشأت منه، ما يعني أنه لا يمكن لأي شخص آخر، بما في ذلك Apple، قراءتها. لمزيد من المعلومات، انظر Secure Enclave.

تطبيق الرسائل في iCloud

تُبقي الرسائل في iCloud سجل رسائل المستخدم بالكامل محدثًا ومتوفرًا على جميع الأجهزة.

باستخدام الحماية القياسية للبيانات، يتم تشفير الرسائل في iCloud بالكامل عند إيقاف نسخ iCloud الاحتياطي. عند تشغيل نسخ iCloud الاحتياطي، يتضمن النسخ الاحتياطي نسخة من مفتاح تشفير الرسائل في iCloud لتتمكن Apple من مساعدة المستخدم على استعادة رسائله حتى إذا فقد الوصول إلى سلسلة مفاتيح iCloud وأجهزته الموثوق بها. إذا أوقف المستخدم نسخ iCloud الاحتياطي، يُنشأ مفتاح جديد على جهازه لحماية الرسائل المستقبلية في iCloud. يُخزَّن المفتاح الجديد في سلسلة مفاتيح iCloud فقط ولا يمكن الوصول إليه إلا من قِبل المستخدم على أجهزته الموثوق بها فقط ولا يمكن فك تشفير البيانات الجديدة المكتوبة في الحاوية باستخدام مفتاح الحاوية القديم.

باستخدام الحماية المتقدمة للبيانات، يتم تشفير الرسائل في iCloud تشفيرًا كاملاً دائمًا. عند تشغيل نسخ iCloud الاحتياطي، يتم تشفير كل شيء بداخله بالكامل، بما في ذلك مفتاح تشفير الرسائل في iCloud. يتم تدوير كل من مفتاح خدمة نسخ iCloud الاحتياطي، بالإضافة إلى مفتاح حاوية الرسائل في iCloud عندما يشغّل المستخدم الحماية المتقدمة للبيانات. لمزيد من المعلومات، انظر مقال دعم Apple نظرة عامة على أمان بيانات iCloud.

أمن إخفاء العنوان باستخدام iCloud

يساعد إخفاء العنوان باستخدام iCloud على حماية المستخدمين بشكل أساسي أثناء تصفح الويب باستخدام تطبيق سفاري، ولكنه يتضمن أيضًا جميع طلبات تحليل اسم DNS. ويساعد ذلك على ضمان عدم تمكن أي طرف، حتى Apple، من ربط عنوان IP الخاص بالمستخدم بنشاط تصفحه. ويقوم بذلك عن طريق استخدام وكلاء مختلفين، وكيل دخول، تديره شركة Apple ووكيل خروج يديره مزوِّد محتوى. لاستخدام إخفاء العنوان باستخدام iCloud، يتعين على المستخدم تثبيت iOS 15 أو iPadOS 15 أو macOS 12.0.1 أو أحدث، وأن يقوم بتسجيل الدخول إلى حساب iCloud+ باستخدام حساب Apple ID الخاص به، ومن ثم يمكن تشغيل إخفاء العنوان باستخدام iCloud من الإعدادات > iCloud أو إعدادات النظام > iCloud.

لمزيد من المعلومات، انظر نظرة عامة على إخفاء العنوان باستخدام iCloud.

أمن جهة اتصال استرداد الحساب

يمكن للمستخدمين إضافة ما يصل إلى خمسة أشخاص يثقون بهم كجهات اتصال لاسترداد الحساب لمساعدتهم على استرداد حسابهم وبياناتهم على iCloud، بما في ذلك جميع بياناتهم المشفرة بالكامل، سواء قاموا بتشغيل الحماية المتقدمة للبيانات أم لا. لا تمتلك Apple ولا جهة اتصال الاسترداد المعلومات اللازمة بشكل فردي لاسترداد بيانات iCloud المشفرة بالكامل الخاصة بالمستخدم.

تم تصميم جهات اتصال الاسترداد مع مراعاة خصوصية المستخدم. لا تعرف Apple جهات اتصال الاسترداد التي اختارها المستخدم. ولا تعرف خوادم Apple المعلومات حول جهة اتصال الاسترداد إلا متأخرًا في أثناء محاولة الاسترداد بعد أن يطلب المستخدم المساعدة من جهة الاتصال وتبدأ جهة الاتصال بالمساعدة على الاسترداد بالفعل. ولا يتم الاحتفاظ بهذه المعلومات بعد اكتمال الاسترداد.

عملية أمن جهة اتصال الاسترداد

عند إعداد المستخدم لجهة اتصال استرداد الحساب، يتم إنشاء مفتاح مرتبط بجهة الاتصال تلك. يحمي هذا المفتاح الوصول إلى بيانات iCloud الخاصة بالمستخدم — بما في ذلك بيانات CloudKit المشفرة بالكامل. بعد ذلك، يتم إنشاء مفتاح AES 256 بت عشوائي ويُستَخدم لتشفير مفتاح جهة اتصال الاسترداد لإنشاء حزمة جهة اتصال الاسترداد. يتم إرسال الحزمة المشفرة إلى جهة اتصال الاسترداد لحفظها، ويتم تخزين مفتاح AES العشوائي لدى Apple. ولا يوفر مفتاح AES ولا الحزمة أي معلومات عن المفتاح الأساسي بمفردها. وعند الاسترداد، بعد حصول جهاز المستخدم بنجاح على كل من حزمة جهة اتصال الاسترداد من جهة اتصال الاسترداد ومفتاح AES من Apple، يمكنه جمعهما لاسترداد المفتاح الأصلي والوصول إلى بيانات iCloud الخاصة بالمستخدم.

لإعداد جهة اتصال استرداد الحساب، يتصل جهاز المستخدم بخوادم Apple لتحميل جزء معلومات المفاتيح التي ستحتفظ بها Apple (مفتاح AES المذكور أعلاه). ثم ينشئ حاوية CloudKit مشفرة بالكامل مع جهة اتصال الاسترداد لمشاركة الجزء الذي تحتاج إليه جهة اتصال الاسترداد (حزمة جهة اتصال الاسترداد المشفرة باستخدام مفتاح AES). وتتم كذلك مشاركة سر تخويل، تم إنشاؤه بواسطة Apple، مع جهة اتصال الاسترداد. سيتم استخدام ذلك لاسترداد الحساب والمساعدة على إعادة تعيين كلمة السر على الحساب. ويحدث الاتصال لدعوة وقبول جهات اتصال الاسترداد من خلال قناة خدمة هوية (IDS) مُصادَق عليها بشكل متبادل. تخزِّن جهة اتصال الاسترداد المعلومات المستلمة في سلسلة مفاتيح iCloud تلقائيًا. لا يمكن لـ Apple الوصول إلى محتويات حاوية CloudKit ولا سلسلة مفاتيح iCloud التي تخزن هذه المعلومات. عند إجراء المشاركة، لا تعرض خوادم Apple سوى معرف مجهول لجهة اتصال الاسترداد.

لاحقًا، عندما يحتاج المستخدم إلى استرداد حسابه وبيانات iCloud، يمكنه طلب المساعدة من جهة اتصال الاسترداد. في هذا الوقت، يتم إنشاء رمز استرداد بواسطة جهاز جهة اتصال الاسترداد الذي توفره بعد ذلك جهة اتصال الاسترداد إلى المستخدم خارج النطاق (على سبيل المثال، شخصيًا أو عبر مكالمة هاتفية). يقوم المستخدم بعد ذلك بإدخال رمز الاسترداد على جهازه لإنشاء اتصال آمن بين الأجهزة باستخدام بروتوكول SPAKE2+ الذي لا تستطيع Apple الوصول إلى محتوياته. يُنظم هذا التفاعل باستخدام خوادم Apple، لكن لا يمكن لـ Apple بدء عملية الاسترداد.

بعد إنشاء الاتصال الآمن وإكمال جميع عمليات التحقق من الأمان المطلوبة، يقوم جهاز جهة اتصال الاسترداد بإرجاع الجزء الخاص به من معلومات المفاتيح وكلمة سر التخويل التي تم إنشاؤها سابقًا إلى المستخدم الذي يطلب الاسترداد. يقدم المستخدم كلمة سر التخويل هذه إلى خادم Apple الذي يمنح الوصول إلى معلومات المفاتيح التي تحتفظ بها Apple. يؤدي توفير سر التخويل أيضًا إلى تخويل إعادة تعيين كلمة سر الحساب لاستعادة الوصول إلى الحساب.

أخيرًا، يعيد جهاز المستخدم تجميع معلومات المفاتيح الواردة من Apple وجهة اتصال الاسترداد، ثم يستخدمها لفك تشفير بيانات iCloud واستردادها.

توجد إجراءات وقائية لمنع جهة اتصال الاسترداد من بدء الاسترداد من دون موافقة المستخدم التي تشمل التحقق من مدى فعالية حساب المستخدم. إذا كان الحساب قيد الاستخدام النشط، فإن الاسترداد باستخدام جهة اتصال الاسترداد يتطلب أيضًا معرفة أحدث رمز دخول للجهاز أو رمز أمن iCloud.

أمن جهة الاتصال الوارثة

إذا أراد المستخدم أن تكون بياناته في متناول أشخاص مستفيدين معينين بعد وفاته، يمكنه إعداد جهة اتصال وارثة على حسابه. ويتم إنشاء جهة اتصال وارثة بشكل يشبه جهة اتصال الاسترداد إلى حد كبير، باستثناء أن معلومات المفاتيح المستخدمة بواسطة مستفيد ما لا تتضمن المعلومات الضرورية لفك تشفير سلسلة مفاتيح iCloud الخاصة بالمتوفى. وتركيب المفتاح المستخدم هو نفسه التركيب المستخدم لجهة اتصال استرداد الحساب، باستثناء أن في هذه الحالة تخزن Apple الحزمة المشفرة ويحتفظ المستفيد بمفتاح AES. يسمح ذلك بأن يكون الجزء الذي يتلقاه المستفيد أقصر - مما يسهِّل من عملية طباعته عند الضرورة - مع متابعة تقديم الخاصية نفسها حيث لا يقدم أي جزء أي معلومات حول المفتاح الأساسي بمفرده.

يشار إلى معلومات المفاتيح التي يتلقاها المستفيد على أنها مفتاح وصول في الوثائق المقدمة للمستخدم. ويُحفظ مفتاح الوصول تلقائيًا على الأجهزة المدعومة، لكن يمكن كذلك طباعته وتخزينه ماديًا للاستخدام. لمزيد من المعلومات، انظر مقال دعم Apple تعرَّف على كيفية إضافة جهة اتصال وارثة إلى حساب Apple ID.

بعد وفاة المستخدم، تسجل جهات الاتصال الوارثة الدخول إلى موقع مطالبة Apple الإلكتروني لبدء الوصول. يتطلب هذا شهادة وفاة ومصرح به جزئيًا مع سر التفويض المذكور في القسم السابق. بعد اكتمال جميع فحوصات الأمن، تُصدر Apple اسم مستخدم وكلمة سر للحساب الجديد وتُصدر معلومات المفاتيح الضرورية لجهة الاتصال الوارثة.

لإدخال مفتاح الوصول بسهولة أكبر عند الحاجة، يتم تقديمه كرمز أبجدي رقمي مع رمز الاستجابة السريعة (QR) المرتبط به. بعد إدخاله، يتم استعادة الوصول إلى بيانات iCloud الخاصة بالمتوفى. يمكن إجراء ذلك على جهاز أو يمكن إنشاء الوصول عبر الإنترنت. لمزيد من المعلومات، انظر مقال دعم Apple طلب الوصول إلى حساب Apple كجهة اتصال وارثة.

إدارة رموز الدخول وكلمات السر

نظرة عامة على أمن كلمة السر

يسهل iOS و iPadOS و macOS على المستخدمين المصادقة على تطبيقات ومواقع ويب الجهات الخارجية التي تستخدم كلمات السر. وأفضل طريقة لإدارة كلمات السر تتمثل في عدم الحاجة إلى استخدام كلمة سر. يتيح تسجيل الدخول باستخدام Apple للمستخدمين تسجيل الدخول إلى تطبيقات ومواقع ويب الجهات الخارجية دون الحاجة إلى إنشاء حسابات أو كلمات سر إضافية وإدارتها مع حماية عملية تسجيل الدخول باستخدام المصادقة بخطوتين لحساب Apple ID. وبالنسبة للمواقع التي لا تدعم تسجيل الدخول باستخدام Apple، تتيح ميزة كلمة السر القوية التلقائية تمكين أجهزة المستخدم من إنشاء كلمات سر قوية فريدة للمواقع والتطبيقات ومزامنتها وإدخالها تلقائيًا. في iOS و iPadOS، تُحفَظ كلمات السر في سلسلة مفاتيح خاصة لتعبئة كلمة السر تلقائيًا، ويتم التحكم فيها وإدارتها بواسطة المستخدم بالانتقال إلى الإعدادات > كلمات السر.

في macOS، يمكن إدارة كلمات السر المحفوظة في تفضيلات كلمات السر الخاصة بتطبيق سفاري. ويمكن أيضًا استخدام نظام المزامنة هذا لمزامنة كلمات السر المنشأة يدويًا بواسطة المستخدم.

أمن تسجيل الدخول باستخدام Apple

يعد تسجيل الدخول باستخدام Apple بديلاً لأنظمة تسجيل الدخول الموحد الأخرى يحافظ على الخصوصية. ويوفر أريحية وكفاءة تسجيل الدخول بضغطة واحدة مع منح المستخدم مزيدًا من الشفافية والتحكم في معلوماته الشخصية.

يتيح تسجيل الدخول باستخدام Apple للمستخدم إعداد حساب وتسجيل الدخول إلى التطبيقات ومواقع الويب باستخدام Apple ID الذي لديه بالفعل، ويمنحه مزيدًا من التحكم في معلوماته الشخصية. يمكن للتطبيقات أن تطلب فقط اسم المستخدم وعنوان البريد الإلكتروني عند إعداد حساب، ويكون للمستخدم دائمًا حرية الاختيار: يمكنه مشاركة عنوان بريده الإلكتروني الشخصي مع التطبيق، أو اختيار الاحتفاظ بخصوصية بريده الإلكتروني الشخصي واستخدام خدمة ترحيل البريد الإلكتروني الخاصة الجديدة من Apple بدلاً من ذلك. وتقوم خدمة ترحيل البريد الإلكتروني هذه بمشاركة عنوان بريد إلكتروني فريد مجهول الهوية يُعيد التوجيه إلى عنوان المستخدم الشخصي بحيث يظل بإمكانه تلقي الاتصالات المفيدة من المطوّر مع الحفاظ على درجة من الخصوصية والتحكم في معلوماته الشخصية.

تم تصميم تسجيل الدخول باستخدام Apple لأغراض أمنية. يُطلب من كل مستخدم يستخدم تسجيل الدخول باستخدام Apple تمكين المصادقة بخطوتين لحساب Apple ID الخاص به. وتساعد المصادقة بخطوتين في تأمين ليس فقط Apple ID الخاص بالمستخدم، بل أيضًا الحسابات التي ينشئها من خلال تطبيقاته. علاوة على ذلك، طوّرت Apple إشارة لمكافحة الاحتيال مناسبة للخصوصية ودمجتها في ميزة تسجيل الدخول باستخدام Apple. هذه الإشارة تمنح المطورين الثقة بأن المستخدمين الجدد الذين يحصلون عليهم أشخاصٌ حقيقيون وليسوا روبوتات أو حسابات مبرمجة.

كلمات السر القوية التلقائية

عند تمكين سلسلة مفاتيح iCloud، يُنشئ iOS و iPadOS و macOS كلمات سر قوية عشوائية فريدة عند قيام المستخدمين بالتسجيل على موقع إلكتروني على سفاري أو تغيير كلمة السر عليه. في iOS و iPadOS، يتوفر أيضًا إنشاء كلمات السر القوية التلقائية في التطبيقات. ويجب على المستخدمين إيقاف استخدام كلمات السر القوية. تُحفظ كلمات السر المنشأة في سلسلة المفاتيح وتُحدَّث أولًا بأول عبر الأجهزة باستخدام سلسلة مفاتيح iCloud، عند التمكين.

بشكل افتراضي، يبلغ طول كلمة السر المنشأة بواسطة iOS و iPadOS 20 حرفًا. وتحتوي على رقم واحد وحرف كبير واثنتين من الواصلات و16 حرفًا صغيرًا. وتكون كلمات السر المنشأة هذه قوية، حيث إنها تحتوي على 71 وحدة بت من الإنتروبيا.

يتم إنشاء كلمات السر بناءً على الأساليب البحثية التي تحدد ما إذا كانت واجهة حقل كلمة السر مخصصة لإنشاء كلمة السر أم لا. إذا فشلت الأساليب البحثية في التعرف على كلمة السر الخاصة بالسياق التي يتم استخدامها عند إنشاء كلمة سر، يمكن لمطوري التطبيقات تعيين `UITextContentType.newPassword` في حقل النص، ويمكن لمطوري الويب تعيين `autocomplete= "new-password"` في عناصر <input>.

لضمان توافق كلمات السر المنشأة مع الخدمات ذات الصلة، يمكن للتطبيقات ومواقع الويب وضع القواعد. يضع المطورون هذه القواعد باستخدام `UITextInputPasswordRules` أو سمة `passwordrules` في عناصر الإدخال. ومن ثم تنشئ الأجهزة أقوى كلمة سر يمكنها استيفاء هذه القواعد.

أمن التعبئة التلقائية لكلمة السر

تعمل التعبئة التلقائية لكلمة السر على ملء بيانات الاعتماد المخزنة في سلسلة المفاتيح تلقائيًا. يوفر مدير كلمات السر في سلسلة مفاتيح iCloud وميزة التعبئة التلقائية لكلمة السر الميزات التالية:

- تعبئة بيانات الاعتماد في التطبيقات ومواقع الويب
- إنشاء كلمات سر قوية
- حفظ كلمات السر في كل من التطبيقات ومواقع الويب في سفاري
- مشاركة كلمات السر بشكل آمن مع جهات اتصال المستخدم
- توفير كلمات السر لجهاز Apple TV قريب يطلب بيانات اعتماد

لا يتوفر إنشاء كلمات السر وحفظها داخل التطبيقات، بالإضافة إلى توفير كلمات السر لجهاز Apple TV، إلا في iOS و iPadOS.

التعبئة التلقائية لكلمة السر في التطبيقات

يتيح iOS و iPadOS للمستخدمين إدخال أسماء المستخدمين وكلمات السر المحفوظة في الحقول ذات الصلة ببيانات الاعتماد في التطبيقات، على غرار طريقة عمل التعبئة التلقائية لكلمة السر في سفاري. في iOS و iPadOS، يضغط المستخدم على عنصر مفتاح وظيفي في شريط الكتابة السريعة بلوحة المفاتيح البرمجية. وفي macOS، بالنسبة للتطبيقات المنشأة باستخدام Mac Catalyst، تظهر قائمة منسدلة باسم كلمات السر أسفل الحقول المرتبطة ببيانات الاعتماد.

عندما يرتبط أحد التطبيقات ارتباطًا وثيقًا بموقع ويب باستخدام نفس آلية اقتران التطبيق بموقع الويب، مدعومًا بملف Apple-app-site-association نفسه، فإن شريط الكتابة السريعة في iOS و iPadOS والقائمة المنسدلة في macOS تقترح بيانات اعتماد للتطبيق، إذا تم حفظ أي منها في سلسلة مفاتيح التعبئة التلقائية لكلمة السر. يتيح ذلك للمستخدمين اختيار الكشف عن بيانات الاعتماد المحفوظة في سفاري للتطبيقات التي لها نفس الخصائص الأمنية، دون الحاجة إلى اعتماد واجهة API في التطبيقات.

لا تكشف ميزة التعبئة التلقائية لكلمة السر عن أية معلومات متعلقة ببيانات الاعتماد لتطبيق ما حتى يوافق المستخدم على الكشف عن بيانات الاعتماد للتطبيق. يتم سحب قوائم بيانات الاعتماد أو عرضها من خلال عملية التطبيق.

عندما يكون بين التطبيق وموقع الويب علاقة موثوق بها ويُرسل المستخدم بيانات الاعتماد داخل التطبيق، فقد يُطالب iOS و iPadOS المستخدم بحفظ بيانات الاعتماد هذه في سلسلة مفاتيح التعبئة التلقائية لكلمة السر لاستخدامها لاحقًا.

وصول التطبيق إلى كلمات السر المحفوظة

يمكن أن تطلب تطبيقات iOS و iPadOS و macOS مساعدة سلسلة مفاتيح التعبئة التلقائية لكلمة السر لتسجيل دخول مستخدم باستخدام `ASAuthorizationPasswordProvider` و `SecAddSharedWebCredential`. ويمكن استخدام موفر كلمة السر وطلبه بالتزامن مع ميزة تسجيل الدخول باستخدام Apple، بحيث يتم استدعاء واجهة API ذاتها لمساعدة المستخدمين على تسجيل الدخول إلى التطبيق، بغض النظر عما إذا كان حساب المستخدم يستند إلى كلمة السر أو تم إنشاؤه باستخدام ميزة تسجيل الدخول باستخدام Apple.

لا تستطيع التطبيقات الوصول إلى كلمات السر المحفوظة إلا إذا وافق مطور التطبيق ومسؤول موقع الويب بجانب موافقة المستخدم. ويعرب مطورو التطبيقات عن نيتهم في الوصول إلى كلمات السر المحفوظة في سفاري عن طريق تضمين استحقاق في تطبيقاتهم. ويسرد الاستحقاق أسماء النطاقات كاملة الأهلية لمواقع الويب المرتبطة بها، ويجب أن تضع مواقع الويب ملفًا على الخادم الخاص بها يسرد معرّفات التطبيقات الفريدة للتطبيقات المعتمدة من قِبل Apple.

عند تثبيت تطبيق به الاستحقاق com.Apple.developer.associated-domains، يقدم iOS و iPadOS طلب TLS إلى كل موقع ويب مدرج، لطلب ملف من الملفات التالية:

- Apple-app-site-association
- well-known/Apple-app-site-association.

إذا كان الملف يسرد معرف التطبيق الخاص بالتطبيق الجاري تثبيته، فإن iOS و iPadOS يميّزان موقع الويب والتطبيق على أن بينهما علاقة موثوقًا بها. فقط عند استدعاء علاقة موثوق بها لواجهتي API هاتين تنتج مطالبة إلى المستخدم، الذي يجب أن يوافق قبل إصدار أي كلمات سر إلى التطبيق أو تحديثها أو حذفها.

توصيات أمن كلمة السر

تشير قائمة كلمات السر الخاصة بالتعبئة التلقائية لكلمة السر على iOS و iPadOS و macOS إلى كلمات سر المستخدم المحفوظة التي **سيُعاد استخدامها** مع المواقع الإلكترونية الأخرى وكلمات السر التي تعد **ضعيفة**، وكذلك كلمات السر التي تم اختراقها بسبب **تسريب البيانات**.

نظرة عامة

قد يؤدي استخدام كلمة السر نفسها لأكثر من خدمة واحدة إلى جعل هذه الحسابات عرضة لهجوم تكديس بيانات الاعتماد. إذا تم اختراق إحدى الخدمات وتسربت كلمات السر، فقد يجرّب المهاجمون بيانات الاعتماد ذاتها على خدمات أخرى لاختراق حسابات إضافية.

- يتم تمييز كلمات السر بوصفها كلمات سر **مُعاد استخدامها** إذا تم اكتشاف استخدام كلمة السر ذاتها لأكثر من كلمة سر محفوظة عبر نطاقات مختلفة.
- يتم تمييز كلمات السر بأنها **ضعيفة** إذا زادت احتمالية تخمينها بسهولة من قِبل المهاجمين. ويكتشف iOS و iPadOS و macOS الأنماط الشائعة المستخدمة لإنشاء كلمات سر يسهل تذكرها، مثل استخدام الكلمات الموجودة في القواميس، أو بدائل الأحرف الشائعة (مثل استخدام "p4ssw0rd" بدلاً من "password")، أو الأنماط الموجودة بلوحة مفاتيح (مثل "q12we34r"من لوحة مفاتيح QWERTY)، أو التسلسلات المتكررة (مثل"123123"). غالبًا ما تُستخدم هذه الأنماط لإنشاء كلمات سر تستوفي الحد الأدنى لمتطلبات كلمة السر بالنسبة للخدمات، ولكنها تُستخدم أيضًا بشكل شائع من قِبل المهاجمين الذين يحاولون الحصول على كلمة السر باستخدام القوة الغاشمة.

  نظرًا لأن العديد من الخدمات تتطلب تحديدًا رمز PIN المكون من أربعة أو ستة أرقام، يتم تقييم رموز الدخول القصيرة هذه باستخدام قواعد مختلفة. ويُعتبر رمز PIN ضعيفًا إذا كان من رموز PIN الأكثر شيوعًا، أو إذا كان تسلسلاً متزايدًا أو متناقصًا مثل "1234" أو "8765"، أو إذا اتبع نمط تكرار مثل "123123" أو "123321".
- يتم تمييز كلمات السر على أنها **مُسرّبة** إذا تمكنت ميزة مراقبة كلمات السر من التثبُّت من أنها كانت موجودة في تسريب البيانات. لمزيد من المعلومات، انظر مراقبة كلمات السر.

تتم الإشارة إلى كلمات السر الضعيفة والمُعاد استخدامها والمُسرّبة إما في قائمة كلمات السر (macOS) أو تكون موجودة في واجهة توصيات الأمن المخصصة (iOS و iPadOS). وإذا سجّل المستخدم الدخول إلى موقع ويب في سفاري باستخدام كلمة سر محفوظة سابقًا تتسم بالضعف الشديد أو تم اختراقها بواسطة تسريب بيانات، يظهر له تنبيه يحثّه بشدة على الترقية إلى كلمة سر قوية تلقائية.

ترقية أمن مصادقة الحساب على iOS و iPadOS

يمكن للتطبيقات التي تُطبّق ملحقات تعديل مصادقة الحساب (في إطار عمل خدمات المصادقة) توفير ترقيات سهلة بضغطة زر للحسابات المستندة إلى كلمة السر—أي أنه يمكن تحويلها إلى استخدام تسجيل الدخول باستخدام Apple أو استخدام كلمة سر قوية تلقائية. وتتوفر نقطة الملحق هذه في iOS و iPadOS.

إذا قام أحد التطبيقات بتطبيق نقطة الملحق وتم تثبيته على الجهاز، فسيرى المستخدمون خيارات ترقية الملحق عند عرض توصيات الأمن لبيانات الاعتماد المقترنة بالتطبيق في إدارة كلمات السر في سلسلة مفاتيح iCloud في الإعدادات. يتم أيضًا عرض الترقيات على المستخدم عندما يسجّل الدخول إلى التطبيق باستخدام بيانات الاعتماد المعرضة للخطر. تتمتع التطبيقات بإمكانية إبلاغ النظام بعدم عرض خيارات الترقية على المستخدمين بعد تسجيل الدخول. باستخدام واجهة برمجة تطبيقات AuthenticationServices الجديدة، يمكن للتطبيقات أيضًا استدعاء الملحقات الخاصة بها وتنفيذ الترقيات بنفسها، وعادةً ما يتم ذلك من خلال إعدادات الحساب أو شاشة إدارة الحساب في التطبيق.

يمكن للتطبيقات اختيار دعم ترقيات كلمات السر القوية، أو ترقيات تسجيل الدخول باستخدام Apple، أو كليهما. في ترقية كلمة السر القوية، يقوم النظام بإنشاء كلمة سر قوية تلقائية للمستخدم. وعند الضرورة، يمكن للتطبيق توفير قواعد مخصصة لكلمة السر لاتباعها عند إنشاء كلمة السر الجديدة. عندما يُحوّل المستخدم حسابًا من استخدام كلمة السر إلى استخدام "تسجيل الدخول باستخدام Apple"، يوفر النظام بيانات اعتماد جديدة لميزة "تسجيل الدخول باستخدام Apple" إلى الملحق لربط الحساب به. ولا يتم توفير البريد الإلكتروني لحساب Apple ID الخاص بالمستخدم كجزء من بيانات الاعتماد. بعد نجاح ترقية "تسجيل الدخول باستخدام Apple"، يحذف النظام بيانات اعتماد كلمة السر المستخدمة سابقًا من سلسلة المفاتيح الخاصة بالمستخدم، إذا كانت محفوظة هناك.

تتوفر لملحقات تعديل مصادقة الحساب فرصة إجراء مصادقة إضافية للمستخدم قبل تنفيذ الترقية. وبالنسبة إلى الترقيات التي تبدأ ضمن إدارة كلمات السر أو بعد تسجيل الدخول إلى تطبيق ما، يوفر الملحق اسم المستخدم وكلمة السر للحساب المطلوب ترقيته. أما بالنسبة إلى الترقيات داخل التطبيق، يتم توفير اسم المستخدم فقط. إذا كان الملحق يتطلب مصادقة إضافية من المستخدم، يمكنه طلب إظهار واجهة مستخدم مخصصة قبل الاستمرار في الترقية. إن حالة الاستخدام المقصودة لإظهار واجهة المستخدم هذه هي أن يقوم المستخدم بإدخال عامل ثانٍ من المصادقة لتخويل الترقية.

مراقبة كلمات السر

تعد مراقبة كلمات السر ميزة تُطابق كلمات السر المُخزّنة في سلسلة مفاتيح التعبئة التلقائية لكلمة السر الخاصة بالمستخدم مع قائمة مُنسّقة ومُحدثّة باستمرار تضم كلمات السر المعروف أنها قد تعرضت للتسريب من مؤسسات مختلفة عبر الإنترنت. إذا كانت تلك الميزة قيد التشغيل، فإن البروتوكول الأساسي يراقب باستمرار كلمات سر سلسلة مفاتيح التعبئة التلقائية لكلمة السر الخاصة بالمستخدم مع القائمة المُنسّقة.

طريقة عمل المراقبة

يُجري جهاز المستخدم باستمرار عمليات تحقق ذات ترتيب دوري من كل كلمات سر المستخدم، مع الاستعلام على أساس فاصل زمني عن استقلالية كلمات سر المستخدم أو أنماط استخدام مدير كلمات السر. وهذا يساعد على ضمان بقاء حالات التحقُّق مُحدّثة وفقًا للقائمة الحالية المُنسّقة التي تضم كلمات السر المُتسرّبة. للمساعدة على منع تسرّب المعلومات المتعلقة بعدد كلمات السر الفريدة التي لدى المستخدم، يتم تجميع الطلبات وتنفيذها بالتوازي. كما يتم التحقق من عدد محدد من كلمات السر بالتوازي مع كل عملية تحقُّق، وإذا كان لدى المستخدم عدد أقل من هذا الرقم، يتم إنشاء كلمات سر عشوائية وإضافتها إلى الاستعلامات بهدف تعويض النقص.

كيفية مطابقة كلمات السر

تتم مطابقة كلمات السر في عملية من شقّين. يتم تضمين كلمات السر المتسربة الأكثر شيوعًا في قائمة محلية على جهاز المستخدم. وإذا ظهرت كلمة سر المستخدم في هذه القائمة، يتم إعلام المستخدم على الفور من دون أي تفاعل خارجي. وقد تم التصميم بتلك الطريقة لضمان عدم تسرب أي معلومات حول كلمات السر التي لدى المستخدم وتكون عرضة للخطر بشكل كبير بسبب خرق كلمة السر.

إذا لم تكن كلمة السر موجودة في قائمة الأكثر شيوعًا، تتم مطابقتها مع كلمات السر المتسربة الأقل شيوعًا.

مقارنة كلمات سر المستخدمين بقائمة مُنسّقة

للتحقق من عدم وجود كلمة السر في القائمة المحلية، تتم عملية مطابقة تتضمن بعض التفاعل مع خوادم Apple. للمساعدة في ضمان عدم إرسال كلمات سر المستخدمين السليمة إلى Apple، تم إرسال نموذج من نماذج تقاطع **مجموعة تشفير خاصة** تقارن كلمات سر المستخدمين بمجموعة كبيرة من كلمات السر المسربة. وقد تم التصميم بتلك الطريقة لضمان عدم مشاركة معلومات قليلة مع Apple حول كلمات السر الأقل عرضة لخطر الاختراق. وبالنسبة إلى كلمة سر المستخدم، تقتصر هذه المعلومات على بادئة مكونة من 15 بت من تجزئة التشفير. علمًا بأن إزالة كلمات السر التي يتم تسريبها بشكل متكرر من هذه العملية التفاعلية، باستخدام القائمة المحلية لكلمات السر التي يتم تسريبها بشكل شائع، تقلل معدل التكرار النسبي لكلمات السر في مجموعات خدمة الويب، مما يجعل من غير العملي استنتاج كلمات سر المستخدم من عمليات البحث هذه.

يقسّم البروتوكول الأساسي قائمة كلمات السر المُنسّقة، والتي تحتوي على ما يقرب من 1.5 مليار كلمة سر في وقت كتابة هذا التقرير، إلى 2^{15} مجموعة مختلفة. تستند المجموعة التي تنتمي إليها كلمة السر إلى أول 15 وحدة بت من قيمة تجزئة SHA256 الخاصة بكلمة السر. بالإضافة إلى ذلك، ترتبط كل كلمة سر مسربة، أو pw، بنقطة منحنى بيضاوي على منحنى NIST P256: $P_{pw} = \alpha \cdot H_{SWU}(pw)$، حيث α عبارة عن مفتاح عشوائي سري لا تعرفه سوى Apple، بينما H_{SWU} عبارة عن دالة عشوائية من Oracle تربط كلمات السر بنقاط المنحنى باستخدام طريقة Shallue-van de Woestijne-Ulas. تم تصميم هذا التحويل لإخفاء قيم كلمات السر حسابيًا والمساعدة على منع الكشف عن كلمات السر المُسرّبة حديثًا من خلال مراقبة كلمات السر.

لحساب تقاطع المجموعة الخاصة، يحدد جهاز المستخدم الحاوية التي تنتمي إليها كلمة سر المستخدم باستخدام λ، بادئة من 15 بت لـ SHA256(upw)، حيث تعد upw إحدى كلمات سر المستخدم. يعمل الجهاز على إنشاء ثابت عشوائي خاص به، β، ويرسل النقطة $\beta \cdot H_{SWU}(upw) = P_c$ إلى الخادم، إلى جانب طلب للحاوية المقابلة لـ λ. وهنا يقوم β بإخفاء المعلومات المتعلقة بكلمة سر المستخدم ويقصر على λ المعلومات المكشوفة من كلمة السر إلى Apple. وأخيرًا، يأخذ الخادم النقطة التي يرسلها جهاز المستخدم، ويحسب، $\alpha\beta \cdot H_{SWU}(upw) = \alpha P_c$، ويعرض الناتج، إلى جانب مجموعة من النقاط المناسبة $B\lambda = \{P_{pw} \mid SHA256(pw)$ تبدأ بالبادئة λ} للجهاز.

تسمح المعلومات التي تم إرجاعها للجهاز بحساب $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$، وتتأكد من تسرب كلمة سر المستخدم إذا كان $\alpha P_c \in B'_\lambda$.

إرسال كلمات السر إلى مستخدمين آخرين أو أجهزة Apple أخرى

ترسل Apple كلمات السر بشكل آمن إلى المستخدمين الآخرين أو أجهزة Apple باستخدام الإرسال السريع وعبر Apple TV.

حفظ بيانات الاعتماد على جهاز آخر باستخدام الإرسال السريع

عند تمكين iCloud، يمكن للمستخدمين استخدام الإرسال السريع لإرسال بيانات اعتماد محفوظة إلى جهاز آخر. وتتضمن بيانات الاعتماد اسم المستخدم وكلمة السر والمواقع الإلكترونية المحفوظة من أجلها. ويعمل إرسال بيانات الاعتماد باستخدام الإرسال السريع دائمًا في نمط جهات الاتصال فقط، بغض النظر عن إعدادات المستخدم. على جهاز الاستقبال، بعد موافقة المستخدم، يتم تخزين بيانات الاعتماد في سلسلة مفاتيح التعبئة التلقائية لكلمة السر الخاصة بالمستخدم.

تعبئة بيانات الاعتماد في التطبيقات على Apple TV

تتوفر ميزة التعبئة التلقائية لكلمة السر لتعبئة بيانات الاعتماد في التطبيقات على Apple TV. عندما يركز المستخدم على حقل النص الخاص باسم المستخدم أو كلمة السر في tvOS، يبدأ Apple TV في الإعلان عن طلب التعبئة التلقائية لكلمة السر عبر Bluetooth منخفض الطاقة (BLE).

يعرض أي iPhone أو iPad قريب مطالبةً تدعو المستخدم لمشاركة بيانات الاعتماد مع Apple TV. وفيما يلي كيفية إنشاء طريقة التشفير:

- إذا كان الجهاز و Apple TV يستخدمان نفس حساب iCloud، يحدث التشفير بين الجهازين تلقائيًا.
- إذا تم تسجيل دخول الجهاز إلى حساب iCloud غير الحساب الذي يستخدمه Apple TV، يُطلب من المستخدم إنشاء اتصال مشفر من خلال استخدام رمز PIN. لتلقي هذه المطالبة، يجب أن يكون الـ iPhone غير مقفل وعلى مقربة من Siri Remote المقترن بجهاز Apple TV هذا.

بعد إجراء الاتصال المشفر باستخدام تشفير رابط BLE، يتم إرسال بيانات الاعتماد إلى Apple TV وتعبئتها تلقائيًا في حقول النص ذات الصلة في التطبيق.

ملحقات موفر بيانات الاعتماد

في iOS و iPadOS و macOS، يمكن للمستخدمين تعيين تطبيق مشارك تابع لجهة خارجية كموفر بيانات اعتماد لميزة التعبئة التلقائية لكلمة السر في إعدادات كلمات السر (iOS و iPadOS) أو في إعدادات الملحقات في إعدادات النظام (macOS 13 أو أحدث) أو تفضيلات النظام (macOS 12 أو أقدم). وهذه الآلية مبنية على ملحقات التطبيق. و**يجب أن يوفر** ملحق موفر بيانات الاعتماد عرضًا لاختيار بيانات الاعتماد. **يمكن أن يوفر الملحق اختياريًا** بيانات تعريف حول بيانات الاعتماد المحفوظة حتى يمكن تقديمها مباشرة على شريط الكتابة السريعة (على iOS و iPadOS) أو في اقتراح الإكمال التلقائي (على macOS). وتتضمن بيانات التعريف موقع الويب الخاص ببيانات الاعتماد واسم المستخدم المرتبط، ولكن ليست كلمة السر الخاصة به. ومن ثم يتواصل iOS و iPadOS و macOS مع الملحق للحصول على كلمة السر عندما يختار المستخدم تعبئة بيانات اعتماد في تطبيق أو موقع ويب في سفاري. يتم تخزين بيانات التعريف الخاصة ببيانات الاعتماد داخل حاوية التطبيقات لدى موفر بيانات الاعتماد، وتتم إزالتها تلقائيًا عند إلغاء تثبيت التطبيق.

سلسلة مفاتيح iCloud

نظرة عامة على أمن سلسلة مفاتيح iCloud

تسمح سلسلة مفاتيح iCloud للمستخدمين بمزامنة كلمات السر ومفاتيح المرور بشكل آمن بين أجهزة iPhone و iPad وأجهزة كمبيوتر Mac دون كشفها لشركة Apple. بالإضافة إلى المستوى العالي من الخصوصية والأمن، تمثَّلت الأهداف الأخرى لتصميم وبنية سلسلة مفاتيح iCloud في سهولة الاستخدام والقدرة على استرداد محتويات سلسلة المفاتيح حتى في حالة عدم القدرة على الوصول إلى جميع أجهزة المستخدم. وتتكون سلسلة مفاتيح iCloud من خدمتين: مزامنة سلسلة المفاتيح واسترداد سلسلة المفاتيح.

صُممت سلسلة مفاتيح iCloud واسترداد سلسلة المفاتيح بحيث تظل كلمات سر ومفاتيح المرور الخاصة بالمستخدم محمية في الحالات التالية:

- اختراق حساب المستخدم على iCloud.
- اختراق iCloud بواسطة مهاجم خارجي أو موظف.
- وصول جهة خارجية إلى حسابات المستخدم.

تكامل مدير كلمات السر مع سلسلة مفاتيح iCloud

يستطيع iOS و iPadOS و macOS إنشاء سلاسل عشوائية قوية مشفرة تلقائيًا لاستخدامها ككلمات سر للحساب في سفاري. ويستطيع iOS و iPadOS أيضًا إنشاء كلمات سر قوية للتطبيقات. ويتم تخزين كلمات السر المُنشأة في سلسلة المفاتيح ومزامنتها مع الأجهزة الأخرى. ويتم نقل عناصر سلسلة المفاتيح من جهاز لآخر عبر خوادم Apple، ولكن يتم تشفيرها بشكل شامل حتى لا يُمكن لـ Apple والأجهزة الأخرى قراءة محتوياتها.

مزامنة سلسلة المفاتيح بشكل آمن

عندما يشغل مستخدم سلسلة مفاتيح iCloud لأول مرة على حساب مُفعَّل به المصادقة بخطوتين، ينشئ الجهاز هوية مزامنة لنفسه. تتكون هوية المزامنة من مفاتيح بيضاوية غير متناظرة (باستخدام P-384)، ويتم تخزينها في سلسلة مفاتيح الجهاز. يحتفظ كل جهاز بقائمة هويات مزامنة لأجهزة المستخدم الأخرى ويوقع هذه القائمة باستخدام مفتاح من مفاتيح الهوية الخاصة به. وهذه القوائم مخزنة في CloudKit، ما يسمح لأجهزة المستخدم الاتفاق على كيفية مزامنة بيانات سلسلة المفاتيح فيما بينها بشكل آمن.

للتوافق مع أجهزة iCloud الأقدم، يتم إنشاء دائرة ثقة مزامنة مشابهة ويتم تكوين هوية مزامنة أخرى. يُوضع المفتاح العام لهوية المزامنة في الدائرة، ويتم التوقيع على الدائرة مرتين: أولاً بواسطة المفتاح الخاص لهوية المزامنة، ثم مرة أخرى باستخدام مفتاح بيضاوي غير متناظر (باستخدام P-256) مشتق من كلمة سر حساب iCloud الخاص بالمستخدم. وتُخزَّن كذلك في الدائرة المعامِلات (القيمة العشوائية المضافة والتكرارات) المستخدمة لإنشاء المفتاح الذي يستند إلى كلمة سر iCloud الخاصة بالمستخدم.

تخزين iCloud لدائرة المزامنة

بالنسبة إلى حسابات المصادقة بخطوتين، تُخزَّن قائمة الأجهزة الموثوقة لكل جهاز في CloudKit. ولا يمكن قراءة القوائم دون معرفة كلمة سر iCloud الخاصة بالمستخدم، كما لا يمكن تعديلها دون امتلاك المفاتيح الخاصة للجهاز المالك.

وعلى نحو مماثل، يتم تخزين دائرة المزامنة الموقَّعة في منطقة تخزين مفاتيح-قيم iCloud الخاصة بالمستخدم، ولا يمكن قراءتها من دون معرفة كلمة سر iCloud الخاصة بالمستخدم، ولا يمكن تعديلها بشكل صالح من دون امتلاك المفتاح الخاص لهوية المزامنة الخاصة بعضوها.

كيفية إضافة أجهزة المستخدم الأخرى إلى دائرة المزامنة

تنضم الأجهزة الجديدة، عند تسجيل الدخول إلى iCloud، إلى دائرة مزامنة سلسلة مفاتيح iCloud بإحدى طريقتين: إمّا عن طريق الاقتران بجهاز حالي به سلسلة مفاتيح iCloud وتكون مدعومة من قِبله وإمّا باستخدام استرداد سلسلة مفاتيح iCloud.

أثناء تدفقات الاقتران، ينشئ الجهاز مقدم الطلب هويات مزامنة جديدة لكل من دائرة المزامنة وقوائم المزامنة (لحسابات المصادقة بخطوتين) ويقدمها إلى الجهاز الراعي. يضيف الجهاز الراعي المفتاح العام للعضو الجديد إلى دائرة المزامنة ويوقع عليه مرة أخرى باستخدام كل من هوية المزامنة الخاصة به والمفتاح المشتق من كلمة سر iCloud الخاصة بالمستخدم. وتُوضع دائرة المزامنة الجديدة في iCloud، حيث يتم توقيعها بالمثل بواسطة العضو الجديد في الدائرة. في حسابات المصادقة بخطوتين، يزود الجهاز الراعي كذلك الجهاز المنضم **بقسيمة** موقعة باستخدام مفاتيح الهوية الخاصة به، ما يوضح أنه يجب الوثوق في الجهاز مقدم الطلب. ومن ثم يحدث قائمته الفردية لهويات المزامنة الموثوقة لتشمل مقدم الطلب.

يوجد الآن عضوان في دائرة التوقيع، ولدى كل عضو المفتاح العام الخاص بنظيره. يبدآن الآن في تبادل عناصر سلسلة المفاتيح الفردية عبر CloudKit أو منطقة تخزين مفاتيح-قيم iCloud، أيهما أكثر ملاءمةً للموقف. إذا كان لدى عضوي الدائرة تحديثات على العنصر نفسه، يتم اختيار أحدهما أو الآخر، ما ينتج عنه توافق في النهاية. يتم تشفير كل عنصر تمت مزامنته بحيث لا يمكن فك تشفيره إلا عن طريق جهاز داخل دائرة ثقة المستخدم؛ لا يمكن فك تشفيره بواسطة أي أجهزة أخرى أو بواسطة Apple.

