Pusat Sertifikasi dan Kepatuhan Keamanan

Desember 2021

Konten

Pengantar jaminan keamanan Apple

Sebagai bagian dari komitmen kami terhadap keamanan, Apple secara berkala berpartisipasi dengan organisasi pihak ketiga untuk menyertifikasi dan mengesahkan keamanan perangkat keras, perangkat lunak, dan layanan Apple. Organisasi yang dikenal pada skala internasional ini menyediakan sertifikasi untuk Apple yang sesuai dengan setiap perilisan sistem operasi besar. Dengan cara ini, organisasi menyediakan pengukuran kepercayaan—yaitu, jaminan keamanan—yang memenuhi kebutuhan keamanan sistem. Untuk area teknis yang tidak diterima berdasarkan pengaturan pengakuan bersama (MRA) atau yang kekurangan standar sertifikasi keamanan yang matang, Apple berpartisipasi dalam mengembangkan standar keamanan yang sesuai. Tujuan kami adalah untuk mendorong cakupan sertifikasi keamanan komprehensif yang diterima secara global di semua perangkat keras, sistem operasi, app, dan layanan Apple.

Sertifikasi biasanya penting untuk memenuhi persyaratan legislasi, regulasi, dan norma industri. Layanan seperti Apple School Manager dan Apple Business Manager dicakup berdasarkan sertifikasi ISO/IEC 27001 dan ISO/IEC 27018 Apple. Semua pelanggan, termasuk agensi pemerintahan dan perusahaan serta organisasi pendidikan yang menyebarkan perangkat Apple dapat menggunakan perangkat keras, sistem operasi, perangkat lunak, dan sertifikasi layanan untuk mendukung pemberlakuan kepatuhan.

Sertifikasi perangkat keras

Karena perangkat lunak yang aman memerlukan landasan keamanan yang terintegrasi ke dalam perangkat keras, semua perangkat Apple—yang menjalankan iOS, iPadOS, macOS, tvOS, atau watchOS—memiliki kemampuan keamanan yang dirancang ke dalam silikon. Ini meliputi kemampuan CPU khusus yang mendukung fitur dan silikon keamanan sistem yang didedikasikan untuk fungsi keamanan. Komponen paling penting adalah koprosesor Secure Enclave, yang terdapat di semua perangkat iOS, iPadOS, watchOS, dan perangkat tvOS terbaru, di semua komputer Mac dengan Apple Silicon, serta komputer Mac berbasis Intel dengan Keping Keamanan T2 Apple. Secure