عند انضمام أجهزة جديدة إلى دائرة المزامنة، يتم تكرار "عملية الانضمام" هذه. على سبيل المثال، عند انضمام جهاز ثالث، يمكن إقرانه بأي من الجهازين الموجودين. عند إضافة نظراء جدد، يتزامن كل نظير مع النظير الجديد. وقد تم التصميم بتلك الطريقة لضمان حصول جميع الأعضاء على عناصر سلسلة المفاتيح ذاتها.

تتم مزامنة عناصر معينة فقط

بعض عناصر سلسلة المفاتيح تعد خاصة بالجهاز، مثل مفاتيح iMessage، ولهذا يلزم بقاؤها على الجهاز. لتجنب نقل البيانات غير المتوقع، يجب تمييز كل عنصر ستتم مزامنته بوضوح بالسمة `kSecAttrSynchronizable`.

عيّنت Apple هذه السمة لبيانات مستخدم سفاري (بما في ذلك أسماء المستخدمين وكلمات السر وأرقام بطاقات الائتمان)، وكذلك كلمات سر Wi-Fi ومفاتيح تشفير HomeKit وعناصر سلسلة المفاتيح الأخرى التي تدعم تشفير iCloud الكامل.

بالإضافة إلى ذلك، لا تتم مزامنة عناصر سلسلة المفاتيح المضافة بواسطة تطبيقات الجهات الخارجية، بشكل افتراضي. ويجب على المطورين تعيين السمة `kSecAttrSynchronizable` عند إضافة عناصر إلى سلسلة المفاتيح.

أمن استرداد سلسلة مفاتيح iCloud

تعمل سلسلة مفاتيح iCloud على إيداع بيانات سلسلة المفاتيح الخاصة بالمستخدمين مع Apple دون السماح لشركة Apple بقراءة كلمات السر والبيانات الأخرى التي تحتوي عليها. حتى إذا كان لدى المستخدم جهاز واحد فقط، يوفر استرداد سلسلة المفاتيح شبكة أمان ضد فقدان البيانات. يكون لذلك أهمية خاصة عند استخدام سفاري لإنشاء كلمات سر أو مفاتيح مرور عشوائية وقوية لحسابات الويب، لأن التسجيل الوحيد لكلمات السر هذه يكون في سلسلة المفاتيح.

من الركائز الأساسية في استرداد سلسلة المفاتيح المصادقة الثانوية وخدمة الضمان الآمن المنشأة من قِبل Apple خصوصًا لدعم هذه الميزة. يتم تشفير سلسلة مفاتيح المستخدم باستخدام رمز دخول قوي، ولا توفر خدمة الضمان نسخة من سلسلة المفاتيح إلا في حالة استيفاء مجموعة صارمة من الشروط.

استخدام المصادقة الثانوية

توجد عدة طرق لإنشاء رمز دخول قوي:

- إذا تم تمكين المصادقة بخطوتين لحساب المستخدم، يتم استخدام رمز دخول الجهاز لاسترداد سلسلة المفاتيح المودعة في الضمان.
- وإذا لم يتم إعداد المصادقة بخطوتين، يُطلب من المستخدم إنشاء رمز أمن iCloud من خلال توفير رمز دخول مكون من ستة أرقام. بدلاً من ذلك، دون المصادقة بخطوتين، يمكن للمستخدم تحديد رمز أطول يكون خاصًا به أو يمكنه السماح لجهازه بإنشاء رمز عشوائي مشفر يمكنه تسجيله والاحتفاظ به.

عملية إيداع سلسلة المفاتيح

بعد إنشاء رمز الدخول، يتم إيداع سلسلة المفاتيح لدى Apple. في البداية، يُصدّر جهاز iOS أو iPadOS أو macOS نسخة من سلسلة مفاتيح المستخدم، ثم يشفّرها مُغلفةً بالمفاتيح في حافظة مفاتيح غير متماثلة، ويضعها في منطقة تخزين قيمة مفتاح iCloud الخاصة بالمستخدم. ويتم تغليف حافظة المفاتيح برمز أمن iCloud الخاص بالمستخدم وبالمفتاح العام لمجموعة وحدات أمن المكونات المادية (HSM) التي تُخزّن سجل الضمان. ويصبح هذا **سجل ضمان iCloud** الخاص بالمستخدم. بالنسبة إلى حسابات المصادقة بخطوتين، يتم تخزين سلسلة المفاتيح كذلك في CloudKit وتغليفها بمفاتيح وسيطة يمكن استردادها فقط باستخدام محتويات سجل ضمان iCloud، ومن ثم يتم توفير مستوى الحماية ذاته.

تسمح محتويات سجل الضمان كذلك لجهاز الاسترداد بالانضمام مرة أخرى إلى سلسلة مفاتيح iCloud، ما يثبت لأي أجهزة موجودة أن جهاز الاسترداد قد نجح في تنفيذ عملية الضمان، ومن ثم تم التصريح به من قِبل مالك الحساب.

ملاحظة: بالإضافة إلى إنشاء رمز أمن، يجب على المستخدمين تسجيل رقم هاتف لحساب iCloud الخاص بهم. وهذا يوفر مستوى ثانويًا من المصادقة أثناء استرداد سلسلة المفاتيح. يتلقى المستخدم رسالة SMS يجب الرد عليها حتى تتم متابعة عملية الاسترداد.

أمن الضمان في سلسلة مفاتيح iCloud

يوفر iCloud بنية تحتية آمنة لتأمين سلسلة المفاتيح للمساعدة في ضمان عدم تمكّن سوى المستخدمين المعتمدين والأجهزة المعتمدة من إجراء الاسترداد. بشكل طوبوغرافي، تقع خلف iCloud مجموعات وحدات أمن المكونات المادية (HSMs) التي تحمي سجلات الضمان. كما هو موضح سابقًا في هذا المستند، تحتوي كل مجموعة على مفتاح يُستخدم لتشفير سجلات الضمان التي تحت مراقبتها.

لاسترداد سلسلة المفاتيح، يجب على المستخدم المصادقة باستخدام حساب iCloud وكلمة السر والرد على رسالة SMS المرسلة إلى رقم هاتفه المسجل. وبعد القيام بذلك، يجب على المستخدم إدخال رمز أمن iCloud. تتحقق مجموعة HSM من أن المستخدم يعرف رمز أمن iCloud الخاص به باستخدام بروتوكول كلمة السر البعيدة الآمنة (SRP)؛ ولا يُرسَل الرمز نفسه إلى Apple. ويتحقق كل عضو من أعضاء المجموعة بشكل مستقل من أن المستخدم لم يتجاوز الحد الأقصى لعدد المحاولات المسموح بها لاستعادة سجله، كما هو موضح أدناه. وإذا وافقت الأغلبية، تقوم المجموعة بفك تغليف سجل الضمان وإرساله إلى جهاز المستخدم.

بعد ذلك، يستخدم الجهاز البيانات التي تم إيداعها لفك تغليف المفتاح العشوائي المستخدم لتشفير سلسلة مفاتيح المستخدم. ومن ثم فإن سلسلة المفاتيح التي تم استردادها من تخزين قيمة مفتاح CloudKit و iCloud يتم فك تشفيرها واستعادتها إلى الجهاز، باستخدام هذا المفتاح. لا تسمح خدمة الضمان سوى بعدد 10 محاولات لمصادقة سجل الضمان واسترداده. وبعد عدة محاولات فاشلة، يتم قفل السجل ويجب على المستخدم الاتصال بدعم Apple لمنحه المزيد من المحاولات. بعد المحاولة الفاشلة العاشرة، تقوم مجموعة HSM بإتلاف سجل الضمان وتُفقَد سلسلة المفاتيح إلى الأبد. وهذا يوفر الحماية ضد محاولة الهجوم بقوة غاشمة لاسترداد السجل، على حساب التضحية ببيانات سلسلة المفاتيح ردًا على ذلك.

يتم ترميز هذه السياسات في برنامج HSM الثابت. ويتم إتلاف بطاقات الوصول الإداري التي تسمح بتغيير البرنامج الثابت. ومن ثم فإن أي محاولة لتغيير البرنامج الثابت أو الوصول إلى المفتاح الخاص تؤدي إلى قيام مجموعة HSM بحذف المفتاح الخاص. في حالة حدوث ذلك، يتلقى مالك كل سلسلة مفاتيح تحميها المجموعة رسالة لإعلامه بأن سجل الضمان الخاص به قد تعرض للفقدان. ويمكنه بعد ذلك اختيار إعادة التسجيل.

Apple Pay

نظرة عامة على أمن Apple Pay

باستخدام Apple Pay، يستطيع المستخدمون استخدام أجهزة iPhone و iPad وApple Watch وMac المدعومة للدفع بطريقة سهلة وآمنة وخاصة في المتاجر والتطبيقات وعلى الويب في سفاري. ويمكن للمستخدمين كذلك إضافة بطاقات مواصلات تدعم Apple Pay وبطاقات هوية الطلاب وبطاقات الوصول إلى Apple Wallet. إنها خدمة سهلة للمستخدمين ومصممة بأمان متكامل في كل من المكونات المادية والبرامج.

تم تصميم Apple Pay لحماية معلومات المستخدم الشخصية أيضًا. ولا تجمع Apple Pay أي معلومات عن المعاملات يمكن إعادة ربطها بالمستخدم. كما تتم معاملات الدفع بين المستخدم والتاجر وجهة إصدار البطاقة.

أمن مكونات Apple Pay

يستخدم Apple Pay العديد من ميزات المكونات المادية والبرامج لتوفير عمليات شراء آمنة وموثوقة.

Secure Element

Secure Element عبارة عن شريحة معتمدة قياسية مثبت عليها نظام Java Card الأساسي، وهي متوافقة مع متطلبات القطاع المالي فيما يتعلق بعمليات الدفع الإلكترونية. وقد تم اعتماد IC ونظام Java Card الأساسي لـ Secure Element وفقًا لعملية التقييم الأمني من EMVCo. بعد الانتهاء بنجاح من التقييم الأمني، تصدر EMVCo شهادة فريدة لكل من IC والنظام الأساسي.

تم اعتماد IC لـ Secure Element وفقًا لمقاييس شهادة المعايير العامة.

وحدة تحكم NFC

تعالج وحدة تحكم NFC بروتوكولات الاتصال بالحقل القريب وتوجِّه الاتصالات بين معالج التطبيق و Secure Element، وبين Secure Element والوحدة الطرفية لنقطة البيع.

Apple Wallet

يُستخدم تطبيق Apple Wallet لإضافة بطاقات الائتمان والسحب والمتاجر وإدارتها وكذلك لإجراء عمليات الدفع باستخدام Apple Pay. ويمكن للمستخدم عرض بطاقاته وقد يتمكن من عرض معلومات إضافية مقدمة من جهة إصدار البطاقة، مثل سياسة خصوصية جهة إصدار البطاقة والمعاملات الأخيرة والمزيد في Apple Wallet. ويستطيع المستخدم أيضًا إضافة بطاقات إلى Apple Pay في:

- مساعد الإعداد والإعدادات في iOS و iPadOS
- تطبيق Watch في Apple Watch
- المحفظة وApple Pay في إعدادات النظام (macOS 13 أو أحدث) أو تفضيلات النظام (macOS 12 أو أقدم) لأجهزة كمبيوتر Mac المزودة ببصمة الإصبع

بالإضافة إلى ذلك، يتيح Apple Wallet للمستخدمين إضافة وإدارة بطاقات المواصلات وبطاقات المكافآت وبطاقات صعود الطائرة والتذاكر وبطاقات الهدايا وبطاقات هويات الطلاب وبطاقات الوصول والمزيد.

Secure Enclave

على iPhone و iPad و Apple Watch وأجهزة كمبيوتر Mac المزودة ببصمة الإصبع وأجهزة كمبيوتر Mac المزودة برقاقات Apple التي تستخدم لوحة مفاتيح ماجيك المزودة ببصمة الإصبع، يدير Secure Enclave عملية المصادقة ويسمح بمتابعة معاملة الدفع.

على Apple Watch، يجب فتح قفل الجهاز ويجب على المستخدم النقر مرتين على الزر الجانبي. يتم اكتشاف النقر المزدوج وتمريره مباشرة إلى Secure Element أو Secure Enclave حيثما كان ذلك متاحًا، دون المرور عبر معالج التطبيق.

خوادم Apple Pay

تدير خوادم Apple Pay إعداد وتوفير بطاقات الائتمان والسحب والمواصلات وهوية الطالب وبطاقات الوصول في تطبيق Apple Wallet. وتدير الخوادم أيضًا أرقام حسابات الجهاز المخزنة في Secure Element. وتتواصل مع كل من الجهاز ومع شبكة الدفع أو خوادم جهة إصدار البطاقة. كما أن خوادم Apple Pay مسؤولة أيضًا عن إعادة تشفير بيانات اعتماد الدفع لعمليات الدفع داخل التطبيقات أو على الويب.

كيف يحافظ Apple Pay على حماية مشتريات المستخدمين

Secure Element

تستضيف Secure Element تطبيقًا صغيرًا مصممًا خصوصًا لإدارة Apple Pay. وتتضمن أيضًا تطبيقات صغيرة معتمدة من شبكات الدفع أو جهات إصدار البطاقات. تُرسَل بيانات بطاقة الائتمان أو السحب أو البطاقة مسبقة الدفع من شبكة الدفع أو جهة إصدار البطاقة مُشفرةً إلى هذه التطبيقات الصغيرة باستخدام مفاتيح لا تكون معروفة إلا لشبكة الدفع أو جهة إصدار البطاقة ونطاق أمن التطبيقات الصغيرة. ويتم تخزين هذه البيانات داخل هذه التطبيقات الصغيرة وحمايتها باستخدام ميزات Secure Element الأمنية. أثناء المعاملة، تتصل الوحدة الطرفية مباشرةً بـ Secure Element من خلال وحدة تحكم الاتصال بالحقل القريب (NFC) عبر ناقل مادي مخصص.

وحدة تحكم NFC

باعتبارها بوابة إلى Secure Element، تساعد وحدة تحكم NFC على ضمان إجراء جميع معاملات الدفع غير التلامسية باستخدام وحدة طرفية لنقطة البيع تكون على مسافة قريبة من الجهاز. وتقوم وحدة تحكم NFC بتمييز طلبات الدفع الواردة من وحدة طرفية في المجال فقط على أنها معاملات غير تلامسية.

بعد اعتماد عملية دفع عبر بطاقة ائتمان أو سحب أو بطاقة مسبقة الدفع (بما في ذلك بطاقات المتجر) من قِبل حامل البطاقة باستخدام بصمة الوجه أو بصمة الإصبع أو رمز الدخول أو على Apple Watch غير مقفلة عن طريق النقر مرتين على الزر الجانبي، يتم توجيه الردود غير التلامسية التي أعدّتها تطبيقات الدفع الصغيرة داخل Secure Element حصريًا بواسطة وحدة التحكم إلى حقل NFC. وبالتالي، يتم تضمين تفاصيل تخويل الدفع لمعاملات الدفع غير التلامسية في حقل NFC المحلي ولا يتم كشفها أبدًا لمعالج التطبيق. في المقابل، يتم توجيه تفاصيل تخويل الدفع لعمليات الدفع التي تتم داخل التطبيقات وعلى الويب إلى معالج التطبيق، ولكن لا يتم ذلك إلا بعد التشفير بواسطة Secure Element إلى خادم Apple Pay.

بطاقات الائتمان والسحب والبطاقات مسبقة الدفع

نظرة عامة على أمان توفير البطاقة

عندما يضيف المستخدم بطاقة ائتمان أو سحب أو بطاقة مسبقة الدفع (بما في ذلك بطاقات المتجر) إلى Apple Wallet، ترسل Apple معلومات البطاقة بشكل آمن، إلى جانب معلومات أخرى حول حساب المستخدم وجهازه، إلى جهة إصدار البطاقة أو موفر الخدمة المعتمد لدى جهة إصدار البطاقة (شبكة الدفع عادة). باستخدام هذه المعلومات، تحدد جهة إصدار البطاقة (أو موفر الخدمة) ما إذا كانت ستوافق على إضافة البطاقة إلى Apple Wallet أم لا. كجزء من عملية توفير البطاقة، تستخدم Apple Pay ثلاثة اتصالات من جانب الخادم لإرسال واستقبال الاتصال مع جهة إصدار البطاقة أو شبكة الدفع:

- الحقول المطلوبة
- فحص البطاقة
- الربط والتوفير

وتستخدم جهة إصدار البطاقة أو شبكة الدفع هذه الاتصالات لتمكين جهة إصدار البطاقة من التحقق من البطاقات والموافقة عليها وإضافتها إلى Apple Wallet. تستخدم جلسات العميل-الخادم هذه بروتوكول TLS 1.2 لنقل البيانات.

لا يتم تخزين أرقام البطاقات الكاملة على الجهاز أو على خوادم Apple Pay. بدلاً من ذلك، يتم إنشاء رقم حساب جهاز فريد وتشفيره ثم تخزينه في Secure Element. ويتم تشفير رقم حساب الجهاز الفريد هذا بطريقة لا تُمكّن Apple من الوصول إليه. ويكون رقم حساب الجهاز فريدًا ومختلفًا عن معظم أرقام بطاقات الائتمان أو السحب؛ ويمكن لجهة إصدار البطاقة أو شبكة الدفع منع استخدامه على بطاقات الأشرطة الممغنطة أو عبر الهاتف أو على مواقع الويب. لا يُخزَّن أبدًا رقم حساب الجهاز الموجود في Secure Element على خوادم Apple Pay أو يُنسَخ احتياطيًا إلى iCloud، ويكون في معزل عن أجهزة iOS و iPadOS و watchOS وعن أجهزة كمبيوتر Mac التي تحتوي على بصمة الإصبع وأجهزة كمبيوتر Mac المزودة برقاقات Apple التي تستخدم لوحة مفاتيح ماجيك مزودة ببصمة الإصبع.

يتم توفير بطاقات للاستخدام مع Apple Watch لخدمة Apple Pay باستخدام تطبيق Apple Watch على الـ iPhone أو داخل تطبيق جهة إصدار البطاقة على الـ iPhone. وتتطلب إضافة بطاقة إلى Apple Watch أن تكون الساعة ضمن نطاق اتصالات Bluetooth. يتم تسجيل البطاقات على وجه التحديد للاستخدام مع Apple Watch ويكون لها أرقام حسابات الأجهزة الخاصة بها، والتي يتم تخزينها داخل Secure Element على Apple Watch.

عند إضافة بطاقات ائتمان أو سحب أو بطاقات مسبقة الدفع (بما في ذلك بطاقات المتجر)، تظهر في قائمة بطاقات أثناء تشغيل مساعد الإعداد على الأجهزة التي تم تسجيل دخولها إلى حساب iCloud نفسه. وتظل هذه البطاقات في تلك القائمة طالما كانت نشطة على جهاز واحد على الأقل. بينما تتم إزالة البطاقات من هذه القائمة بعد إزالتها من جميع الأجهزة لمدة 7 أيام. تتطلب هذه الميزة تمكين المصادقة بخطوتين على حساب iCloud ذي الصلة.

إضافة بطاقات ائتمان أو سحب إلى Apple Pay

يمكن إضافة بطاقات الائتمان يدويًا إلى Apple Pay في أجهزة Apple.

إضافة بطاقة ائتمان أو سحب يدويًا

لإضافة بطاقة يدويًا، يتم استخدام الاسم ورقم البطاقة وتاريخ انتهاء الصلاحية ورقم CVV لتسهيل عملية التوفير. من داخل الإعدادات أو Apple Wallet أو تطبيق Apple Watch، يمكن أن يدخل المستخدم هذه المعلومات إمّا عن طريق التقاطها باستخدام كاميرا الجهاز. عندما تلتقط الكاميرا معلومات البطاقة، تحاول Apple تعبئة الاسم ورقم البطاقة وتاريخ انتهاء الصلاحية. ولا يتم حفظ الصورة على الجهاز أو تخزينها في مكتبة الصور. بعد ملء جميع الحقول، تقوم عملية التحقق من البطاقة بالتحقق من الحقول الأخرى غير CVV. ويتم تشفيرها بعد ذلك وإرسالها إلى خادم Apple Pay.

إذا أسفرت عملية التحقق من البطاقة عن معرف بنود وشروط، تقوم Apple بتنزيل وعرض بنود وشروط جهة إصدار البطاقة للمستخدم. وإذا قبل المستخدم البنود والشروط الخاصة بجهة إصدار الطاقة، ترسل Apple معرف البنود التي تم قبولها وكذلك رقم CVV إلى عملية الربط والتوفير. بالإضافة إلى ذلك، كجزء من عملية الربط والتوفير، تشارك Apple المعلومات من الجهاز مع جهة إصدار البطاقة أو الشبكة. هذا يشمل معلومات إزاء (أ) نشاط حساب المستخدم على iTunes و App Store (على سبيل المثال، ما إذا كان لدى المستخدم سجل طويل من المعاملات داخل iTunes) و(ب) جهاز المستخدم (على سبيل المثال، رقم الهاتف والاسم وطراز جهاز المستخدم بالإضافة إلى أي جهاز Apple مصاحب ضروري لإعداد Apple Pay) و(ج) الموقع التقريبي للمستخدم في الوقت الذي يضيف فيه المستخدم بطاقته (إذا كان المستخدم قد قام بتمكين خدمات الموقع). باستخدام هذه المعلومات، تحدد جهة إصدار البطاقة ما إذا كانت ستوافق على إضافة البطاقة إلى Apple Pay أم لا.

نتيجة لعملية الربط والتوفير، يحدث أمران:

- يبدأ الجهاز بتنزيل ملف بطاقة Apple Wallet الذي يمثل بطاقة الائتمان أو السحب.
- يبدأ الجهاز في ربط البطاقة بـ Secure Element.

يحتوي ملف البطاقة على عناوين URL لتنزيل غلاف البطاقة وبيانات التعريف حول البطاقة مثل معلومات الاتصال وتطبيق جهة الإصدار ذات الصلة والميزات المدعومة. ويحتوي أيضًا على حالة البطاقة، والتي تتضمن معلومات مثل ما إذا كان إضفاء الطابع الشخصي على Secure Element قد اكتمل أم لا، أو ما إذا كانت البطاقة موقوفة حاليًا من قِبل جهة إصدار البطاقة أم لا، أو ما إذا كان يلزم إجراء تحقق إضافي قبل أن تتمكن البطاقة من إجراء عمليات دفع باستخدام Apple Pay أم لا.

إضافة بطاقات الائتمان أو السحب من حساب iTunes Store

بالنسبة لبطاقات الائتمان أو السحب في ملف على iTunes، قد يُطلب من المستخدم إعادة إدخال كلمة سر Apple ID. ويتم استرداد رقم البطاقة من iTunes، وتبدأ عملية التحقق من البطاقة. إذا كانت البطاقة مؤهلة لاستخدام Apple Pay، يقوم الجهاز بتنزيل وعرض البنود والشروط الخاصة بجهة إصدار البطاقة، ثم يُرسل مباشرةً معرف البنود ورمز أمن البطاقة إلى عملية الربط والتوفير. وقد يحدث التحقق الإضافي لبطاقات حساب iTunes الموجودة في الملف.

إضافة بطاقات الائتمان أو السحب من تطبيق جهة إصدار البطاقة

عند تسجيل تطبيق للاستخدام مع Apple Pay، يتم إنشاء مفاتيح للتطبيق ولخادم جهة إصدار البطاقة. وتُستخدم هذه المفاتيح لتشفير معلومات البطاقة التي يتم إرسالها إلى جهة إصدار البطاقة. وقد تم التصميم بتلك الطريقة لمنع جهاز Apple من قراءة المعلومات. يتشابه تدفق التوفير مع التدفق المستخدم للبطاقات المضافة يدويًا، الموضحة سابقًا، باستثناء كلمات السر لمرة واحدة التي يتم استخدامها بدلاً من CVV.

إضافة بطاقات الائتمان أو السحب من الموقع الإلكتروني لجهة إصدار البطاقة

توفر بعض جهات إصدار البطاقات القدرة على بدء عملية توفير البطاقة لـ Apple Wallet مباشرةً من المواقع الإلكترونية الخاصة بها. في هذه الحالة، يبدأ المستخدم المهمة عن طريق تحديد بطاقة لتوفيرها على الموقع الإلكتروني الخاص بجهة إصدار البطاقة. ومن ثم يُعاد توجيه المستخدم إلى تجربة تسجيل دخول مستقلة من Apple(مضمنة في نطاق Apple) ويُطلب منه تسجيل الدخول باستخدام Apple ID. عقب تسجيل الدخول بنجاح، يختار المستخدم جهازًا واحدًا أو أكثر لتوفير البطاقة له ويطلب منه تأكيد نتيجة التوفير على كل جهاز مستهدف معني.

إضافة عملية تحقق إضافية

يمكن لجهة إصدار البطاقة أن تقرر ما إذا كانت بطاقة الائتمان أو السحب تتطلب عملية تحقق إضافي أم لا. وحسب ما تقدمه جهة إصدار البطاقة، قد يكون بإمكان المستخدم الاختيار بين خيارات مختلفة لعملية تحقق إضافية، مثل رسالة نصية أو رسالة بريد إلكتروني أو مكالمة خدمة العملاء أو طريقة في تطبيق تابع لجهة خارجية معتمدة، لإكمال عملية التحقق. بالنسبة للرسائل النصية أو رسائل البريد الإلكتروني، يُعرَض على المستخدم خيار للاختيار من معلومات الاتصال التي تكون موجودة لدى جهة الإصدار في الملف بالفعل. يتم إرسال رمز يجب إدخاله في Apple Wallet أو الإعدادات أو تطبيق Apple Watch. بالنسبة لخدمة العملاء أو التحقق باستخدام تطبيق، تُجري جهة الإصدار عملية الاتصال الخاصة بها.

تخويل الدفع باستخدام Apple Pay

بالنسبة للأجهزة التي تحتوي على Secure Enclave، لا يمكن إجراء أي عملية دفع إلا بعد تلقي تخويل من Secure Enclave. على iPhone أو iPad أو Mac المزود ببصمة الإصبع (أو المقترن بلوحة مفاتيح ماجيك المزودة ببصمة الإصبع)، يشمل ذلك تأكيد أن المستخدم قام بالمصادقة باستخدام المصادقة ببيانات بيومترية أو رمز الدخول وكلمة السر للجهاز. المصادقة ببيانات بيومترية، إذا كانت متوفرة، هي الطريقة الافتراضية، لكن يمكن استخدام رمز الدخول أو كلمة السر في أي وقت ويتم عرض هذا الخيار تلقائيًا بعد ثلاث محاولات فاشلة لمطابقة بصمة الإصبع أو (بالنسبة إلى iPhone أو iPad) محاولتين فاشلتين لمطابقة الوجه؛ وبعد خمس محاولات فاشلة، يلزم إدخال رمز الدخول أو كلمة السر. يلزم استخدام رمز الدخول أو كلمة السر كذلك في حال عدم تكوين المصادقة البيومترية أو عدم تشغيلها لـ Apple Pay. لإجراء عملية الدفع على Apple Watch، يجب فتح قفل الجهاز برمز الدخول ويجب النقر مرتين على الزر الجانبي.

استخدام مفتاح اقتران مشترك

يتواصل Secure Enclave و Secure Element عبر واجهة تسلسلية — باستخدام التشفير والمصادقة استنادًا إلى AES، وباستخدام قيم مشفرة غير قابلة لإعادة التشغيل للحماية من هجمات إعادة التشغيل. وعلى الرغم من أن الجانبين غير متصلين مباشرةً، فإنهما يتواصلان بأمان باستخدام مفتاح اقتران مشترك تم توفيره خلال التصنيع. خلال هذه العملية، ينشئ Secure Enclave مفتاح الاقتران من مفتاح معرف UID الخاص به ومن معرف Secure Element الفريد. ثم ينقل مفتاح الاقتران بأمان إلى وحدة أمن المكونات المادية (HSM) في المصنع. ثم تُدخِل وحدة أمن المكونات المادية (HSM) مفتاح الاقتران في Secure Element.

تخويل المعاملات الآمنة

عندما يصرّح المستخدم بإجراء معاملة تتضمن إيماءة فعلية يتم توصيلها مباشرةً إلى Secure Enclave، ترسل Secure Enclave بيانات مُوقَّعة حول نوع المصادقة وتفاصيل حول نوع المعاملة (غير تلامسية أو داخل التطبيقات) إلى Secure Element، وتكون مرتبطة بقيمة تخويل عشوائي (AR). يتم إنشاء قيمة AR في Secure Enclave عندما يقوم المستخدم أولاً بتوفير بطاقة ائتمان مع استمرار ذلك أثناء تمكين Apple Pay، وتكون محمية بتشفير Secure Enclave وآلية مكافحة التراجع. ويتم تسليمها بشكل آمن إلى Secure Element من خلال الاستفادة من مفتاح الاقتران. عند استلام قيمة AR جديدة، يقوم Secure Element بتمييز أي بطاقات تمت إضافتها سابقًا على أنها منتهية.

استخدام تشفير الدفع للأمن الديناميكي

تتضمن معاملات الدفع التي تنشأ من تطبيقات الدفع الصغيرة تشفيرًا لعملية الدفع بجانب رقم حساب الجهاز. ويتم حساب هذا الرمز المشفر المخصص للاستخدام مرة واحدة باستخدام عدّاد معاملات ومفتاح. ويزداد عدّاد المعاملات مع كل معاملة جديدة. بينما يتم توفير المفتاح في تطبيق الدفع الصغير أثناء التخصيص ويكون معروفًا لدى شبكة الدفع أو جهة إصدار البطاقة أو كليهما. وحسب نظام الدفع، قد تُستخدم أيضًا بيانات أخرى في عملية الحساب، بما في ذلك التالي:

- رقم وحدة طرفية غير متوقع لمعاملات الاتصال بالحقل القريب (NFC)
- قيمة غير قابلة لإعادة التشغيل لخادم Apple Pay، للمعاملات داخل التطبيقات
- نتائج التحقق من المستخدم، مثل معلومات طريقة التحقق من حامل البطاقة (CVM).

يتم تقديم رموز الأمن هذه إلى شبكة الدفع وإلى جهة إصدار البطاقة، مما يتيح لجهة الإصدار التحقق من كل معاملة. وقد يختلف طول رموز الأمان هذه بناءً على نوع المعاملة.

الدفع بالبطاقات باستخدام Apple Pay

يمكن استخدام Apple Pay لدفع مقابل المشتريات في المتاجر وداخل التطبيقات وفي المواقع الإلكترونية.

الدفع باستخدام البطاقات في المتاجر

إذا كان الـ iPhone أو الـ Apple Watch قيد التشغيل واكتشف حقل NFC، فإنه يقدم للمستخدم البطاقة المطلوبة (إذا كان التحديد التلقائي قيد التشغيل لتلك البطاقة) أو البطاقة الافتراضية التي تتم إدارتها في الإعدادات. ويمكن للمستخدم كذلك الانتقال إلى Apple Wallet واختيار بطاقة، أو عند قفل الجهاز يمكنه:

- النقر مرتين على الزر الجانبي على الأجهزة التي بها بصمة الوجه
- النقر مرتين على زر الشاشة الرئيسية على الأجهزة التي بها بصمة الإصبع
- استخدام ميزات إمكانية الوصول التي تشغل Apple Pay من شاشة القفل

بعد ذلك، قبل إرسال معلومات الدفع، يجب على المستخدم المصادقة باستخدام بصمة الوجه أو بصمة الإصبع أو رمز الدخول الخاص به. عند فتح قفل Apple Watch، يؤدي النقر مرتين على الزر الجانبي إلى تنشيط البطاقة الافتراضية للدفع. ولا يتم إرسال معلومات الدفع دون مصادقة المستخدم.

بعد مصادقة المستخدم، يتم استخدام رقم حساب الجهاز ورمز الأمن الديناميكي الخاص بالمعاملة عند معالجة عملية الدفع. ولا ترسل Apple أو جهاز المستخدم أرقام بطاقات الائتمان أو السحب الكاملة إلى التجار. وقد تتلقى Apple معلومات مجهولة عن المعاملة مثل الوقت والموقع التقريبيين للمعاملة، مما يساعد في تحسين Apple Pay ومنتجات وخدمات Apple الأخرى.

الدفع باستخدام البطاقات داخل التطبيقات

يمكن استخدام Apple Pay أيضًا لإجراء عمليات الدفع في تطبيقات iOS و iPadOS و macOS و watchOS. عندما يدفع المستخدمون داخل التطبيقات باستخدام Apple Pay، تتلقى Apple معلومات المعاملة المشفرة لتوجيهها إلى المطور أو التاجر. وقبل إرسال هذه المعلومات إلى المطور أو التاجر، تقوم Apple بتشفير المعاملة باستخدام مفتاح خاص بالمطور. وتحتفظ Apple Pay بمعلومات المعاملة المجهولة، مثل مبلغ الشراء التقريبي. ولا يمكن ربط هذه المعلومات بالمستخدم ولا تتضمن مطلقًا معلومات حول ما يشتريه المستخدم.

عندما يبدأ أحد التطبيقات معاملة دفع عبر Apple Pay، تتلقى خوادم Apple Pay المعاملة المشفرة من الجهاز قبل التاجر الذي يستلمها. ومن ثم تقوم خوادم Apple Pay بإعادة تشفير المعاملة باستخدام مفتاح خاص بالتاجر قبل ترحيلها إلى التاجر.

عندما يطلب أحد التطبيقات إجراء عملية دفع، فإنه يستدعي واجهة API لتحديد ما إذا كان الجهاز يدعم Apple Pay أم لا وما إذا كان لدى المستخدم بطاقات ائتمان أو سحب يمكنها إجراء عمليات دفع على شبكة دفع يقبلها التاجر أم لا. ويطلب التطبيق أي معلومات يحتاجها لمعالجة المعاملة وإتمامها، مثل عنوان الفوترة والشحن ومعلومات الاتصال. يطلب التطبيق بعد ذلك من iOS أو iPadOS أو macOS أو watchOS تقديم ورقة Apple Pay التي بدورها تطلب معلومات للتطبيق، والمعلومات الضرورية الأخرى، مثل البطاقة التي يتم استخدامها.

في تلك الأثناء، يتم تزويد التطبيق بمعلومات المدينة والولاية والرمز البريدي لحساب تكلفة الشحن النهائية. كما لا يتم توفير مجموعة المعلومات المطلوبة بالكامل للتطبيق حتى يخوّل المستخدم عملية الدفع باستخدام بصمة الإصبع أو بصمة الوجه أو رمز دخول الجهاز. وبعد تخويل الدفع، يتم نقل المعلومات المقدمة في ورقة Apple Pay إلى التاجر.

الدفع باستخدام البطاقات داخل عينات التطبيقات

عينة التطبيق عبارة عن جزء صغير من التطبيق الذي يسمح للمستخدم بتنفيذ مهمة بسرعة (مثل استئجار دراجة أو الدفع مقابل ركن السيارات) دون تنزيل التطبيق الكامل. إذا كانت عينة التطبيق تدعم عمليات الدفع، يمكن للمستخدم استخدام تسجيل الدخول باستخدام Apple، ثم إجراء الدفع باستخدام Apple Pay. عندما يجري مستخدم عملية دفع من عينة تطبيق، تكون جميع تدابير الأمن والخصوصية مماثلة لنظيرتها عند قيام المستخدم بالدفع داخل التطبيق.

كيف يخوّل المستخدمون عمليات الدفع في التطبيقات، وكيف يتحقق منها التجار

يضمن المستخدمون والتجار أمان عمليات الدفع في التطبيقات عن طريق تمرير المعلومات إلى خوادم Apple و Secure Element والجهاز وواجهة برمجة التطبيقات الخاصة بالتطبيق. أولًا، عندما يخوّل المستخدم عملية دفع في تطبيق، يحصل التطبيق على قيمة مشفرة غير قابلة لإعادة التشغيل عن طريق الاتصال بخوادم Apple Pay. وترسل الخوادم هذه القيمة وبيانات المعاملة الأخرى إلى Secure Element لحساب بيانات اعتماد عملية الدفع التي تكون مشفّرة باستخدام مفتاح Apple. يعيد Secure Element بعد ذلك بيانات اعتماد عملية الدفع إلى خوادم Apple Pay لتتمكن من فك تشفيرها والتحقق من قيمتها غير القابلة لإعادة التشغيل مقابل القيمة غير القابلة لإعادة التشغيل التي أرسلتها خوادم Apple Pay في الأصل، وإعادة تشفيرها باستخدام معرف التاجر المرتبط بمفتاح التاجر. تعيد خوادم Apple بعد ذلك عملية الدفع إلى الجهاز، الذي يعيدها بدوره إلى واجهة برمجة التطبيقات الخاصة بالتطبيق، ثم تمررها واجهة برمجة التطبيقات إلى نظام التاجر للمعالجة. يفك التاجر تشفير بيانات اعتماد عملية الدفع للتحقق من أنه مُستلم المعاملة الصحيح.

تتطلب واجهات API استحقاقًا يحدد معرفات التجار المدعومة. يمكن أن يتضمن التطبيق أيضًا بيانات إضافية (مثل رقم الطلب أو هوية العميل) لإرسالها إلى Secure Element لتوقيعها، مما يضمن أنه لا يمكن تحويل المعاملة إلى عميل آخر. ويتم تحقيق ذلك بواسطة مطور التطبيق، الذي يمكنه تحديد applicationData في PKPaymentRequest. يتم تضمين تجزئة هذه البيانات في بيانات عملية الدفع المشفرة. ومن ثم يتحمل التاجر مسؤولية التحقق من أن تجزئة بيانات التطبيق الخاصة به تتطابق مع ما يتم تضمينه في بيانات عملية الدفع.

الدفع باستخدام البطاقات على مواقع الويب

يمكن استخدام Apple Pay لإجراء عمليات الدفع على مواقع الويب على iPhone وiPad وApple Watch وأجهزة كمبيوتر Mac المزودة ببصمة الإصبع. يمكن أيضًا بدء معاملات Apple Pay على Mac وإكمالها على iPhone أو Apple Watch يدعم Apple Pay باستخدام حساب iCloud نفسه.

تتطلب Apple Pay على الويب من جميع مواقع الويب المشارِكة أن تقوم بالتسجيل لدى Apple. بعد تسجيل النطاق، يتم التحقق من صحة اسم النطاق فقط بعد أن تصدر Apple شهادة عميل TLS. ويُشترط على مواقع الويب التي تدعم Apple Pay تقديم محتواها عبر HTTPS. بالنسبة لكل معاملة دفع، تحتاج مواقع الويب إلى الحصول على جلسة تاجر آمنة وفريدة مع خادم من خوادم Apple باستخدام شهادة عميل TLS الصادرة من Apple. ويتم توقيع بيانات جلسة التاجر بواسطة Apple. بعد التحقق من توقيع جلسة التاجر، قد يستعلم موقع الويب عما إذا كان لدى المستخدم جهاز يدعم Apple Pay أم لا وما إذا كانت لديه بطاقة ائتمان أو سحب أو بطاقة مسبقة الدفع منشطة على الجهاز أم لا. ولا تتم مشاركة تفاصيل أخرى. إذا كان المستخدم لا يريد مشاركة هذه المعلومات، يمكنه تعطيل استعلامات Apple Pay في إعدادات خصوصية سفاري على أجهزة iPhone daPig و Mac.

بعد التحقق من صحة جلسة التاجر، تكون جميع إجراءات الخصوصية والأمن مماثلة لنظيرتها التي تتم عند قيام المستخدم بالدفع داخل التطبيق.

إذا كان المستخدم ينقل معلومات متعلقة بعملية الدفع من Mac إلى iPhone أو Apple Watch، تستخدم التسليم في Apple Pay بروتوكول خدمة الهوية من Apple (IDS) ذات التشفير الكامل لنقل المعلومات المتعلقة بالدفع بين Mac الخاص بالمستخدم وجهاز التخويل. يستخدم عميل IDS على Mac مفاتيح جهاز المستخدم لتنفيذ التشفير بحيث لا يستطيع أي جهاز آخر فك تشفير هذه المعلومات، ولا تكون المفاتيح متاحة لشركة Apple. تحتوي معلومات اكتشاف الجهاز بالنسبة للتسليم في Apple Pay على النوع والمعرف الفريد لبطاقات ائتمان المستخدم إلى جانب بعض بيانات التعريف. ولا تتم مشاركة رقم حساب الجهاز الخاص ببطاقة المستخدم ويظل مُخزنًا كما هو بشكل آمن على iPhone أو Apple Watch الخاص بالمستخدم. تنقل Apple أيضًا معلومات الاتصال وعناوين الشحن والفوترة المستخدمة مؤخرًا الخاصة بالمستخدم عبر سلسلة مفاتيح iCloud بشكل آمن.

بعد أن يخوّل المستخدم عملية الدفع باستخدام بصمة الوجه أو بصمة الإصبع أو رمز دخول أو النقر مرتين على الزر الجانبي في Apple Watch، — يتم بشكل آمن نقل رمز دفع مشفر بطريقة فريدة — لكل شهادة من شهادات تجار المواقع الإلكترونية من iPhone أو Apple Watch الخاص بالمستخدم إلى Mac الخاص به، ثم تسليمه إلى الموقع الإلكتروني الخاص بالتاجر.

لا يمكن طلب الدفع وإكماله إلا من قِبل الأجهزة القريب بعضها من بعض فقط. ويتم تحديد التقارب من خلال إعلانات Bluetooth منخفض الطاقة (BLE).

رموز التاجر وعمليات الدفع التلقائي

في iOS 16 أو أحدث، يمكن للتطبيقات والمواقع الإلكترونية التي توفِّر ميزة Apple Pay استخدام رموز التاجر في Apple Pay التي تتيح عمليات دفع آمنة متكررة عبر أجهزة المستخدم. تؤدي صفحة الدفع المُحدَّثة في Apple Pay في iOS 16 أيضًا إلى تحسين تجارب الدفع المصرح بها مسبقًا. تسمح أنواع المعاملات الجديدة في واجهة برمجة التطبيقات في Apple Pay لمطوري التطبيقات والمواقع الإلكترونية بتصميم تجربة صفحة دفع مناسبة لتسديد الاشتراكات والفواتير المتكررة ودفع الأقساط وإعادة تحميل أرصدة البطاقات تلقائيًا.

رموز التاجر ليست خاصة بالجهاز، لذلك فإنها تسمح بمتابعة عمليات الدفع المتكررة في حالة قيام المستخدم بإزالة بطاقة الدفع من الجهاز.

مدفوعات لتجار متعددين

في iOS 16 أو أحدث، يوفِّر Apple Pay إمكانية تحديد مبلغ الشراء لأكثر من تاجر ضمن صفحة دفع واحدة في Apple Pay. يوفِّر ذلك مزيدًا من المرونة للسماح للعملاء بإجراء عمليات شراء مجمعة، مثل باقة سفر متضمنة تذاكر طيران وسيارة مستأجرة وحجز فندق، ثم إرسال المدفوعات إلى كل تاجر على حدة.

البطاقات الذكية في Apple Pay

لنقل البيانات من البطاقات المدعومة إلى وحدات NFC الطرفية المتوافقة، تستخدم Apple بروتوكول خدمات القيمة المضافة (Apple VAS) من Apple. يمكن تطبيق بروتوكول VAS على الوحدات الطرفية غير التلامسية أو في تطبيقات الـ iPhone ويستخدم NFC للتواصل مع أجهزة Apple المدعومة. كما يعمل بروتوكول VAS على مسافة قصيرة ويمكن استخدامه لتقديم البطاقات غير التلامسية بشكل مستقل أو كجزء من معاملة Apple Pay.

عندما يكون الجهاز بالقرب من وحدة NFC الطرفية، تبدأ الوحدة الطرفية في تلقي معلومات البطاقة عن طريق إرسال طلب للحصول على بطاقة. إذا كان لدى المستخدم بطاقة بها معرف خاص بموفر البطاقة، يُطلب من المستخدم تخويل استخدامها باستعمال بصمة الوجه أو بصمة الإصبع أو رمز الدخول. وتُستخدم معلومات البطاقة وطابع الوقت ومفتاح ECDH P-256 عشوائي للاستخدام مرة واحدة مع المفتاح العام لموفر البطاقة لاشتقاق مفتاح تشفير لبيانات البطاقة يتم إرساله إلى الوحدة الطرفية.

من iOS 12.0.1 إلى iOS 13، يمكن للمستخدم تحديد بطاقة يدويًا قبل تقديمها إلى وحدة NFC الطرفية الخاصة بالتاجر. وفي iOS 13.1 أو أحدث، يمكن لموفري البطاقات تكوين البطاقات المحددة يدويًا إما للمطالبة بمصادقة المستخدم أو لاستخدامها دون مصادقة.

جعل البطاقات غير صالحة للاستخدام مع Apple Pay

لا يمكن استخدام بطاقات الائتمان والسحب والبطاقات مسبقة الدفع المضافة إلى Secure Element إلا إذا تم تقديم Secure Element مع تخويل باستخدام نفس مفتاح الاقتران وقيمة تخويل عشوائي (AR) من تاريخ إضافة البطاقة. عند استلام قيمة AR جديدة، يقوم Secure Element بتمييز أي بطاقات تمت إضافتها سابقًا على أنها منتهية. وهذا يسمح لنظام التشغيل بتوجيه Secure Enclave إلى جعل البطاقات غير صالحة للاستخدام من خلال تمييز نسختها من AR باعتبارها غير صالحة وفقًا للسيناريوهات التالية:

الطريقة	الجهاز
تم تعطيل رمز المرور.	iPhone أو iPad أو Apple Watch
تم تعطيل كلمة السر.	Mac
يقوم المستخدم بتسجيل الخروج من iCloud.	iPhone أو iPad أو Mac أو Apple Watch
يقوم المستخدم بتحديد مسح جميع المحتويات والإعدادات.	iPhone أو iPad أو Mac أو Apple Watch
تم استعادة الجهاز من وضع الاسترداد.	iPhone أو iPad أو Mac أو Apple Watch
إلغاء الاقتران	Apple Watch

تعليق البطاقات وإزالتها ومسحها

يمكن للمستخدم تعليق Apple Pay على الـ iPhone والـ iPad والـ Apple Watch من خلال وضع أجهزته في نمط الفقدان باستخدام تحديد الموقع. كما يمكن للمستخدمين إزالة بطاقاتهم ومسحها من Apple Pay باستخدام تحديد الموقع أو iCloud.com أو مباشرةً على أجهزتهم باستخدام Apple Wallet. على Apple Watch، يمكن إزالة البطاقات باستخدام إعدادات iCloud أو تطبيق Apple Watch على الـ iPhone أو مباشرة على الساعة. يتم تعليق إمكانية إجراء عمليات الدفع باستخدام البطاقات الموجودة على الجهاز أو إزالتها من Apple Pay بواسطة جهة إصدار البطاقة أو شبكة الدفع المعنية، حتى إذا كان الجهاز دون اتصال بالإنترنت وغير متصل بشبكة خلوية أو شبكة Wi-Fi. ويمكن للمستخدمين كذلك الاتصال بجهة إصدار البطاقة الخاصة بهم لتعليق البطاقة أو إزالتها من Apple Pay.

عندما يمسح المستخدم الجهاز بالكامل؛ باستخدام مسح جميع المحتويات والإعدادات أو باستخدام تحديد الموقع أو استعادة جهازه؛ تقوم أجهزة iPhone و iPad و Mac و Apple Watch بتوجيه Secure Element لتمييز جميع البطاقات على أنها منتهية. ويكون لذلك تأثير تغيير البطاقات على الفور إلى حالة غير صالحة للاستعمال حتى يمكن الاتصال بخوادم Apple Pay لمسح البطاقات بالكامل من Secure Element. وبشكل مستقل، تميّز Secure Enclave قيمة AR على أنها غير صالحة بحيث لا يمكن إجراء المزيد من تخويلات الدفع للبطاقات المسجلة سابقًا. عندما يكون الجهاز متصلاً بالإنترنت، يحاول الاتصال بخوادم Apple Pay لضمان مسح جميع البطاقات في Secure Element.

أمن Apple Card

في الطرز المدعومة من iPhone و Mac، يمكن للمستخدم التقدم بأمان للحصول على Apple Card.

تطبيق Apple Card

في iOS 12.4 أو أحدث، و macOS 10.14.6 أو أحدث و watchOS 5.3 أو أحدث، يمكن استخدام Apple Card مع Apple Pay لإجراء عمليات الدفع في المتاجر وفي التطبيقات وعلى الويب.

للتقدم بطلب للحصول على Apple Card، يجب تسجيل دخول المستخدم إلى حساب iCloud على iPhone أو iPad متوافق مع Apple Pay مع إعداد المصادقة بخطوتين على حساب iCloud، أو يمكنه التقدم بطلب على apply.Applecard.Apple بعد تسجيل الدخول باستخدام Apple ID. بعد الموافقة على الطلب، تتوفر Apple Card في Apple Wallet أو ضمن الإعدادات > Wallet و Apple Pay عبر أي من الأجهزة المؤهلة التي سجل المستخدم الدخول إليها باستخدام Apple ID الخاص به.

عندما يتقدم المستخدم بطلب للحصول على Apple Card، يتم التحقق من معلومات هوية المستخدم بشكل آمن بواسطة شركاء موفري الهويات من Apple ثم مشاركتها مع Goldman Sachs Bank USA لأغراض تقييم الهوية والائتمان.

يتم نقل المعلومات، مثل رقم الضمان الاجتماعي أو صورة وثيقة الهوية، المقدَّمة أثناء الطلب بشكل آمن إلى شركاء موفري الهويات من Apple و/أو Goldman Sachs Bank USA مُشفرةً باستخدام مفاتيحها ذات الصلة. ولا تستطيع Apple فك تشفير هذه البيانات.

يتم نقل معلومات الدخل المقدمة خلال الطلب ومعلومات الحساب البنكي المستخدمة لدفع الفواتير بشكل آمن إلى Goldman Sachs Bank USA مُشفرةً باستخدام مفاتيحها. وتُحفظ معلومات الحساب البنكي في سلسلة المفاتيح. ولا تستطيع Apple فك تشفير هذه البيانات.

عند إضافة Apple Card إلى Apple Wallet، فإن المعلومات ذاتها التي تتوفر عندما يضيف مستخدم بطاقة ائتمان أو سحب قد تتم مشاركتها مع بنك Goldman Sachs Bank USA، شريك Apple، ومع شركة Apple Payments Inc.. ولا تُستخدم تلك المعلومات إلا لاستكشاف الأخطاء وإصلاحها ومنع الاحتيال وللأغراض التنظيمية.

في iOS 14.6 أو أحدث و iPadOS 14.6 أو أحدث و watchOS 7.5 أو أحدث، يمكن لمنظم عائلة iCloud باستخدام بطاقة Apple Card مشاركة بطاقته مع أفراد عائلة iCloud الذين تزيد أعمارهم عن 13 عامًا. تلزم مصادقة المستخدم لتأكيد الدعوة. يستخدم Apple Wallet مفتاحًا في Secure Enclave لحساب توقيع يربط المالك والمدعوين. يتم التحقق من صحة هذا التوقيع على خوادم Apple.

اختياريًا، يمكن للمنظم تعيين حد معاملة للمشاركين. يمكن كذلك قفل بطاقات المشاركين لإيقاف إنفاقهم مؤقتًا في أي وقت من خلال Apple Wallet. عندما يقبل مالك مشارك أو مشارك يزيد عمره عن 18 عامًا الدعوة ويقدمها، يخضع لعملية التقديم نفسها كما هو محدد في قسم تطبيق Apple Card في Apple Wallet.

استخدام Apple Card

يمكن طلب بطاقة حقيقية من Apple Card في Apple Wallet. بعد أن يستلم المستخدم البطاقة الحقيقية، يتم تنشيطها باستخدام علامة NFC الموجودة في مُغلّف البطاقة الحقيقية ثنائي الطيّات. وتكون العلامة فريدة لكل بطاقة ولا يمكن استخدامها لتنشيط بطاقة مستخدم آخر. بدلاً من ذلك، يمكن تنشيط البطاقة يدويًا في إعدادات Apple Wallet. بالإضافة إلى ذلك، يمكن للمستخدم كذلك اختيار قفل أو فتح قفل البطاقة الحقيقية في أي وقت من Apple Wallet.

عمليات الدفع باستخدام Apple Card وتفاصيل بطاقة Apple Wallet

يمكن إجراء المدفوعات المستحقة على حساب Apple Card من متصفح ويب أو من Apple Wallet في iOS باستخدام Apple Cash وحساب بنكي. ويمكن جدولة مدفوعات الفواتير على أنها متكررة أو بوصفها مدفوعات لمرة واحدة بتاريخ محدد باستخدام Apple Cash وحساب بنكي. عندما يجري المستخدم عملية دفع، يتم إجراء اتصال بخوادم Apple Pay للحصول على قيمة مشفرة غير قابلة لإعادة التشغيل كما هو الحال مع Apple Cash. ويتم تمرير القيمة غير القابلة لإعادة التشغيل، إلى جانب تفاصيل إعداد عملية الدفع، إلى Secure Element لحساب توقيع. وبعد ذلك يتم إرجاع التوقيع إلى خوادم Apple Pay. وتتحقق خوادم Apple Pay من مصادقة عملية الدفع وتكاملها وصحتها من خلال التوقيع والقيمة غير القابلة لإعادة التشغيل، ويتم تمرير الطلب إلى Goldman Sachs Bank USA للمعالجة.

يتم استرداد رقم Apple Card بواسطة Apple Wallet عن طريق تقديم شهادة. يتحقق خادم Apple Pay من صحة الشهادة للتأكد من أن المفتاح تم إنشاؤه في Secure Enclave. ومن ثم يستخدم هذا المفتاح لفك تشفير رقم Apple Card قبل إعادته إلى Apple Wallet، حتى لا يتمكن سوى الـ iPhone الذي طلب Apple Card من فك تشفيره. بعد فك التشفير، يُحفَظ رقم Apple Card في سلسلة مفاتيح iCloud.

إن عرض تفاصيل رقم Apple Card في البطاقة باستخدام Apple Wallet يتطلب مصادقة المستخدم باستخدام بصمة الوجه أو بصمة الإصبع أو رمز الدخول. ويمكن استبدالها بواسطة المستخدم في قسم معلومات البطاقة، وتعطيل البطاقة السابقة.

حماية متقدمة من الاحتيال

في iOS 15 أو أحدث و iPadOS 15 أو أحدث، يمكن لمستخدم Apple Card تمكين الحماية المتقدمة من الاحتيال في Apple Wallet. عند التمكين، يتم تحديث رمز أمن البطاقة كل بضعة أيام.

أمن Apple Cash

في iOS 11.2 أو أحدث، و iPadOS 13.1 أو أحدث، و watchOS 4.2 أو أحدث، يمكن استخدام Apple Cash على iPhone أو iPad أو Apple Watch لإرسال الأموال واستقبالها وطلبها من المستخدمين الآخرين. عندما يتلقى المستخدم الأموال، تتم إضافتها إلى حساب Apple Cash الذي يمكن الوصول إليه في Apple Wallet أو ضمن الإعدادات > Wallet و Apple Pay عبر أي من الأجهزة المؤهلة التي سجل المستخدم الدخول إليها باستخدام Apple ID الخاص به.

في iOS 14 و iPadOS 14 و watchOS 7، يمكن لمنظم عائلة iCloud الذي أثبت هويته باستخدام Apple Cash تمكين Apple Cash لأفراد عائلته الذين تقل أعمارهم عن 18 عامًا. ويمكن للمنظم، اختياريًا، تقييد إمكانيات إرسال الأموال لهؤلاء المستخدمين على أفراد العائلة فقط أو جهات الاتصال فقط. إذا كان فرد العائلة الذي يقل عمره عن 18 عامًا يمر عبر استرداد حساب Apple ID، يجب على منظم العائلة إعادة تمكين بطاقة Apple Cash لهذا المستخدم يدويًا. إذا لم يعد فرد العائلة الذي يقل عمره عن 18 عامًا جزءًا من عائلة iCloud، فسيتم نقل رصيد Apple Cash الخاص به تلقائيًا إلى حساب المنظم.

عندما يقوم المستخدم بإعداد Apple Cash، فإن المعلومات ذاتها التي تتوفر عندما يضيف المستخدم بطاقة ائتمان أو سحب قد تتم مشاركتها مع بنك Green Dot Bank الشريك لنا ومع Apple Payments Inc.، وهي شركة فرعية مملوكة بالكامل تم تأسيسها لحماية خصوصية المستخدم من خلال تخزين المعلومات ومعالجتها بشكل منفصل عن بقية شركة Apple وبطريقة لا تعرفها بقية شركة Apple. ولا تُستخدم هذه المعلومات إلا لاستكشاف الأخطاء وإصلاحها ومنع الاحتيال وللأغراض التنظيمية.

استخدام Apple Cash في iMessage

لاستخدام عمليات الدفع من شخص لآخر و Apple Cash، يجب تسجيل دخول المستخدم إلى حساب iCloud الخاص به على جهاز متوافق مع Apple Cash وأن يتم إعداد المصادقة بخطوتين على حساب iCloud. يتم بدء طلبات وتحويلات الأموال بين المستخدمين من داخل تطبيق الرسائل أو عن طريق سؤال Siri. وعندما يحاول المستخدم إرسال الأموال، يعرض iMessage ورقة Apple Pay. دائمًا ما يُستخدم رصيد Apple Cash أولاً. وإذا لزم الأمر، تُسحب أموال إضافية من بطاقة ائتمان أو سحب ثانية أضافها المستخدم إلى Apple Wallet.

استخدام Apple Cash في المتاجر والتطبيقات وعلى الويب:

يمكن استخدام بطاقة Apple Cash في Apple Wallet مع Apple Pay لإجراء عمليات في المتاجر والتطبيقات وعلى الويب. ويمكن أيضًا تحويل الأموال الموجودة في حساب Apple Cash إلى حساب بنكي. بالإضافة إلى الأموال التي يتم تلقيها من مستخدم آخر، يمكن إضافة الأموال إلى حساب Apple Cash من بطاقة سحب أو بطاقة مسبقة الدفع في Apple Wallet.

تقوم Apple Payments Inc. بتخزين بيانات معاملات المستخدم، وقد تستخدمها لاستكشاف الأخطاء وإصلاحها ومنع الاحتيال وللأغراض التنظيمية بمجرد إتمام المعاملة. ولا تعرف بقية Apple من أرسل المستخدم الأموال إليه أو من تلقى المستخدم الأموال منه أو مكان شراء المستخدم باستخدام بطاقة Apple Cash الخاصة به.

عندما يرسل المستخدم أموالاً باستخدام Apple Pay أو يضيف أموالاً إلى حساب Apple Cash أو يحوّل أموالاً إلى حساب بنكي، يتم إجراء اتصال بخوادم Apple Pay للحصول على قيمة مشفرة غير قابلة لإعادة التشغيل مشابهة للقيمة التي تم إرجاعها لـ Apple Pay داخل التطبيقات. ويتم تمرير القيمة غير القابلة لإعادة التشغيل، إلى جانب بيانات المعاملة الأخرى، إلى Secure Element لحساب توقيع دفع. يتم إرجاع التوقيع إلى خوادم Apple Pay. وتتحقق خوادم Apple Pay من مصادقة المعاملة وتكاملها وصحتها من خلال توقيع عملية الدفع والقيمة غير القابلة لإعادة التشغيل. يتم بعد ذلك بدء تحويل الأموال وإخطار المستخدم بمعاملة مكتملة.

إذا كانت المعاملة تتضمن:

- بطاقة سحب لإضافة الأموال إلى Apple Cash
- توفير أموال إضافية إذا كان رصيد Apple Cash غير كافٍ

يتم كذلك إنتاج بيانات اعتماد دفع مشفّرة وإرسالها إلى خوادم Apple Pay، على غرار طريقة عمل Apple Pay داخل التطبيقات والمواقع الإلكترونية.

بعد أن يتجاوز رصيد حساب Apple Cash مبلغًا معينًا أو في حالة اكتشاف نشاط غير عادي، تتم مطالبة المستخدم بالتحقق من هويته. المعلومات المقدمة للتحقق من هوية المستخدم؛ مثل رقم الضمان الاجتماعي أو الإجابات على الأسئلة (على سبيل المثال، لتأكيد اسم الشارع الذي عاش فيه المستخدم سابقًا)؛ يتم نقلها بشكل آمن إلى شريك Apple وتشفيرها باستخدام مفتاحها. ولا تستطيع Apple فك تشفير هذه البيانات. تتم مطالبة المستخدم بإثبات هويته مرة أخرى إذا قام باسترداد حساب Apple ID، قبل استعادة الوصول إلى رصيد Apple Cash الخاص به.

أمن Tap to Pay on iPhone

تسمح ميزة قرب للدفع على iPhone، المتوفرة في iOS 15.4 أو أحدث للتجار بقبول Apple Pay والمدفوعات غير التلامسية الأخرى باستخدام iPhone وتطبيق iOS الذي يدعمه الشريك. بفضل تلك الخدمة، يمكن للمستخدمين الذين لديهم أجهزة iPhone المدعومة قبول المدفوعات غير التلامسية وبطاقات Apple Pay التي تدعم NFC بأمان. باستخدام Tap to Pay on iPhone، لا يحتاج التجار إلى مكونات مادية إضافية لقبول المدفوعات غير التلامسية.

صممت ميزة Tap to Pay on iPhone لحماية المعلومات الشخصية للمسدد. لا تجمع هذه الخدمة معلومات عن المعاملات التي يمكن إعادة ربطها بالمسدد. يتم تأمين معلومات بطاقة الدفع مثل رقم بطاقة الائتمان/السحب (PAN) باستخدام Secure Element ولا تُعرَض على جهاز التاجر. تبقى معلومات بطاقة الدفع لدى مقدم خدمة الدفع للتاجر والمسدد وجهة إصدار البطاقة. بالإضافة إلى ذلك، لا تجمع خدمة Tap to Pay أسماء المسددين أو عناوينهم أو أرقام هواتفهم.

تم تقييم ميزة قرب للدفع على iPhone خارجيًا بواسطة مختبر أمني مصدّق وتم اعتمادها للاستخدام بواسطة جميع شبكات الدفع المقبولة في المناطق المتوفرة فيها.

أمن مكون الدفع غير التلامسي

- **Secure Element:** يستضيف Secure Element أنوية الدفع التي تقرأ بيانات بطاقة الدفع غير التلامسية وتؤمنها.
- **وحدة تحكم NFC:** تعالج وحدة تحكم NFC بروتوكولات الاتصال بالحقل القريب وتوجّه الاتصالات بين معالج التطبيق و Secure Element، وبين Secure Element وبطاقة الدفع غير التلامسية.
- **خوادم Tap to Pay on iPhone:** تدير خوادم Tap to Pay on iPhone إعداد أنوية الدفع وتوفيرها في الجهاز. تراقب الخوادم كذلك أمن أجهزة Tap Pay on iPhone بطريقة متوافقة مع معيار المدفوعات غير التلامسية في البرمجيات التجارية الجاهزة (COTS) (CPoC) من مجلس معايير أمن صناعة بطاقات الدفع (PCI SSC) وتكون متوافقة مع معايير أمن بيانات صناعة بطاقات الدفع (PCI DSS).

كيف تقرأ خدمة Tap to Pay بطاقة الائتمان والسحب والبطاقات مسبقة الدفع

كيف توفر خدمة Tap to Pay الأمن

عند أول استخدام لخدمة Tap to Pay on iPhone باستخدام تطبيق مؤهل بشكل كافٍ، يحدد خادم Tap to Pay on iPhone ما إذا كان الجهاز يفي بمعايير الاستحقاق مثل طراز الجهاز وإصدار الـ iOS وما إذا كان قد تم تعيين رمز مرور. بعد إتمام هذا التحقق، يتم تنزيل تطبيق قبول الدفع الصغير من خادم Tap to Pay on iPhone ويتم تثبيته على Secure Element بجانب تكوين نواة الدفع المقترنة. يتم تنفيذ هذه العملية بأمان بين خوادم Tap to Pay on iPhone و Secure Element. يتحقق Secure Element من سلامة هذه البيانات وصحتها قبل التثبيت.

كيف تقرأ خدمة Tap to Pay البطاقات بأمان

عندما يطلب تطبيق قرب للدفع على iPhone قراءة البطاقة من إطار عمل ProximityReader، تُعرض صفحة - يتحكم فيها iOS - ويُطلب من المستخدم الضغط على بطاقة دفع. لا يمكن لأي تطبيقات قراءة أي مستشعرات يمكنها الكشف عن أي جزء من بيانات البطاقة الحساسة أثناء الوقت الذي تكون فيه شاشة الضغط نشطة. يقوم iOS بتشغيل قارئ بطاقات الدفع ثم يطلب من نواة الدفع في Secure Element بدء قراءة البطاقة.

في هذه المرحلة، يبدأ Secure Element في السيطرة على وحدة تحكم NFC في وضع القارئ. يتيح هذا الوضع تبادل بيانات البطاقة بين بطاقة الدفع و Secure Element فقط من خلال وحدة تحكم NFC. لا يمكن قراءة بطاقات الدفع إلا في هذا الوضع.

بعد أن يكمل تطبيق قبول الدفع الصغير الموجود على Secure Element قراءة بطاقة الدفع، يفك تشفير بيانات البطاقة ويوقع عليها. تبقي بيانات بطاقة الدفع مشفرة ومصدقًا عليها إلى أن تصل إلى مقدم خدمة الدفع. لا يتمكن أحد من فك تشفير بيانات بطاقة الدفع سوى مقدم خدمة الدفع الذي يستخدمه التطبيق لطلب قراءة البطاقة فقط. يتعين على مقدم خدمة الدفع طلب مفتاح فك تشفير بيانات بطاقة الدفع من خادم قرب للدفع على iPhone. يُصدِر خادم قرب للدفع على iPhone مفاتيح فك التشفير إلى مقدم خدمة الدفع (توفر الخدمات) بعد التحقق من سلامة البيانات وصحتها، وبعد التحقق من تنفيذ قراءة البطاقة في غضون 60 ثانية من طلب مفتاح فك تشفير بيانات بطاقة الدفع.

يساعد هذا النموذج على ضمان عدم إمكانية فك تشفير بيانات بطاقة الدفع من قِبل أي شخص آخر غير مقدم خدمة الدفع (PSP)، الذي يعالج هذه المعاملة لصالح التاجر.

استخدام إدخال رمز PIN لتخويل المعاملات

يسمح إدخال رمز PIN، المتوفر في iOS 16.0 أو أحدث، للمسدِّد بإدخال رمز PIN على جهاز التاجر لتخويل المعاملة. وقد يتم تشغيل شاشة إدخال رمز PIN فورًا بعد الضغط استنادًا إلى المعلومات التي تم تبادلها مع بطاقة الدفع. أو يمكن لمقدم خدمة الدفع تشغيل شاشة رمز PIN عن طريق توفير رمز موقع، ويكون صالحًا لمعاملة واحدة فقط.

تم تقييم آلية إدخال رمز PIN خارجيًا بواسطة مختبر أمني مصدق وتم اعتمادها للاستخدام بواسطة جميع شبكات الدفع المقبولة في المناطق المتاحة فيها. إن شاشة إدخال رمز PIN محمية من لقطات الشاشة وانعكاس الشاشة، ولا يمكن لأي تطبيق قراءة أي من المستشعرات التي قد تمنح أي جزء من قيمة رمز PIN خلال الوقت التي تكون فيه شاشة إدخال رمز PIN نشطة.

يلتقط Secure Element أرقام رمز PIN المدخلة بشكل آمن. وباستخدام أرقام رمز PIN هذه، ينشئ Secure Element كتلة رمز PIN مشفرة متوافقة مع معايير صناعة الدفع. توفر Apple كتلة رمز PIN المشفرة بشكل آمن من خادمها المتوافق مع رمز PIN لصناعة بطاقات الدفع (PCI) إلى مقدم خدمة الدفع (PSP) لاستكمال المعالجة.

قيمة رمز PIN:

- لا تكون متاحة أبدًا للتاجر على جهازه
- لا يتم فك تشفيرها أبدًا بواسطة Apple في أي وقت
- لا يتم تخزينها أبدًا بواسطة Apple

استخدام Apple Wallet

إمكانية الوصول باستخدام Apple Wallet

في Apple Wallet على أجهزة iPhone وApple Watch المدعومة، يمكن للمستخدمين تخزين العديد من أنواع المفاتيح. عندما يصل مستخدم إلى أحد الأبواب، يمكن تقديم المفتاح الصحيح تلقائيًا (إذا كان النمط السريع مشغلًا ويدعمه هذا المفتاح)، ما يتيح له الدخول بضغطة واحدة باستخدام الاتصال قريب المدى (NFC).

راحة المستخدم

النمط السريع

عند إضافة مفتاح إلى Apple Wallet، يُشغَّل النمط السريع بشكل افتراضي. وتتفاعل المفاتيح في النمط السريع مع قبول الوحدات الطرفية دون استخدام بصمة الوجه أو بصمة الإصبع أو مصادقة رمز الدخول أو النقر المزدوج على الزر الجانبي في Apple Watch. لتعطيل هذه الميزة، يمكن للمستخدمين إيقاف النمط السريع عن طريق الضغط على زر المزيد في مقدمة البطاقة الذي يمثل المفتاح في Apple Wallet. ولإعادة تشغيل النمط السريع، يتعين عليهم استخدام بصمة الوجه، أو بصمة الإصبع أو رمز الدخول.

مشاركة المفتاح

في iOS 16 أو أحدث، تتوفر مشاركة المفتاح لبعض أنواع المفاتيح المعينة.

يمكن أن يشارك المستخدمون حق الوصول إلى المفتاح (على سبيل المثال، مفتاح منزل أو سيارة)، مع تطبيق تدابير الأمن والخصوصية من iPhone مالك المفتاح إلى iPhone مستلم المفتاح المدعو. تتم مشاركة المفاتيح من خلال الضغط على أيقونة مشاركة الخاصة بالمفتاح في Apple Wallet ويمكن مشاركتها باستخدام الطرق التي تظهر في صفحة المشاركة. يمكن أيضًا أن يختار مالك المفاتيح مستوى الوصول والفترة الزمنية الصالحة لكل مفتاح مشترك. يمكن لمالك المفتاح الاطلاع على جميع المفاتيح التي شاركها ويمكنه إلغاء الوصول لأي مفتاح مشترك، ومن ضمن ذلك أي حالات تتم فيها مشاركة المفتاح مرة أخرى مع مستخدم آخر بواسطة مستلم المفتاح الأولي.

تُخزَّن دعوة مشاركة المفتاح دون الإفصاح عن هويتها ويتم تأمينها باستخدام خادم مخصص داخل صندوق بريد، وتتم حمايتها بمفتاح تشفير AES 128 أو 256. لا تتم مشاركة مفتاح التشفيرمع الخادم أو أي شخص مطلقًا، باستثناء مستلم المفتاح المقصود، ولا يمكن لأحد فك تشفير الدعوة سوى مستلم المفتاح فقط. عند إنشاء صندوق البريد، يرسل iPhone الخاص بمالك المفتاح مطالبة بجهاز ترتبط بصندوق البريد هذا فقط باستخدام الخادم. عندما يصل iPhone مستلم المفتاح إلى صندوق البريد هذا في البداية، فإنه يقدم مطالبة بجهاز مستلم المفتاح. لا يمكن الوصول إلى صندوق البريد هذا سوى لـ iPhone مالك المفتاح ومستلمه الذي يقدم مطالبات جهاز صالحة. يتم تخصيص قيمة UUID فريدة لكل مطالبة جهاز iPhone وفقًا لـ RFC4122.

باعتباره تدبيرًا أمنيًا إضافيًا، يمكن لمالك المفتاح تشغيل رمز التنشيط المكون من 6 أرقام الذي تم إنشاؤه عشوائيًا والمطلوب إدخاله على iPhone مستلم المفتاح. يُفرَض عدد مرات لمحاولات إدخال الرمز والتحقق من صحتها بواسطة إمّا مالك المفتاح وإمّا خادم الشريك. يجب أن يرسل مالك المفتاح رمز التنشيط هذا إلى مستلم المفتاح كما يجب على مستلم المفتاح تقديم هذا الرمز عند المطالبة للتحقق من صحته بواسطة إمّا مالك المفتاح وإمّا خادم الشريك.

بعد أن يسترد مستلم المفتاح الدعوة، يتم مسحها فورًا من الخادم عن طريق iPhone المستلم. يتميز صندوق البريد الذي يتضمن دعوة مشاركة المفتاح بعمر محدود أيضًا، يتم تعيينه عند إنشاء صندوق البريد ويطبّقه الخادم. يمسح الخادم أي دعوات منتهية الصلاحية تلقائيًا.

حسب الشركة المصنعة الأصلية، قد تتم أيضًا مشاركة المفاتيح مع أجهزة غير تابعة لشركة Apple، لكن طريقة تأمين مشاركة المفاتيح قد تختلف عن طريقة Apple.

الخصوصية والأمن

تستخدم مفاتيح الوصول في Apple Wallet الخصوصية والأمن المدمجين في iPhone وApple Watch بشكل كامل. لا تتم مشاركة معلومات بشأن الوقت أو المكان الذي يستخدم فيه شخص ما مفاتيحه في Apple Wallet مع Apple أو تخزينها على خوادم Apple، وتُخزَّن بيانات الاعتماد بأمان داخل Secure Element للأجهزة المدعومة. يستضيف Secure Element التطبيقات الصغيرة المصممة خصيصًا لإدارة المفاتيح بأمان، ما يضمن عدم إمكانية استخراج أو تسريبها.

قبل توفير أي مفاتيح، يتعين على المستخدم تسجيل الدخول إلى حسابه على iCloud لديه على iPhone متوافق وتفعيل المصادقة بخطوتين لحسابه على iCloud، باستثناء هوية الطالب، (حيث لا تتطلب تشغيل المصادقة بخطوتين).

عندما يبدأ مستخدم عملية التوفير، تحدث خطوات مماثلة لتلك التي تحدث في عملية توفير بطاقة الائتمان والسحب، مثل الربط والتوفير. أثناء المعاملة، يتصل القارئ بـ Secure Element من خلال وحدة تحكم الاتصال بالحقل القريب (NFC) باستخدام قناة آمنة ثابتة.

يتم تحديد عدد الأجهزة، بما في ذلك iPhone و Apple Watch، التي يمكن تزويدها بمفتاح والتحكم فيها بواسطة كل شريك ويمكن أن يختلف الأمر من شريك إلى آخر. يسمح هذا النهج لكل شريك بالتحكم في الحد الأقصى لعدد المفاتيح المتوفرة لكل نوع جهاز بما يتناسب مع احتياجاته الخاصة. ولتحقيق هذا الهدف، تزود Apple الشركاء بنوع الجهاز ومعرّفات الجهاز مجهولة المصدر. تختلف المعرفات لكل شريك لأسباب تتعلق بالخصوصية والأمن.

يتلقى الشركاء أيضًا معرفات مستخدم، تكون مجهولة المصدر وفريدة لكل شريك، مما يسمح لهم بربط المفتاح بحساب المستخدم على iCloud بشكل آمن أثناء عملية التوفير الأولي. يؤدي هذا التدبير إلى منع توفير المفاتيح عن طريق مستخدم آخر في حالة تعرض حساب المستخدم الذي تم إنشاؤه عن طريق الشريك للاختراق - على سبيل المثال - في سيناريو هجوم الاستيلاء على الحساب.

يمكن تعطيل المفاتيح أو إزالتها عن طريق:

- مسح الجهاز عن بُعد باستخدام تحديد الموقع
- تمكين نمط الفقدان باستخدام تحديد الموقع
- تلقي أمر مسح برنامج إدارة الأجهزة المحمولة (MDM) عن بُعد
- إزالة كل البطاقات من صفحة حساب Apple ID الخاصة
- إزالة كل البطاقات من iCloud.com
- إزالة كل البطاقات من Apple Wallet
- إزالة البطاقة في تطبيق جهة الإصدار

في iOS 15.4 أو أحدث، عندما ينقر المستخدم مرتين على الزر الجانبي لـ iPhone مزود ببصمة الوجه أو ينقر مرتين على زر الشاشة الرئيسية لـ iPhone مزود ببصمة الإصبع، لا يتم عرض بطاقته وتفاصيل مفتاح الوصول حتى يقوم بالمصادقة على الجهاز. يلزم وجود بصمة الوجه أو بصمة الإصبع أو المصادقة برمز الدخول قبل تمرير معلومات محددة بما في ذلك تفاصيل حجز الفندق المعروضة في Apple Wallet.

أنواع مفتاح الوصول

ثمة أنواع مختلفة من الوصول من خلال Apple Wallet، مثل الضيافة وشارات الشركات وهويات الطلاب ومفاتيح المنازل ومفاتيح السيارات.

الضيافة

تساعد مفاتيح غرف الفندق الموجودة في Apple Wallet على توفير تجربة سهلة وغير تلامسية بدءًا من تسجيل الوصول إلى تسجيل المغادرة، مع توفير مزايا إضافية إزاء الخصوصية والأمن للنزلاء، بالإضافة إلى بطاقات مفاتيح الفنادق البلاستيكية التقليدية. يمكن لنزلاء الفنادق الموجودين في أماكن مدعومة النقر لإلغاء القفل باستخدام مفاتيح الغرفة االموجودة في Apple Wallet على الـ iPhone وApple Watch Series 4 أو أحدث.

صممت الإمكانات في Apple Wallet خصوصًا لتقليل التواصل للعميل:

- توفير مسبق من تطبيق الفندق لإضافة بطاقة إلى Apple Wallet قبل الإقامة
- بطاقات تسجيل الدخول لبدء عمليات تسجيل الدخول وعمليات تخصيص الغرفة من Apple Wallet
- تحديثات المفتاح اللاحقة لعملية التوفير، لدعم تمديد الإقامات الحالية أو تعديلها
- دعم المفتاح متعدد الغرف لبطاقة واحدة في Apple Wallet
- أرشفة تلقائية للمفاتيح منتهية الصلاحية في Apple Wallet

تذاكر Disney MagicMobile

يمكن أن يضيف المستخدمون تذكرة Disney MagicMobile إلى Apple Wallet على iPhone أو Apple Watch للدخول إلى ملاهي Disney المشاركة. يمكن استخدام تذاكر MagicMobile للدخول من مداخل الملاهي وكذلك في القارئات الأخرى الموجودة في جميع أنحاء الملاهي.

لإضافة تذكرة Disney MagicMobile، بالإضافة إلى تمكين المصادقة بخطوتين على حسابك في iCloud، يجب أن يمتلك المستخدم تذاكر أو حجوزات لملهى مشارك مرتبط بحساب صالح على My Disney Experience. من تطبيق My Disney Experience على iPhone، يمكن أن يختار المستخدم تذكرة واحدة أو أكثر لإضافتها إلى Apple Wallet. إذا كان المستخدم يمتلك Apple Watchمقترنة، تتوفر التذاكر المحددة تلقائيًا على كلٍّ من iPhone المستخدم و Apple Watch المقترنة. النمط السريع مشغَّل بشكل افتراضي للتذاكر المُضافة إلى كلٍّ من iPhone و Apple Watch. لسهولة الاستخدام، عند تشغيل النمط السريع، يتم تشغيله لجميع تذاكر MagicMobile الموجودة حاليًا على الجهاز.

يمكن إضافة تذاكر متعددة إلى جهاز واحد حتى يتمكن المستخدمون من إدارة التذاكر لجميع أعضاء مجموعتهم. يمكن أيضًا أن يختار المستخدمون استخدام تطبيق My Disney Experience لمشاركة التذاكر مع مستخدمين آخرين. بهذه الطريقة، يمكن أن يضيف المستلمون التذاكر المشتركة إلى Apple Wallet على أجهزتهم.

شارات الشركات

يمكن إضافة شارات الموظفين للشركاء المدعومين إلى Apple Wallet على الـ iPhone والـ Apple Watch، ما يتيح للموظفين في جميع أنحاء العالم بالدخول إلى أماكن عملهم دون تلامس. لإضافة شارة، يجب أن يكون لدى الموظف مصادقة متعددة العوامل مفعلة على حسابه المستخدم لتسجيل الدخول إلى التطبيق المقدم من صاحب العمل.

تستفيد شارة الموظف من إمكانات الوصول الخاصة بـ Apple، ما يتيح للمستخدمين الآتي:

- إضافة شارة موظف تلقائيًا إلى Apple Watch المقترنة من خلال توفير الدفع الذي لا يتطلب تثبيت تطبيق الشريك
- الوصول بسلاسة إلى وسائل الراحة المكتبية باستخدام النمط السريع
- إمكانية الوصول إلى مكان العمل حتى بعد نفاد بطارية iPhone

بطاقات هويات الطلاب

في iOS 12 أو أحدث، يمكن للطلاب وأعضاء هيئة التدريس وفريق العمل في الجامعات المشاركة إضافة بطاقات هويات الطلاب الخاصة بهم إلى Apple Wallet على طرز الـ iPhone والـ Apple Watch المدعومة للوصول إلى المواقع والدفع أينما يتم قبول بطاقتهم.

يضيف مستخدم بطاقة هوية الطالب الخاصة به إلى Apple Wallet من خلال تطبيق تقدمه جهة إصدار البطاقة أو المدرسة المشاركة. علمًا بأن العملية التقنية التي يحدث هذا من خلالها هي العملية نفسها الموضحة في إضافة بطاقات الائتمان أو السحب من تطبيق جهة إصدار البطاقة. بالإضافة إلى ذلك، يجب أن تدعم التطبيقات المُصدِرة المصادقة بخطوتين في الحسابات التي تحمي الوصول إلى هويات الطلاب. يمكن إعداد بطاقة على iPhone مستخدم و Apple Watch مقترنة في وقت واحد.

منازل متعددة العائلات

يمكن للمستأجرين والعاملين في المرافق الشريكة المدعومة استخدام مفتاح المنزل في Apple Wallet للدخول إلى المبنى والوحدة والمناطق العامة التابعة لهم. كما يمكن توفير مفتاح المنزل من التطبيق المقدم من الشريك. وبالنسبة إلى الشركاء الذين يدعمون عملية توفير من دون تواصل، يمكن لمديري العقارات إرسال رابط إلى المستأجرين لبدء عملية التوفير باستخدام قناة المراسلة المفضلة لديهم (على سبيل المثال، البريد الإلكتروني أو الرسائل النصية SMS) بحيث لا يحتاج المستأجر سوى إلى النقر فوق الرابط لاسترداد المفتاح. توفر كذلك عينات التطبيق تجربة آمنة وسلسة، ما يجعل من الممكن توفير مفتاح دون تثبيت تطبيق الشريك. لمزيد من المعلومات، انظر مقال دعم Apple استخدام عينات التطبيقات على الـ iPhone.

يمكن أيضًا استخدام مفتاح المنزل لعدة عائلات في النمط السريع ويمكن مشاركته بشكل آمن مع الأصدقاء وأفراد العائلة. لمزيد من المعلومات، انظر مشاركة المفتاح.

مفتاح المنزل

يمكن استخدام مفتاح المنزل في Apple Wallet لفتح أقفال الأبواب المدعومة التي تدعم NFC بنقرة بسيطة على الـ iPhone أو Apple Watch. لمزيد من المعلومات حول كيفية إعداد المستخدم مفتاح المنزل واستخدامه، انظر مقال دعم Apple فتح قفل الباب باستخدام مفتاح المنزل على الـ iPhone.

عندما يقوم المستخدم بإعداد مفتاح منزل، يتلقى جميع المقيمين في منزله كذلك مفتاح المنزل تلقائيًا. لمشاركة مفتاح منزل أو إزالة فرد من منزل مشترك على نطاق واسع، يمكن لمالك المنزل استخدام تطبيق المنزل لإدارة الدعوات والأفراد. عندما يختار مستخدم قبول دعوة للانضمام إلى منزل باستخدام مفتاح المنزل، فيبدأ هذا التطبيق في توفير مفتاح المنزل في Apple Wallet على جهازه. إذا اختار المستخدم مغادرة المنزل أو إذا سحب مالك المنزل إمكانية الوصول، فإن هذه الإجراءات تزيل كذلك مفتاح المنزل من Apple Wallet.

مفتاح السيارة

يكون تخزين مفاتيح السيارة رقميًا في Apple Wallet متاحًا في الأساس في أجهزة الـ iPhone المدعومة وأجهزة Apple Watch المقترنة. ويتم تمثيل مفاتيح السيارة بوصفها بطاقات (أنشأتها Apple نيابةً عن صانع السيارة) في Apple Wallet وتدعم دورة حياة بطاقة Apple Pay بالكامل (نمط الفقدان في iCloud والمسح عن بُعد وحذف البطاقة المحلية ومسح كل المحتوى والإعدادات). وكما هو الحال في بطاقات Apple Pay القياسية، يمكن حذف مفاتيح السيارة المشتركة من الـ iPhone والـ Apple Watch الخاصين بالمالك وفي واجهة Human Machine Interface (HMI).

يمكن استخدام مفاتيح السيارة، على سبيل المثال، لفتح قفل السيارة وقفلها أو فتح حقيبة السيارة وغلقها أو تشغيل الإنذار وإيقافه أو بدء تشغيل المحرك أو ضبط السيارة في وضع القيادة. توفر "المعاملة القياسية" مصادقة متبادلة وهي إلزامية لبدء تشغيل المحرك. قد تستخدم معاملات فتح القفل أو إغلاقه "المعاملات السريعة" عند الحاجة لأسباب تتعلق بالأداء.

يتم إنشاء المفاتيح من خلال توصيل iPhone (أو إقرانه) بسيارة مملوكة ومدعومة. ويتم إنشاء كل المفاتيح داخل Secure Element استنادًا إلى إنشاء مفتاح منحنى القطع الناقص (NIST P-256) في السيارة (ECC-OBKG)، ولا تغادر المفاتيح الخاصة Secure Element مطلقًا. يتم استخدام إما NFC أو مجموعة مكونة من ®Bluetooth منخفض الطاقة (LE) والنطاق العريض للغاية (UWB) للتواصل بين الأجهزة والسيارة. تستخدم إدارة المفاتيح واجهة برمجة التطبيقات للخادم المقدمة من Apple إلى الشركة المصنعة للسيارة بروتوكول TLS مصادَق عليه بشكل متبادل. بعد إقران مفتاح مع iPhone، تستطيع أي Apple Watch مقترنة بهذا الـ iPhone تلقي مفتاح كذلك. عند حذف مفتاح سواء من السيارة أو على الجهاز، لا يمكن استعادته. يمكن تعليق واستئناف المفاتيح الموجودة على الأجهزة المفقودة أو المسروقة، ولكن إعادة توفيرها على جهاز جديد يتطلب اقترانًا أو مشاركة جديدة.

يمكن أيضًا استخدام مفاتيح السيارة في النمط السريع ويمكن مشاركتها بشكل آمن مع الأصدقاء وأفراد العائلة. لمزيد من المعلومات، انظر مشاركة المفتاح. لمزيد من المعلومات عن أمن وخصوصية مفاتيح السيارة الرقمية، انظر أمن مفاتيح السيارة في iOS.

مفتاح سكوتر

في iOS 17 أو أحدث وفي بعض البلدان أو المناطق المعينة التي يوجد بها شركاء مدعومون، يمكن أن يحصل المستخدمون على مفتاح السكوتر المقدم من تطبيق الشريك مباشرةً في Apple Wallet على iPhone مدعوم و Apple Watch مقترنة للأغراض التالية:

- الضغط لقفل السكوتر أو فتح قفله
- الضغط لقفل صندوق السكوتر الخلفي أو فتح قفله (إن كان متوفرًا)

يختص تطبيق صغير مخصص في Secure Element بالتعامل الآمن مع بيانات الاعتماد المشفرة المرتبطة بمفتاح السكوتر ويسمح بإجراء معاملات آمنة باستخدام السكوتر.

على الجزء الخلفي من التذكرة، يمكن للمستخدمين الوصول إلى معلومات إضافية حول السكوتر، مثل آخر أربعة أرقام من رقم تعريف المركبة (VIN) ورخصتها أو لوحة أرقامها. قد تُعتبر هذه المعلومات خاصة ولا يمكن الوصول إليها إلا عند استخدام المصادقة البيومترية أو رمز الدخول للجهاز فقط.

يمكن أيضًا استخدام مفاتيح السكوتر في النمط السريع ويمكن مشاركتها بشكل آمن مع الأصدقاء وأفراد العائلة. لمزيد من المعلومات، انظر مشاركة المفتاح.

أمن مفاتيح السيارة في iOS

يمكن للمطورين دعم استخدام طرق آمنة دون مفاتيح فعلية للتعامل مع السيارة من خلال الـ iPhone المدعوم والـ Apple Watch المقترنة.

إقران المالك

يجب أن يثبت المالك امتلاكه للسيارة (تعتمد الطريقة على الشركة المصنعة للسيارة) ويمكنه بدء عملية الإقران في تطبيق الشركة المصنعة للسيارة، باستخدام رابط بريد إلكتروني يتم تلقيه من الشركة المصنعة للسيارة أو من قائمة السيارة. في جميع الحالات، يجب على المالك تقديم كلمة سر إقران سرية لمرة واحدة إلى الـ iPhone، وتُستخدم لإنشاء قناة إقران آمنة باستخدام بروتوكول SPAKE2+ مع منحنى NIST P-256. عند استخدام التطبيق أو رابط البريد الإلكتروني، يتم نقل كلمة السر تلقائيًا إلى الـ iPhone بينما يجب إدخالها يدويًا عند بدء الإقران من السيارة.

مشاركة المفتاح

يستطيع الـ iPhone المقترن الخاص بالمالك مشاركة المفاتيح مع أفراد العائلة المؤهلين وأجهزة الـ iPhone الخاصة بالأصدقاء (وأجهزة Apple Watch المقترنة الخاصة بهم) عن طريق إرسال دعوة خاصة بالجهاز باستخدام iMessage وخدمة الهوية من Apple (IDS). ويتم تبادل جميع أوامر المشاركة باستخدام ميزة IDS المشفرة بالكامل. يمنع iPhone المقترن الخاص بالمالك قناة IDS من التغيير أثناء عملية المشاركة بهدف الحماية من تحويل الدعوة.

عند قبول الدعوة، يُنشئ الـ iPhone الخاص بفرد العائلة أو صديقه مفتاحًا رقميًا ويُرسل سلسلة شهادة إنشاء المفتاح مرة أخرى إلى الـ iPhone المقترن الخاص بالمالك للتحقق من إنشاء المفتاح على جهاز Apple مصادق. يُوقّع الـ iPhone المقترن الخاص بالمالك مفتاح ECC العام الخاص بالـ iPhone الخاص بفرد العائلة أو أحد الأصدقاء ويُرسل التوقيع مرة أخرى إلى الـ iPhone الخاص بفرد العائلة أو أحد الصديق. تتطلب عملية التوقيع في جهاز المالك مصادقة المستخدم (بصمة الوجه أو بصمة الإصبع أو إدخال رمز دخول) ومقصد مستخدم آمن موصوفة في استخدامات بصمة الوجه وبصمة الإصبع. يُطلب التخويل عند إرسال الدعوة ويتم تخزينه في العنصر الآمن لاستخدامه عندما يقوم الجهاز الصديق بإعادة إرسال طلب التوقيع. يتم تقديم استحقاقات المفتاح إلى السيارة إما عبر الإنترنت بواسطة خادم الشركة المصنعة للمعدات الأصلية للسيارة أو من خلال الاستخدام الأول للمفتاح المشترك في السيارة.

حذف المفتاح

يمكن حذف المفاتيح الموجودة على الجهاز حامل المفاتيح من جهاز المالك وفي السيارة. تكون عمليات الحذف على الـ iPhone حامل المفاتيح فعالة على الفور، حتى إذا كان حامل المفاتيح يستخدم المفتاح. لذلك يظهر تحذير قوي قبل الحذف. قد يكون حذف المفاتيح في السيارة ممكنًا في أي وقت أو قد يكون ممكنًا فقط عندما تكون السيارة متصلة بالإنترنت.

وفي كلتا الحالتين، يتم الإبلاغ عن الحذف على الجهاز حامل المفاتيح أو السيارة إلى خادم تخزين المفاتيح (KIS) الخاص بالشركة المصنعة للسيارة، والذي يسجل المفاتيح الصادرة للسيارة لأغراض التأمين.

يمكن للمالك طلب الحذف من الجزء الخلفي من بطاقة المالك. يتم إرسال الطلب أولاً إلى الشركة المصنعة للسيارة لإزالة المفتاح من السيارة. تحدد الشركة المصنعة للسيارة شروط إزالة المفتاح من السيارة. فقط عند إزالة المفتاح من السيارة، يُرسل خادم الشركة المصنعة للسيارة طلب إنهاء عن بُعد إلى الجهاز حامل المفاتيح.

عندما يتم إنهاء مفتاح في جهاز ما، يقوم التطبيق الصغير الذي يدير مفاتيح السيارة الرقمية بإنشاء شهادة إنهاء موقعة مشفرة، والتي يتم استخدامها كدليل على الحذف بواسطة الشركة المصنعة للسيارة ويتم استخدامها لإزالة المفتاح من خادم KIS.

معاملات NFC القياسية

بالنسبة إلى السيارات التي تستخدم مفتاح NFC، يتم بدء قناة آمنة بين القارئ والـ iPhone عن طريق إنشاء أزواج من المفاتيح المؤقتة على القارئ والـ iPhone. باستخدام طريقة اتفاقية المفتاح، يمكن اشتقاق سر مشترك على كلا الجانبين واستخدامه لإنشاء مفتاح متماثل مشترك باستخدام Diffie-Hellman، وهي وظيفة اشتقاق مفاتيح وتوقيعات من المفتاح طويل الأجل الذي تم إنشاؤه عند الاقتران.

يتم توقيع المفتاح العام المؤقت الذي يتم إنشاؤه على جانب السيارة بالمفتاح الخاص طويل المدى للقارئ، مما يؤدي إلى مصادقة القارئ بواسطة الـ iPhone. من منظور الـ iPhone، تم تصميم هذا البروتوكول لمنع الكشف عن بيانات الخصوصية الحساسة لأي جهة تعترض الاتصال.

وأخيرًا، يستخدم الـ iPhone القناة الآمنة المنشأة لتشفير مُعرِّف مفتاحه العام جنبًا إلى جنب مع التوقيع المحسوب على بيانات القارئ المستمدة من التحدي وبعض البيانات الإضافية الخاصة بالتطبيق. هذا التحقق من توقيع الـ iPhone بواسطة القارئ يسمح للقارئ بمصادقة الجهاز.

المعاملات السريعة

يُنشئ الـ iPhone تشفيرًا مستندًا إلى سر تمت مشاركته سابقًا أثناء معاملة قياسية. ويسمح هذا التشفير للسيارة بمصادقة الجهاز بسرعة في سيناريوهات حساسة للأداء. وبشكل اختياري، يتم إنشاء قناة آمنة بين السيارة والجهاز من خلال اشتقاق مفاتيح الجلسة من سر تمت مشاركته مسبقًا خلال معاملة قياسية وزوج مفاتيح مؤقتة جديد. تقوم قدرة المركبة على إنشاء قناة آمنة بمصادقة السيارة على الـ iPhone.

معاملات BLE/UWB القياسية

بالنسبة إلى السيارات التي تستخدم مفتاح UWB، يتم إنشاء جلسة Bluetooth منخفضة الطاقة (LE) بين السيارة وجهاز الـ iPhone. على غرار معاملة NFC، يتم استخراج سر مشترك من كلا الجانبين واستخدامه لإنشاء جلسة آمنة. تُستخدم هذه الجلسة لاحقًا لاستخراج مفتاح سري بنطاق UWB (URSK) والموافقة عليه. يتم توفير مفتاح URSK إلى أجهزة راديو UWB في جهاز المستخدم وفي السيارة لتفعيل التركيز الدقيق لجهاز المستخدم إلى موقع محدد بالقرب من السيارة أو داخلها. ثم تستخدم السيارة موضع الجهاز لاتخاذ قرارات إزاء السماح بفتح أو تشغيل السيارة. تتمتع مفاتيح URSK بـ TTL محددة سابقًا. ولتجنب انقطاع النطاق عند انتهاء صلاحية TTL، يمكن استخراج مفاتيح URSK سابقًا في SE للجهاز وSEMSH/ للسيارة عندما يكون النطاق الآمن غير نشط ولكن تكون تقنية BLE متصلة. وهذا من شأنه إلغاء الحاجة إلى معاملة قياسية لاستخراج مفتاح URSK جديد في الأوقات الحرجة. يمكن أن ينتقل مفتاح URSK المستخرج سابقًا بسرعة كبيرة إلى أجهزة راديو UWB الخاصة بالسيارة والجهاز لتجنب انقطاع نطاق UWB.

الخصوصية

لا يُخزّن خادم تخزين المفاتيح (KIS) الخاص بالشركة المصنعة للسيارة مُعرِّف الجهاز أو SEID أو Apple ID. بل يخزن فقط مُعرِّفًا متغيرًا، وهو معرف CA المثيل. لا يرتبط هذا المُعرِّف بأي بيانات خاصة في الجهاز أو بواسطة الخادم، ويُحذف عندما يمسح المستخدم جهازه تمامًا (باستخدام مسح جميع المحتويات والإعدادات).

إضافة بطاقات مواصلات و eMoney إلى Apple Wallet

في العديد من الأسواق العالمية، يمكن للمستخدمين إضافة بطاقات مواصلات و eMoney مدعومة إلى Apple Wallet على طرز الـ iPhone والـ Apple Watch المدعومة. حسب المشغّل، قد يتم ذلك عن طريق نقل القيمة أو بطاقة السفر (أو كليهما) من بطاقة حقيقية إلى تمثيل رقمي مقابل في Apple Wallet أو عن طريق توفير بطاقة مواصلات أو eMoney جديدة من Apple Wallet أو تطبيق جهة إصدار البطاقة. بعد إضافة بطاقات المواصلات إلى Apple Wallet، يمكن للمستخدم ركوب المواصلات ببساطة عن طريق تقريب iPhone أو Apple Watch من قارئ بطاقات المواصلات. ويمكن كذلك استخدام بعض بطاقات المواصلات لإجراء عمليات الدفع.

كيف تعمل بطاقات المواصلات والـ eMoney

ترتبط بطاقات المواصلات والـ eMoney المضافة بحساب المستخدم على iCloud. إذا أضاف المستخدم أكثر من بطاقة واحدة إلى Apple Wallet، فقد تتمكن Apple أو جهة إصدار البطاقة من ربط المعلومات الشخصية للمستخدم ومعلومات الحساب المرتبطة بين البطاقات. وتتم حماية بطاقات المواصلات والـ eMoney والمعاملات بواسطة مجموعة من مفاتيح التشفير الهرمية.

أثناء عملية نقل الرصيد من بطاقة حقيقية إلى Apple Wallet، يُطلب من المستخدمين إدخال معلومات خاصة بالبطاقة. وقد يحتاج المستخدم أيضًا إلى تقديم معلومات شخصية لإثبات حيازة البطاقة. عند نقل البطاقات من الـ iPhone إلى Apple Watch، يجب أن يكون كلا الجهازين متصلين بالإنترنت.

يمكن إعادة شحن الرصيد بأموال من بطاقات الائتمان والسحب والبطاقات مسبقة الدفع من خلال Apple Wallet أو من خلال تطبيق جهة إصدار بطاقة المواصلات أو الـ eMoney. لفهم أمن إعادة تحميل الرصيد عند استخدام Apple Pay، انظر الدفع باستخدام البطاقات داخل التطبيقات. لمعرفة كيفية توفير البطاقة من داخل تطبيق جهة إصدار البطاقة، انظر إضافة بطاقات الائتمان أو السحب من تطبيق جهة إصدار البطاقة.

إذا كان التوفير من بطاقة حقيقية مدعومًا، فإن جهة إصدار بطاقة المواصلات أو الـ eMoney تكون بها مفاتيح التشفير اللازمة للمصادقة على البطاقة الحقيقية والتحقق من بيانات المستخدم المُدخلة. وبعد التحقق من البيانات، يمكن للنظام إنشاء رقم حساب الجهاز لـ Secure Element وتنشيط البطاقة المضافة حديثًا في Apple Wallet مع الرصيد المنقول. بالنسبة إلى بعض البطاقات، بعد اكتمال التوفير من البطاقة الحقيقية، يتم تعطيل البطاقة الحقيقية.

بعد انتهاء أي نوع من أنواع التوفير، إذا كان رصيد البطاقة مخزّنًا على الجهاز، يتم تشفيره وتخزينه في تطبيق صغير مخصص في Secure Element. وتكون لدى المشغّل مفاتيح تنفيذ عمليات التشفير على بيانات البطاقة لمعاملات الرصيد.

بشكل افتراضي، يستفيد مستخدم بطاقة المواصلات من تجربة المواصلات السريعة السلسة التي تتيح له الدفع وركوب المواصلات دون الحاجة إلى بصمة الوجه أو بصمة الإصبع أو رمز دخول. يمكن الوصول إلى معلومات مثل المحطات التي تمت زيارتها مؤخرًا وسجل تاريخ المعاملات وتذاكر إضافية بواسطة أي قارئ بطاقات ذكي قريب تم تمكين النمط السريع عليه. يستطيع المستخدم تشغيل متطلب التخويل باستخدام بصمة الوجه أو بصمة الإصبع أو رمز الدخول في إعدادات المحفظة و Apple Pay عن طريق تعطيل المواصلات السريعة. النمط السريع غير مدعوم لبطاقات eMoney.

كما هو الحال مع بطاقات Apple Pay الأخرى، يمكن للمستخدمين تعليق أو إزالة بطاقات eMoney عن طريق:

- مسح الجهاز عن بُعد باستخدام تحديد الموقع
- تمكين نمط الفقدان باستخدام تحديد الموقع
- الدخول في أمر مسح إدارة جهاز الجوال (MDM) عن بُعد
- إزالة كل البطاقات من صفحة حساب Apple ID الخاصة
- إزالة كل البطاقات من iCloud.com
- إزالة كل البطاقات من Apple Wallet
- إزالة البطاقة في تطبيق جهة الإصدار

تقوم خوادم Apple Pay بإخطار مشغّل البطاقة بتعليق هذه البطاقات أو تعطيلها. إذا أزال المستخدم بطاقة المواصلات أو الـ eMoney من جهاز متصل بالإنترنت، يمكن استرداد الرصيد عن طريق إضافة البطاقة مرة أخرى إلى جهاز تم تسجيل الدخول إليه باستخدام Apple ID ذاته. إذا كان الجهاز غير متصل بالإنترنت أو متوقفًا عن التشغيل أو غير صالح للاستخدام، فقد لا يكون الاسترداد ممكنًا.

إضافة بطاقات مواصلات و eMoney إلى Apple Watch الخاصة بفرد من العائلة

في iOS 15 أو أحدث و watchOS 8 أو أحدث، يمكن لمنظم عائلة iCloud إضافة بطاقات مواصلات و eMoney إلى أجهزة Apple Watch الخاصة بأفراد عائلته من خلال تطبيق Watch app على iPhone. عند توفير بطاقة من تلك البطاقات إلى Apple Watch الخاصة بفرد من العائلة، يجب أن تكون الساعة قريبة ومتصلة بجهاز الـ iPhone الخاص بالمنظم باستخدام Wi-Fi أو Bluetooth. يُطلب من أفراد العائلة تشغيل المصادقة بخطوتين لـ Apple ID الخاص بهم حتى يحدث ذلك.

يمكن لأفراد العائلة إرسال طلب لإضافة أموال إلى بطاقة مواصلات أو eMoney من Apple Watch لديهم باستخدام iMessage. يتم حماية محتوى الرسالة باستخدام تشفير كامل، كما هو موضح في نظرة عامة على أمن iMessage. يمكن إضافة أموال إلى بطاقة على Apple Watch الخاصة بأحد أفراد العائلة عن بُعد باستخدام الـ Wi-Fi أو اتصال خلوي. التقارب غير مطلوب.

ملاحظة: قد لا تكون هذه الميزة متوفرة في جميع البلدان أو المناطق.

بطاقات الائتمان والسحب

في بعض المدن، تقبل قارئات بطاقات المواصلات بطاقات EMV (الذكية) لدفع تكاليف ركوب وسائل النقل. عندما يقوم المستخدم بتقديم بطاقة ائتمان أو بطاقة سحب من نوع EMV إلى هذه القارئات، فإن مصادقة المستخدم تكون مطلوبة تمامًا، كما هو الحال عند استخدام "الدفع بواسطة بطاقات الائتمان والسحب في المتاجر".

في iOS 12.3 أو أحدث، يمكن تفعيل بعض بطاقات الائتمان/السحب الحالية من نوع EMV في Apple Wallet من أجل المواصلات السريعة. يتيح "المواصلات السريعة" للمستخدمين دفع رحلة في مشغلات وسائل مواصلات مدعومة من دون طلب بصمة الوجه أو بصمة الإصبع أو رمز دخول. عندما يقدّم مستخدم بطاقة ائتمان أو سحب من نوع EMV، فإن أول بطاقة يتم توفيرها لـ Apple Wallet يتم تفعيلها للمواصلات السريعة. يستطيع المستخدم الضغط على زر المزيد في مقدمة البطاقة في Apple Wallet وتعطيل المواصلات السريعة لتلك البطاقة عن طريق تعيين إعدادات المواصلات السريعة إلى "لا شيء". ويمكن للمستخدم كذلك تحديد بطاقة ائتمان أو سحب مختلفة لتكون بطاقة المواصلات السريعة الخاصة به باستخدام Apple Wallet. يلزم إدخال بصمة الوجه أو بصمة الإصبع أو رمز دخول لإعادة تفعيل أو تحديد بطاقة مختلفة للمواصلات السريعة.

Apple Card و Apple Cash مؤهلة للترانزيت السريع.

الهويات في Apple Wallet

الهويات في Apple Wallet

على iPhone 8 أو أحدث المثبت عليه iOS 15.4 أو أحدث و Apple Watch Series 4 أو أحدث المثبت عليها watchOS 8.4 أو أحدث، يمكن للمستخدمين إضافة هوية الولاية أو رخصة القيادة إلى Apple Wallet والضغط على الـ iPhone أو الـ Apple Watch لتقديمها بسلاسة وأمان عند المواقع المشاركة.

ملاحظة: هذه الميزة متاحة فقط في ولايات الولايات الأمريكية المشاركة.

تستخدم الهويات في Apple Wallet ميزات أمن مدمجة في المكونة المادية والبرامج لجهاز المستخدم للمساعدة على حماية هويته والمساعدة على بقاء معلوماته الشخصية آمنة.

إضافة رخصة قيادة أو هوية ولاية إلى Apple Wallet

على الـ iPhone، يمكن للمستخدمين ببساطة الضغط على زر الإضافة (+) أعلى الشاشة في Apple Wallet لبدء إضافة رخصة القيادة أو الهوية. إذا كان لدى المستخدمين Apple Watch مقترنة في وقت الإعداد، فسيطلب منهم كذلك إضافة رخصة القيادة أو الهوية إلى Apple Wallet على الـ Apple Watch.

في البداية، يطلب من المستخدمين استخدام الـ iPhone لمسح الجزء الأمامي والخلفي من رخصة القيادة الحقيقية أو بطاقة هوية الولاية. يطور الـ iPhone جودة الصور ونوعها ليساعد على ضمان أن الصور المقدمة مقبولة من قِبل جهة الإصدار الخاصة بالولاية. تكون صور بطاقة الهوية تلك مشفرة إلى مفتاح جهة الإصدار الخاصة بالولاية على الجهاز ثم يرسل إلى جهة الإصدار الخاصة بالولاية.

بعد ذلك، يُطلب من المستخدم إكمال سلسلة من حركات الوجه والرأس. يتم تقييم هذه الحركات بواسطة جهاز المستخدم ومن خلال Apple للمساعدة على تقليل مخاطر استخدام شخص ما لصورة أو فيديو أو قناع لمحاولة إضافة هوية شخص آخر إلى Apple Wallet. تُرسل نتائج تحليل هذه الحركات بعد ذلك إلى جهة الإصدار الخاصة بالولاية، وليس فيديو الحركات ذاتها.

للمساعدة على التأكد من أن الشخص الذي يضيف بطاقة الهوية إلى Apple Wallet هو الشخص نفسه الذي تنتمي إليه بطاقة الهوية، يُطلب من المستخدمين التقاط صورة شخصية. قبل إرسال صورة المستخدم إلى جهة الإصدار الخاصة بالولاية، تقارن خوادم Apple وجهاز المستخدم الصورة بمظهر الشخص الذي أجرى سلسلة حركات الوجه والرأس وتساعد على ضمان أن الصورة المقدمة هي لشخص حي يشبه الشخص نفسه الموجود في بطاقة الهوية. بعد القيام بالمقارنة، يتم تشفير الصورة على الجهاز ثم إرسالها إلى جهة الإصدار الخاصة بالولاية لمقارنتها بصورتها المسجلة في ملف الهوية.

أخيرًا، يُطلب من المستخدمين إجراء مصادقة باستخدام بصمة الوجه أو بصمة الإصبع. يربط جهاز المستخدم المقاييس البيومترية لبصمة الوجه أو بصمة الإصبع الفردية المطابقة بهوية الولاية للمساعدة على ضمان أن الشخص الذي أضاف الهوية إلى iPhone هذا هو الوحيد الذي يمكنه تقديمها؛ لا يمكن استخدام معلومات المقاييس البيومترية الأخرى المسجلة للتخويل بتقديم الهوية. يحدث هذا بشكل صارم على الجهاز ولا يتم إرساله إلى جهة الإصدار الخاصة بالولاية.

ستتلقى جهة الإصدار الخاصة بالولاية المعلومات اللازمة لإعداد الهوية الرقمية. يتضمن ذلك صورًا للجزء الأمامي والخلفي لهوية المستخدم والبيانات المقروءة من الرمز الشريطي، PDF417 بالإضافة إلى الصورة الشخصية التي التقطها المستخدم كجزء من عملية التحقق من الهوية. تتلقى كذلك الولاية المصدرة قيمة مكونة من رقم واحد، تستخدم لتساعد على منع الاحتيال، استنادًا إلى أنماط استخدام جهاز المستخدم وبيانات الإعدادات والمعلومات حول Apple ID الشخصي. ومن ثم، فإن القرار النهائي بقبول إضافة الهوية إلى Apple Wallet أو رفضها يعود إلى الولاية المصدرة.

بعد أن تصرح جهة الإصدار الخاصة بالولاية إضافة هوية الولاية أو رخصة القيادة إلى Apple Wallet، يتم إنشاء زوج مفاتيح في Secure Element بواسطة الـ iPhone الذي يربط هوية المستخدم بهذا الجهاز المحدد. في حالة الإضافة إلى Apple Watch، يتم إنشاء زوج مفاتيح في Secure Element بواسطة Apple Watch.

بعد إضافة الهوية إلى الـ iPhone، يتم تخزين البيانات الموجودة في هوية المستخدم في Apple Wallet كنسخة مشفرة ومحمية بواسطة Secure Enclave.

استخدام رخصة قيادة أو هوية ولاية في Apple Wallet مع قارئ هوية

لاستخدام الهوية في Apple Wallet، يحتاج المستخدمون المصادقة باستخدام بصمة الوجه أو بصمة الإصبع في الجهاز المقترن بالهوية في Apple Wallet قبل أن يقدم iPhone المعلومات إلى قارئ الهوية.

لاستخدام الهوية في Apple Wallet على Apple Watch، يحتاج المستخدمون لفتح قفل iPhone باستخدام مظهر بصمة الوجه المقترن أو بصمة الإصبع في كل مرة يرتدون فيها Apple Watch. ومن ثم، يمكنهم استخدام هويتهم في Apple Wallet من دون الحاجة إلى المصادقة مرة أخرى حتى يخلعوا الـ Apple Watch مجددًا. تستفيد هذه الإمكانية من إمكانات الفتح التلقائي الأساسية الموضحة بالتفصيل في أمن النظام لـ watchOS.

عندما يحمل المستخدمون iPhone أو Apple Watch بالقرب من قارئ الهوية أو عند مشاركة هويتهم في تطبيق ما، يرى المستخدمون تنبيهًا فوريًا على الجهاز يعرض المعلومات المحددة التي يتم طلبها والجهة التي تطلبها وما إذا كانت تعتزم تخزينها أم لا. بعد التخويل باستخدام بصمة الوجه أو بصمة الإصبع، يتم تحرير معلومات الهوية المطلوبة من الجهاز.

هام: لا يحتاج المستخدمون إلى فتح قفل جهازهم أو عرضه أو تسليمه لعرض هويتهم.

إذا كان لدى المستخدمين ميزة إمكانية الوصول مثل التحكم الصوتي أو التحكم بالتبديل أو اللمس المساعد بدلاً من تفعيل بصمة الوجه أو بصمة الإصبع، يمكنهم استخدام رمز الدخول للوصول إلى المعلومات وعرضها.

يتبع نقل بيانات الهوية إلى قارئ الهوية معيار ISO/IEC 18013-5، الذي يوفر آليات أمن متعددة متاحة وقادرة على كشف المخاطر الأمنية ومنعها وتخفيف آثارها. وتتكون هذه الآليات من سلامة بيانات الهوية ومكافحة تزييفها وربط الجهاز والموافقة المستنيرة وسرية بيانات المستخدم عبر الارتباطات اللاسلكية.

استخدام رخصة قيادة أو هوية ولاية في Apple Wallet مع تطبيقات iOS

يمكن للمستخدمين كذلك مشاركة معلومات رخصة القيادة أو هوية الولاية الخاصة بهم في Apple Wallet مع تطبيقات iOS. عندما يشارك مستخدم هويته مع تطبيق، تجلب المحفظة شهادة تشفير مسجلة مع مطور التطبيق وتتحقق من صحتها.

ستُستخدم هذه الشهادة لتشفير المعلومات التي وافق المستخدم على مشاركتها. تشفر المحفظة هذه المعلومات باستخدام HPKE ولا تتوفر لـ Apple مطلقًا. تستعلم المحفظة من خوادم Apple بانتظام للتحقق من أن الهوية لا تزال صالحة. وإذا لم يتم إجراء تحقق مؤخرًا، فقد يُجرى تحقق عندما يشارك المستخدم هويته مع تطبيق ما.

أمن الهويات في Apple Wallet

تساعد الميزات التالية على زيادة مستويات الأمن عند استخدام الهويات في Apple Wallet.

سلامة بيانات الهوية ومكافحة تزييفها

تستخدم الهويات في Apple Wallet التوقيع المقدم من جهة الإصدار للسماح لأي قارئ متوافق مع معيار ISO/IEC 18013-5 بالتحقق من هوية المستخدم في Apple Wallet. بالإضافة إلى ذلك، يتم حماية جميع عناصر بيانات الهوية في Wallet بشكل فردي من الاحتيال. يتيح ذلك لقارئ الهوية طلب مجموعة فرعية محددة من عناصر البيانات الموجودة على الهوية في Apple Wallet، وبالنسبة إلى الهوية في Apple Wallet يتيح لها الرد بالمجموعة الفرعية ذاتها، ومن ثم مشاركة البيانات المطلوبة فقط وزيادة خصوصية المستخدم.

ربط الجهاز

تستخدم الهويات في مصادقة Apple Wallet توقيع جهاز للحماية من استنساخ الهوية وإعادة تشغيل عرض هوية. تخزن Apple Wallet المفتاح الخاص لمصادقة الهوية في Secure Element لجهاز iPhone، وثمن ثمَّ تكون الهوية مرتبطة بالجهاز نفسه الذي أنشأت جهة الإصدار الخاصة بالولاية الهوية له.

الموافقة المستنيرة

قد تستخدم الهويات في Apple Wallet المصادقة لتحديد هوية القارئ باستخدام البروتوكول المحدد في معيار ISO/IEC 18013-5. وخلال العرض، إذا كان للقارئ شهادة خاصة به موثوقة بواسطة Apple Wallet، تظهر للمستخدمين أيقونة للتأكيد لهم أنهم يتعاملون مع الجهة المطلوبة.

سرية بيانات المستخدم عبر الارتباطات اللاسلكية

يساعد تشفير الجلسة على ضمان أن جميع معلومات التعريف الشخصية (PII) متبادلة بين الهوية في Apple Wallet وأن قارئ الهوية مشفر. يتم إجراء التشفير بواسطة طبقة التطبيق. لذلك لا يعتمد أمن تشفير الجلسة على الأمن الذي توفره طبقة النقل (على سبيل المثال، NFC و Bluetooth و Wi-Fi).

تساعد الهويات في Apple Wallet على الحفاظ على خصوصية معلومات المستخدمين

تلتزم الهويات في Apple Wallet بعملية "استرداد الجهاز" الموضحة في معيار ISO/IEC 18013-5. يغني استرداد الجهاز عن الحاجة إلى إجراء مكالمات الخادم أثناء العرض، ومن ثم حماية المستخدمين من تعقب Apple وجهة الإصدار.

أمن مدقق الهوية

في iOS 17 أو أحدث، يمكن للشركات والمؤسسات الأمريكية استخدام iPhone لقراءة هويات الأجهزة المحمولة المتوافقة مع معيار ISO 18013-5 مباشرةً بسلاسة وأمان دون الحاجة إلى أجهزة خارجية. يمكن استخدام مدقق الهوية بطريقتين مختلفتين، حسب حالة استخدام التحقق من الصحة:

- **شاشة مدقق الهوية فقط:** يسمح ذلك باستخدام واجهة مستخدم iOS لعرض بيانات الاسم والعمر وصورة الهوية والعمر فوق **"رقم"** لحالات الاستخدام التي تتطلب تأكيدًا مرئيًا فقط. لا تسمح هذه الخدمة بجمع **المعلومات التي تدل على الهوية الشخصية** (PII) التي يمكن إعادة ربطها بالجهة المقدمة.
- **نقل بيانات مدقق الهوية:** تسمح هذه الميزة للتطبيقات بطلب عناصر بيانات إضافية، مثل تاريخ الميلاد والعنوان، للتوافق مع متطلبات التحقق القانوني. يُدار حق الوصول إلى واجهة برمجة تطبيقات نقل بيانات مدقق الهوية من خلال الاستحقاقات، ويجب أن تتوافق التطبيقات مع المتطلبات المرتبطة بكيفية استخدام البيانات. على سبيل المثال، يجب أن تقدِّم التطبيقات متطلبًا قانونيًا لطلب بيانات الهوية. يُطلب من التطبيقات أيضًا الحفاظ على سياسة الخصوصية التي توضح تفاصيل المعالجة أو التخزين أو الاستخدام الآخر لبيانات الهوية المطلوبة.

قراءة هوية الأجهزة المحمولة

يلتزم مدقق الهوية باتباع البروتوكول المُحدَّد في معيار ISO/IEC 18013-5. عندما يطلب تطبيق يستخدم واجهة برمجة تطبيقات مدقق الهوية قراءة هوية الأجهزة المحمولة، تُعرض صفحة - يتحكم فيها iOS - وتطلب من حامل هوية الأجهزة المحمولة تثبيت جهازه بالقرب من قارئ الهوية. تؤدي هذه المشاركة الأولية بتقنية الاتصال قريب المدى (كما هو محدد في معيار ISO/IEC 18013-5، يمكن استخدام رمز QR لبدء عملية تسليم Bluetooth بدلًا من الاتصال قريب المدى) إلى إنشاء اتصال آمن عبر تقنية ®Bluetooth منخفض الطاقة (BLE) بين كلا الجهازين. في هذه المرحلة، يمكن لحامل هوية الأجهزة المحمولة مراجعة المعلومات المطلوبة على أجهزته. بعد موافقة حامل هوية الأجهزة المحمولة، تُنقَل بيانات الهوية المطلوبة إلى جهاز القراءة. تتلقى التطبيقات التي تستخدم واجهة برمجة تطبيقات نقل بيانات مدقق الهوية بيانات الاستجابة للمعالجة، بينما تطّلع التطبيقات التي تستخدم واجهة برمجة تطبيقات شاشة مدقق الهوية فقط على البيانات المعروضة باستخدام iOS مباشرةً.

يوفر معيار ISO/IEC 18013-5 آليات أمنية متعددة لاكتشاف المخاطر الأمنية والتصدي لها والتخفيف من حدتها. ومن بين هذه الآليات، يجري مدقق الهوية عملية التحقق من صحة توقيع كل من جهة الإصدار والجهاز. وبالإضافة إلى ذلك، يدعم مدقق الهوية مصادقة القارئ باتباع البروتوكول المُحدَّد في معيار ISO/IEC 18013-5. يمكن أن تختار التطبيقات عرض أيقونة واسم للتأكد من أن حامل الهوية يتعامل مع الطرف المقصود باستخدام شهادة القارئ.

التحقق من صحة جهة الإصدار والجهاز

للحماية من عمليات التزييف، يجري مدقق الهوية عملية التحقق من صحة توقيع عنصر أمن الأجهزة المحمولة من قبل جهة الإصدار الموثوقة لهوية الأجهزة المحمولة. يوفر نقل بيانات مدقق الهوية أيضًا واجهة برمجة التطبيقات التي تمكِّن التطبيقات من إجراء التحقق من صحة توقيعها، بدلًا من iOS، عند الحاجة. لتقديم ضمان للشركة أو المؤسسة بعدم نسخ هوية الأجهزة المحمولة من جهاز إلى آخر، يجري مدقق الهوية التحقق من صحة التوقيع عبر بيانات الجلسة.

مصادقة القارئ

في وقت التقديم، يتم توقيع طلب قارئ مدقق الهوية باستخدام المفتاح الخاص المرتبط بشهادة مصادقة القارئ الذي يُوثَّق بالجهة الموثوقة Apple Root (CA)، والذي يحتوي على ملحقات x509 المخصصة ذات الصلة للتوضيح للحامل ما إذا كانت الشركة تنوي تخزين البيانات أم لا. إذا كان أحد التطبيقات يهدف إلى عرض الاسم والأيقونة لحامل الهوية، يجب على مسؤول التطبيق التسجيل باستخدام Apple Business Register وتقديم معلومات دقيقة عن العلامة التجارية. بعد نجاح التحقق من المعلومات المقدمة، في وقت المعاملة، تزود شهادة مصادقة القارئ حامل الهوية بالمعلومات حول الكيان من Apple Register عبر شهادة مصادقة القارئ.

iMessage

نظرة عامة على أمن iMessage

Apple iMessage عبارة عن خدمة مراسلة لأجهزة iPhone و iPad و Apple Watch وأجهزة كمبيوتر Mac. وتدعم iMessage الرسائل النصية والمرفقات مثل الصور وجهات الاتصال والمواقع والروابط والمرفقات التي يتم إرفاقها مباشرةً في الرسالة، مثل أيقونة إبهام لأعلى. وتظهر الرسائل على جميع أجهزة المستخدم المسجلة بحيث يمكن متابعة المحادثة من أي جهاز من أجهزة المستخدم. وتستخدم iMessage خدمة الإشعارات اللحظية من Apple (APNs) على نطاق واسع. لا تسجل Apple محتويات الرسائل أو المرفقات، والتي يحميها التشفير الكامل بحيث لا يستطيع أحد سوى المُرسِل والمُستقبِل الوصول إليها. ولا تستطيع Apple فك تشفير البيانات.

عندما يشغّل المستخدم iMessage على أي جهاز، يقوم الجهاز بإنشاء أزواج من مفاتيح التشفير والتوقيع للاستخدام مع الخدمة. بالنسبة للتشفير، يوجد مفتاح تشفير RSA بمعدل 1280 بت وكذلك مفتاح تشفير EC بمعدل 256 بت على منحنى NIST P-256. بالنسبة للتوقيعات، يتم استخدام مفاتيح التوقيع 256 بت من خوارزمية التوقيع الرقمي لمنحنى القطع الناقص (ECDSA). وتُحفظ المفاتيح الخاصة في سلسلة المفاتيح الخاصة بالجهاز ولا تتوفر إلا بعد فتح القفل الأول. تُرسَل المفاتيح العامة إلى خدمة الهوية من Apple (IDS)، حيث يتم ربطها برقم هاتف المستخدم أو عنوان بريده الإلكتروني، بالإضافة إلى عنوان APNs للجهاز.

عندما يُمكّن المستخدمون أجهزة إضافية للاستخدام مع iMessage، تتم إضافة المفاتيح العامة للتشفير والتوقيع وعناوين APNs وأرقام الهواتف المرتبطة الخاصة بهم إلى خدمة الدليل. ويمكن للمستخدمين أيضًا إضافة المزيد من عناوين البريد الإلكتروني، والتي يتم التحقق منها عن طريق إرسال رابط تأكيد. ويتم التحقق من أرقام الهواتف بواسطة شبكة الاتصالات وبطاقة SIM. في بعض الشبكات، يتطلب ذلك استخدام SMS (يتم تقديم مربع حوار تأكيد إلى المستخدم إذا كانت SMS بلا تصنيف). وقد يتطلب الأمر التحقق من رقم الهاتف لاستخدام عددٍ من خدمات الأنظمة بالإضافة إلى iMessage، مثل فيس تايم و iCloud. تعرض جميع أجهزة المستخدم المسجلة رسالة تنبيه عند إضافة جهاز أو رقم هاتف أو عنوان بريد إلكتروني جديد.

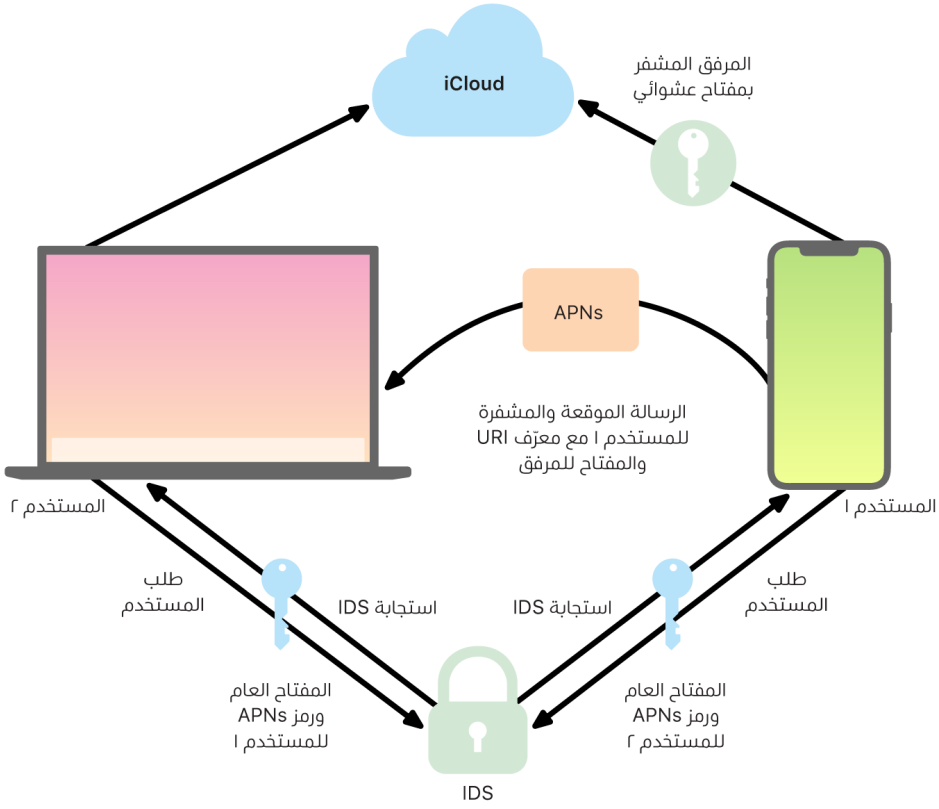
كيفية إرسال واستقبال iMessage للرسائل بشكل آمن.

يبدأ المستخدم محادثة iMessage جديدة بإدخال عنوان أو اسم. وإذا أدخل رقم هاتف أو عنوان بريد إلكتروني، يتصل الجهاز بخدمة الهوية من Apple (IDS) لاسترداد المفاتيح العامة وعناوين APNs لجميع الأجهزة المرتبطة بالمرسل إليه. إذا أدخل المستخدم اسمًا، يستخدم الجهاز أولاً تطبيق جهات اتصال لدى المستخدم لجمع أرقام الهواتف وعناوين البريد الإلكتروني المرتبطة بهذا الاسم، ثم يحصل على المفاتيح العمومية وعناوين APN من IDS.

يتم تشفير رسالة المستخدم الصادرة بشكل فردي لكل جهاز من أجهزة المُستقبِل. ويتم استرداد مفاتيح التشفير العامة ومفاتيح التوقيع الخاصة بأجهزة الاستقبال من IDS. بالنسبة لكل جهاز استقبال، ينشئ جهاز الإرسال قيمة 88 بت عشوائية ويستخدمها كمفتاح HMAC-SHA256 لإنشاء قيمة 40 بت مشتقة من المفتاح العام للمرسل والمُستقبِل والنص العادي. يعمل تسلسل قيمتي 88 بت و 40 بت على إنشاء مفتاح 128 بت الذي يشفّر الرسالة التي تحتوي عليه باستخدام AES في نمط العداد (CTR). وتُستخدم قيمة 40 بت من جانب المُستقبِل للتحقق من تكامل النص العادي غير المشفر. يتم تشفير مفتاح AES هذا لكل رسالة باستخدام RSA-OAEP إلى المفتاح العام لجهاز الاستقبال. يتم بعد ذلك تجزئة مجموعة نص الرسالة المشفرة ومفتاح الرسالة المشفرة باستخدام SHA-1، ويتم توقيع التجزئة مع خوارزمية التوقيع الرقمي لمنحنى القطع الناقص (ECDSA) باستخدام مفتاح التوقيع الخاص لجهاز الإرسال. في iOS 13 أو أحدث و iPadOS 13.1 أو أحدث، قد تستخدم الأجهزة تشفير نظام التشفير المتكامل لمنحنى القطع الناقص (ECIES) بدلاً من تشفير RSA.

تتكون الرسائل الناتجة، رسالة لكل جهاز استقبال، من نص الرسالة المشفرة ومفتاح الرسالة المشفرة والتوقيع الرقمي للمرسل. ثم يتم إرسالها بعد ذلك إلى APNs للتسليم. ولا يتم تشفير بيانات التعريف، مثل طابع الوقت ومعلومات توجيه APN. بينما يتم تشفير الاتصالات مع APNs باستخدام قناة TLS ذات توجيه سري.

تستطيع APNs ترحيل الرسائل التي يصل حجمها إلى 4 أو 16 كيلوبايت فقط، حسب إصدار iOS أو iPadOS. إذا كان نص الرسالة طويلاً جدًا أو إذا تم تضمين مرفق مثل صورة، يتم تشفير المرفق باستخدام AES في نمط CTR بمفتاح 256 بت منشأ عشوائيًا وتحميله إلى iCloud. بعد ذلك، يتم إرسال مفتاح AES الخاص بالمرفق ومعرف الموارد المنتظم (URI) وتجزئة SHA-1 للنموذج المشفر إلى المستلم كمحتويات iMessage، مع حماية سريتها وتكاملها من خلال تشفير iMessage العادي، كما هو مبين في المخطط التالي.



بالنسبة للمحادثات الجماعية، تتكرر هذه العملية لكل مستلم وأجهزته.

على الجانب المستقبِل، يتلقى كل جهاز نسخته من الرسالة من sNPA، وإذا لزم الأمر، يسترد المرفق من duolCi. وتتم مطابقة رقم الهاتف الوارد أو عنوان البريد الإلكتروني للمرسل مع جهات اتصال المستقبِل بحيث يمكن عرض الاسم عندما يكون ذلك ممكنًا.

كما هو الحال مع جميع الإشعارات الموجهة، تُحذف الرسالة من sNPA بعد تسليمها. ولكن على عكس إشعارات sNPA الأخرى، تُوضع رسائل egasseMi في قائمة الانتظار للتسليم إلى الأجهزة غير المتصلة بالإنترنت. وتُخزَّن الرسائل على خوادم elppA لمدة تصل إلى 03 يومًا.

أمن مشاركة اسم وصورة iMessage

تتيح مشاركة اسم وصورة iMessage للمستخدم مشاركة الاسم والصور باستخدام iMessage. ويمكن للمستخدم تحديد معلومات "بطاقتي" الخاصة به أو تخصيص الاسم وتضمين أي صورة يختارها. بينما تستخدم مشاركة اسم وصورة iMessage نظامًا من مرحلتين لتوزيع الاسم والصورة.

يتم تقسيم البيانات في الحقول، كلٌّ مشفرة ومصادق عليها بشكل منفصل وكذلك مصادق عليها مع العملية أدناه. توجد ثلاثة حقول:

- الاسم
- الصورة
- اسم ملف الصورة

تتمثل الخطوة الأولى لإنشاء البيانات في إنشاء مفتاح 128 بت للسجل بشكل عشوائي على الجهاز. ثم يتم اشتقاق مفتاح السجل هذا مع HKDF-HMAC-SHA256 لإنشاء ثلاثة مفاتيح فرعية: Key 1:Key 2:Key 3 = HKDF(record key, "nicknames"). بالنسبة لكل حقل، يتم إنشاء متجه تهيئة (IV) بمعدل 96 بت عشوائي ويتم تشفير البيانات باستخدام AES-CTR والمفتاح 1. يتم بعد ذلك حساب رمز مصادقة الرسالة (MAC) مع HMAC-SHA256 باستخدام المفتاح 2 مع تغطية اسم الحقل وقيمة IV للحقل والنص المشفر للحقل. أخيرًا، تتم سلسلة مجموعة قيم MAC الفردية للحقل ويتم حساب MAC الخاص بها مع HMAC-SHA256 باستخدام المفتاح 3. يتم تخزين MAC سعة 256 بت جنبًا إلى جنب مع البيانات المشفرة. يتم استخدام قيمة 128 بت الأولى لهذا الـ MAC باعتبارها RecordID.

يتم بعد ذلك تخزين هذا السجل المشفر في قاعدة بيانات CloudKit العامة تحت RecordID. ولا يتم تغيير هذا السجل أبدًا وعندما يختار المستخدم تغيير الاسم والصورة، يتم إنشاء سجل جديد مشفر في كل مرة. عندما يختار المستخدم 1 مشاركة الاسم والصورة مع المستخدم 2، يرسل مفتاح السجل مع recordID داخل حمولة iMessage الخاصة به، والتي يتم تشفيرها.

عندما يتلقى جهاز المستخدم 2 حمولة iMessage هذه، يلاحظ أن الحمولة تحتوي على recordID ومفتاح للاسم المستعار والصورة. ينتقل جهاز المستخدم 2 بعد ذلك إلى قاعدة بيانات CloudKit العامة لاسترداد الاسم المشفر والصور المشفرة في معرف السجل ويرسلهما عبر iMessage.

بعد استرداد الرسالة، يفك جهاز المستخدم 2 تشفير الحمولة ويتحقق من التوقيع باستخدام recordID نفسه. إذا تم تجاوز ذلك، يتم تقديم الاسم والصورة إلى المستخدم 2، ويمكنه اختيار إضافة تلك المعلومات إلى جهات الاتصال لديه أو استخدامها في الرسائل.

أمن مراسلة الشركات من Apple

مراسلة الشركات من Apple هي خدمة مراسلة تتيح للمستخدمين التواصل مع الشركات باستخدام تطبيق الرسائل. باستخدام مراسلة الشركات من Apple، يكون المستخدم دائمًا في وضع التحكم في المحادثة. يمكنه أيضًا حذف المحادثة ومنع الشركة من مراسلته في المستقبل. بالنسبة للخصوصية، لا تتلقى الشركة رقم هاتف المستخدم أو عنوان بريده الإلكتروني أو معلومات حساب iCloud الخاص به. بدلاً من ذلك ، يتم إنشاء معرّف فريد مخصص يسمى **المعرّف غير الشفاف** بواسطة خدمة الهوية من Apple (IDS) ومشاركته مع الشركة. يعد المعرّف غير الشفاف معرفًا مميزًا للعلاقة بين Apple ID الخاص بالمستخدم ومعرّف النشاط التجاري. ويكون للمستخدم معرّف غير شفاف مختلف لكل شركة يتواصل معها باستخدام مراسلة الشركات من Apple. يقرر المستخدم ما إذا كان سيشارك معلومات التعريف الشخصية مع الشركة ومتى يتم ذلك، ولا تخزن خدمة مراسلة الشركات من Apple سجل المحادثة إطلاقًا.

تدعم مراسلة الشركات من Apple حسابات Apple ID المُدارة من Apple Business Manager وتحدد ما إذا كانت ممكّنة لـ iMessage وفيس تايم في Apple School Manager.

يتم تشفير الرسائل المرسلة إلى الشركة بين جهاز المستخدم وخوادم المراسلة لدى Apple باستخدام نفس وسائل الأمن المستخدمة على خوادم المراسلة لدى Apple في iMessages. تقوم خوادم المراسلة لدى Apple بفك تشفير هذه الرسائل في ذاكرة RAM، ونقلها إلى الشركة عبر رابط مشفر باستخدام TLS 1.2. لا يتم تخزين الرسائل في شكل غير مشفر أثناء النقل عبر خدمة مراسلة الشركات من Apple. يتم أيضًا إرسال ردود الشركات باستخدام TLS 1.2 إلى خوادم المراسلة لدى Apple، حيث يتم تشفيرها باستخدام المفاتيح العامة الفريدة لكل جهاز مستلم.

إذا كانت أجهزة المستخدم متصلة بالإنترنت، يتم تسليم الرسالة على الفور ولا يتم تخزينها مؤقتًا على خوادم المراسلة لدى Apple. وإذا لم يكن جهاز المستخدم متصلاً بالإنترنت، فسيتم تخزين الرسالة المشفرة مؤقتًا لمدة تصل إلى 30 يومًا لتمكين المستخدم من استلامها عند إعادة اتصال الجهاز بالإنترنت. بمجرد أن يعود الجهاز إلى وضع الاتصال بالإنترنت، يتم تسليم الرسالة وحذفها من ذاكرة التخزين المؤقت. بعد 30 يومًا، تنتهي صلاحية الرسالة المخزنة مؤقتًا التي لم يتم تسليمها ويتم حذفها نهائيًا.

أمن فيس تايم

تطبيق فيس تايم عبارة خدمة مكالمات الفيديو والصوت من Apple. على غرار iMessage، تستخدم مكالمات فيس تايم خدمة الإشعارات اللحظية من Apple (APNs) لإنشاء اتصال أولي بأجهزة المستخدم المسجلة. وتكون محتويات الصوت/الفيديو في مكالمات فيس تايم محمية بالتشفير الكامل، وبذلك لا يستطيع أحد سوى المرسل والمستقبل الوصول إليها. ولا تستطيع Apple فك تشفير البيانات.

يتم إجراء اتصال فيس تايم الأولي من خلال بنية خادم Apple الأساسية التي تنقل حزم البيانات بين أجهزة المستخدمين المسجلة. باستخدام إشعارات APNs ورسائل Session Traversal Utilities for NAT (STUN) عبر الاتصال المُرحَّل، تتحقق الأجهزة من شهادات الهوية وتنشئ سرًا مشتركًا لكل جلسة. ويُستخدم السر المشترك لاشتقاق مفاتيح الجلسة لقنوات الوسائط المتدفقة باستخدام بروتوكول النقل الآمن في الوقت الفعلي (SRTP). يتم تشفير حزم SRTP باستخدام AES256 في نمط العدّاد ويتم المصادقة عليها باستخدام HMAC-SHA1. بعد إعداد الاتصال الأولي والأمن، يستخدم فيس تايم كلاً من STUN و Internet Connectivity Establishment (ICE) لإنشاء اتصال نظير إلى نظير بين الأجهزة، إن أمكن.

يعد فيس تايم الجماعي امتدادًا لتطبيق فيس تايم لدعم ما يصل إلى 33 مشاركًا متزامنًا. وكما هو الحال مع فيس تايم التقليدي الفردي، يتم تشفير المكالمات بالكامل بين أجهزة المشاركين المدعوين. على الرغم من أن فيس تايم الجماعي يُعيد استخدام جزء كبير من البنية الأساسية وتصميم فيس تايم الفردي، تتميز هذه المكالمات الجماعية بآلية إنشاء مفاتيح مبنية على أعلى أسس الأصالة التي توفرها خدمة الهوية من Apple (IDS). ويوفر هذا البروتوكول سرية التوجيه، ما يعني أن اختراق جهاز المستخدم لن يسرّب محتويات المكالمات السابقة. يتم تغليف مفاتيح الجلسة باستخدام AES-SIV ويتم توزيعها بين المشاركين باستخدام بنية تشفير نظام التشفير المتكامل لمنحنى القطع الناقص (ECIES) مع مفاتيح P-256 ECDH سريعة الزوال.

عند إضافة رقم هاتف أو عنوان بريد إلكتروني جديد إلى مكالمة فيس تايم جماعي جارية، تنشئ الأجهزة النشطة مفاتيح وسائط جديدة ولا تشارك أبدًا المفاتيح المستخدمة سابقًا مع الأجهزة التي تمت دعوتها حديثًا.

تحديد الموقع

أمن تطبيق تحديد الموقع

صُمِّم تطبيق تحديد الموقع لأجهزة Apple على أساس تشفير المفتاح العام المتقدم.

نظرة عامة

يجمع تطبيق تحديد الموقع بين العثور على الـ iPhone والعثور على أصدقائي في تطبيق واحد في iOS و iPadOS و macOS. يستطيع تحديد الموقع مساعدة المستخدم على تحديد موقع جهاز مفقود، حتى لو كان Mac غير متصل بالإنترنت. يمكن للجهاز المتصل بالإنترنت الإبلاغ ببساطة عن موقعه للمستخدم عبر iCloud. يعمل تحديد الموقع في وضع عدم الاتصال عن طريق إرسال إشارات Bluetooth قصيرة المدى من الجهاز المفقود يمكن اكتشافها بواسطة أجهزة Apple الأخرى المستخدمة في مكان قريب. ومن ثم تنقل هذه الأجهزة القريبة معلومات الموقع الذي تم اكتشافه للجهاز المفقود إلى iCloud حتى يتمكن المستخدمون من تحديد موقعه في تطبيق تحديد الموقع — كل ذلك مع حماية خصوصية وأمن جميع المستخدمين المعنيين. كما يعمل تطبيق تحديد الموقع مع أي Mac غير متصل بالإنترنت وفي وضع الإسبات.

باستخدام تقنية Bluetooth ومئات الملايين من أجهزة iOS و iPadOS و macOS المستخدمة بنشاط في جميع أنحاء العالم، يمكن لأي مستخدم تحديد موقع جهاز مفقود، حتى إذا كان لا يمكنه الاتصال بشبكة Wi-Fi أو شبكة خلوية. يمكن لأي جهاز مثبت عليه iOS أو iPadOS أو macOS وممكّن عليه "العثور عند عدم الاتصال" في إعدادات تحديد الموقع أن يكون بمثابة "جهاز بحث". وهذا يعني أن الجهاز يستطيع اكتشاف وجود جهاز آخر مفقود في وضع عدم الاتصال باستخدام Bluetooth ثم استخدام اتصاله بالشبكة لإبلاغ مالك الجهاز المفقود بالموقع التقريبي. وإذا كان الجهاز ممكّنًا عليه "العثور عند عدم الاتصال"، فهذا يعني أيضًا أنه يمكن تحديد موقعه بواسطة مشاركين آخرين بالطريقة نفسها. هذا التفاعل بأكمله مشفر تشفيرًا تامًا ومجهول الهوية ومصمم ليكون فعالاً في استخدام البطارية والبيانات. ثمة تأثير ضئيل في عمر البطارية واستخدام خطة البيانات الخلوية، ويتم حماية خصوصية المستخدم بشكل أفضل.

ملاحظة: قد لا يكون تطبيق تحديد الموقع متوفرًا في بعض البلدان أو المناطق.

التشفير الكامل

تم تصميم تطبيق تحديد الموقع على أساس تشفير المفتاح العام المتقدم. عند تمكين "العثور عند عدم الاتصال" في إعدادات تحديد الموقع، يتم إنشاء زوج مفاتيح تشفير خاص P-224 (EC) باسم {d,P} مباشرةً على الجهاز حيث **d** هو المفتاح الخاص بينما **P** هو المفتاح العام. بالإضافة إلى ذلك، تتم تهيئة SK_0 سري 256 بت وعداد $_i$ إلى صفر. ولا يُرسَل زوج المفاتيح الخاص هذا والسر إلى Apple مطلقًا ولا تتم مزامنتهما إلا بين أجهزة المستخدم الأخرى بطريقة مشفرة بالكامل باستخدام سلسلة مفاتيح iCloud. يُستخدم السر والعداد لاشتقاق مفتاح SK_i المتماثل الحالي بالبناء التكراري التالي: $KDF = SK_i(SK_{i-1}$, "update").

بناءً على المفتاح SK_i، يتم حساب عددين صحيحين كبيرين u_i و v_i مع $KDF = (u_i,v_i)(SK_i$, "diversify"). يتم اشتقاق كل من المفتاح الخاص P-224 المشار إليه بالحرف **d** والمفتاح العام المقابل المشار إليه بالحرف **P** باستخدام علاقة تآلفية تتضمن العددين الصحيحين لحساب زوج مفاتيح قصير الأمد: المفتاح الخاص المشتق هو d_i حيث $d_i = d * u_i + v_i$ (باقي قسمة ترتيب منحنى P-224) والمفتاح العام المقابل هو P_i ويتحقق من أن $P_i = u_i*P + G*v_i$.

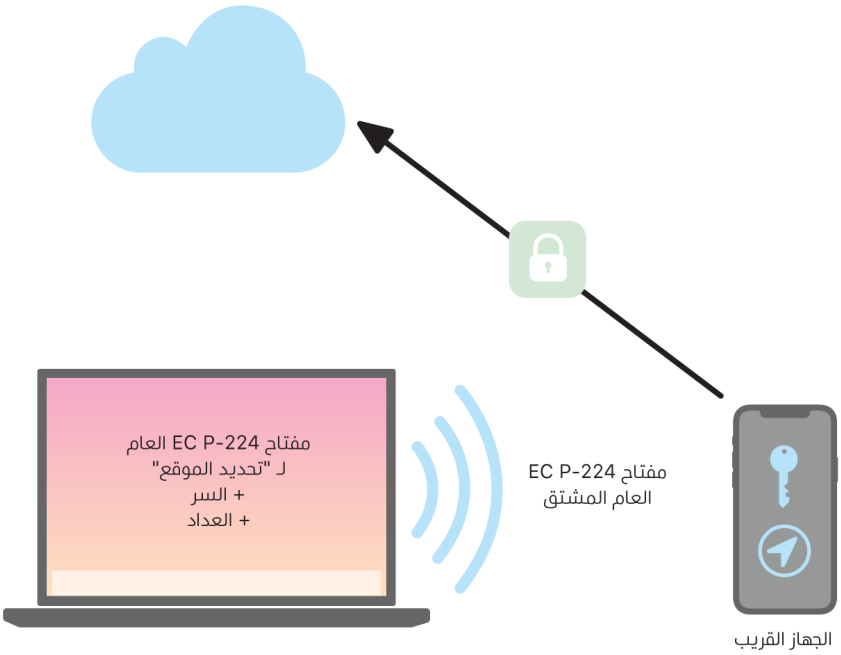
عندما يُفقد جهاز ما ولا يستطيع الاتصال بشبكة Wi-Fi أو شبكة خلوية—على سبيل المثال، عند ترك Macbook Pro على مقعد في حديقة—يبدأ في بث دوريّ للمفتاح العام المشتق P_i لفترة محدودة من الوقت في حمولة Bluetooth. باستخدام P-224، يمكن أن يتناسب تمثيل المفتاح العام مع حمولة Bluetooth واحدة. ومن ثم تستطيع الأجهزة المحيطة المساعدة في العثور على الجهاز غير المتصل بالإنترنت عن طريق تشفير موقعه إلى المفتاح العام. كل 15 دقيقة تقريبًا، يحل مفتاح جديد محل المفتاح العام باستخدام قيمة متزايدة من العداد والعملية المذكورة أعلاه بحيث لا يمكن تعقب المستخدم بواسطة معرف ثابت. وقد تم تصميم آلية الاشتقاق لمنع المفاتيح العامة P_i المختلفة من الارتباط بالجهاز ذاته.

إخفاء هوية المستخدمين والأجهزة

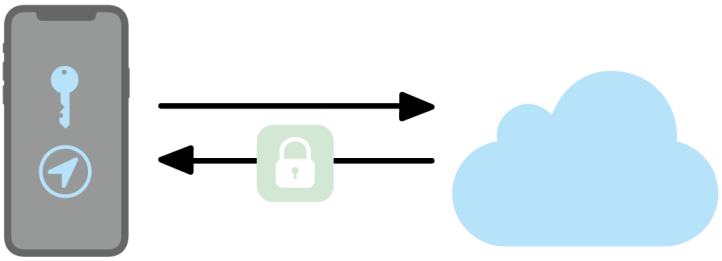
بالإضافة إلى التأكد من تشفير معلومات الموقع والبيانات الأخرى بشكل كامل، تظل هويات المشاركين سرية بالنسبة لبعضهم بعضًا وبالنسبة لشركة Apple. ولا تحتوي حركة المرور المرسلة إلى Apple بواسطة أجهزة البحث على أي معلومات مصادقة في المحتويات أو الرؤوس. نتيجة لذلك، لا تعرف Apple هوية الباحث أو جهازه الذي تم العثور عليه. علاوة على ذلك، لا تسجل Apple معلومات قد يكون من شأنها أن تكشف عن هوية الباحث، ولا تحتفظ بأي معلومات قد تسمح لأي شخص بالربط بين الباحث والمالك. ولا يتلقى مالك الجهاز سوى معلومات الموقع المشفرة التي يتم فك تشفيرها وعرضها في تطبيق تحديد الموقع دون أي إشارة إلى هوية من عثر على الجهاز.

استخدام تطبيق تحديد الموقع لتحديد موقع أجهزة Apple المفقودة

يستطيع أي جهاز من أجهزة Apple ضمن نطاق Bluetooth ممكّن عليه "العثور عند عدم الاتصال" اكتشاف إشارة من جهاز Apple آخر تم تكوينه للسماح بميزة تحديد الموقع وقراءة مفتاح البث الحالي P_i. باستخدام بنية ECIES والمفتاح العام P_i من البث، تُشفِّر أجهزة البحث معلومات موقعها الحالي وتنقلها إلى Apple. يرتبط الموقع المشفر بفهرس خادم يتم حسابه كتجزئة SHA256 لمفتاح P-224 العام P_i الذي تم الحصول عليه من حمولة Bluetooth. ولا تمتلك Apple مفتاح فك التشفير مطلقًا، لذلك لا تستطيع Apple قراءة الموقع المشفر بواسطة جهاز البحث. ويمكن لمالك الجهاز المفقود إعادة بناء الفهرس وفك تشفير الموقع المشفر.



حلتفملا ةفرعمبو .عقوملا نع ثحبلا ةرتفا دادّعلا ميقل عقوتملا قاطنلا ريدقت مترب ،دوقفملا زاهجلا عقوم حيحصت ةلواحم دنع ميقلا ةعومجم ءانبو ةدعاقلا كلذكو ،ثحبلا ةرتفا دادّعلا ميقو قاطنلا يف SK_i ةيرسلا ميقلاو **d** يلاصألا صاخلا P-224 تاملعلا عارجإ دوقفملا زاهجلا عقوم حيحصت مدختسملل كلذكو زاهجلا نكمي امك .اهلمكأب ثحبلا ةرتفا {$(i_م)$SHA256 ،d_i} قيبطتلا كّفي مث نمو .مداخلا نم ةرفشملا عقاوملا لي‌زنتو $(i_م)$SHA256 سرهفلا ميقو ةعومجم مادختسإ مداخلا ىلإ زاهجلا اي‌بيرقت اهّقوم ض‌رعيو ةقباطملا d_i ةصاخلا حيتافملا مادختسإ اي‌تلدم ةرفشملا عقاوملا ريفشت عقوملا حيحصت رثكأ تاملعم نيوكتل ةددعتم ثحبك ةزهجأ نم ةدراولا عقوملا ريراقت كلذكلا قيبطت جمدي كلذ دعبو .قيبطتلا يف دوقفملا .عقوملا نع ةقد



تحديد موقع الأجهزة غير المتصلة بالإنترنت

إذا كان المستخدم قد مكّن العثور على الـ iPhone على جهازه، يتم تمكين "العثور عند عدم الاتصال" بشكل افتراضي عند ترقية الجهاز إلى iOS 13 أو أحدث و iPadOS 13.1 أو أحدث و macOS 10.15 أو أحدث. وقد تم التصميم على هذا النحو لضمان أن تتوفر لكل مستخدم أفضل فرصة ممكنة لتحديد موقع جهازه في حالة فقدانه. ومع ذلك، إذا قرر المستخدم في أي وقت عدم المشاركة، بمكنه تعطيل "العثور عند عدم الاتصال" في إعدادات تحديد الموقع على جهازه. عند تعطيل "العثور عند عدم الاتصال"، يتوقف الجهاز عن العمل كجهاز بحث ولا تستطيع أجهزة البحث الأخرى اكتشافه. ومع ذلك، يظل بإمكان المستخدم تحديد موقع الجهاز طالما يمكنه الاتصال بشبكة Wi-Fi أو شبكة خلوية.

عند تحديد موقع جهاز مفقود غير متصل بالإنترنت، يتلقى المستخدم إشعارًا ورسالة بريد إلكتروني لإعلامه بالعثور على الجهاز. لعرض موقع الجهاز المفقود، يفتح المستخدم تطبيق تحديد الموقع ويحدد علامة تبويب الأجهزة. وبدلاً من إظهار الجهاز على خريطة فارغة كما كان سيظهر قبل تحديد موقع الجهاز، يعرض تحديد الموقع موقعًا على خريطة مع عنوان تقريبي ومعلومات حول توقيت اكتشاف الجهاز. في حالة ظهور المزيد من تقارير الموقع، يتم تحديث كل من الموقع وطابع الوقت الحالي تلقائيًا. بينما لا يمكن للمستخدم تشغيل صوت على جهاز غير متصل بالإنترنت أو مسحه عن بُعد، إلا إنه يمكنه استخدام معلومات الموقع لتقفي أثره أو اتخاذ إجراءات أخرى لمساعدته على استرداده.

الاستمرارية

نظرة عامة على أمن الاستمرارية

تستفيد ميزة الاستمرارية من تقنيات مثل iCloud و Bluetooth و Wi-Fi لتمكين المستخدم من متابعة نشاط من جهاز إلى آخر وإجراء واستقبال المكالمات الهاتفية وإرسال واستلام الرسائل النصية ومشاركة اتصال إنترنت خلوي.

أمن التسليم

تتعامل Apple مع عمليات التسليم بشكل آمن، سواء من جهاز إلى آخر أو بين تطبيق محلي والموقع الإلكتروني—حتى في حالة عمليات التسليم بكميات كبيرة من البيانات.

كيفية عمل التسليم بأمان

باستخدام التسليم، عندما تكون أجهزة iOS و iPadOS و macOS الخاصة بالمستخدم بالقرب من بعضها بعضًا، يستطيع المستخدم تلقائيًا تمرير كل ما يعمل عليه من جهاز إلى الآخر. تتيح التسليم للمستخدم التبديل بين الأجهزة ومواصلة العمل على الفور.

عندما يسجل المستخدم الدخول إلى iCloud على جهاز ثانٍ يدعم التسليم، ينشئ الجهازان إقران Bluetooth منخفض الطاقة (BLE) 4.2 خارج - النطاق باستخدام APNs. يتم تشفير الرسائل الفردية بطريقة تشبه كثيرًا ما يحدث للرسائل في iMessage. بعد إقران الجهازين، ينشئ كل جهاز مفتاح AES متماثلاً 256 بت يتم تخزينه في سلسلة المفاتيح بالجهاز. ويستطيع هذا المفتاح تشفير ومصادقة إعلانات BLE التي تُبلغ النشاط الحالي للجهاز بأجهزة iCloud الأخرى المقترنة باستخدام AES256 في وضع GCM، مع تدابير حماية إعادة التشغيل.

في المرة الأولى التي يتلقى فيها الجهاز إعلانًا من مفتاح جديد، ينشئ اتصال BLE بالجهاز المصدر ويُجري تبادلاً لمفتاح تشفير الإعلانات. ويتم تأمين هذا الاتصال باستخدام تشفير BLE 4.2 القياسي وكذلك تشفير الرسائل الفردية الذي يشبه طريقة تشفير iMessage. في بعض الحالات، تُرسَل هذه الرسائل باستخدام APNs بدلاً من BLE. وتتم حماية حمولة النشاط ونقلها بالطريقة ذاتها المتبعة في iMessage.

التسليم بين التطبيقات الأصلية ومواقع الويب

يتيح التسليم لتطبيقات iOS أو iPadOS أو macOS الأصلية استئناف نشاط المستخدم على صفحات الويب في النطاقات التي يتحكم فيها مطورو التطبيقات بصورة مشروعة. ويتيح أيضًا استئناف نشاط مستخدم التطبيق الأصلي في متصفح الويب.

للمساعدة في منع التطبيقات الأصلية من المطالبة باستئناف مواقع الويب التي لا يتحكم فيها المطور، يجب أن يُظهر التطبيق تحكمًا مشروعًا في نطاقات الويب التي يريد استئنافها. ويتم تأسيس التحكم في نطاق موقع الويب باستخدام آلية بيانات اعتماد الويب المشتركة. لمعرفة التفاصيل، انظر وصول التطبيق إلى كلمات السر المحفوظة. يجب على النظام التحقق من صحة التحكم في اسم النطاق الخاص بالتطبيق قبل السماح للتطبيق بقبول تسليم نشاط المستخدم.

يمكن أن يكون مصدر تسليم صفحة الويب أي متصفح يعتمد واجهات API لتطبيق التسليم. وعندما يعرض المستخدم صفحة الويب، يُعلن النظام عن اسم نطاق صفحة الويب في وحدات بايت إعلان التسليم المشفر. يمكن لأجهزة المستخدم الأخرى فقط فك تشفير وحدات بايت الإعلان.

على جهاز الاستقبال، يكتشف النظام أن التطبيق الأصلي المثبت يقبل التسليم من اسم النطاق المعلن ويعرض أيقونة التطبيق الأصلي كخيار للتسليم. عند بدء التشغيل، يتلقى التطبيق الأصلي عنوان URL الكامل وعنوان صفحة الويب. ولا يتم تمرير أي معلومات أخرى من المتصفح إلى التطبيق الأصلي.

في الاتجاه المعاكس، قد يحدد التطبيق الأصلي عنوان URL احتياطيًا عندما لا يكون جهاز استقبال التسليم مثبتًا عليه التطبيق الأصلي ذاته. وفي هذه الحالة، يعرض النظام المتصفح الافتراضي للمستخدم كخيار لتطبيق التسليم (إذا كان ذلك المتصفح قد اعتمد واجهات API لتطبيق التسليم). عند طلب التسليم، يتم تشغيل المتصفح وتحديد عنوان URL الاحتياطي الذي يوفره التطبيق المصدر. ولا يوجد أي متطلب بأن يقتصر عنوان URL الاحتياطي على أسماء النطاقات التي يتحكم فيها مطور التطبيق الأصلي.

تسليم البيانات الكبيرة

بالإضافة إلى استخدام الميزة الأساسية في التسليم، قد تختار بعض التطبيقات استخدام واجهات API التي تدعم إرسال كميات أكبر من البيانات عبر تقنية Wi-Fi من نظير إلى نظير التي أنشأتها Apple (مثل الإرسال السريع بشكل كبير). على سبيل المثال، يستخدم تطبيق البريد واجهات API هذه لدعم تسليم مسودات البريد التي قد تتضمن مرفقات كبيرة.

عندما يستخدم أحد التطبيقات واجهات API هذه، يبدأ التبادل بين الجهازين تمامًا كما في التسليم. لكن بعد استلام الحمولة الأولية باستخدام تقنية Bluetooth منخفض الطاقة (BLE)، يبدأ جهاز الاستقبال اتصالاً جديدًا عبر Wi-Fi. يتم تشفير هذا الاتصال (باستخدام TLS) ويستمد الثقة من خلال هوية مشتركة من قِبل سلسلة مفاتيح iCloud. يتم التحقق من الهوية الموجودة في الشهادات مقابل هوية المستخدم. كما تُرسَل بيانات الحمولة الإضافية عبر هذا الاتصال المشفر حتى اكتمال النقل.

الحافظة العامة

تستفيد الحافظة العامة من التسليم لنقل محتوى حافظة المستخدم بأمان عبر الأجهزة بحيث يتمكن من النسخ على جهاز واللصق على جهاز آخر. وتتم حماية المحتوى بنفس طريقة حماية بيانات التسليم الأخرى ومشاركته بشكل افتراضي مع الحافظة العامة، إلا إذا اختار مطور التطبيق عدم السماح بالمشاركة.

تستطيع التطبيقات الوصول إلى بيانات الحافظة بغض النظر عما إذا كان المستخدم قد لصق الحافظة في التطبيق أم لا. باستخدام الحافظة العامة، يمتد هذا الوصول إلى البيانات ليشمل التطبيقات التي تعمل على أجهزة المستخدم الأخرى (كما هو محدد من خلال تسجيل دخولها إلى iCloud).

أمن ترحيل المكالمات الخلوية على الـ iPhone

عندما يكون Mac أو iPad أو HomePod الخاص بالمستخدم متصلًا بشبكة Wi-Fi ذاتها المتصل بها iPhone الخاص به، يمكنه إجراء واستقبال المكالمات الهاتفية باستخدام الاتصال الخلوي على iPhone. ويتطلب التكوين تسجيل دخول الأجهزة إلى كل من iCloud وفيس تايم باستخدام حساب Apple ID ذاته.

عند وصول مكالمة واردة، يتم إعلام جميع الأجهزة التي تم تكوينها باستخدام خدمة الإشعارات اللحظية من Apple (APNs)، مع استخدام كل إشعار نفس التشفير الكامل المستخدم في iMessage. وتعرض الأجهزة المتصلة بالشبكة ذاتها واجهة مستخدم إشعارات المكالمات الواردة. عندما يرد المستخدم على المكالمة، يُنقل الصوت بسلاسة من الـ iPhone الخاص بالمستخدم عبر اتصال نظير إلى نظير آمن بين الجهازين.

عند الرد على مكالمة على أي جهاز، يتم إنهاء رنين الأجهزة المقترنة بـ iCloud القريبة من خلال الإعلان لفترة وجيزة باستخدام Bluetooth منخفض الطاقة (BLE). ويتم تشفير وحدات بايت الإعلان باستخدام طريقة إعلانات التسليم ذاتها.

يتم أيضًا ترحيل المكالمات الصادرة إلى الـ iPhone باستخدام خدمة APNs، كما يتم نقل الصوت بطريقة مماثلة عبر رابط نظير إلى نظير آمن بين الأجهزة. ويمكن للمستخدم تعطيل ترحيل المكالمات الهاتفية على جهاز ما بإيقاف مكالمات iPhone خلوية في إعدادات فيس تايم.

أمن تحويل الرسائل النصية على الـ iPhone

يعمل "تحويل الرسائل النصية" تلقائيًا على إرسال رسائل SMS النصية المستلمة على iPhone إلى iPad أو Mac مسجّل لدى المستخدم. ويجب تسجيل دخول كل جهاز إلى خدمة iMessage باستخدام حساب Apple ID ذاته. عند تشغيل تحويل الرسائل النصية، يكون التسجيل تلقائيًا على الأجهزة الموجودة داخل دائرة ثقة المستخدم إذا تم تمكين المصادقة بخطوتين. وخلاف ذلك، يتم التحقق من التسجيل على كل جهاز عن طريق إدخال رمز رقمي عشوائي مكون من ستة أرقام منشأ بواسطة الـ iPhone.

بعد ربط الأجهزة، يقوم الـ iPhone بتشفير وتحويل رسائل SMS النصية الواردة إلى كل جهاز، باستخدام الطرق الموضحة في نظرة عامة على أمن iMessage. ويتم إرسال الردود مرة أخرى إلى الـ iPhone باستخدام الطريقة ذاتها، ثم يرسل الـ iPhone الرد كرسالة نصية باستخدام آلية نقل رسائل SMS الخاصة بشركة الاتصالات. يمكن تشغيل أو إيقاف تحويل الرسائل النصية في إعدادات الرسائل.

أمن نقطة اتصال مباشرة

تقوم نقطة اتصال مباشرة بتوصيل أجهزة Apple الأخرى بنقطة اتصال شخصية على iPhone و iPad. وتستخدم أجهزة iPhone و iPad التي تدعم نقطة اتصال مباشرة تقنية Bluetooth منخفض الطاقة (BLE) لاكتشاف جميع الأجهزة التي سجلت الدخول إلى حساب iCloud الشخصي ذاته والتواصل معها أو الحسابات المستخدمة مع المشاركة العائلية (في iOS 13 و iPadOS). وتستخدم أجهزة كمبيوتر Mac المتوافقة المثبت عليها OS X 10.10 أو أحدث التقنية ذاتها لاكتشاف أجهزة iPhone و iPad المثبت عليها نقطة اتصال مباشرة والتواصل معها.

في البداية، عندما يُدخل المستخدم إعدادات Wi-Fi على الجهاز، يُصدر الجهاز إعلان BLE يحتوي على معرف تتفق عليه جميع الأجهزة التي سجلت الدخول إلى حساب iCloud ذاته. ويتم إنشاء المعرف من DSID (معرف تبادل إشارات الوجهة) المرتبط بحساب iCloud، ويتم تدويره بشكل دوري. عندما تكون الأجهزة الأخرى التي سجلت الدخول إلى حساب iCloud ذاته على مقربة من بعضها وتدعم نقطة اتصال شخصية، فإنها تكتشف الإشارة وتستجيب لها، مما يشير إلى توفر استخدام نقطة اتصال مباشرة.

عندما يختار المستخدم، الذي ليس جزءًا من المشاركة العائلية، أي iPhone أو iPad لنقطة اتصال شخصية، يُرسَل طلب لتشغيل نقطة الاتصال الشخصية إلى هذا الجهاز. ويُرسَل الطلب عبر رابط يتم تشفيره باستخدام تشفير BLE، كما يتم تشفير الطلب بطريقة مماثلة لتشفير iMessage. يستجيب الجهاز بعد ذلك عبر رابط BLE نفسه باستخدام التشفير ذاته لكل رسالة مع توفير معلومات الاتصال بنقطة الاتصال الشخصية.

بالنسبة للمستخدمين الذين يمثلون جزءًا من المشاركة العائلية، تتم مشاركة معلومات اتصال نقطة الاتصال الشخصية بشكل آمن باستخدام آلية مشابهة لتلك المستخدمة من قبل أجهزة HomeKit لمزامنة المعلومات. وعلى وجه التحديد، يتم تأمين الاتصال الذي يشارك معلومات نقطة الاتصال بين المستخدمين باستخدام مفتاح ECDH (Curve25519) سريع الزوال الذي تمت مصادقته باستخدام مفاتيح Ed25519 العامة الخاصة بكل جهاز للمستخدم. وتكون المفاتيح العامة المستخدمة هي تلك التي تمت مزامنتها سابقًا بين أعضاء المشاركة العائلية باستخدام IDS وقت إنشاء المشاركة العائلية.

أمن الشبكات

نظرة عامة على أمن الشبكات

بالإضافة إلى الضمانات المضمّنة التي تستخدمها Apple لحماية البيانات المخزّنة على أجهزة Apple، يوجد العديد من التدابير التي يمكن للمؤسسات اتخاذها للحفاظ على أمن المعلومات أثناء انتقالها من الجهاز وإليه. وكل هذه الاحترازات والتدابير تندرج تحت أمن الشبكات.

نظرًا لأنه يجب أن يمتلك المستخدمون إمكانية الوصول إلى شبكات الشركات من أي مكان في العالم، فمن المهم التأكد من أنهم مصرح لهم بذلك وأن تكون بياناتهم محمية أثناء الإرسال. ولتحقيق هذه الأهداف الأمنية، يعمل كل من iOS و iPadOS و macOS على دمج التقنيات المجرّبة وأحدث المعايير لكل من اتصالات Wi-Fi وشبكة البيانات الخلوية. ولهذا السبب تستخدم أنظمة التشغيل لدينا — وتوفر وصولاً للمطور إلى — بروتوكولات الشبكات القياسية للاتصالات المصادق عليها والمصرح بها والمشفرة.

أمن TLS

يدعم iOS و iPadOS و macOS أمن طبقة النقل (TLS 1.0 و TLS 1.1 و TLS 1.2 و TLS 1.3) وأمن طبقة نقل مخططات البيانات (DTLS). ويدعم بروتوكول TLS كلاً من AES128 و AES256، ويفضل مجموعات التشفير سرية التوجيه. تستخدم تطبيقات الإنترنت مثل سفاري والتقويم والبريد تلقائيًا هذا البروتوكول لتمكين قناة اتصال مشفرة بين الجهاز وخدمات الشبكة. تُسهّل واجهات API عالية المستوى (مثل CFNetwork) على المطورين اعتماد TLS في تطبيقاتهم، بينما توفر واجهات API منخفضة المستوى (مثل .Network framework) تحكمًا دقيقًا. ولا يسمح CFNetwork بـ SSL 3، ويُحظر على التطبيقات التي تستخدم WebKit (مثل سفاري) إجراء اتصال SSL 3.

في iOS 11 أو أحدث و macOS 10.13 أو أحدث، لم تعد شهادات SHA-1 مسموحًا بها لاتصالات TLS ما لم تكن خاضعة لثقة المستخدم. كما أن الشهادات التي تحتوي على مفاتيح RSA تقل عن 2048 بت غير مسموح بها. تم إبطال مجموعة التشفير المتماثلة RC4 في iOS 10 و macOS 10.12. وبشكل افتراضي، عملاء TLS أو الخوادم التي يتم تطبيقها باستخدام واجهات API لـ SecureTransport لا يتم تمكين مجموعات تشفير RC4 بها، ولا يكون بإمكانها الاتصال عندما تكون RC4 هي مجموعة التشفير الوحيدة المتاحة. لمزيد من الأمن، يجب ترقية الخدمات أو التطبيقات التي تتطلب RC4 لاستخدام مجموعات التشفير الآمنة. في iOS 12.1، الشهادات الصادرة بعد 15 أكتوبر 2018 من شهادة جذر يثق بها النظام، يجب تسجيلها في أحد سجلات شفافية الشهادة الموثوق بها حتى يُسمح لها بإجراء اتصالات TLS. وفي iOS 12.2، يتم تمكين TLS 1.3 بشكل افتراضي لواجهات API في كل من Network.framework و NSURLSession. ولا يمكن لعملاء TLS الذين يستخدمون واجهات API لـ SecureTransport استخدام TLS 1.3.

أمن نقل التطبيقات

يوفر أمن نقل التطبيقات متطلبات الاتصال الافتراضية بحيث تلتزم التطبيقات بأفضل ممارسات الاتصالات الآمنة عند استخدام واجهات API في NSURLConnection أو CFURL أو NSURLSession. بشكل افتراضي، يعمل أمن نقل التطبيقات على تقييد تحديد التشفير ليشمل فقط المجموعات التي توفر سرية التوجيه، وتحديدًا:

- ECDHE_ECDSA_AES و ECDHE_RSA_AES في نمط Galois/Counter (GCM)
- نمط تسلسل كتلة التشفير (CBC)

ويكون بإمكان التطبيقات تعطيل متطلبات سرية التوجيه لكل مجال، وفي هذه الحالة تتم إضافة RSA_AES إلى مجموعة الشفرات المتاحة.

يجب أن تدعم الخوادم TLS 1.2 وسرية التوجيه، ويجب أن تكون الشهادات صالحة وموقَّعة باستخدام SHA256 أو أقوى مع مفتاح RSA سعة 2048 بت أو مفتاح منحنى القطع الناقص سعة 256 بت كحد أدنى.

ستفشل اتصالات الشبكة التي لا تستوفي هذه المتطلبات، إلا إذا تجاوز التطبيق أمن نقل التطبيقات. ودائمًا ما تؤدي الشهادات غير الصالحة إلى فشل كبير وعدم الاتصال. يتم تطبيق أمن نقل التطبيقات تلقائيًا على التطبيقات التي يتم تجميعها في iOS 9 أو أحدث و macOS 10.11 أو أحدث.

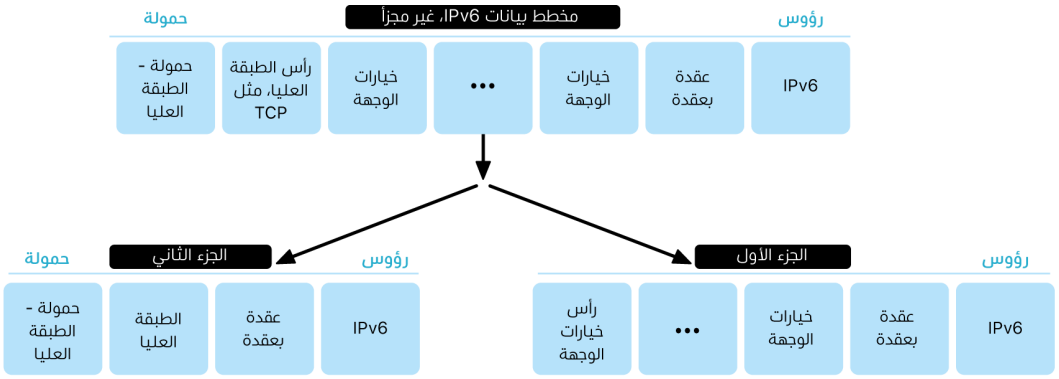
التحقق من صلاحية الشهادة

يتم تنفيذ تقييم الحالة الموثوقة لشهادة TLS وفقًا للمعايير المهنية المعمول بها، على النحو المنصوص عليه في RFC 5280، ويتضمن المعايير الناشئة مثل RFC 6962 (شفافية الشهادة). في iOS 11 أو أحدث و macOS 10.13 أو أحدث، يتم تحديث أجهزة Apple بشكل دوري بقائمة متجددة تضم الشهادات المُلغاة والمقيّدة. يتم تجميع القائمة من قوائم إلغاء الشهادات (CRLs) التي تنشرها كل جهة من جهات إصدار الشهادات الجذرية المضمَّنة التي تثق بها Apple، بالإضافة إلى جهات إصدار الشهادات التابعة لها. وقد تشمل القائمة أيضًا قيودًا أخرى وفقًا لتقدير Apple. يتم الرجوع إلى هذه المعلومات عند استخدام أي وظيفة API للشبكة لإجراء اتصال آمن. في حالة وجود عدد كبير جدًا من الشهادات المُلغاة من جانب إحدى جهات إصدار الشهادات التي تتطلب إدراجها بشكل فردي، قد يتطلب تقييم الثقة بدلاً من ذلك وجود استجابة لحالة الشهادة عبر الإنترنت (OCSP)، ويفشل تقييم الثقة في حالة عدم توفر الاستجابة.

أمن IPv6

توفر جميع أنظمة التشغيل من Apple دعم IPv6، وتنفذ عدة آليات لحماية خصوصية المستخدمين واستقرار حزمة الشبكات. عند استخدام التكوين التلقائي للعنوان عديم الحالة (SLAAC)، يتم إنشاء عناوين IPv6 لكل الواجهات بطريقة تساعد على منع أجهزة التعقب عبر الشبكات وفي الوقت نفسه تسمح بتجربة جيدة للمستخدم من خلال ضمان استقرار العنوان عند عدم حدوث أي تغييرات في الشبكة. تستند خوارزمية إنشاء العناوين إلى عناوين تم إنشاؤها بطريقة مشفرة وفقًا للمعيار RFC 3972، ويتم تحسينها بواسطة مُعدِّل خاص بالواجهة لضمان أن يكون للواجهات المختلفة أيضًا على الشبكة نفسها عناوين مختلفة في النهاية. علاوة على ذلك، يتم إنشاء العناوين المؤقتة بعمر مفضل يبلغ 24 ساعة، ويتم استخدامها افتراضيًا لأي اتصالات جديدة. واستنادًا إلى ميزة عنوان Wi-Fi الخاص المتوفرة في iOS 14 و iPadOS 14 و watchOS 7، يتم إنشاء عنوان رابط محلي فريد لكل شبكة Wi-Fi ينضم إليها الجهاز. ويتم دمج SSID الخاص بالشبكة كعنصر إضافي لإنشاء العنوان، على غرار معامل Network_ID في RFC 7217. يستخدم هذا الأسلوب في iOS 14 و iPadOS 14 و watchOS 7.

للحماية من الهجمات التي تستند إلى رؤوس امتداد IPv6 والتجزئة، تنفذ أجهزة Apple إجراءات الحماية المحددة في RFC 6980 و RFC 7112 و RFC 8021. من بين مقاييس أخرى، تمنع هذه الهجمات حيث لا يمكن العثور على رأس الطبقة العليا إلا في الجزء الثاني (كما هو موضح أدناه)، والذي بدوره يمكن أن يسبب غموضًا في ضوابط الأمن مثل فلاتر الحزم عديمة الحالة.



بالإضافة إلى ذلك، للمساعدة على ضمان موثوقية حزمة IPv6 لأنظمة تشغيل Apple، تفرض أجهزة Apple قيودًا مختلفة على هياكل البيانات المتعلقة بـ IPv6، مثل عدد البادئات لكل واجهة.

أمن الشبكات الخاصة الظاهرية (VPN)

تتطلب خدمات الشبكة الآمنة مثل الشبكات الخاصة الظاهرية (VPN) الحد الأدنى من الإعداد والتكوين للتعامل مع أجهزة iPhone و iPad و Mac.

البروتوكولات المدعومة

وتعمل هذه الأجهزة مع خوادم VPN التي تدعم البروتوكولات وطرق المصادقة التالية:

- IKEv2/IPsec مع المصادقة عن طريق السر المشترك أو شهادات RSA أو شهادات خوارزمية التوقيع الرقمي لمنحنى القطع الناقص (ECDSA) أو EAP-MSCHAPv2 أو EAP-TLS
- SSL-VPN الذي يستخدم تطبيق العميل المناسب من App Store
- L2TP/IPsec مع مصادقة المستخدم عن طريق كلمة سر MS-CHAPV2 ومصادقة الجهاز عن طريق السر المشترك (iOS و iPadOS و macOS) و RSA SecurID أو CRYPTOCard (macOS فقط)
- Cisco IPsec مع مصادقة المستخدم عن طريق كلمة سر و RSA SecurID أو CRYPTOCard ومصادقة الجهاز عن طريق السر المشترك والشهادات (macOS فقط)

عمليات نشر VPN المدعومة

يدعم iOS و iPadOS و macOS التالي:

- **VPN حسب الطلب:** للشبكات التي تستخدم المصادقة المستندة إلى الشهادة. وتحدد سياسات تقنية المعلومات المجالات التي تتطلب اتصال VPN باستخدام ملف تعريف تكوين VPN.
- **VPN لكل تطبيق:** لتسهيل اتصالات VPN على أساس أكثر دقة. تستطيع حلول إدارة جهاز الجوال (MDM) تحديد اتصال لكل تطبيق مُدار ومجالات محددة في سفاري. وهذا يساعد في ضمان انتقال البيانات الآمنة دائمًا من شبكة الشركة وإليها مع عدم انتقال أي بيانات شخصية خاصة بالمستخدم.

يدعم iOS و iPadOS الميزات التالية:

- **VPN دائم التشغيل:** للأجهزة المُدارة من خلال حل MDM والإشراف عليها باستخدام أداة إعداد Apple لـ Mac أو Apple School Manager أو Apple Business Essentials Apple Business Manager. يُلغي VPN دائم التشغيل حاجة المستخدمين إلى تشغيل VPN لتمكين الحماية عند الاتصال بالشبكات الخلوية وشبكات Wi-Fi. كما يتيح للمؤسسة إمكانية التحكم الكامل في حركة المرور على الجهاز من خلال نقل حركة مرور IP بالكامل إلى المؤسسة مرة أخرى. يؤمن التبادل الافتراضي للمعلمات والمفاتيح الخاصة بالتشفير اللاحق،IKEv2، نقل حركة مرور البيانات من خلال تشفير البيانات. ويمكن للمؤسسة مراقبة وتصفية حركة المرور من أجهزتها وإليها وتأمين البيانات داخل شبكتها وتقييد وصول الأجهزة إلى الإنترنت.

أمن Wi-Fi

الوصول الآمن إلى الشبكات اللاسلكية

تدعم جميع أنظمة Apple الأساسية بروتوكولات مصادقة وتشفير Wi-Fi متوافقة مع المعايير المهنية، لتوفير وصول معتمد وسرية تامة عند الاتصال بالشبكات اللاسلكية الآمنة التالية:

- WPA2 شخصي
- WPA2 على مستوى المؤسسة
- WPA2/WPA3 انتقالي
- WPA3 شخصي
- WPA3 على مستوى المؤسسة
- أمن WPA3 على مستوى المؤسسة 192 بت

يعمل كل من WPA2 و WPA3 على مصادقة كل اتصال، ويوفر تشفير AES سعة 128 بت للمساعدة على ضمان سرية البيانات المرسلة عبر الأثير. وهذا يمنح المستخدمين أعلى مستوى من الضمان بأن تظل بياناتهم محمية عند إرسالهم واستقبالهم الاتصالات عبر اتصال شبكة Wi-Fi.

دعم WPA3

WPA3 مدعوم على أجهزة Apple التالية:

- iPhone 7 أو أحدث
- iPad الجيل الخامس أو أحدث
- Apple TV 4K أو أحدث
- Apple Watch series 3 أو أحدث
- أجهزة كمبيوتر Mac (أواخر 2013 أو أحدث، مع 802.11ac أو أحدث)

تدعم الأجهزة الأحدث المصادقة باستخدام أمن WPA3 على مستوى المؤسسة 192 بت، حيث يشمل ذلك دعم تشفير AES سعة 256 بت عند الاتصال بنقاط وصول لاسلكي متوافقة (APs). ويوفر هذا التشفيروسائل حماية أقوى لسرية حركة المرور المرسلة عبر الأثير. يتم دعم أمن WPA3 على مستوى المؤسسة 192 بت في جميع طُرُز iPhone 11 أو أحدث وكل طُرُز iPad بدءًا من الجيل السابع للـ iPad وكل أجهزة كمبيوتر Mac المزودة بسيليكون Apple.

دعم PMF

بالإضافة إلى حماية البيانات المرسلة عبر الأثير، تقوم أنظمة Apple الأساسية بتوسيع نطاقات الحماية على مستوى WPA2 و WPA3 لتشمل إطارات إدارة البث الأحادي والبث المتعدد من خلال خدمة إطار الإدارة المحمي (PMF) المحددة في 802.11w. ويتوفر دعم PMF على أجهزة Apple التالية:

- iPhone 6 أو أحدث
- iPad Air 2 أو أحدث
- Apple TV HD أو أحدث
- Apple Watch series 3 أو أحدث
- أجهزة كمبيوتر Mac (أواخر 2013 أو أحدث، مع 802.11ac أو أحدث)

باستخدام دعم 802.1X، يمكن دمج أجهزة Apple في نطاق واسع من بيئات مصادقة RADIUS. طرق المصادقة اللاسلكية 802.1X المدعومة تشمل EAP-TLS و EAP-TTLS و EAP-FAST و EAP-SIM و PEAPv0 و PEAPv1.

وسائل حماية الأنظمة الأساسية

تعمل أنظمة التشغيل في Apple على حماية الجهاز من الثغرات الأمنية في البرنامج الثابت لمعالج الشبكة. وهذا يعني أن وحدات التحكم في الشبكة المزودة بتقنية Wi-Fi تتمتع بوصول محدود إلى ذاكرة معالج التطبيقات.

- عند استخدام USB أو SDIO (الإدخال/الإخراج الرقمي الآمن) للتفاعل مع معالج الشبكة، لا يستطيع معالج الشبكة بدء معاملات الوصول المباشر للذاكرة (DMA) إلى معالج التطبيق.
- عند استخدام PCIe، يكون كل معالج شبكة على ناقل PCIe معزول خاص به. علمًا بأن وحدة إدارة ذاكرة الإدخال/الإخراج (IOMMU) على كل ناقل PCIe تقيّد وصول DMA الخاص بمعالج الشبكة إلى الذاكرة والموارد فقط التي تحتوي على حِزم الشبكة وهياكل التحكم الخاصة به.

البروتوكولات المهملة

تدعم منتجات Apple بروتوكولات مصادقة وتشفير Wi-Fi المهملة التالية:

- WEP مفتوح، مع كل من مفاتيح 40 بت و104 بت
- WEP مشترك، مع كل من مفاتيح 40 بت و104 بت
- WEP ديناميكي
- بروتوكول تكامل المفتاح المؤقت (TKIP)
- WPA
- WPA/WPA2 انتقالي

لم تعد هذه البروتوكولات آمنة، ولا يُنصح مطلقًا باستخدامها لأسباب تتعلق بالتوافق والموثوقية والأداء والأمن. ويتم دعمها لأغراض التوافق مع الإصدارات القديمة فقط، ويمكن إزالتها في إصدارات البرامج المستقبلية.

نوصي بأن يتم ترحيل عمليات تنفيذ Wi-Fi إلى WPA3 شخصي أو WPA3 على مستوى المؤسسة، لتوفير اتصالات Wi-Fi أكثر قوة وأمنًا وتوافقًا قدر الإمكان.

خصوصية Wi-Fi

عشوائية عنوان MAC

تستخدم أنظمة Apple الأساسية عنوانًا عشوائيًا لوحدة تحكم وصول الوسائط (عنوان MAC) عند إجراء عمليات بحث عن Wi-Fi أثناء عدم الارتباط بشبكة Wi-Fi. ويمكن إجراء عمليات البحث هذه للعثور على شبكة Wi-Fi معروفة والاتصال بها أو لمساعدة خدمات الموقع في التطبيقات التي تستخدم السياج الجغرافي، مثل التذكيرات المستندة إلى الموقع أو تحديد موقع في خرائط Apple. لاحظ أن عمليات البحث عن Wi-Fi التي تحدث أثناء محاولة الاتصال بشبكة Wi-Fi مفضلة لا يتم جعلها عشوائية. دعم عشوائية عنوان MAC لشبكة Wi-Fi متوفر على iPhone 5 أو أحدث.

تستخدم أنظمة Apple الأساسية أيضًا عنوان MAC عشوائيًا عند إجراء عمليات بحث لتفريغ الشبكة المفضلة المحسّن (ePNO) عندما لا يكون الجهاز مرتبطًا بشبكة Wi-Fi أو عندما يكون معالج الجهاز في حالة إسبات. ويتم تشغيل عمليات بحث ePNO عندما يستخدم الجهاز خدمات الموقع في التطبيقات التي تستخدم السياج الجغرافي، مثل التذكيرات المستندة إلى الموقع التي تحدد ما إذا كان الجهاز بالقرب من موقع معين أم لا.

نظرًا لأن عنوان MAC الخاص بالجهاز يتغير عند قطع اتصاله بشبكة Wi-Fi، فلا يمكن استخدامه لتعقب الجهاز باستمرار بواسطة المراقبين السلبيين لحركة مرور Wi-Fi، حتى عندما يكون الجهاز متصلاً بشبكة خلوية. أبلغت Apple الجهات المصنعة لشبكات Wi-Fi أن عمليات البحث عن Wi-Fi في iOS و iPadOS تستخدم عنوان MAC عشوائيًا، وأنه لا يمكن لشركة Apple أو الجهات المصنعة التنبؤ بعناوين MAC العشوائية هذه.

في iOS 14 أو أحدث و iPadOS 14 أو أحدث و watchOS 7 أو أحدث، عند اتصال iPhone أو iPad أو Apple Watch بشبكة Wi-Fi، يعرّف نفسه بعنوان MAC (عشوائي) فريد لكل شبكة. ويمكن تعطيل هذه الميزة إما بواسطة المستخدم أو باستخدام خيار جديد في حمولة Wi-Fi. في ظل ظروف معينة، يرجع الجهاز إلى عنوان MAC الفعلي.

لمزيد من المعلومات، انظر مقال دعم Apple استخدام عناوين Wi-Fi خاصة في iPhone و iPad و Apple Watch.

عشوائية الرقم التسلسلي لإطار Wi-Fi

تتضمن إطارات Wi-Fi رقمًا تسلسليًا، يُستخدم بواسطة بروتوكول 802.11 منخفض المستوى لتمكين اتصالات Wi-Fi الفعالة والموثوقة. ونظرًا لأن هذه الأرقام التسلسلية تزداد على كل إطار مرسل، يمكن استخدامها لربط المعلومات المرسلة أثناء عمليات البحث عن Wi-Fi، مع الإطارات الأخرى المرسلة بواسطة الجهاز نفسه.

لتجنب ذلك، تقوم أجهزة Apple بالتوزيع العشوائي للأرقام التسلسلية كلما تم تغيير عنوان MAC إلى عنوان عشوائي جديد. وذلك يتضمن التوزيع العشوائي للأرقام التسلسلية لكل طلب بحث جديد يتم تشغيله أثناء عدم ارتباط الجهاز. هذا التوزيع العشوائي مدعوم على الأجهزة التالية:

- iPhone 7 أو أحدث
- iPad الجيل الخامس أو أحدث
- Apple TV 4K أو أحدث
- Apple Watch series 3 أو أحدث
- iMac Pro (ريتنا 5K، 27 بوصة، 2017) أو أحدث
- Macbook Pro (13 بوصة، 2018) أو أحدث
- Macbook Pro (15 بوصة، 2018) أو أحدث
- Macbook Air (ريتنا، 13 بوصة، 2018) أو أحدث

- Mac Mini (2018) أو أحدث
- iMac (ريتنا 4K، 21,5 بوصة، 2019) أو أحدث
- iMac (ريتنا 5K، 27 بوصة، 2019) أو أحدث
- Mac Pro (2019) أو أحدث

اتصالات Wi-Fi

تنشئ Apple عناوين MAC عشوائية لاتصالات Wi-Fi من نظير إلى نظير المستخدمة في الإرسال السريع والبث السريع. وتُستخدم العناوين العشوائية أيضًا لنقطة الاتصال الشخصية في iOS و iPadOS (مع بطاقة SIM) ولمشاركة الإنترنت في macOS.

يتم إنشاء عناوين عشوائية جديدة عند بدء واجهات الشبكة هذه، ويتم إنشاء عناوين فريدة بشكل مستقل لكل واجهة حسب الحاجة.

الشبكات المخفية

يتم تعريف شبكات Wi-Fi باسم الشبكة الخاص بها، والمعروف باسم **معرِّف مجموعة الخدمات (SSID)**. ويتم تكوين بعض شبكات Wi-Fi لإخفاء SSID الخاص بها، مما يؤدي إلى عدم بث نقطة الوصول اللاسلكية لاسم الشبكة. وتُعرف هذه باسم **الشبكات المخفية**. يكتشف iPhone 6s والأجهزة الأحدث تلقائيًا الحالات التي تكون الشبكة فيها مخفية. إذا كانت الشبكة مخفية، يرسل جهاز iOS أو iPadOS طلب فحص يتضمن SSID في البحث — لا شيء غير ذلك. وهذا يساعد على منع الجهاز من بث أسماء الشبكات المخفية التي كان المستخدم متصلاً بها من قبل، وبالتالي ضمان الخصوصية بشكل أكبر.

أمن Bluetooth

هناك نوعان من Bluetooth في أجهزة Apple، هما Bluetooth الكلاسيكي و Bluetooth منخفض الطاقة (BLE). يتضمن نموذج أمن Bluetooth لكلا الإصدارين ميزات الأمن المميزة التالية:

- **الاقتران:** عملية إنشاء مفتاح أو أكثر من المفاتيح السرية المشتركة
- **الربط:** تخزين المفاتيح المنشأة أثناء الاقتران لاستخدامها في الاتصالات اللاحقة من أجل تكوين زوج جهاز موثوق به
- **المصادقة:** التحقق من أن الجهازين لهما نفس المفاتيح
- **التشفير:** سرية الرسالة
- **تكامل الرسالة:** الحماية ضد تزوير الرسائل
- **الاقتران البسيط الآمن:** الحماية ضد التنصت السلبي والحماية ضد هجمات الوسيط

أضاف الإصدار 4.1 من Bluetooth ميزة الاتصالات الآمنة إلى النقل المادي (BR/EDR) من Bluetooth الكلاسيكي.

فيما يلي ميزات الأمن لكل نوع من أنواع Bluetooth.

الدعم	Bluetooth الكلاسيكي	Bluetooth منخفض الطاقة
الاقتران	منحنى القطع الناقص P-256	الخوارزميات المعتمدة من FIPS (AES-CMAC) ومنحنى القطع الناقص P-256)
الربط	تُخزَّن معلومات الاقتران في موقع آمن في أجهزة iOS و iPadOS و macOS و tvOS و watchOS	تُخزَّن معلومات الاقتران في موقع آمن في أجهزة iOS و iPadOS و macOS و tvOS و watchOS
المصادقة	الخوارزميات المعتمدة من FIPS (HMAC-SHA256 و AES-CTR)	الخوارزميات المعتمدة من FIPS
التشفير	تشفير AES-CCM الذي يتم تنفيذه في وحدة التحكم	تشفير AES-CCM الذي يتم تنفيذه في وحدة التحكم
تكامل الرسالة	AES-CCM، يُستخدم لتكامل الرسالة	AES-CCM، يُستخدم لتكامل الرسالة
الاقتران البسيط الآمن: الحماية ضد التنصت السلبي	تبادل منحنى القطع الناقص Diffie-Hellman سريع الزوال (ECDHE)	تبادل منحنى القطع الناقص Diffie-Hellman (ECDHE)
الاقتران البسيط الآمن: الحماية ضد هجمات الوسيط (MITM)	طريقتان رقميتان يساعد فيهما المستخدم: المقارنة العددية أو إدخال مفتاح المرور	طريقتان رقميتان يساعد فيهما المستخدم: المقارنة العددية أو إدخال مفتاح المرور تتطلب عمليات الاقتران استجابة من المستخدم، بما في ذلك جميع أنماط الاقتران بخلاف MITM
Bluetooth 4.1 أو أحدث	iMac أواخر 2015 أو أحدث Macbook Pro أوائل 2015 أو أحدث	iOS 9 أو أحدث iPadOS 13.1 أو أحدث macOS 10.12 أو أحدث tvOS 9 أو أحدث watchOS 2.0 أو أحدث
Bluetooth 4.2 أو أحدث	iPhone 6 أو أحدث	iOS 9 أو أحدث iPadOS 13.1 أو أحدث macOS 10.12 أو أحدث tvOS 9 أو أحدث watchOS 2.0 أو أحدث

خصوصية Bluetooth منخفض الطاقة

للمساعدة في تأمين خصوصية المستخدم، تشتمل BLE على الميزتين التاليتين: عشوائية العنوان واشتقاق مفتاح النقل المتقاطع.

عشوائية العنوان ميزة تقلل من القدرة على تعقب جهاز BLE على مدار فترة زمنية من خلال تغيير عنوان جهاز Bluetooth على أساس متكرر. ليتمكن الجهاز الذي يستخدم ميزة الخصوصية من إعادة الاتصال بالأجهزة المعروفة، يجب أن يكون عنوان الجهاز، المشار إليه باسم **العنوان الخاص**، قابلاً للحل من قِبل الجهاز الآخر. يتم إنشاء العنوان الخاص باستخدام مفتاح حل هوية الجهاز الذي تم تبادله أثناء إجراء الاقتران.

يتمتع كل من iOS 13 أو أحدث و iPadOS 13.1 أو أحدث بالقدرة على اشتقاق مفاتيح الربط عبر عمليات النقل، وهي ميزة معروفة باسم **اشتقاق مفتاح النقل المشترك**. على سبيل المثال، يمكن استخدام مفتاح رابط تم إنشاؤه بواسطة BLE لاشتقاق مفتاح رابط Bluetooth كلاسيكي. بالإضافة إلى ذلك، أضافت Apple دعم Bluetooth الكلاسيكي إلى BLE للأجهزة التي تدعم ميزة الاتصالات الآمنة التي كانت مقدمة في مواصفات Bluetooth الأساسية 4.1 (انظر مواصفات Bluetooth الأساسية 5.1).

تقنية النطاق فائق العرض في iOS

تستخدم شريحة U1 الجديدة التي صممتها Apple تقنية النطاق فائق العرض لتوفير الوعي المكاني—السماح لكل من iPhone 11 و iPhone 11 Pro و iPhone 11 Pro Max أو طرز الـ iPhone الأحدث بتحديد موقع أجهزة Apple المزودة بشريحة U1 على وجه الدقة. تستخدم تقنية النطاق فائق العرض التقنية ذاتها لتخصيص البيانات الموجودة في أجهزة Apple المدعومة الأخرى:

- عشوائية عنوان MAC
- عشوائية الرقم التسلسلي لإطار Wi-Fi

أمن تسجيل الدخول الموحد

تسجيل الدخول الموحد

يدعم iOS و iPadOS المصادقة لشبكات المؤسسات من خلال تسجيل الدخول الموحد (SSO). ويعمل SSO مع الشبكات المستندة إلى Kerberos لمصادقة المستخدمين للخدمات المخوّل لهم الوصول إليها. ويمكن استخدام SSO لمجموعة من أنشطة الشبكات، من جلسات سفاري الآمنة حتى تطبيقات الجهات الخارجية. المصادقة المستندة إلى الشهادة، مثل PKINIT، مدعومة أيضًا.

يدعم macOS المصادقة لشبكات المؤسسات باستخدام Kerberos. ويمكن للتطبيقات استخدام Kerberos لمصادقة المستخدمين للخدمات المخوّل لهم الوصول إليها. كما يمكن أيضًا استخدام Kerberos لمجموعة من أنشطة الشبكات، من جلسات سفاري الآمنة ومصادقة نظام ملف الشبكة حتى تطبيقات الجهات الخارجية. المصادقة المستندة إلى الشهادة مدعومة، على الرغم من أن اعتماد التطبيق لواجهة API خاصة بالمطوّر مطلوب.

يستخدم SSO في iOS و iPadOS و macOS رموز SPNEGO وبروتوكول HTTP Negotiate للعمل مع بوابات المصادقة المستندة إلى Kerberos وأنظمة المصادقة المتكاملة لـ Windows التي تدعم تذاكر Kerberos. ويستند دعم SSO إلى مشروع Heimdal مفتوح المصدر.

أنواع التشفير التالية مدعومة في iOS و iPadOS و macOS:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

يدعم سفاري ميزة SSO، كما يمكن أيضًا تكوين تطبيقات الجهات الخارجية التي تستخدم واجهات API لشبكات iOS و iPadOS القياسية بغرض استخدامها. لتكوين SSO، يدعم iOS و iPadOS حمولة ملف تعريف تكوين تتيح لحلول إدارة جهاز الجوال (MDM) دفع الإعدادات الضرورية إلى أسفل. ويتضمن ذلك تعيين اسم المستخدم الرئيسي (أي، حساب مستخدم Active Directory) وإعدادات مجال Kerberos، بالإضافة إلى تكوين التطبيقات وعناوين URL الخاصة بسفاري على الويب التي يجب السماح لها باستخدام SSO.

تسجيل الدخول الموحد القابل للتجديد

يمكن لمطوري التطبيقات توفير عمليات تنفيذ تسجيل الدخول الموحد الخاصة بهم باستخدام ملحقات SSO. يتم استدعاء ملحقات SSO عندما يحتاج تطبيق أصلي أو تطبيق ويب إلى استخدام أي موفر هوية لمصادقة المستخدم. ويمكن للمطورين توفير نوعين من الملحقات: تلك التي تُعيد التوجيه إلى HTTPS وتلك التي تستخدم آلية التحدي/الاستجابة مثل Kerberos. وذلك يتيح إمكانية دعم أنظمة مصادقة OpenID و OAuth و SAML2 و Kerberos بواسطة تسجيل الدخول الموحد القابل للتجديد. يمكن لملحقات SSO كذلك دعم مصادقة macOS عن طريق استخدام بروتوكول SSO أصلي، حيث يسمح باسترداد رموز SSO خلال تسجيل الدخول على macOS.

لاستخدام أحد ملحقات تسجيل الدخول الموحد، يمكن للتطبيق إما استخدام واجهة برمجة التطبيقات AuthenticationServices أو الاعتماد على آلية اعتراض عناوين URL التي يوفرها نظام التشغيل. يوفر WebKit و CFNetwork طبقة اعتراض تتيح الدعم السلس لتسجيل الدخول الموحد لأي تطبيق أصلي أو تطبيق WebKit. لكي يتم استدعاء أحد ملحقات تسجيل الدخول الموحد، يجب تثبيت أي تكوين يوفره المسؤول من خلال أحد ملفات تعريف إدارة جهاز الجوال (MDM). بالإضافة إلى ذلك، يجب أن تستخدم ملحقات نوع إعادة التوجيه حمولة المجالات المرتبطة لإثبات أن خادم الهوية الذي تدعمه يدرك وجودها.

الملحق الوحيد المتوفر مع نظام التشغيل هو ملحق KerberOS SSO.

أمن الإرسال السريع

تستخدم أجهزة Apple التي تدعم الإرسال السريع تقنية Bluetooth منخفض الطاقة (BLE) وتقنية Wi-Fi من نظير إلى نظير التي أنشأتها Apple لإرسال الملفات والمعلومات إلى الأجهزة القريبة، بما في ذلك أجهزة iOS التي تدعم الإرسال السريع وأجهزة iPad المثبت عليها iOS 7 أو أحدث وأجهزة كمبيوتر Mac المثبت عليها OS X 10.11 أو أحدث. يتم استخدام تردد Wi-Fi اللاسلكي للاتصال مباشرة بين الأجهزة دون استخدام أي اتصال إنترنت أو نقطة وصول (AP) لاسلكية. يكون هذا الاتصال مشفرًا باستخدام TLS.

يتم تعيين الإرسال السريع للمشاركة مع جهات الاتصال فقط بشكل افتراضي. ويمكن للمستخدمين أيضًا اختيار استخدام الإرسال السريع للمشاركة مع الجميع أو إيقاف الميزة بالكامل. يمكن للمؤسسات تقييد استخدام الإرسال السريع للأجهزة أو التطبيقات التي تتم إدارتها باستخدام حل إدارة جهاز الجوال (MDM).

عملية تشغيل الإرسال السريع

يستخدم الإرسال السريع خدمات iCloud لمساعدة المستخدمين على المصادقة. عندما يسجّل المستخدم الدخول إلى iCloud، يتم تخزين هوية RSA سعة 2048 بت على الجهاز وعندما يقوم المستخدم بتشغيل الإرسال السريع، يتم إنشاء تجزئة هوية قصيرة للإرسال السريع بناءً على عناوين البريد الإلكتروني وأرقام الهواتف المرتبطة بحساب Apple ID الخاص بالمستخدم.

عندما يختار المستخدم الإرسال السريع كطريقة لمشاركة العنصر، يُصدر جهاز الإرسال إشارة الإرسال السريع عبر تقنية BLE تتضمن تجزئة الهوية القصيرة للإرسال السريع الخاصة بالمستخدم. أجهزة Apple الأخرى التي تكون نشطة وعلى مقربة ومشغّل عليها الإرسال السريع، تكتشف الإشارة وتستجيب باستخدام Wi-Fi من نظير إلى نظير، بحيث يمكن لجهاز الإرسال اكتشاف هوية أي أجهزة مستجيبة.

في نمط جهات الاتصال فقط، تتم مقارنة تجزئة الهوية القصيرة للإرسال السريع المُستلَمة مع تجزئات الأشخاص في تطبيق جهات الاتصال في جهاز الاستقبال. وفي حالة العثور على تطابق، يستجيب جهاز الاستقبال عبر Wi-Fi من نظير إلى نظير مع معلومات هويته. وإذا لم يوجد تطابق، فلا يستجيب الجهاز.

في نمط الجميع، تُستخدم العملية الكلية ذاتها. لكن يستجيب جهاز الاستقبال حتى إذا لم يوجد تطابق في تطبيق جهات الاتصال بالجهاز.

ثم يبدأ جهاز الإرسال اتصال الإرسال السريع باستخدام Wi-Fi من نظير إلى نظير، باستخدام هذا الاتصال لإرسال تجزئة هوية طويلة إلى جهاز الاستقبال. وإذا تطابقت تجزئة الهوية الطويلة مع تجزئة شخص معروف في جهات الاتصال بجهاز الاستقبال، يستجيب جهاز الاستقبال بتجزئة هويته الطويلة.

إذا تم التحقق من التجزئات، يتم عرض الاسم الأول والصورة للمستلم (إذا كان موجودًا في جهات الاتصال) في ورقة مشاركة الإرسال السريع الخاصة بالمرسل. في iOS و iPadOS، يتم عرضهما في قسم "الأشخاص" أو "الأجهزة". يتم عرض الأجهزة التي لم يتم التحقق منها أو مصادقتها في ورقة مشاركة الإرسال السريع الخاصة بالمرسل وعليها أيقونة صورة ظلية واسم الجهاز، كما هو محدد في الإعدادات > عام > حول > الاسم. وفي iOS و iPadOS، يتم وضعها في قسم "أشخاص آخرون" في ورقة مشاركة الإرسال السريع.

يمكن بعد ذلك للمستخدم المرسل تحديد من يريد المشاركة معه. عقب انتهاء المستخدم من التحديد، يبدأ جهاز الإرسال اتصال (TLS) مشفرًا مع جهاز الاستقبال يتم خلاله تبادل شهادات هويات iCloud الخاصة بهما. يتم التحقق من الهوية الموجودة في الشهادات مقابل تطبيق جهات الاتصال لدى كل مستخدم.

إذا تم التحقق من الشهادات، يُطلب من المستخدم المُستقبِل قبول عملية النقل الواردة من المستخدم أو الجهاز المعرّف. في حالة تحديد مستلمين متعددين، تتكرر هذه العملية لكل وجهة.

أمن مشاركة كلمة سر Wi-Fi على iPhone و iPad

تستخدم أجهزة iPhone و iPad التي تدعم مشاركة كلمة سر Wi-Fi آلية مماثلة للإرسال السريع من أجل إرسال كلمة سر Wi-Fi من جهاز إلى آخر.

عندما يحدد المستخدم شبكة Wi-Fi (الطالب) ويُطلب منه كلمة سر Wi-Fi، يبدأ جهاز Apple إعلان Bluetooth منخفض الطاقة (BLE) للإشارة إلى أنه يريد كلمة سر Wi-Fi. بينما أجهزة Apple الأخرى التي تكون نشطة وعلى مقربة ولديها كلمة سر شبكة Wi-Fi المحددة تتصل باستخدام BLE لدى الجهاز الطالب.

يتطلب الجهاز الذي يحتوي على كلمة سر Wi-Fi (المانح) معلومات جهة الاتصال الخاصة بالطالب، ويجب على الطالب إثبات هويته باستخدام آلية مماثلة للإرسال السريع. بعد إثبات الهوية، يرسل المانح إلى الطالب رمز الدخول الذي يمكن استخدامه للانضمام إلى الشبكة.

يمكن للمؤسسات تقييد استخدام مشاركة كلمة سر Wi-Fi للأجهزة أو التطبيقات التي تتم إدارتها عبر حل إدارة جهاز الجوال (MDM).

أمن جدار الحماية في macOS

يتضمن macOS جدار حماية مضمّنًا لحماية الـ Mac من وصول الشبكة وهجمات قطع الخدمة. يمكن تكوينه عن طريق الانتقال إلى إعدادات النظام > الخصوصية والأمن (macOS 13 أو أحدث) أو تفضيلات النظام (macOS 12 أو أقدم) أو عن طريق استخدام ملف تعريف تكوين مع حمولة جدار الحماية المثبتة يدويًا أو المقدمة بواسطة حل MDM. التكوينات الآتية مدعومة:

- حظر جميع الاتصالات الواردة، بغض النظر عن التطبيق.
- السماح تلقائيًا للبرامج المضمنة بتلقي الاتصالات الواردة.
- السماح تلقائيًا للبرامج التي تم تنزيلها وتوقيعها بتلقي الاتصالات الواردة.
- إضافة أو رفض الوصول بناءً على التطبيقات التي يحددها المستخدم.
- منع الـ Mac من الاستجابة لطلبات فحص ICMP (بروتوكول رسائل مراقبة الإنترنت) وطلبات فحص المنافذ.

أمن مجموعة أدوات المطورين

نظرة عامة على أمن مجموعة أدوات المطورين

توفر Apple عددًا من إطارات العمل "مجموعة أدوات" لتمكين مطوري الجهات الخارجية من توسيع خدمات Apple. تم تصميم إطارات العمل هذه مع وضع خصوصية المستخدم وأمنه في جوهرها:

- HomeKit
- CloudKit
- SiriKit
- WidgetKit
- DriverKit
- ReplayKit
- ARKit

أمن HomeKit

أمن اتصالات HomeKit

توفر HomeKit بنية أساسية لأتمتة المنزل تستخدم ميزات أمن iCloud والجهاز لحماية البيانات الخاصة ومزامنتها دون كشفها لشركة Apple.

تستند هوية وأمن HomeKit إلى أزواج المفاتيح العامة-الخاصة Ed25519. يتم إنشاء زوج مفاتيح Ed25519 على جهاز المستخدم، حيث يصبح هوية HomeKit الخاصة به. يُستخدم زوج المفاتيح كجزء من بروتوكول ملحقات HomeKit (HAP) لمصادقة التواصل المباشر بين أجهزة Apple الخاصة بالمستخدم وملحقات HomeKit الخاصة به.

بالنسبة إلى المنازل التي يوجد بها جهاز توزيع منزلي، يمكن لأعضاء المنزل المشترك إرسال أوامر إلى الملحقات من خلال جهاز التوزيع المنزلي هذا. تُرسَل هذه الأوامر، مصادقة ومشفرة بالكامل، من جهاز المستخدم إلى جهاز التوزيع المنزلي باستخدام خدمة الهوية من Apple (IDS)، حيث يُعاد توجيهها إلى الملحقات ذات الصلة باستخدام بروتوكول ملحقات HomeKit (HAP) أو Matter، وهو معيار اتصال للمنازل الذكية.

يتم دائمًا تحديث المفاتيح — المخزنة في سلسلة المفاتيح والمضمنة فقط في النُّسخ الاحتياطية لسلسلة المفاتيح المشفرة — بين الأجهزة التي تستخدم سلسلة مفاتيح iCloud.

التواصل بين ملحقات HomeKit

تنشئ ملحقات HomeKit زوج مفاتيح Ed25519 الخاص بها لاستخدامه في التواصل مع أجهزة Apple. وإذا تمت استعادة الملحق إلى إعدادات المصنع، يتم إنشاء زوج مفاتيح جديد.

لتأسيس علاقة بين جهاز Apple وملحق HomeKit، يتم تبادل المفاتيح باستخدام بروتوكول كلمة السر البعيدة الآمنة (3072 بت) باستخدام رمز من ثمانية أرقام توفره الجهة المصنعة للملحق، ويتم إدخاله على جهاز المستخدم، ثم يتم تشفيره باستخدام ChaCha20-Poly1305 AEAD مع مفاتيح HKDF-SHA512 المشتقة. يتم التحقق من شهادة MFi الخاصة بالملحق أيضًا أثناء الإعداد. ويمكن للملحقات التي لا تحتوي على شريحة MFi إنشاء دعم لمصادقة البرامج في iOS 11.3 أو أحدث.

عندما يتواصل الجهاز مع ملحق HomeKit في أثناء الاستخدام، يصادق كل منهما الآخر باستخدام المفاتيح المتبادلة في العملية المذكورة أعلاه. ويتم إنشاء كل جلسة باستخدام بروتوكول محطة إلى محطة ويتم تشفيرها باستخدام مفاتيح HKDF-SHA512 مشتقة بناءً على مفاتيح Curve25519 لكل جلسة. ينطبق هذا على كل من الملحقات المستندة إلى بروتوكول IP وملحقات Bluetooth منخفض الطاقة (BLE).

بالنسبة إلى أجهزة BLE التي تدعم إشعارات البث، يتم تزويد الملحق بمفتاح تشفير بث بواسطة جهاز مقترن عبر جلسة آمنة. ويُستخدم هذا المفتاح لتشفير البيانات المتعلقة بتغييرات الحالة على الملحق، والتي يتم الإبلاغ بها عبر إعلانات BLE. مفتاح تشفير البث هو مفتاح HKDF-SHA512 مشتق، ويتم تشفير البيانات باستخدام خوارزمية ChaCha20-Poly1305 AEAD. يتم تغيير مفتاح تشفير البث بشكل دوري ويتم تحديثه على الأجهزة الأخرى باستخدام iCloud كما هو موضح في أمن بيانات HomeKit.

التواصل مع ملحقات Matter

تستند الهوية والأمن مع ملحقات Matter إلى الشهادات. وبالنسبة إلى منازل Apple، يتم إنشاء جذر الثقة للجهة الموثقة (CA) على جهاز المستخدم الأولي ("المالك") ويُخزَّن المفتاح الخاص للجهة الموثقة في سلسلة مفاتيح iCloud الخاصة به. وينشئ كل جهاز Apple في المنزل طلب توقيع شهادة (CSR) باستخدام NIST P256. ويتم تضمين طلب توقيع الشهادة هذا بواسطة جهاز المالك الذي ينشئ شهادة هوية Matter للجهاز باستخدام المفتاح الخاص للجهة الموثقة الخاص به. تُستخدم هذه الشهادة لاحقًا لمصادقة التواصل بين أجهزة المستخدمين وملحقاتهم.

تنشئ ملحقات Matter زوج مفاتيح NIST P256 وطلب توقيع الشهادة (CSR) الخاصين بها وتتلقى شهادة من الجهة الموثقة (CA) خلال إقران الملحق. وقبل إنشاء أزواج المفاتيح، يتبادل ملحق Matter وأجهزة مالك المنزل المفاتيح — باستخدام بروتوكول SPAKE2+ مع رمز PIN تقدمه الجهة المصنعة للملحق — ويتم تنفيذ عملية مصادقة الجهاز. بعد ذلك يتم تبادل طلب توقيع الشهادة (CSR) والشهادة عبر هذه القناة المشفرة باستخدام AES-CCM مع مفاتيح HKDF-SHA256 المشتقة. وإذا تمت استعادة الملحق إلى إعدادات المصنع، يتم إنشاء زوج مفاتيح وطلب توقيع شهادة جديدين ويتم إصدار شهادة جديدة للملحق خلال الإقران.

عندما يتواصل جهاز Apple مع ملحق Matter خلال الاستخدام، يصادق كل منهما الآخر باستخدام شهادته الخاصة. ويتم إنشاء كل جلسة باستخدام بروتوكول من ثلاث مراحل (سيغما) ويتم تشفيرها باستخدام مفاتيح HKDF-SHA256 مشتقة استنادًا إلى مفاتيح P256 لكل جلسة.

لمزيد من المعلومات حول طريقة تفاعل أجهزة Apple مع ملحقات Matter بأمان، انظر دعم Matter في iOS 16 على موقع ويب مطور Apple.

HomeKit و Siri

يمكن استخدام Siri للاستعلام عن الملحقات والتحكم فيها، ولتنشيط المشاهد. ويتم توفير الحد الأدنى من المعلومات حول تكوين المنزل بشكل مجهول إلى Siri، لتوفير أسماء الغرف والملحقات والمشاهد الضرورية للتعرف على الأوامر. قد يشير الصوت المرسل إلى Siri إلى ملحقات أو أوامر محددة، ولكن لا ترتبط بيانات Siri هذه بميزات Apple الأخرى مثل HomeKit.

ملحقات HomeKit التي تدعم Siri

يمكن للمستخدمين تمكين ميزات جديدة مثل Siri وميزات HomePod الأخرى، مثل أجهزة ضبط الوقت وأجهزة الإنذار والاتصال الداخلي وجرس الباب، على الملحقات التي تدعم Siri باستخدام تطبيق المنزل. عند تمكين تلك الميزات، يقوم الملحق بالتنسيق مع HomePod المقترن بالشبكة المحلية التي تستضيف ميزات Apple هذه. يتم تبادل الصوت بين الأجهزة عن طريق القنوات المشفرة التي تستخدم بروتوكولات HomeKit والبث السريع.

عند تشغيل استمع إلى "يا Siri"، يستمع الملحق إلى عبارة "يا Siri" باستخدام محرك اكتشاف عبارة التشغيل الذي يتم تشغيله محليًا. إذا اكتشف هذا المحرك العبارة، فإنه يرسل إطارات الصوت مباشرةً إلى HomePod المقترن باستخدام HomeKit. يقوم HomePod بالتحقق مجددًا من الصوت وقد يلغي الجلسة الصوتية إذا لم تُظهر العبارةُ احتواءها على عبارة التشغيل.

عند تشغيل Touch for Siri، يمكن للمستخدم الضغط على زر مخصص على الملحق لبدء محادثة مع Siri. يتم إرسال إطارات الصوت مباشرة إلى HomePod المقترن.

بعد اكتشاف استدعاء ناجح لـ Siri، يقوم HomePod بإرسال الصوت إلى خوادم Siri ويفي بمقصد المستخدم باستخدام إجراءات حماية الأمن والخصوصية والتشفير ذاتها التي يطبقها HomePod على استدعاءات المستخدم إلى HomePod نفسه. وإذا كان لدى Siri رد صوتي فسيتم إرسال استجابة Siri عبر القناة الصوتية البث السريع إلى الملحق. تتطلب بعض طلبات Siri معلومات إضافية من المستخدم (على سبيل المثال، السؤال عمّا إذا كان المستخدم يريد سماع المزيد من الخيارات). في هذه الحالة، يتلقى الملحق إشارة بوجوب مطالبة المستخدم، ويتم بث الصوت الإضافي إلى HomePod.

يجب أن يتضمن الملحق مؤشرًا مرئيًا للإشارة إلى مستخدم عندما يستمع بشكل نشط (على سبيل المثال، مؤشر LED). ليس لدى الملحق علم بالمقصد من طلب Siri، باستثناء الوصول إلى التدفقات الصوتية، لا يتم تخزين أي بيانات للمستخدم على الملحق.

أمن بيانات HomeKit

بالنسبة إلى المنازل التي تمت ترقيتها إلى بنية HomeKit الجديدة (متوفر في iOS 16.2 و iPadOS 16.2)، تتم مزامنة بيانات HomeKit بأمان بين أجهزة Apple الخاصة بالمستخدم باستخدام iCloud وسلسلة مفاتيح iCloud. وخلال هذه العملية، تُشفَّر بيانات HomeKit باستخدام تشفير iCloud الكامل ولا يمكن لـ Apple الوصول إليها.

يمكن للمستخدم الذي قام في البداية بإنشاء المنزل في HomeKit ("المالك") أو مستخدم آخر لديه أذونات التحرير إضافة مستخدمين جدد. ويُكوّن جهاز المالك الملحقات باستخدام المفتاح العام للمستخدم الجديد بحيث يمكن للملحق المصادقة على أوامر المستخدم الجديد وقبولها. عندما يضيف مستخدم لديه أذونات التحرير مستخدمًا جديدًا، يتم تفويض العملية إلى جهاز توزيع منزلي لإكمال العملية.

بيانات المنزل والتطبيقات

يتحكم المستخدمون في وصول التطبيقات إلى بيانات المنزل من خلال إعدادات الخصوصية. يُطلب من المستخدمين منح حق الوصول عندما تطلب التطبيقات بيانات المنزل، على غرار كيفية الوصول إلى جهات الاتصال والصور ومصادر بيانات iOS و iPadOS و macOS الأخرى. وإذا وافق المستخدم، يمكن للتطبيقات الوصول إلى أسماء الغرف وأسماء الملحقات والغرفة التي يوجد بها كل ملحق، وغيرها من المعلومات كما هو موضح بالتفصيل في وثائق مطور HomeKit على https://developer.Apple.com/homekit/.

التخزين المحلي للبيانات

يخزّن HomeKit البيانات المتعلقة بالمنازل والملحقات والمشاهد والمستخدمين على أجهزة Apple الخاصة بالمستخدم. تُخزَّن هذه البيانات باستخدام فئة حماية البيانات "محمية حتى أول مصادقة من المستخدم" وفي مخزن بيانات. لا تُنسَخ بيانات HomeKit احتياطيًا في النُسخ الاحتياطية المحلية.

تأمين أجهزة التوجيه باستخدام HomeKit

يمكن للمستخدمين تحسين أمان شبكتهم المنزلية باستخدام أجهزة التوجيه التي تدعم HomeKit. باستخدام أجهزة التوجيه هذه، يمكن للمستخدمين إدارة وصول ملحقات HomeKit الخاصة بشبكة Wi-Fi إلى شبكتهم المحلية والإنترنت. تدعم أجهزة التوجيه أيضًا مصادقة PPSK الخاصة (PPSK)، وبذلك يمكن إضافة الملحقات إلى شبكة Wi-Fi باستخدام مفتاح خاص بالملحق ويمكن إبطاله عند الحاجة. تحسّن مصادقة PPSK الأمن من خلال عدم كشف كلمة سر Wi-Fi الرئيسية للملحقات، وكذلك بالسماح لجهاز التوجيه بالتعرف على الملحق بشكل آمن حتى إذا تم تغيير عنوان MAC الخاص به.

باستخدام تطبيق المنزل، يمكن للمستخدم تكوين قيود الوصول لمجموعات من الملحقات على النحو التالي:

- **لا توجد قيود:** السماح بالوصول غير المقيَّد إلى الإنترنت والشبكة المحلية.
- **تلقائي:** هذا هو الإعداد الافتراضي. السماح بالوصول إلى الإنترنت والشبكة المحلية بناءً على قائمة تضم مواقع الإنترنت والمنافذ المحلية يتم تقديمها إلى Apple بواسطة جهة تصنيع الملحق. تشمل هذه القائمة جميع المواقع والمنافذ التي يحتاج إليها الملحق للعمل بشكل صحيح. (لا تُفرض أي قيود حتى يتم توفير مثل هذه القائمة.)
- **تقييد إلى تطبيق المنزل:** لا يمكن الوصول إلى الإنترنت أو الشبكة المحلية باستثناء الاتصالات التي يتطلبها HomeKit لاكتشاف الملحق والتحكم فيه من الشبكة المحلية (بما في ذلك الاتصالات من جهاز التوزيع المنزلي لدعم التحكم عن بعد).

PPSK هي عبارة مرور WPA2 شخصي قوية خاصة بالملحق يتم إنشاؤها تلقائيًا بواسطة HomeKit، ويتم إبطالها في حالة إزالة الملحق لاحقًا من تطبيق المنزل. وتُستخدم PPSK عند إضافة ملحق إلى شبكة Wi-Fi بواسطة HomeKit في تطبيق المنزل الذي تم تكوينه باستخدام جهاز توجيه HomeKit؛ وتنعكس هذه الإضافة على أنها بيانات اعتماد Wi-Fi: HomeKit مُدار على شاشة الإعدادات الخاصة بالملحق في تطبيق المنزل. تتم إعادة تكوين الملحقات المضافة إلى شبكة Wi-Fi قبل إضافة جهاز التوجيه لاستخدام PPSK إذا كان الملحق يدعم ذلك، وإلا ستحتفظ ببيانات الاعتماد الموجودة.

كتدبير أمني إضافي، يجب على المستخدم تكوين جهاز توجيه HomeKit باستخدام تطبيق جهة تصنيع جهاز التوجيه، بحيث يمكن للتطبيق التحقق من أن المستخدم لديه حق الوصول إلى جهاز التوجيه ويمكنه إضافته إلى تطبيق المنزل.

أمن كاميرا HomeKit

ترسل الكاميرات المزودة بعنوان بروتوكول الإنترنت (عنوان IP) في HomeKit تدفقات الفيديو والصوت مباشرة إلى جهاز iOS و iPadOS و tvOS و macOS على الشبكة المحلية التي تتمتع بالوصول إلى التدفق. يتم تشفير التدفقات باستخدام مفاتيح منشأة عشوائيًا على الجهاز وكاميرا بروتوكول الإنترنت (كاميرا IP)، حيث يتم تبادلها عبر جلسة HomeKit الآمنة إلى الكاميرا. عندما لا يكون الجهاز موجودًا على الشبكة المحلية، يتم ترحيل التدفقات المشفرة عبر جهاز التوزيع المنزلي إلى الجهاز. لا يقوم جهاز التوزيع المنزلي بفك تشفير التدفقات، ويعمل فقط كترحيل بين الجهاز وكاميرا IP. عندما يعرض أحد التطبيقات عرض فيديو كاميرا HomeKit IP للمستخدم، يعرض HomeKit إطارات الفيديو بشكل آمن من عملية نظام منفصلة. نتيجة لذلك، يتعذر على التطبيق الوصول إلى تدفق الفيديو أو تخزينه. بالإضافة إلى ذلك، لا يُسمح للتطبيقات بالتقاط لقطات شاشة من هذا التدفق.

فيديوهات HomeKit الآمنة

يوفر HomeKit آلية خاصة وآمنة شاملة لتسجيل وتحليل وعرض المقاطع من كاميرات HomeKit IP دون كشف محتويات تلك الفيديوهات لشركة Apple أو لأي جهة خارجية. عندما تكتشف كاميرا IP الحركة، يتم إرسال مقاطع الفيديو مباشرة إلى جهاز Apple يعمل كجهاز توزيع منزلي، باستخدام اتصال شبكة محلية مخصص بين جهاز التوزيع المنزلي وكاميرا IP. يتم تشفير اتصال الشبكة المحلية باستخدام زوج مفاتيح HKDF-SHA512 مشتق لكل جلسة يتم التفاوض عليه عبر جلسة HomeKit بين جهاز التوزيع المنزلي وكاميرا IP. يفكّ HomeKit تشفير تدفقات الصوت والفيديو على جهاز التوزيع المنزلي ويحلّل إطارات الفيديو محليًا لأي حدث مهم. في حالة اكتشاف حدث مهم، يفك HomeKit تشفير مقطع الفيديو باستخدام AES-256-GCM مع مفتاح AES256 يتم إنشاؤه عشوائيًا. ينشئ HomeKit أيضًا إطارات ملصقات لكل مقطع ويتم تشفير إطارات الملصقات هذه باستخدام نفس مفتاح AES256. يتم تحميل إطار الملصق المشفَّر وبيانات الصوت والفيديو إلى خوادم iCloud. كما يتم تحميل بيانات التعريف ذات الصلة لكل مقطع بما في ذلك مفتاح التشفير إلى CloudKit باستخدام تشفير iCloud الكامل.

بالنسبة لتصنيف الوجه، تخزّن HomeKit كل البيانات المستخدمة لتصنيف وجه شخص معين في CloudKit باستخدام تشفير iCloud الكامل. وتتضمن البيانات المُخزّنة معلومات عن كل شخص، مثل الاسم، فضلاً عن الصور التي تمثل وجه ذلك الشخص. يمكن الحصول على صور الوجه هذه من الصور الخاصة بالمستخدم إذا اختار ذلك، أو يمكن تجميعها من فيديو كاميرا IP الذي تم تحليله سابقًا. تستخدم جلسة تحليل فيديوهات HomeKit الآمنة بيانات التصنيف هذه للتعرف على الوجوه في تدفق الفيديو الآمن الذي تتلقاه مباشرةً من كاميرا IP وتتضمن معلومات التعريف هذه في بيانات تعريف المقطع المذكورة سابقًا.

عند استخدام تطبيق المنزل لعرض مقاطع من الكاميرا، يتم تنزيل البيانات من iCloud ويتم فك تغليف المفاتيح المستخدمة لتشفير التدفقات محليًا باستخدام فك التشفير الكامل من iCloud. يتم إجراء تدفق لمحتوى الفيديو المشفر من الخوادم وفك تشفيره محليًا على جهاز iOS قبل عرضه في العارض. وربما يتم تقسيم كل جلسة من جلسات مقاطع الفيديو إلى أقسام فرعية حيث يقوم كل قسم فرعي بتشفير تدفق المحتوى باستخدام مفتاحه الفريد الخاص.

أمن HomeKit على Apple TV

يقوم HomeKit بتوصيل بعض ملحقات التحكم عن بُعد التابعة لجهات خارجية بأمان بـ Apple TV ويدعم إضافة ملفات تعريف المستخدم إلى مالك Apple TV في المنزل.

استخدام ملحقات التحكم عن بُعد التابعة لجهات خارجية على Apple TV

توفر بعض ملحقات التحكم عن بُعد التابعة لجهات خارجية أحداث تصميم الواجهات البشرية (HID) وصوت Siri إلى Apple TV مرتبط تمت إضافته باستخدام تطبيق المنزل. يرسل جهاز التحكم عن بُعد أحداث HID عبر الجلسة الآمنة إلى Apple TV. يُرسل جهاز التحكم عن بُعد في التلفاز الذي يدعم Siri بيانات الصوت إلى Apple TV عندما يقوم المستخدم صراحةً بتنشيط الميكروفون على جهاز التحكم عن بُعد باستخدام زر مخصص لـ Siri. يرسل جهاز التحكم عن بُعد إطارات الصوت مباشرة إلى Apple TV باستخدام اتصال شبكة محلية مخصص. يتم استخدام زوج مفاتيح HKDF-SHA 512 مشتق لكل جلسة يتم التفاوض عليه عبر جلسة HomeKit بين Apple TV وجهاز التحكم عن بُعد الخاص بالتلفزيون لتشفير اتصال الشبكة المحلية. يقوم HomeKit بفك تشفير إطارات الصوت على Apple TV وإعادة توجيهها إلى تطبيق Siri، حيث يتم التعامل معها باستخدام نفس وسائل حماية الخصوصية مثل جميع مدخلات Siri الصوتية.

ملفات تعريف Apple TV ومنازل HomeKit

عندما يضيف أحد المستخدمين في منزل HomeKit ملف التعريف الخاص به إلى مالك Apple TV في المنزل، فإنه يمنح ذلك المستخدم إمكانية الوصول إلى برامج التلفاز والموسيقى وملفات البودكاست الخاصة به. وتتم مشاركة الإعدادات لكل مستخدم فيما يتعلق باستخدام ملف التعريف الخاص به على Apple TV إلى حساب iCloud الخاص بالمالك باستخدام تشفير iCloud الكامل. وتكون البيانات مملوكة لمستخدمها وتتم مشاركتها مع المالك للقراءة فقط. يمكن لكل مستخدم للمنزل تغيير هذه القيم في تطبيق المنزل ويستخدم Apple TV الخاص بالمالك هذه الإعدادات.

عند تشغيل إعداد، تتم إتاحة حساب iTunes الخاص بالمستخدم على Apple TV. وعند إيقاف إعداد، يتم حذف جميع الحسابات والبيانات المتعلقة بهذا المستخدم على Apple TV. يبدأ جهاز المستخدم مشاركة CloudKit الأولية ويتم إرسال الرمز المميز لإنشاء مشاركة CloudKit الآمنة عبر نفس القناة الآمنة التي يتم استخدامها لمزامنة البيانات بين مستخدمي المنزل.

أمن SiriKit لـ iOS و iPadOS و watchOS

يستخدم Siri نظام ملحقات التطبيقات للتواصل مع تطبيقات الجهات الخارجية. ويستطيع Siri على أي جهاز الوصول إلى معلومات الاتصال الخاصة بالمستخدم وموقع الجهاز الحالي. ولكن قبل أن يوفر البيانات المحمية لأحد التطبيقات، يتحقق Siri من أذونات الوصول التي يتحكم فيها المستخدم الخاصة بالتطبيق. وفقًا لتلك الأذونات، يقوم Siri بتمرير المقطع ذي الصلة فقط من نُطق المستخدم الأصلي إلى ملحق التطبيق. على سبيل المثال، إذا لم يكن للتطبيق حق الوصول إلى معلومات الاتصال، فلن يحل Siri العلاقة في طلب المستخدم مثل "ادفع لوالدتي 10 دولارات باستخدام تطبيق الدفع". في هذه الحالة، لن يشاهد التطبيق إلا المصطلح الحرفي "والدتي".

لكن إذا منح المستخدم التطبيق حق الوصول إلى معلومات الاتصال، فسيتلقى التطبيق معلومات تم حلها عن والدة المستخدم. إذا تمت الإشارة إلى علاقة في الجزء الأساسي من الرسالة؛ على سبيل المثال، "أخبر والدتي على تطبيق الرسائل بأن أخي رائع"؛ لا يحل Siri كلمة "أخي" بغض النظر عن أذونات التطبيق.

يمكن للتطبيقات التي تدعم SiriKit إرسال مفردات خاصة بالتطبيق أو خاصة بالمستخدم إلى Siri، مثل أسماء جهات الاتصال لدى المستخدم. تتيح هذه المعلومات التعرف على الكلام في Siri وفهم اللغة الطبيعية للتعرف على المفردات الخاصة بهذا التطبيق، وترتبط بمعرف عشوائي. وتظل المعلومات المخصصة متوفرة طالما أن المعرف قيد الاستخدام، أو حتى يقوم المستخدم بتعطيل تكامل Siri في الإعدادات بالتطبيق، أو حتى يتم إلغاء تثبيت التطبيق الذي يدعم SiriKit.

بالنسبة لمنطوق مثل "خذني في رحلة إلى منزل أمي باستخدام RideShareApp"، يطلب الطلب بيانات الموقع من جهات اتصال المستخدم. بالنسبة لهذا الطلب فقط، يوفر Siri المعلومات المطلوبة إلى ملحق التطبيق، بغض النظر عن إعدادات أذونات المستخدم للموقع أو معلومات الاتصال الخاصة بالتطبيق.

أمن WidgetKit

WidgetKit هو إطار العمل الذي يستخدمه المطورون لعرض الأدوات ومشاهدة الإضافات. قد يعرض كلاهما معلومات حساسة ويمكن أن يكونا ظاهرين بشكل كبير، خاصة على الأجهزة المزودة بشاشة تشغيل دومًا.

في iOS، يمكن للمستخدمين تكوين ما إذا كانوا يرغبون في إظهار البيانات الحساسة على شاشة القفل وأثناء التشغيل دومًا أم لا. في الإعدادات، يمكنهم إلغاء تنشيط إمكانية الوصول إلى البيانات لأدوات شاشة القفل في قسم "السماح بالوصول عند القفل" في الإعدادات > بصمة الوجه ورمز الدخول.

في Apple Watch، يمكن للمستخدمين تكوين ما إذا كانوا يرغبون في إظهار البيانات الحساسة أثناء التشغيل دومًا عن طريق اختيار الإعدادات > شاشة العرض والإضاءة > تشغيل دومًا > إخفاء الإضافات الحساسة. يمكنهم أيضًا اختيار عرض المحتوى المنقَّح لجميع الإضافات أو لبعض الإضافات الفردية.

إذا اختار المستخدم إخفاء محتوى يعتبره خاصًا، فسيعرض WidgetKit عنصرًا نائبًا أو تنقيحات. لتكوين تنقيحات، يجب على أحد المطورين:

1. تنفيذ إعادة الاتصال `redacted(reason:)`.

2. قراءة خاصية `privacy`.

3. توفير طرق عرض العناصر النائبة المخصصة.

يمكن للمطورين أيضًا عرض طريقة العرض على أنها غير منقحة باستخدام مفتاح تعديل طريقة العرض `unredacted()`.

باعتباره بديلًا لتمييز طرق العرض الفردية على أنها حساسة من حيث الخصوصية، على سبيل المثال، إذا كان محتوى أداة بأكمله حساسًا من حيث الخصوصية، يمكن للمطور إضافة إمكانية حماية البيانات إلى ملحق أداة. إلى أن يلغي المستخدم قفل جهازه ليتوافق مع مستوى الخصوصية المحدد، يعرض WidgetKit عناصر نائبة بدلًا من محتوى الأداة. يجب على المطور تمكين إمكانية حماية البيانات لملحق الأداة في Xcode ثم تعيين استحقاق `Data Protection` على القيمة التي تناسب مستوى الخصوصية الذي يريد تقديمه:

- `NSFileProtectionComplete`
- `NSFileProtectionCompleteUnlessOpen`

يخفي WidgetKit محتوى تلك الأدوات ويعرض عنصرًا نائبًا إلى أن يجري المستخدم المصادقة بعد إعادة تشغيل أجهزته. إضافة إلى ذلك، لا تتوفر أدوات iOS هذه باعتبارها أدوات iPhone على Mac.

أمن DriverKit لـ macOS

DriverKit هو إطار العمل الذي يسمح للمطورين بإنشاء برامج تشغيل للأجهزة يقوم المستخدم بتثبيتها على الـ Mac. تعمل برامج التشغيل المضمنة مع DriverKit في مساحة المستخدم، بدلاً من ملحقات kernel، لتحسين أمن النظام واستقراره. وهذا يسهّل التثبيت ويزيد من استقرار وأمن macOS.

يقوم المستخدم ببساطة بتنزيل التطبيق (ليست المُثبّتات ضرورية عند استخدام ملحقات النظام أو DriverKit) ولا يتم تمكين الملحق إلا عند الحاجة. وتحل هذه العناصر محل kexts في العديد من حالات الاستخدام، والتي تتطلب امتيازات المسؤول للتثبيت في /النظام/المكتبة أو /المكتبة.

بالنسبة لمسؤولي تقنية المعلومات الذين يستخدمون برامج تشغيل الأجهزة وحلول التخزين السحابي والشبكات وتطبيقات الأمن التي تتطلب ملحقات kernel، يُفضّل الانتقال إلى إصدارات أحدث تكون مبنية على ملحقات النظام. هذه الإصدارات الأحدث تقلل إلى حد كبير من إمكانية حدوث مشكلات kernel على الـ Mac وكذلك تقلل من الأجزاء المعرضة للهجوم. وتعمل هذه الملحقات الجديدة في مساحة المستخدم، ولن تتطلب امتيازات خاصة مطلوبة للتثبيت، وتتم إزالتها تلقائيًا عند نقل تطبيق التجميع إلى سلة المهملات.

يوفر إطار عمل DriverKit فئات C++ لخدمات I/O ومطابقة الجهاز وواصفات الذاكرة وقوائم انتظار الإرسال. كما أنه يحدد أنواع I/O المناسبة للأرقام والمجموعات والسلاسل والأنواع الشائعة الأخرى. يستخدم المستخدم هذه العناصر مع إطارات عمل برامج التشغيل الخاصة بالعائلة مثل USBDriverKit و HIDDriverKit. يمكنك استخدام إطار عمل ملحقات النظام لتثبيت برنامج تشغيل وترقيته.

أمن ReplayKit في iOS و iPadOS

يُعد ReplayKit إطار عمل يسمح للمطورين بإضافة إمكانات التسجيل والبث المباشر إلى تطبيقاتهم. بالإضافة إلى ذلك، يتيح للمستخدمين التعليق على تسجيلاتهم وبثّهم باستخدام الكاميرا الأمامية والميكروفون في الجهاز.

تسجيل الأفلام

توجد عدة طبقات من الأمن مضمّنة في تسجيل الأفلام:

- **مربع حوار الأذونات:** قبل بدء التسجيل، يعرض ReplayKit تنبيهًا بموافقة المستخدم يطلب من المستخدم تأكيد قصد تسجيل الشاشة والميكروفون والكاميرا الأمامية. يتم تقديم هذا التنبيه مرة واحدة لكل عملية في التطبيق، ويتم تقديمه مرة أخرى إذا تُرك التطبيق في الخلفية لمدة تزيد عن 8 دقائق.
- **التقاط الشاشة والصوت:** يحدث التقاط الشاشة والصوت خارج عملية التطبيق في إعادة تشغيل البرنامج الخفي في ReplayKit. وقد تم التصميم بتلك الطريقة لضمان عدم تمكين الوصول إلى المحتوى المُسجّل أبدًا من خلال عملية التطبيق.
- **التقاط الشاشة والصوت في التطبيق:** يسمح هذا للتطبيق بالحصول على الفيديو وعينات المخازن المؤقتة، والتي يحرسها مربع حوار الأذونات.
- **إنشاء الأفلام والتخزين:** تتم كتابة ملف الفيلم إلى دليل لا يمكن الوصول إليه إلا في أنظمة ReplayKit الفرعية ولا يستطيع أي تطبيق الوصول إليه. وهذا يساعد على منع الجهات الخارجية من استخدام التسجيلات دون موافقة المستخدم.
- **المعاينة والمشاركة من قِبل المستخدم النهائي:** تتوفر لدى المستخدم إمكانية معاينة ومشاركة الفيلم عبر واجهة مستخدم توفرها ReplayKit. يتم تقديم واجهة المستخدم خارج العملية من خلال البنية الأساسية لملحقات iOS ويكون لديها حق الوصول إلى ملف الفيلم المنشأ.

بث ReplayKit

توجد عدة طبقات من الأمن مضمّنة في بثّ الأفلام:

- **التقاط الشاشة والصوت:** تشبه آلية التقاط الشاشة والصوت أثناء البث تسجيل الأفلام وتحدث في `replayd`.
- **ملحقات البث:** لكي تشارك خدمات الجهات الخارجية في بث ReplayKit، يُطلب منها إنشاء ملحقين جديدين يتم تكوينهما باستخدام نقطة نهاية com.Apple.broadcast-services:
  - ملحق واجهة مستخدم يسمح للمستخدم بإعداد البث الخاص به
  - ملحق تحميل يعالج تحميل بيانات الفيديو والصوت إلى خوادم الخدمة الخلفية

تضمن البنية أن لا تمتلك تطبيقات الاستضافة أي امتيازات لمحتويات الفيديو والصوت التي يتم بثها. ويكون حق الوصول لدى ReplayKit وملحقات البث التابعة لجهات خارجية فقط.

- **منتقي البث:** باستخدام منتقي البث، يبدأ المستخدمون عمليات البث في النظام مباشرةً من تطبيقاتهم باستخدام نفس واجهة المستخدم المحددة من قِبل النظام التي يمكن الوصول إليها باستخدام مركز التحكم. يتم تطبيق واجهة المستخدم باستخدام API خاص وتكون عبارة عن ملحق يتواجد ضمن إطار عمل ReplayKit. ويكون هذا الملحق خارج العملية من تطبيق الاستضافة.
- **ملحق التحميل:** يستخدم الملحق الذي تنفذه خدمات البث التابعة لجهات خارجية لمعالجة محتوى الفيديو والصوت أثناء البث عينات من المخازن المؤقتة الأولية غير المشفرة. أثناء نمط المعالجة هذا، تتم سلسلة بيانات الفيديو والصوت وتمريرها إلى ملحق التحميل التابع لجهة خارجية في الوقت الفعلي من خلال اتصال XPC المباشر. يتم تشفير بيانات الفيديو عن طريق استخراج كائن IOSurface من عينة المخزن المؤقت للفيديو، وترميزها بشكل آمن ككائن XPC، وإرسالها عبر XPC إلى ملحق الجهة الخارجية، وفك تشفيرها مرة أخرى بشكل آمن إلى كائن IOSurface.

أمن ARKit في iOS و iPadOS

ARKit عبارة عن إطار عمل يسمح للمطورين بإنتاج تجارب الواقع المُعزّز في تطبيقاتهم أو ألعابهم. يمكن للمطورين إضافة عناصر ثنائية الأبعاد أو ثلاثية الأبعاد باستخدام الكاميرا الأمامية أو الخلفية في جهاز iOS أو iPadOS.

صممت Apple الكاميرات مع مراعاة الخصوصية، ويجب أن تحصل تطبيقات الجهات الخارجية على موافقة المستخدم قبل الوصول إلى الكاميرا. في iOS و iPadOS، عندما يمنح المستخدم أحد التطبيقات حق الوصول إلى الكاميرا، يمكن لهذا التطبيق الوصول إلى الصور في الوقت الفعلي من الكاميرات الأمامية والخلفية. ولا يُسمح للتطبيقات باستخدام الكاميرا في الخفاء دون إيضاح أن الكاميرا قيد الاستخدام.

قد تحتوي الصور والفيديوهات التي تم التقاطها بالكاميرا على معلومات أخرى، مثل مكان وزمان التقاطها وعمق المجال والالتقاط الزائد. إذا كان المستخدم لا يريد أن تتضمن الصور والفيديوهات الملتقطة باستخدام تطبيق الكاميرا موقعًا، يمكنه التحكم في ذلك في أي وقت من خلال الانتقال إلى الإعدادات > الخصوصية > خدمات الموقع > الكاميرا. إذا كان المستخدم لا يرغب في أن تتضمن الصور والفيديوهات موقعًا عند المشاركة، يمكنه إيقاف الموقع في قائمة خيارات في صفحة المشاركة.

لتحسين تجربة AR لدى المستخدم، يمكن للتطبيقات التي تستخدم ARKit استخدام معلومات التعقب العالمي أو تعقب الوجه من الكاميرا الأخرى. يستخدم التعقب العالمي خوارزميات على جهاز المستخدم لمعالجة المعلومات من هذه المستشعرات لتحديد موضعها بالنسبة إلى الحيّز الفعلي. ويتيح التعقب العالمي ميزات مثل التوجه البصري في الخرائط.

إدارة الأجهزة الآمنة

نظرة عامة على إدارة الأجهزة الآمنة

يدعم iOS و iPadOS و macOS و tvOS و watchOS سياسات وتكوينات الأمن المرنة التي يسهل تنفيذها وإدارتها. ومن خلالها، يمكن للمؤسسات حماية معلومات الشركة والمساعدة على ضمان استيفاء الموظفين للمتطلبات المؤسسية، حتى إذا كانوا يستخدمون الأجهزة التي أحضروها بأنفسهم—على سبيل المثال، كجزء من برنامج "أحضر جهازك الخاص" (BYOD).

يمكن أن تستخدم المؤسسات إطار عمل إدارة الأجهزة المحمولة (MDM) الذي يتم تنفيذه بواسطة حل MDM لفرض متطلبات رمز الدخول وتكوين الإعدادات وتقييد الأداء ومسح بيانات الشركة عن بُعد على الأجهزة المُدارة. يساعد ذلك على الحفاظ على أمن بيانات الشركة، حتى عندما يستخدم الموظفون أجهزتهم الشخصية للوصول إلى هذه البيانات.

أمن نموذج الاقتران للـ iPhone والـ iPad

يستخدم iOS و iPadOS نموذج اقتران للتحكم في الوصول إلى الجهاز من كمبيوتر مضيف. يؤسس الاقتران علاقة ثقة بين الجهاز والمضيف المتصل به، ويتم التدليل على ذلك بتبادل المفاتيح العامة. ويستخدم iOS و iPadOS أيضًا دلالة الثقة هذه لتمكين وظائف إضافية مع المضيف المتصل، مثل مزامنة البيانات. في iOS 9 أو أحدث، ينطبق ما يلي على الخدمات:

- لا يمكن بدء الخدمات التي تتطلب الاقتران إلا بعد أن يفتح المستخدم قفل الجهاز
- لن تبدأ الخدمات إلا إذا كان قد تم فتح قفل الجهاز مؤخرًا
- قد تتطلب بعض الخدمات (مثل مزامنة الصور) فتح قفل الجهاز للبدء

تتطلب عملية الاقتران من المستخدم فتح قفل الجهاز وقبول طلب الاقتران من المضيف. في iOS 9 أو أحدث، يُطلب من المستخدم أيضًا إدخال رمز الدخول، وبعد ذلك يقوم المضيف والجهاز بتبادل وحفظ مفاتيح RSA سعة 2048 بت العامة. بعد ذلك، يتم تزويد المضيف بمفتاح 256 بت يمكنه فتح قفل حافظة مفاتيح ضمان مخزنة على الجهاز. وتُستخدم المفاتيح المتبادلة لبدء جلسة SSL مشفرة، الأمر الذي يتطلبه الجهاز قبل إرساله البيانات المحمية إلى المضيف أو بدء أي خدمة (مزامنة iTunes أو فايندر ونقل الملفات وتطوير Xcode وما إلى ذلك). لاستخدام هذه الجلسة المشفرة في جميع الاتصالات، يحتاج الجهاز إلى اتصالات من مضيف عبر Wi-Fi، لذلك يجب أن يكون قد تم إقرانه سابقًا عبر USB. ويُمكّن الاقتران أيضًا العديد من الإمكانات التشخيصية. في iOS 9، إذا لم يُستخدم سجل الاقتران لأكثر من ستة أشهر، تنتهي صلاحيته. ويتم اختصار هذا الإطار الزمني إلى 30 يومًا في iOS 11 أو أحدث.

تكون بعض الخدمات التشخيصية، بما في ذلك com.Apple.mobile.pcapd، مقيَّدة بالعمل فقط عبر USB. بالإضافة إلى ذلك، تتطلب خدمة com.apple.file_relay تثبيت ملف تعريف تكوين موقَّع من قِبل Apple. في iOS 11 أو أحدث، يستطيع Apple TV استخدام بروتوكول كلمة السر البعيدة الآمنة لإنشاء علاقة اقتران لاسلكيًا.

ويمكن للمستخدم مسح قائمة المضيفين الموثوق بهم باستخدام خيارات إعادة تعيين إعدادات الشبكة أو إعادة تعيين الموقع والخصوصية.

إدارة جهاز الجوال

نظرة عامة على أمن إدارة جهاز الجوال

تدعم أنظمة تشغيل Apple إدارة جهاز الجوال (MDM) التي تتيح للمؤسسات تكوين وإدارة عمليات نشر أجهزة Apple محددة الحجم بشكل آمن.

كيفية عمل MDM بأمان

وتعتمد إمكانات MDM على تقنيات نظام التشغيل، مثل التكوينات، والتسجيل عبر الأثير وخدمة الإشعارات اللحظية من Apple (APNs). على سبيل المثال، تُستخدم خدمة الإشعارات اللحظية من Apple (APNs) لتنشيط الجهاز وتشغيله حتى يتمكن من التواصل مباشرة مع حل MDM عبر اتصال آمن. ولا يتم نقل أي معلومات سرية أو ذات ملكية خاصة عبر خدمة الإشعارات اللحظية من Apple (APNs).

باستخدام MDM، يمكن لأقسام تقنية المعلومات تسجيل أجهزة Apple في بيئة مؤسسية أو تعليمية وتكوين الإعدادات وتحديثها لاسلكيًا ومراقبة الامتثال وإدارة تحديث البرامج وحتى مسح الأجهزة المُدارة أو قفلها عن بُعد.

في iOS 13 و iPadOS 13.1 و macOS 10.15 أو أحدث، تدعم أجهزة Apple خيار تسجيل جديدًا مصممًا خصيصًا لبرامج BYOD "أحضر جهازك الخاص". يوفر تسجيل المستخدم مزيدًا من الاستقلالية للمستخدمين على أجهزتهم الخاصة، بينما تزيد من أمن بيانات المؤسسة عن طريق فصل البيانات المُدارة في بيئة محمية بالتشفير. ويوفر ذلك توازنًا أفضل بين الأمن والخصوصية وتجربة المستخدم لبرامج BYOD. أُضيفَت آلية فصل بيانات مماثلة لتسجيلات الأجهزة المستندة إلى الحساب في iOS 17 و iPadOS 17 و macOS 14 أو أحدث.

أنواع التسجيل

- **تسجيل المستخدم:** تم تصميم تسجيل المستخدم للأجهزة التي يملكها المستخدم ويتم دمجها مع حسابات Apple ID المُدارة لتأسيس هوية للمستخدم على الجهاز. يلزم توفير حسابات Apple ID مُدارة لبدء التسجيل، ويجب على المستخدم إكمال المصادقة بنجاح حتى ينجح التسجيل. يمكن استخدام Apple ID المُدار إلى جانب Apple ID الشخصي الذي سجَّل المستخدم الدخول به بالفعل. تستخدم التطبيقات والحسابات المُدارة حسابات Apple ID المُدار، وتستخدم التطبيقات والحسابات الشخصية Apple ID شخصيًا.
- **تسجيل الجهاز:** يتيح تسجيل الجهاز للمؤسسات السماح للمستخدمين بتسجيل الأجهزة يدويًا، ثم إدارة العديد من جوانب استخدام الجهاز المختلفة، بما في ذلك إمكانية مسح الجهاز. يتضمن تسجيل الجهاز أيضًا مجموعة أكبر من التكوينات والقيود التي يمكن تطبيقها على الجهاز. عندما يُزيل المستخدم ملف تعريف التسجيل، تتم إزالة كل التكوينات والإعدادات والتطبيقات المُدارة المستندة إلى ملف تعريف التسجيل هذا. على غرار تسجيل المستخدم، يمكن أيضًا دمج تسجيل الجهاز مع حساب Apple ID مُدار. يتيح تسجيل الجهاز المستند إلى الحساب أيضًا إمكانية استخدام حساب Apple ID مُدار مع Apple ID شخصي ويفصل بيانات الشركة في بيئة محمية بالتشفير.
- **تسجيل الجهاز المؤتمت:** يسمح تسجيل الجهاز التلقائي للمؤسسات بتكوين الأجهزة وإدارتها من اللحظة التي يتم فيها إخراج الأجهزة. وتكون هذه الأجهزة معروفة على أنها **خاضعة للإشراف**، ويتوفر للمستخدمين خيار منع إزالة ملف تعريف MDM من قِبل المستخدم. تم تصميم تسجيل الجهاز المؤتمت للأجهزة التي تملكها المؤسسة.

قيود الجهاز

يمكن للمسؤولين تمكين القيود، أو تعطيلها في بعض الحالات، للمساعدة على منع المستخدمين من الوصول إلى تطبيق معين أو خدمة أو وظيفة معينة على iPhone أو iPad أو Mac أو Apple TV أو Apple Watch المسجَّل في حل MDM. تُرسَل القيود إلى الأجهزة في حمولة قيود تعد جزءًا من التكوين. قد يتم عكس بعض القيود المفروضة على iPhone على Apple Watch مقترنة.

إدارة إعدادات رمز الدخول وكلمة السر

بشكل افتراضي، يمكن تحديد رمز دخول المستخدم على أنه رمز PIN رقمي على iOS و iPadOS و watchOS. في أجهزة iPhone و iPad التي تحتوي على بصمة الوجه أو بصمة الإصبع، يبلغ الطول الافتراضي لرمز الدخول ستة أرقام بينما يبلغ الحد الأدنى أربعة أرقام. نظرًا لأن رموز الدخول الأطول والأكثر تعقيدًا يصعب تخمينها أو مهاجمتها، فإنه من المستحسن استخدامها.

يمكن أن يفرض المسؤولون متطلبات معقدة وسياسات أخرى لرمز الدخول باستخدام MDM أو على iOS و iPadOS و Microsoft Exchange. ويلزم توفير كلمة سر مسؤول عند تثبيت حمولة سياسة رمز دخول macOS يدويًا. قد تتطلب سياسات رموز الدخول طولًا أو تكوينًا معينًا أو سمات أخرى لرمز الدخول.

تستخدم Apple Watch رموز الدخول الرقمية بشكل افتراضي. إذا تتطلبت سياسة رمز الدخول المطبقة على Apple Watch مُدارة استخدام أحرف غير رقمية، يجب استخدام iPhone المقترن لفتح قفل الجهاز.

فرض التكوين

التكوينات هي الطريقة الأساسية التي يقدم بها حل MDM السياسات والقيود ويديرها على الأجهزة المُدارة. إذا كانت المؤسسات تريد تكوين عدد كبير من الأجهزة أو تقديم الكثير من إعدادات البريد الإلكتروني المخصصة أو إعدادات الشبكة أو الشهادات لعدد كبير من الأجهزة، فإن التكوينات تعد طريقة آمنة لتنفيذ ذلك.

التكوينات

التكوين عبارة عن ملف تعريف XML أو ملف بصيغة json يتبع بنية معينة ويتكون من حمولات تقوم بتحميل معلومات المصادقة والإعدادات على أجهزة Apple. تعمل التكوين على التنفيذ التلقائي لتكوين الإعدادات والحسابات والقيود وبيانات الاعتماد. يمكن إنشاء هذه الملفات بواسطة حل MDM أو أداة إعداد Apple لـ Mac، أو يمكن إنشاؤها يدويًا. قبل أن ترسل المؤسسات التكوين إلى جهاز Apple، يجب عليها تسجيل الجهاز في حل MDM باستخدام ملف تعريف التسجيل.

ملاحظة: يمكن استخدام أداة إعداد Apple لـ Mac لإدارة ملفات تعريف التكوين على iPhone و iPad و Apple TV فقط.

ملفات تعريف التسجيل

ملف تعريف التسجيل عبارة عن ملف تعريف تكوين يتضمن حمولة MDM تسجِّل الجهاز في حل MDM المحدد لهذا الجهاز. ويتيح ذلك لحل MDM إرسال الأوامر والتكوينات إلى الجهاز والاستعلام عن بعض الجوانب المعينة في الجهاز. عندما يُزيل مستخدم ملف تعريف التسجيل، تتم إزالة كل التكوينات وإعداداتها، وحسب نوع التسجيل والتكوين المُستخدَم، تتم إزالة التطبيقات المُدارة بناءً على ملف تعريف التسجيل هذا أيضًا. ولا يمكن وجود سوى ملف تعريف تسجيل واحد فقط على الجهاز في كل مرة.

مثال عن التكوينات

تكوين يحتوي على عدد من الإعدادات في حمولات معينة يمكن تحديدها، بما في ذلك (على سبيل المثال لا الحصر):

- سياسات رمز الدخول وكلمة السر
- القيود على ميزات الجهاز (على سبيل المثال، تعطيل الكاميرا)
- إعدادات الشبكة و VPN
- إعدادات Microsoft Exchange
- إعدادات البريد
- إعدادات الحساب
- إعدادات خدمة دليل LDAP
- إعدادات خدمة تقويم CalDAV
- بيانات الاعتماد والهويات
- الشهادات
- تحديثات البرامج

توقيع وتشفير ملف التعريف

يمكن توقيع ملفات تعريف التكوين للتحقق من مصدرها وتشفيرها وللمساعدة على ضمان سلامتها وحماية محتوياتها. ويتم تشفير ملفات تعريف التكوين لكل من iOS و iPadOS باستخدام صياغة رسالة الترميز (CMS) المحددة في RFC 5652، مع دعم 3DES و AES128.

تثبيت ملف التعريف

يمكن تثبيت التكوينات على الأجهزة باستخدام حل MDM أو يدويًا عن طريق المستخدمين. أو يمكن استخدام أداة إعداد Apple لـ Mac لنشر التكوينات على جهاز iOS و iPadOS و tvOS. تتطلب بعض التكوينات التثبيت باستخدام حل MDM. للاطلاع على معلومات حول كيفية إزالة ملفات التعريف، انظر مقدمة عن برنامج إدارة الأجهزة المحمولة في نشر أنظمة Apple الأساسية.

ملاحظة: على الأجهزة الخاضعة للإشراف، يمكن أيضًا قفل ملفات تعريف التكوين على الجهاز. وقد تم تصميم ذلك لمنع إزالتها تمامًا أو للسماح بالإزالة فقط باستخدام رمز دخول.

تسجيل الجهاز المؤتمت

يمكن أن تسجِّل المؤسسات أجهزة iOS و iPadOS و macOS و tvOS تلقائيًا في حل إدارة الأجهزة المحمولة (MDM) دون الحاجة إلى لمس الأجهزة باليد أو إعدادها قبل أن يحصل عليها المستخدمون. بعد التسجيل في إحدى الخدمات في Apple School Manager أو Apple Business Manager أو Apple Business Essentials، يسجّل المسؤولون الدخول إلى موقع الخدمة الإلكتروني ويربط البرنامج بحل MDM. ويمكنه بعد ذلك تعيين الأجهزة التي يشتريها للمستخدمين من خلال MDM. أثناء عملية تكوين الجهاز، يستعلم الجهاز عن خوادم Apple لـ MDM المعيَّنة، وإذا كان الأمر كذلك، فإنه يتواصل مع حل MDM لإجراء التسجيل. يسمح استخدام تسجيل الجهاز التلقائي وحل MDM المتوافق للمؤسسات بتنفيذ التدابير الأمنية التالية:

- اطلب من المستخدمين المصادقة كجزء من تدفق الإعداد الأولي في مساعد الإعداد بجهاز Apple أثناء التنشيط.
- قم بتوفير تكوين أولي ذي وصول محدود واشترط تكوينًا إضافيًا بالجهاز للوصول إلى البيانات الحساسة.

- اطلب من الأجهزة تشغيل أقل إصدار من نظام التشغيل قبل التسجيل.
- شغِّل تمكين خزنة الملفات على أجهزة Mac.

بعد تسجيل الجهاز باستخدام MDM، تُثبَّت أي تكوينات أو قيود أو عناصر تلقائيًا.

يمكن تبسيط عملية الإعداد للمستخدمين بشكل أكبر عن طريق إزالة خطوات محددة في مساعد الإعداد بالأجهزة، بحيث يصبح المستخدمون جاهزين للعمل بسرعة. في حالة تخطي الخطوات،يُستخدَم إعداد الحفاظ على الخصوصية بشكل أكبر. على سبيل المثال، في حالة تخطي جزء تكوين خدمات الموقع، لن تُمكَّن الخدمة أثناء استخدام مساعد الإعداد.

ويمكن للمسؤولين أيضًا التحكم فيما إذا كان يمكن للمستخدمين إزالة ملف تعريف MDM من الجهاز والمساعدة على ضمان استخدام التكوينات والقيود خلال دورة حياة الجهاز.

Apple School Manager و Apple Business Manager و Apple Business Essentials

تُعد Apple School Manager و Apple Business Manager و Apple Business Essentials خدمات لمسؤولي تقنية المعلومات لنشر أجهزة Apple التي اشترتها مؤسسة ما مباشرةً من Apple أو من شركات الاتصالات وجهات التوزيع المشاركة المعتمدة لدى Apple.

عند استخدامها مع حل MDM، يمكن للمسؤولين تبسيط عملية الإعداد للمستخدمين وتهيئة إعدادات الجهاز وتوزيع التطبيقات والكتب التي تم شراؤها على هذه الخدمات الثلاث. يتكامل Apple School Manager أيضًا مع أنظمة معلومات الطلاب (SIS) مباشرةً أو باستخدام SFTP، وتدعم جميع الخدمات الثلاث مزامنة الدليل والمصادقة الموحدة، بحيث يمكن توفير الحسابات وتحديثها وإلغاء توفيرها تلقائيًا بناءً على مزود خدمة بطاقة الهوية للمؤسسة (IdP).

تحتفظ Apple بالشهادات على أساس الامتثال لمعياري ISO/IEC 27001 و ISO/IEC 27018 لتمكين عملاء Apple من تلبية التزاماتهم التنظيمية والتعاقدية. وتوفر هذه الشهادات لعملائنا توثيقًا مستقلاً إزاء ممارسات خصوصية وأمن المعلومات التي تنتهجها Apple للأنظمة الواقعة ضمن النطاق. لمزيد من المعلومات، انظر شهادات أمن خدمات الإنترنت من Apple في شهادات أنظمة Apple الأساسية.

ملاحظة: لمعرفة مدى توافر برنامج من برامج Apple في بلد أو منطقة معينة، انظر مقال دعم Apple مدى توفر برامج Apple وطرق الدفع للتعليم والأعمال.

الإشراف على الجهاز

بشكل عام، يعني **الإشراف** أن الجهاز مملوك للمؤسسة، مما يمنحها مزيدًا من التحكم في تكوين الجهاز وقيوده. لمزيد من المعلومات، انظر حول الإشراف على جهاز Apple في نشر أنظمة Apple الأساسية.

يتم تمكين الإشراف تلقائيًا على الجهاز عند استخدام تسجيل الجهاز التلقائي.

أمن قفل التنشيط

تختلف طريقة تطبيق Apple لقفل التنشيط اعتمادًا على ما إذا كان الجهاز عبارة عن iPhone أو iPad أو Mac مزود بسيليكون Apple، أو Mac مستند إلى Intel مزود بشريحة Apple T2 الأمنية.

السلوك على iPhone و iPad

على أجهزة iPhone و iPad، يتم فرض قفل التنشيط من خلال عملية التنشيط بعد شاشة تحديد Wi-Fi في مساعد إعداد iOS و iPadOS. عندما يشير الجهاز إلى أنه قيد التنشيط، فإنه يرسل طلبًا إلى خادم Apple للحصول على شهادة تنشيط. الأجهزة التي تم قفل التنشيط عليها تطالب المستخدم ببيانات اعتماد iCloud للمستخدم الذي قام بتمكين قفل التنشيط في هذا الوقت. ولن يتقدم مساعد إعداد iOS و iPadOS ما لم يتم الحصول على شهادة صالحة.

السلوك على Mac مزود بسيليكون Apple

على الـ Mac المزود بسيليكون Apple، يتحقق LLB من وجود LocalPolicy صالحة للجهاز وأن القيم غير القابلة لإعادة التشغيل لسياسة LocalPolicy تطابق القيم المخزنة في مكون التخزين الآمن. يقوم محمّل إقلاع المستوى الأدنى (LLB) بالتشغيل إلى recoveryOS في الحالات الآتية:

- عدم وجود LocalPolicy في macOS الحالي
- عدم صلاحية LocalPolicy لهذا الـ macOS
- عدم تطابق قيم تجزئة القيم غير القابلة لإعادة الشغيل لسياسة LocalPolicy مع علامات تجزئة القيم المخزنة في مكون التخزين الآمن

يكتشف recoveryOS أن كمبيوتر Mac لم يتم تنشيطه ويتصل بخادم التنشيط للحصول على شهادة تنشيط. إذا تم قفل تنشيط الجهاز، فإن recoveryOS يطالب المستخدم ببيانات اعتماد iCloud للمستخدم الذي قام بتمكين قفل التنشيط في هذا الوقت. بعد الحصول على شهادة تنشيط صالحة، يتم استخدام مفتاح شهادة التنشيط هذا للحصول على شهادة RemotePolicy. يستخدم كمبيوتر Mac مفتاح LocalPolicy وشهادة RemotePolicy لإنتاج LocalPolicy صالحة. لن يسمح LLB بتمهيد macOS ما لم توجد LocalPolicy صالحة.

سلوك أجهزة كمبيوتر Mac المستندة إلى Intel

في الـ Mac المستند إلى Intel المزود بشريحة T2، يتحقق البرنامج الثابت لشريحة T2 من وجود شهادة تنشيط صالحة قبل السماح للكمبيوتر بالتمهيد إلى macOS. ويكون برنامج UEFI الثابت الذي يتم تحميله بواسطة شريحة T2 هو المسؤول عن الاستعلام عن حالة تنشيط الجهاز من شريحة T2 وتشغيل نظام recoveryOS بدلاً من التمهيد إلى macOS في حالة عدم وجود شهادة تنشيط صالحة. يكتشف recoveryOS أن الـ Mac لم يتم تنشيطه ويتصل بخادم التنشيط للحصول على شهادة تنشيط. إذا تم قفل تنشيط الجهاز، فإن recoveryOS يطالب المستخدم ببيانات اعتماد iCloud للمستخدم الذي قام بتمكين قفل التنشيط في هذا الوقت. لن يسمح برنامج UEFI الثابت بتشغيل macOS ما لم يتم الحصول على شهادة تنشيط صالحة.

نمط الفقدان المُدار والمسح عن بُعد

يُستخدم نمط الفقدان المُدار لتحديد موقع الأجهزة الخاضعة للإشراف في حالة سرقتها. بعد تحديد موقعها، يمكن قفلها أو مسحها عن بُعد.

نمط الفقدان المُدار

إذا تم فقد أو سرقة جهاز iOS أو iPadOS خاضع للإشراف مثبت عليه iOS 9 أو أحدث، يستطيع مسؤول إدارة جهاز الجوال (MDM) تمكين نمط الفقدان على هذا الجهاز عن بُعد (يسمى نمط الفقدان المُدار). عند تمكين نمط الفقدان المُدار، يتم تسجيل خروج المستخدم الحالي ولا يمكن فتح قفل الجهاز. وتعرض الشاشة رسالة يمكن للمسؤول تخصيصها، مثل عرض رقم هاتف للاتصال به إذا تم العثور على الجهاز. يستطيع المسؤول أن يطلب من الجهاز إرسال موقعه الحالي (حتى إذا كانت خدمات الموقع معطلة) وتشغيل صوت اختياريًا. عندما يقوم المسؤول بإيقاف نمط الفقدان المُدار، الذي يعد الطريقة الوحيدة التي يمكن بها الخروج من النمط، يتم إعلام المستخدم بهذا الإجراء من خلال رسالة على شاشة القفل أو تنبيه على الشاشة الرئيسية.

المسح عن بُعد

يمكن أن يمسح أحد المسؤولين أو المستخدمين iPhone و iPad و Mac و Apple TV و Apple Watch عن بُعد، مما يؤدي إلى عرض جميع البيانات على أنها غير قابلة للقراءة.

عند تشغيل أمر مسح عن بُعد بواسطة MDM أو iCloud، يرسل جهاز تأكيدًا إلى حل MDM مرة أخرى وينفذ المسح. بالنسبة للمسح عن بُعد عبر Microsoft Exchange ActiveSync، يتحقق الجهاز من خلال خادم Microsoft Exchange قبل إجراء المسح.

ولا يمكن إجراء المسح عن بُعد في الحالات التالية:

- مع تسجيل المستخدم
- استخدام Microsoft Exchange ActiveSync عندما يكون الحساب المثبّت يستخدم تسجيل المستخدم
- استخدام Microsoft Exchange ActiveSync إذا كان الجهاز خاضعًا للإشراف

يمكن أن يمسح المستخدمون أيضًا الأجهزة المدعومة التي بحوزتهم باستخدام الإعدادات (iPhone و iPad) أو إعدادات النظام (Mac). وكما ذُكر، يمكن تعيين أجهزة iPhone و iPad و Apple Watch على المسح تلقائيًا بعد سلسلة من محاولات إدخال رمز الدخول الفاشلة.

يتوفر المسح الفوري عن بُعد على أجهزة كمبيوتر Mac المزودة برقاقات Apple وأجهزة كمبيوتر Mac المزودة بشريحة Apple T2 الأمنية أو في حالة تشغيل خزنة الملفات. يتم المسح الفوري عن بُعد بتجاهل مفتاح الوسائط بأمان.

أمن الـ iPad المشترَك في iPadOS

الـ iPad المشترَك عبارة عن وضع متعدد المستخدمين يُستخدم في عمليات نشر الـ iPad. ويسمح للمستخدمين بمشاركة الـ iPad مع الحفاظ على فصل المستندات والبيانات لكل مستخدم. يحصل كل مستخدم على موقع تخزين خاص به ومحجوز له، يتم تنفيذه كوحدة تخزين APFS (نظام ملفات Apple) محمية ببيانات اعتماد المستخدم. يتطلب iPad المشترك استخدام Apple ID مُدار الصادر والمملوك من قِبل المؤسسة.

باستخدام iPad المشترك، يمكن للمستخدم تسجيل الدخول إلى أي جهاز تملكه المؤسسة وتم تكوينه للاستخدام من قِبل عدة مستخدمين. تُقسَّم بيانات المستخدم إلى أدلة منفصلة، كلٌ في مجالات حماية البيانات الخاصة بها وتكون محمية بواسطة أذونات UNIX ووضع الحماية. في iPadOS 13.4 أو أحدث، يمكن للمستخدمين أيضًا تسجيل الدخول إلى جلسة مؤقتة. عندما يقوم المستخدم بتسجيل الخروج من الجلسة المؤقتة، يتم حذف وحدة بيانات APFS الخاصة به، ويتم إرجاع المساحة المحجوزة إلى النظام.

تسجيل الدخول إلى الـ iPad المشترك

يتم دعم كل من حسابات Apple ID المُدارة المحلية والموحدة عند تسجيل الدخول إلى الـ iPad المشترَك. عند استخدام حساب موحّد للمرة الأولى، يُعاد توجيه المستخدم إلى بوابة تسجيل دخول موفر الهوية (IdP). بعد المصادقة، يتم إصدار رمز وصول قصير الأجل لحسابات Apple ID المُدارة المساندة، وتستمر عملية تسجيل الدخول بشكل مشابه لعملية تسجيل الدخول إلى حسابات Apple ID المُدارة الأصلية. بعد تسجيل الدخول، يطالب مساعد الإعداد على الـ iPad المشترَك المستخدم بإنشاء رمز دخول (بيانات اعتماد) يُستخدم لتأمين البيانات المحلية على الجهاز والمصادقة على شاشة تسجيل الدخول في المستقبل. مثل جهاز المستخدم الفردي، الذي يسجّل معه المستخدم الدخول مرة واحدة إلى Apple ID المُدار الخاص به باستخدام حسابه الموحَّد ثم يفتح قفل جهازه باستخدام رمز الدخول الخاص به، يقوم المستخدم على الـ iPad المشترَك بتسجيل الدخول مرة واحدة باستخدام حسابه الموحَّد، ومن ذلك الحين يستخدم رمز الدخول المكوَّن الخاص به.

عندما يسجل المستخدم دخوله دون مصادقة موحدة، تتم مصادقة Apple ID المُدار مع خدمة الهوية من Apple (IDS) باستخدام بروتوكول SRP. وإذا نجحت المصادقة، يتم منح رمز وصول قصير الأجل خاص بالجهاز. إذا كان المستخدم قد استخدم الجهاز من قبل، فلديه بالفعل حساب مستخدم محلي تم فتح قفله باستخدام بيانات الاعتماد ذاتها.

إذا لم يكن المستخدم قد استخدم الجهاز من قبل أو كان يستخدم ميزة الجلسة المؤقتة، فإن الـ iPad المشترَك يوفر معرف مستخدم UNIX جديدًا ووحدة تخزين APFS لتخزين البيانات الشخصية للمستخدم وسلسلة مفاتيح محلية. نظرًا لأنه يتم تخصيص (حجز) مساحة التخزين للمستخدم وقت إنشاء وحدة تخزين APFS، فقد لا تكون هناك مساحة كافية لإنشاء وحدة تخزين جديدة. في هذه الحالة، يحدد النظام مستخدمًا موجودًا انتهت مزامنة بياناته مع السحابة ويمسح بيانات ذلك المستخدم من الجهاز بحيث يتمكن المستخدم الجديد من تسجيل الدخول. وفي الحالات نادرة الحدوث التي لم يكتمل فيها تحميل البيانات السحابية لجميع المستخدمين الموجودين، يفشل تسجيل دخول المستخدم الجديد. لتسجيل الدخول، سيحتاج المستخدم الجديد إلى انتظار انتهاء مزامنة بيانات أحد المستخدمين، أو أن يقوم المسؤول بحذف حساب أحد المستخدمين الموجودين دون انتظار، وبالتالي المخاطرة بفقدان البيانات.

إذا لم يكن الجهاز متصلاً بالإنترنت (على سبيل المثال، إذا لم يكن لدى المستخدم نقطة وصول إلى شبكة Wi-Fi)، فقد تحدث المصادقة على الحساب المحلي لعدد محدود من الأيام. في هذه الحالة، لا يمكن تسجيل الدخول إلا للمستخدمين الذين لديهم حسابات محلية موجودة سابقًا أو للجلسات المؤقتة. وبعد انتهاء المهلة الزمنية، يُطلب من المستخدم المصادقة عبر الإنترنت، حتى في حالة وجود حساب محلي بالفعل.

بعد فتح قفل الحساب المحلي للمستخدم أو إنشائه، إذا تمت مصادقته عن بُعد، يتم تحويل الرمز قصير الأجل الصادر من خوادم Apple إلى رمز iCloud يسمح بتسجيل الدخول إلى iCloud. بعد ذلك، تتم استعادة إعدادات المستخدم وتتم مزامنة مستنداته وبياناته من iCloud.

بينما تكون جلسة المستخدم نشطة مع استمرار اتصال الجهاز بالإنترنت، يتم تخزين المستندات والبيانات على iCloud عند إنشائها أو تعديلها. بالإضافة إلى ذلك، تساعد آلية مزامنة الخلفية على ضمان دفع التغييرات إلى iCloud أو لخدمات الويب الأخرى باستخدام جلسات NSURLSession في الخلفية، بعد تسجيل خروج المستخدم. بعد اكتمال مزامنة الخلفية لهذا المستخدم، يتم إلغاء تثبيت وحدة تخزين APFS للمستخدم ولا يمكن تثبيتها مرة أخرى دون تسجيل دخول المستخدم مجددًا.

لا تقوم الجلسات المؤقتة بمزامنة البيانات مع iCloud، وعلى الرغم من أن الجلسة المؤقتة تستطيع تسجيل الدخول إلى خدمة مزامنة تابعة لجهة خارجية مثل Box أو Google Drive، فلا توجد إمكانية لمواصلة مزامنة البيانات عند انتهاء الجلسة المؤقتة.

تسجيل الخروج من الـ iPad المشترَك

عندما يسجل المستخدم الخروج من الـ iPad المشترَك، يتم قفل حاوية مفاتيح هذا المستخدم على الفور ويتم إيقاف تشغيل جميع التطبيقات. لتسريع حالة تسجيل دخول مستخدم جديد، يؤجّل iPadOS بعض إجراءات تسجيل الخروج الاعتيادية مؤقتًا ويقدّم نافذة تسجيل دخول للمستخدم الجديد. وإذا سجّل أحد المستخدمين دخوله خلال هذا الوقت (حوالي 30 ثانية)، ينفّذ الـ iPad المشترَك عملية التنظيف المؤجلة كجزء من تسجيل الدخول إلى حساب المستخدم الجديد. لكن إذا ظل الـ iPad المشترَك خاملاً، يتم تشغيل عملية التنظيف المؤجلة. أثناء مرحلة التنظيف، يُعاد تشغيل نافذة تسجيل الدخول كما لو أن تسجيل خروج آخر قد حدث.

عند انتهاء الجلسة المؤقتة، ينفذ الـ iPad المشترَك تسلسل الخروج الكامل ويحذف وحدة تخزين APFS للجلسة المؤقتة على الفور.

أمن أداة إعداد Apple

تتميز أداة إعداد Apple لـ Mac بتصميم مرن آمن متمركز على الجهاز يتيح للمسؤول تكوين جهاز واحد أو عشرات من أجهزة iOS و iPadOS و tvOS المتصلة بـcaM عبر USB (أو أجهزة tvOS المقترنة عبر Bonjour) بسرعة وسهولة قبل تسليمها للمستخدمين. باستخدام أداة إعداد Apple لـ Mac يمكن للمسؤول تحديث البرامج وتثبيت التطبيقات وملفات تعريف التكوين وإعادة تسمية خلفية الشاشة وتغييرها على الأجهزة وتصدير معلومات الجهاز والمستندات والمزيد.

كما يمكن لأداة إعداد Apple لـ Mac إنعاش أو استعادة أجهزة كمبيوتر Mac المزودة برقاقات Apple وتلك المزودة بشريحة Apple T2 الأمنية. عندما يتم إنعاش Mac أو استعادته بهذه الطريقة، يتم تنزيل الملف الذي يحتوي على آخر التحديثات الثانوية لأنظمة التشغيل (macOS أو recoveryOS لرقاقات Apple أو sepOS for T2) بأمان من خوادم Apple وتثبيته مباشرة على الـ Mac. بعد الإنعاش أو الاستعادة الناجحة، يتم حذف الملف من جهاز Mac الذي يشغل أداة إعداد Apple. لا يمكن للمستخدم في أي وقت فحص هذا الملف واستخدامه خارج أداة إعداد Apple.

يمكن للمسؤولين كذلك اختيار إضافة أجهزة إلى Apple School Manager أو Apple Business Manager أو Apple Business Essentials باستخدام أداة إعداد Apple لـ Mac أو أداة إعداد Apple لـ iPhone، حتى إذا لم يتم شراء الأجهزة مباشرةً من Apple أو موزّع معتمد من Apple أو شركة اتصالات خلوية معتمدة. عندما يقوم المسؤول بإعداد جهاز تم تسجيله يدويًا، فإنه يتصرف مثل أي جهاز آخر مسجل في إحدى تلك الخدمات، مع إشراف إلزامي وتسجيل في برنامج إدارة الأجهزة المحمولة (MDM). بالنسبة إلى الأجهزة التي لم يتم شراؤها مباشرةً، تكون لدى المستخدم فترة مؤقتة مدتها 30 يومًا لتحرير الجهاز من إحدى تلك الخدمات والإشراف وحل MDM.

يمكن للمؤسسات كذلك استخدام أداة إعداد Apple لـ Mac لتنشيط أجهزة iOS و iPadOS و tvOS التي لا تحتوي على اتصال بالإنترنت على الإطلاق من خلال توصيلها بجهاز Mac مضيف متصل بالإنترنت أثناء إعداد الأجهزة. يستطيع المسؤولون استعادة الأجهزة وتنشيطها وإعدادها باستخدام تكوينها الضروري، بما في ذلك التطبيقات وملفات التعريف والمستندات، دون حتى الحاجة إلى الاتصال إما بشبكات Wi-Fi أو الشبكات الخلوية. ولا تسمح هذه الميزة للمسؤول بتجاوز أي متطلبات حالية لقفل التنشيط تكون مطلوبة عادةً أثناء التنشيط غير المُقيّد.

أمن مدة استخدام الجهاز

تُعد مدة استخدام الجهاز ميزة مضمنة لرؤية وإدارة الوقت الذي يقضيه البالغون وأطفالهم على التطبيقات والمواقع الإلكترونية والمزيد. ثمة نوعان من المستخدمين: البالغون والأطفال (المُدارون).

على الرغم من أن مدة استخدام الجهاز ليست ميزة أمن جديدة في النظام، فمن المهم فهم كيفية حمايتها لخصوصية وأمن البيانات التي يتم تجميعها ومشاركتها بين الأجهزة. تتوفر ميزة مدة استخدام الجهاز على iOS 12 أو أحدث و iPadOS 13.1 أو أحدث و macOS 10.15 أو أحدث وبعض ميزات watchOS 6 أو أحدث.

يوضح الجدول الوارد أدناه الميزات الرئيسية في خاصية مدة استخدام الجهاز.

الميزة	نظام التشغيل المدعوم
عرض بيانات الاستخدام	iOS iPadOS macOS
فرض قيود إضافية	iOS iPadOS macOS watchOS
تعيين حدود استخدام الويب	iOS iPadOS macOS
تعيين حدود التطبيق	iOS iPadOS macOS watchOS
تكوين وقت التوقف	iOS iPadOS macOS watchOS

بالنسبة للمستخدم الذي يدير استخدام جهازه الخاص، يمكن مزامنة عناصر التحكم وبيانات الاستخدام في مدة استخدام الجهاز عبر الأجهزة المرتبطة بحساب iCloud نفسه باستخدام تشفير CloudKit الكامل. وهذا يتطلب أن يكون حساب المستخدم قد تم تمكين المصادقة بخطوتين عليه (تكون المزامنة قيد التشغيل بشكل افتراضي). تحل ميزة مدة استخدام الجهاز محل ميزة القيود الموجودة في الإصدارات السابقة من iOS و iPadOS وميزة الإشراف العائلي الموجودة في الإصدارات السابقة من macOS.

في iOS 13 أو أحدث و iPadOS 13.1 أو أحدث و macOS 10.15 أو أحدث، يشارك مستخدمو ميزة مدة استخدام الجهاز والأطفال المُدارة حساباتهم استخدامهم تلقائيًا عبر الأجهزة إذا تم تمكين المصادقة بخطوتين لحسابات iCloud الخاصة بهم. وعندما يمسح المستخدم سجل تاريخ سفاري أو يحذف تطبيقًا، تتم إزالة بيانات الاستخدام المقابلة من الجهاز وجميع الأجهزة المتزامنة.

أولياء الأمور ومدة استخدام الجهاز

يستطيع أولياء الأمور أيضًا استخدام ميزة مدة استخدام الجهاز في أجهزة iOS و iPadOS و macOS لفهم استخدام أطفالهم للجهاز والتحكم فيه. إذا كان ولي الأمر منظمًا للعائلة (في المشاركة العائلية على iCloud)، يمكنه عرض بيانات الاستخدام وإدارة إعدادات مدة استخدام الجهاز لأطفاله. يتم إخبار الأطفال عندما يشغّل أولياء أمورهم مدة استخدام الجهاز، ويمكنهم مراقبة استخدامهم الخاص أيضًا. عندما يشغّل أولياء الأمور مدة استخدام الجهاز لأطفالهم، يقوم أولياء الأمور بتعيين رمز دخول حتى لا يتمكن أطفالهم من إجراء تغييرات. وبعد أن يبلغ الطفل سن البلوغ (يختلف العمر حسب البلد أو المنطقة)، يمكنه إيقاف هذه المراقبة.

تُنقل بيانات الاستخدام وإعدادات التكوين بين جهازي ولي الأمر والطفل باستخدام بروتوكول خدمة الهوية من Apple (IDS) المشفرة تشفيرًا كاملاً. قد تُخزَّن البيانات المشفرة لفترة وجيزة على خوادم IDS حتى تتم قراءتها بواسطة جهاز الاستقبال (على سبيل المثال، بمجرد تشغيل iPhone أو iPad، إذا كان مغلقًا). ولا تتوفر لدى Apple إمكانية قراءة هذه البيانات.

تحليلات مدة استخدام الجهاز

إذا شغّل المستخدم مشاركة تحليلات iPhone وhctaW، فلا يتم جمع سوى البيانات المجهولة التالية حتى تتمكن Apple من فهم كيفية استخدام ميزة مدة استخدام الجهاز بشكل أفضل:

- هل تم تشغيل مدة استخدام الجهاز أثناء مساعد الإعداد أم لاحقًا في الإعدادات
- التغيير في استخدام الفئة بعد إنشاء حد له (خلال 90 يومًا)
- هل تم تشغيل مدة استخدام الجهاز
- هل تم تمكين وقت التوقف
- عدد مرات استخدام استعلام "طلب المزيد"
- عدد حدود التطبيقات
- عدد المرات التي عرض فيها المستخدمون معلومات الاستخدام في إعدادات مدة استخدام الجهاز ونوع كل مستخدم ونوع كل عرض (محلي أم بعيد أم أداة)
- عدد مرات تجاهل المستخدمين للحد، حسب نوع المستخدم
- عدد مرات حذف المستخدمين للحد، حسب نوع المستخدم

لا تجمع Apple بيانات أي تطبيق محدد أو استخدام للويب. عندما يرى المستخدم قائمة التطبيقات في معلومات استخدام ميزة مدة استخدام الجهاز، يتم سحب أيقونات التطبيقات مباشرةً من App Store، ومن ثم لا يتم الاحتفاظ بأي بيانات من هذه الطلبات.

المعجم

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

البرامج الثابتة لواجهة البرامج الثابتة القابلة للتوسعة الموحدة (UEFI) تقنية بديلة لـ BIOS تُستخدم لربط البرامج الثابتة بنظام التشغيل الخاص بجهاز الكمبيوتر.

التخزين القابل للمسح مساحة مخصصة لتخزين NAND تُستخدم لتخزين مفاتيح التشفير ويمكن معالجتها مباشرةً ومسحها بشكل آمن. وعلى الرغم من أنها لا توفر الحماية إذا كان الجهاز بحوزة المهاجم فعليًا، يمكن استخدام المفاتيح الموجودة في التخزين القابل للمسح كجزء من تسلسل هرمي للمفاتيح لتسهيل المسح السريع والأمن المتقدم.

التشابك العملية التي يتم من خلالها تحويل رمز الدخول الخاص بالمستخدم إلى مفتاح تشفير وتعزيزه باستخدام معرف UID للجهاز. وتساعد هذه العملية على ضمان حتمية تنفيذ الهجوم بقوة غاشمة على جهاز معين، وبالتالي يكون بمعدل محدود ولا يمكن تنفيذه بشكل متوازٍ. خوارزمية التشابك هي PBKDF2 التي تستخدم AES مرتبطًا بمعرف UID الخاص بالجهاز كوظيفة عشوائية زائفة (PRF) لكل تكرار.

الحارس الرقمي في macOS، يعد تقنية مصممة للمساعدة على ضمان تشغيل البرامج الموثوقة فقط على الـ Mac الخاص بالمستخدم.

الدائرة المتكاملة (IC) معروفة أيضًا باسم **رقاقة**.

المعرف الفريد (UID) مفتاح AES سعة 256 بت يتم نسخه في كل معالج عند التصنيع. ولا يمكن قراءته بواسطة البرامج الثابتة أو البرامج، ولا يُستخدم إلا بواسطة محرك AES في مكونات المعالج المادية. للحصول على المفتاح الفعلي، سيتعين على المهاجم شن هجوم مادي متطور ومكلف للغاية على السيليكون الموجود في المعالج. ولا يرتبط معرف UID بأي معرف آخر على الجهاز بما في ذلك، على سبيل المثال لا الحصر، معرف UDID.

المفتاح المشتق من رمز الدخول (PDK) مفتاح التشفير المشتق من تشابك كلمة سر المستخدم مع مفتاح SKP طويل الأجل والمعرف الفريد الخاص بـ Secure Enclave.

الوصول إلى الذاكرة المباشرة (DMA) ميزة تتيح للأنظمة الفرعية للمكونات المادية الوصول إلى الذاكرة الرئيسية مباشرةً، متجاوزة وحدة المعالجة المركزية (CPU).

تبادل منحنى القطع الناقص Diffie-Hellman (ECDHE) سريع الزوال آلية تبادل المفاتيح المستندة إلى منحنيات القطع الناقص. يتيح ECDHE للطرفين الاتفاق على مفتاح سري بطريقة تمنع من اكتشاف المفتاح بواسطة أي متنصت يراقب الرسائل بين الطرفين.

تخويل برامج النظام عملية تجمع بين مفاتيح التشفير المضمنة في المكونات المادية مع خدمة عبر الإنترنت للتحقق من عدم توفير وتثبيت غير البرامج الشرعية من Apple، المناسبة للأجهزة المدعومة، في وقت الترقية.

تعيين زاوية تدفق النتوء تمثيل رياضي لاتجاه وعرض النتوءات المستخرجة من جزء من بصمة إصبع.

تغليف المفاتيح تشفير مفتاح واحد مع آخر. يستخدم iOS و iPadOS تغليف المفاتيح NIST AES، وفقًا لمعيار RFC 3394.

حافظة المفاتيح بنية بيانات تُستخدم لتخزين مجموعة من مفاتيح الفئات. ويكون لكل نوع (مستخدم أو جهاز أو نظام أو نسخة احتياطية أو ضمان أو نسخة iCloud احتياطية) نفس التنسيق.

يحتوي الرأس على التالي: الإصدار (تم تعيينه على أربعة في iOS 12 أو أحدث) والنوع (نظام أو نسخة احتياطية أو ضمان أو نسخة iCloud احتياطية) ومعرف UUID لحافظة المفاتيح و HMAC إذا تم توقيع حافظة المفاتيح والطريقة المستخدمة في تغليف مفاتيح الفئات—تشابك مع UID أو PBKDF2، بجانب القيمة العشوائية المضافة وعدد التكرار.

قائمة مفاتيح الفئات: معرف UUID للمفتاح والفئة (الملف أو فئة حماية بيانات سلسلة المفاتيح) ونوع التغليف (مفتاح مشتق من معرف UID فقط؛ مفتاح مشتق من معرف UID ومفتاح مشتق من رمز الدخول) ومفتاح الفئة المغلف ومفتاح عام للفئات غير المتماثلة.

حماية البيانات آلية حماية الملفات وسلسلة المفاتيح لأجهزة Apple المدعومة. ويمكن أن تشير أيضًا إلى واجهات API التي تستخدمها التطبيقات لحماية الملفات وعناصر سلسلة المفاتيح.

حماية المفاتيح المؤمنة (SKP) توجد تقنية في آلية حماية البيانات تعمل على حماية أو **تأمين** مفاتيح التشفير باستخدام قياسات البرامج على النظام والمفاتيح المتوفرة في الجهاز فقط (مثل معرف UID الخاص بـ Secure Enclave).

حماية تكامل المعالج الثانوي للنظام (SCIP) آلية تستخدمها Apple مصممة لمنع تعديل البرامج الثابتة للمعالج الثانوي.

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

خدمة الهوية من Apple (IDS) دليل Apple لمفاتيح iMessage العامة وعناوين APNs وأرقام الهواتف وعناوين البريد الإلكتروني المستخدمة للبحث عن المفاتيح وعناوين الأجهزة.

خوارزمية التوقيع الرقمي لمنحنى القطع الناقص (ECDSA) خوارزمية توقيع رقمي تستند إلى تشفير منحنى القطع الناقص.

سجل تقدّم التمهيد (BPR) مجموعة من علامات المكونات المادية لنظام على شريحة (SoC) يمكن للبرامج استخدامها لتعقب أوضاع التمهيد التي يدخلها الجهاز، مثل وضع تحديث البرنامج الثابت للجهاز (DFU) ووضع الاسترداد. بعد تعيين علامة سجل تقدم التمهيد، لا يمكن محوها. وهذا يتيح للبرامج اللاحقة الحصول على مؤشر موثوق به لحالة النظام.

سلسلة المفاتيح البنية الأساسية ومجموعة واجهات API التي تستخدمها أنظمة تشغيل Apple وتطبيقات الجهات الخارجية لتخزين واسترداد كلمات السر والمفاتيح وبيانات الاعتماد الحساسة الأخرى.

عشوائية تخطيط مساحة العنوان (ASLR) تقنية تستخدمها أنظمة التشغيل لجعل نجاح هجوم الأخطاء البرمجية أكثر صعوبة. ومن خلال التأكد من عدم إمكانية التنبؤ بعناوين الذاكرة والإزاحة، لا تستطيع التعليمة البرمجية للهجوم وضع تعليمات برمجية مضمنة في هذه القيم.

مجموعة إجراءات الاختبار المشتركة (JTAG) أداة تصحيح أخطاء المكونات المادية القياسية التي يستخدمها المبرمجون ومطورو الدوائر.

محرك تشفير AES مكون مادي مخصص يقوم بتنفيذ AES.

محمّل إقلاع المستوى الأدنى (LLB) على أجهزة كمبيوتر Mac المزودة ببنية تشغيل ذات مرحلتين، يحتوي LLB على رمز يتم استدعاؤه بواسطة Boot ROM، وبدوره يقوم بتحميل iBoot، كجزء من سلسلة التمهيد الآمن.

مخزن البيانات آلية يتم فرضها بواسطة kernel للحماية من الوصول غير المصرح به إلى البيانات بغض النظر عما إذا كان التطبيق مقدِّم الطلب في حد ذاته محميًا.

معرف الشريحة الحصري (ECID) معرف 64 بت يكون فريدًا للمعالج في كل جهاز iPhone أو iPad.

معرف المجموعة (GID) مثل UID، ولكنه مشترك مع كل معالج في الفئة.

معرف الموارد المنتظم (URI) سلسلة من الأحرف التي تعرّف المورد المستند إلى الويب.

مفتاح الوسائط جزء من التسلسل الهرمي لمفاتيح التشفير الذي يساعد على توفير مسح آمن وفوري. في iOS و iPadOS و tvOS و watchOS، يُغلّف مفتاح الوسائط بيانات التعريف على وحدة تخزين البيانات (وبالتالي بدونه يكون الوصول إلى جميع مفاتيح الملفات مستحيلاً، مما يجعل الوصول إلى الملفات المحمية بحماية البيانات غير ممكن). في macOS، يغلّف مفتاح الوسائط المادة المحمية بالمفاتيح وجميع بيانات التعريف والبيانات الموجودة على وحدة تخزين خزنة الملفات المحمية. وفي كلتا الحالتين، يؤدي مسح مفتاح الوسائط إلى جعل الوصول إلى البيانات المشفرة غير ممكن.

مفتاح لكل ملف المفتاح الذي تستخدمه حماية البيانات لتشفير ملف على نظام الملفات. يتم تغليف المفتاح لكل ملف بواسطة مفتاح فئة ويتم تخزينه في بيانات تعريف الملف.

مفتاح نظام الملفات المفتاح الذي يشفّر بيانات تعريف كل ملف، بما في ذلك مفتاح الفئات الخاص به. ويتم الاحتفاظ به في التخزين القابل للمسح لتسهيل المسح السريع، بدلاً من السرية.

مكافآت Apple للإسهامات الأمنية مكافأة تقدمها Apple للباحث الذي يبلّغ عن ثغرة أمنية تؤثر على أحدث إصدار من أنظمة التشغيل، وعلى أحدث المكونات المادية عند الاقتضاء.

مكون التخزين الآمن شريحة تم تصميمها مع تعليمات ROM برمجية ثابتة ومولّد أرقام عشوائية مادي ومحركات تشفير واكتشاف العبث المادي. في الأجهزة المدعومة، يتم إقران Secure Enclave مع مكون تخزين آمن لتخزين القيم غير القابلة لإعادة التشغيل. لقراءة القيم غير القابلة لإعادة التشغيل وتحديثها، تستخدم Secure Enclave وشريحة التخزين بروتوكولاً آمنًا يساعد على ضمان الوصول الحصري إلى القيم غير القابلة لإعادة التشغيل. وتوجد أجيال متعددة من هذه التقنية مع ضمانات أمنية مختلفة.

ملف تعريف التموين قائمة خصائص (ملف .plist) موقَّعة من قِبل Apple تحتوي على مجموعة من الكيانات والاستحقاقات التي تسمح بتثبيت التطبيقات واختبارها على جهاز iOS أو iPadOS. يسرد ملف تعريف التموين للتطوير الأجهزة التي اختارها المطور للتوزيع المخصص ويحتوي ملف تعريف التموين للتوزيع على معرف التطبيق الخاص بالتطبيق الذي تم تطويره على مستوى المؤسسة.

منظم الإقلاع أداة من أدوات Mac تدعم تثبيت Microsoft Windows على أجهزة كمبيوتر Mac المدعومة.

نظام على شريحة (SoC) دائرة متكاملة (IC) تضم مكونات متعددة في شريحة واحدة. ويُعد معالج التطبيق و Secure Enclave والمعالجات الثانوية الأخرى من مكونات SoC.

واجهة الطرفيات المتسلسلة المحسنة (eSPI) ناقل الكل في واحد مصمم للاتصال المتسلسل المتزامن.

وحدات البت الجذرية البرمجية وحدات بت مخصصة في محرك Secure Enclave AES يتم إلحاقها بمعرف UID عند إنشاء مفاتيح من UID. كل بت جذري برمجي به بت قفل مقابل. يستطيع Boot ROM في Secure Enclave ونظام التشغيل أن يغيرا بشكل مستقل قيمة كل بت جذري برمجي طالما لم يتم تعيين بت القفل المقابل. بعد تعيين بت القفل، لا يمكن تعديل بت الجذر البرمجي أو بت القفل. تتم إعادة تعيين وحدات البت الجذرية البرمجية وأقفالها عند إعادة تمهيد Secure Enclave.

وحدة إدارة ذاكرة الإدخال/الإخراج (IOMMU) وحدة إدارة ذاكرة الإدخال/الإخراج. نظام فرعي في شريحة مدمجة يتحكم في الوصول إلى مساحة العنوان من أجهزة الإدخال/الإخراج والأجهزة الطرفية الأخرى.

وحدة أمن المكونات المادية (HSM) كمبيوتر متخصص مقاوم للعبث يحمي ويدير المفاتيح الرقمية.

وحدة تحكم الذاكرة النظام الفرعي في نظام على شريحة يتحكم في الواجهة بين النظام على شريحة وذاكرته الرئيسية.

وحدة تحكم SSD نظام فرعي للمكونات المادية يدير وسائط التخزين (محرك الأقراص ذو الحالة الصلبة).

وضع الاسترداد وضع يُستخدم لاستعادة العديد من أجهزة Apple إذا لم يتعرف على جهاز المستخدم بحيث يتمكن المستخدم من إعادة تثبيت نظام التشغيل.

وضع ترقية البرنامج الثابت للجهاز (DFU) وضع تنتظر فيه تعليمة Boot ROM البرمجية الخاص بجهاز ما أن يتم استردادها عبر USB. وتكون الشاشة سوداء عندما تكون في وضع DFU، لكن عند الاتصال بكمبيوتر يشغّل iTunes أو فايندر، يتم عرض المطالبة التالية: "اكتشف فايندر (أو iTunes) جهاز (iPhone أو iPad) قيد وضع الاسترداد. يتعين على المستخدم استعادة هذا الـ (iPhone أو iPad) قبل أن يمكن استخدامه مع فايندر (أو iTunes)."

AES (معيار التشفير المتقدم) معيار تشفير عالمي شائع يُستخدم لتشفير البيانات للحفاظ على خصوصيتها.

AES-XTS وضع AES محدد في IEEE 1619-2007 معني بالعمل على تشفير وسائط التخزين.

APFS (نظام ملفات Apple) نظام الملفات الافتراضي لكل من iOS و iPadOS و tvOS و watchOS وأجهزة كمبيوتر Mac المثبت عليها macOS 10.13 أو أحدث. يتميز APFS بالتشفير القوي ومشاركة مساحة التخزين واللقطات والتحجيم السريع للدليل وأساسيات نظام ملفات مُحسَّنة.

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

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

Boot ROM أول تعليمة برمجية ينفذها معالج الجهاز عند تمهيده لأول مرة. وكجزء لا يتجزأ من المعالج، لا يمكن تبديله بواسطة Apple أو أي مهاجم.

CKRecord قاموس لأزواج القيم الأساسية التي تحتوي على بيانات محفوظة في CloudKit أو تم جلبها منه.

HMAC رمز مصادقة الرسائل المستند إلى التجزئة على أساس وظيفة تجزئة التشفير.

iBoot مُحمّل الإقلاع من المرحلة 2 لأجهزة Apple. تعليمة برمجية تقوم بتحميل XNU، كجزء من سلسلة التمهيد الآمن. استنادًا إلى إنشاء نظام على شريحة (SoC)، قد يتم تحميل iBoot بواسطة محمّل إقلاع المستوى الأدنى أو مباشرةً بواسطة Boot ROM.

NAND ذاكرة فلاش غير متطايرة.

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

xART اختصار لتقنية ممتدة لمكافحة إعادة التشغيل. مجموعة من الخدمات التي توفر تخزينًا مستمرًا مشفرًا ومصدقًا عليه لـ Secure Enclave مع إمكانات مكافحة إعادة التشغيل استنادًا إلى بنية التخزين الفعلي. انظر مكون التخزين الآمن.

XNU النواة في قلب أنظمة تشغيل Apple. ومن المفترض أن تكون موثوقة، وتفرض تدابير أمنية مثل توقيع التعليمات البرمجية ووضع الحماية والتحقق من الاستحقاقات وعشوائية تخطيط مساحة العنوان (ASLR).

XProtect في macOS، يعد تقنية حماية من الفيروسات للكشف عن البرامج الضارة وإزالتها استنادًا إلى التوقيع.

سـجل تاريخ مراجعة المستند

سجل تاريخ مراجعة المستند

مايو 2024

الموضوعات المضافة:

- تجزئة ملف بيانات Image4 الخاص بـ Cryptex1 (spih)
- إنشاء Cryptex1(stng)
- BlastDoor للرسائل والمعرفات
- أمن نمط المنع
- معلومات عن أمن App Store
- أمن WidgetKit

الموضوعات المُحدّثة:

- مقدمة عن أمن أنظمة Apple الأساسية
- أمن Apple SoC
- Secure Enclave
- بصمة الوجه وبصمة الإصبع ورموز المرور وكلمات السر
- أمن مطابقة الوجوه
- استخدامات بصمة الوجه وبصمة الإصبع
- البطاقات السريعة في نمط توفير الطاقة
- تكامل نظام التشغيل
- تنشيط اتصالات البيانات بشكل آمن
- التحقق من الملحقات في iPhone و iPad
- أمن الأنظمة لـ watchOS
- رموز الدخول وكلمات السر
- نظرة عامة على حماية البيانات
- حافظات المفاتيح لحماية البيانات
- حماية المفاتيح في أنماط التمهيد البديلة

- حماية بيانات المستخدم في مواجهة الهجوم
- إدارة خزنة الملفات في macOS
- مقدمة عن أمن التطبيقات في iOS و iPadOS
- الحارس الرقمي وحماية وقت التشغيل في macOS
- أمن Apple ID المُدار
- تشفير iCloud
- أمن جهة اتصال استرداد الحساب
- أمن جهة الاتصال الوارثة
- نظرة عامة على أمن سلسلة مفاتيح iCloud
- مزامنة سلسلة المفاتيح بشكل آمن
- أمن الضمان في سلسلة مفاتيح iCloud
- نظرة عامة على أمان توفير البطاقة
- إضافة بطاقات ائتمان أو سحب إلى Apple Pay
- الدفع بالبطاقات باستخدام Apple Pay
- أمن Apple Card
- أمن Tap to Pay on iPhone
- إمكانية الوصول باستخدام Apple Wallet
- أنواع مفتاح الوصول
- الهويات في Apple Wallet
- أمن الهويات في Apple Wallet
- نظرة عامة على أمن مجموعة أدوات المطورين
- أمن اتصالات HomeKit
- نظرة عامة على أمن إدارة جهاز الجوال
- فرض التكوين

ديسمبر 2022

الموضوعات المضافة:

- الحماية المتقدمة للبيانات لـ iCloud

الموضوعات المُحدّثة:

- نظرة عامة على أمن iCloud
- تشفير iCloud
- أمن نسخ iCloud الاحتياطي
- أمن جهة اتصال استرداد الحساب
- أمن جهة الاتصال الوارثة

مايو 2022

تم تحديثه لكل من:

- iOS 15.4
- iPadOS 15.4
- macOS 12.3
- tvOS 15.4
- watchOS 8.5

الموضوعات المضافة:

- قيود recoveryOS المقترن
- إصدار نظام التشغيل المحلي (love)
- مشاركة البيانات الصحية
- أمن جهة اتصال استرداد الحساب
- أمن جهة الاتصال الوارثة
- أمن Tap to Pay on iPhone
- إمكانية الوصول باستخدام Apple Wallet
- أنواع مفتاح الوصول
- الهويات في Apple Wallet
- ملحقات HomeKit التي تدعم Siri

الموضوعات المُحدّثة:

- لوحة مفاتيح ماجيك المزودة ببصمة الإصبع
- بصمة الوجه وبصمة الإصبع ورموز المرور وكلمات السر
- أمن مطابقة الوجوه
- البطاقات السريعة في نمط توفير الطاقة
- أنماط التمهيد في أجهزة كمبيوتر Mac المزودة بسيليكون Apple
- محتويات ملف LocalPolicy لأجهزة كمبيوتر Mac المزودة بسيليكون Apple
- أمن وحدة تخزين النظام
- أمن الأنظمة لـ watchOS
- جهاز الأبحاث الأمنية من Apple
- دور نظام ملفات Apple
- حماية وصول التطبيقات إلى بيانات المستخدم
- مقدمة عن أمن التطبيقات في macOS
- الحماية ضد البرامج الضارة في macOS
- نظرة عامة على أمن iCloud
- مزامنة سلسلة المفاتيح بشكل آمن

- أمن استرداد سلسلة مفاتيح iCloud
- الدفع بالبطاقات باستخدام Apple Pay
- البطاقات الذكية في Apple Pay
- جعل البطاقات غير صالحة للاستخدام مع Apple Pay
- تطبيق Apple Card
- أمن Apple Cash
- إضافة بطاقات مواصلات و eMoney إلى Apple Wallet
- أمن مراسلة الشركات من Apple
- أمن فيس تايم
- أمن مفاتيح السيارة في iOS
- أمن أداة إعداد Apple

الموضوعات المحذوفة:

- ملحقات HomeKit و iCloud

مايو 2021

تم تحديثه لكل من:

- iOS 14.5
- iPadOS 14.5
- macOS 11.3
- tvOS 14.5
- watchOS 7.4

الموضوعات المضافة:

- لوحة مفاتيح ماجيك المزودة ببصمة الإصبع.
- الغرض الآمن والاتصالات الآمنة مع Secure Enclave.
- فتح القفل التلقائي و Apple Watch.
- تجزئة ملف بيانات CustomOS لـ Image4 (coih).

الموضوعات المُحدّثة:

- تمت إضافة معاملتين جديدتين في النمط السريع ضمن قسم البطاقات السريعة في نمط توفير الطاقة.
- تم تحرير ملخص ميزة Secure Enclave.
- تمت إضافة محتوى تحديث البرامج إلى التمهيد المتعدد الآمن (smb3).
- محتوى إضافي في قسم حماية المفاتيح المؤمنة (SKP).

فبراير 2021

تم تحديثه لكل من:

- iOS 14.3
- iPadOS 14.3
- macOS 11.1
- tvOS 14.3
- watchOS 7.2

الموضوعات المضافة:

- تنفيذ iBoot الآمن للذاكرة
- عملية التمهيد في أجهزة كمبيوتر Mac المزودة بسيليكون Apple
- أنماط التمهيد في أجهزة كمبيوتر Mac المزودة بسيليكون Apple
- تتحكم سياسة أمن قرص بدء التشغيل في أجهزة كمبيوتر Mac المزودة بسيليكون Apple
- إنشاء مفتاح توقيع LocalPolicy وإدارته
- محتويات ملف LocalPolicy لأجهزة كمبيوتر Mac المزودة بسيليكون Apple
- أمن وحدة تخزين النظام
- جهاز الأبحاث الأمنية من Apple
- مراقبة كلمات السر
- أمن IPv6
- أمن مفاتيح السيارة في iOS

الموضوعات المُحدّثة:

- Secure Enclave
- قطع اتصال مكون الميكروفون المادي
- recoveryOS وبيئات التشخيص على Mac مستند إلى Intel
- وسائل حماية الوصول إلى الذاكرة المباشرة في أجهزة كمبيوتر Mac
- توسيع ملحق kernel بشكل آمن في macOS
- حماية تكامل النظام
- أمن الأنظمة لـ watchOS
- إدارة خزنة الملفات في macOS
- وصول التطبيق إلى كلمات السر المحفوظة
- توصيات أمن كلمة السر
- أمن Apple Cash
- أمن مراسلة الشركات من Apple
- خصوصية Wi-Fi
- أمن قفل التنشيط
- أمن أداة إعداد Apple

أبريل 2020

تم تحديثه لكل من:

- iOS 13.4
- iPadOS 13.4
- macOS 10.15.4
- tvOS 13.4
- watchOS 6.2

التحديثات:

- إضافة معلومات عن ميزة قطع اتصال مكون الميكروفون المادي في الـ iPad إلى قسم قطع اتصال مكون الميكروفون المادي.
- مخازن البيانات المضافة إلى حماية وصول التطبيقات إلى بيانات المستخدم.
- تحديثات على إدارة خزنة الملفات في macOS وأدوات سطر الأوامر.
- معلومات مضافة عن أداة إزالة البرامج الضارة في قسم الحماية ضد البرامج الضارة في macOS.
- تحديثات على قسم أمن الـ iPad المشترك في iPadOS.

ديسمبر 2019

تم دمج دليل أمن iOS ونظرة عامة على أمن macOS ونظرة عامة على شريحة Apple T2 الأمنية

تم تحديثه لكل من:

- iOS 13.3
- iPadOS 13.3
- macOS 10.15.2
- tvOS 13.3
- watchOS 6.1.1

تمت إزالة ضوابط الخصوصية و Siri واقتراحات Siri ومنع التعقب الذكي في سفاري. انظر https://www.Apple.com/ae-ar/privacy/ للاطلاع على أحدث المعلومات حول تلك الميزات.

مايو 2019

تم تحديثه لـ iOS 12.3

- دعم TLS 1.3
- مراجعة وصف أمن الإرسال السريع
- نمط DFU ووضع الاسترداد
- متطلبات رمز الدخول لتوصيل الملحقات

نوفمبر 2018

تم تحديثه لـ iOS 12.1

- فيس تايم جماعي

سبتمبر 2018

تم تحديثه لـ iOS 12 Secure Enclave

- حماية تكامل نظام التشغيل
- البطاقة السريعة في نمط توفير الطاقة
- نمط DFU ووضع الاسترداد
- ملحقات TV Remote التي تدعم HomeKit
- البطاقات الذكية
- بطاقات هويات الطلاب
- اقتراحات Siri
- الاختصارات في Siri
- تطبيق الاختصارات
- إدارة كلمات سر المستخدم
- مدة استخدام الجهاز
- شهادات الأمن والبرامج الأمنية

يوليو 2018

تم تحديثه لـ iOS 11.4

- سياسات المقاييس الحيوية
- HomeKit
- Apple Pay
- محادثة الشركات
- تطبيق الرسائل في iCloud
- Apple Business Manager

ديسمبر 2017

تم تحديثه لـ iOS 11.2

- Apple Pay Cash

أكتوبر 2017

تم تحديثه لـ iOS 11.1

- شهادات الأمن والبرامج الأمنية
- بصمة الإصبع/بصمة الوجه
- الملاحظات المشتركة
- تشفير CloudKit الكامل
- تحديث TLS
- Apple Pay، الدفع باستخدام Apple Pay على الويب
- اقتراحات Siri
- الـ iPad المشترك

يوليو 2017

تم تحديثه لـ iOS 10.3

- Secure Enclave
- حماية بيانات الملفات
- حافظات المفاتيح
- شهادات الأمن والبرامج الأمنية
- SiriKit
- HealthKit
- أمن الشبكات
- Bluetooth
- الـ iPad المشترك
- نمط الفقدان
- قفل التنشيط
- ضوابط الخصوصية

مارس 2017

تم تحديثه لـ iOS 10 أمن الأنظمة

- فئات حماية البيانات
- شهادات الأمن والبرامج الأمنية
- HomeKit، ReplayKit، SiriKit
- Apple Watch
- Wi-Fi، VPN
- تسجيل الدخول الموحد
- Apple Pay، الدفع باستخدام Apple Pay على الويب
- توفير بطاقة الائتمان والسحب والبطاقة مسبقة الدفع
- اقتراحات سفاري

مايو 2016

تم تحديثه لـ iOS 9.3

- Apple ID المُدار
- المصادقة بخطوتين لـ Apple ID
- حافظات المفاتيح
- شهادات الأمن
- نمط الفقدان، قفل التنشيط
- الملاحظات الآمنة
- Apple School Manager
- الـ iPad المشترك

سبتمبر 2015

تم تحديثه لـ iOS 9 قفل تنشيط Apple Watch

- سياسات رمز الدخول
- دعم API في بصمة الإصبع
- حماية البيانات في A8 تستخدم AES-XTS
- حافظات المفاتيح لتحديثات البرامج دون مراقبة
- تحديثات الشهادات
- نموذج الثقة في تطبيقات المؤسسات
- حماية البيانات لإشارات سفاري المرجعية
- أمن نقل التطبيقات
- مواصفات VPN
- الوصول إلى iCloud عن بُعد لـ HomeKit
- بطاقات الجوائز في Apple Pay، تطبيق جهة إصدار بطاقة Apple Pay
- فهرسة الباحث على الجهاز
- نموذج اقتران iOS
- أداة إعداد Apple 2
- القيود

حقوق النشر

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

AB028-00780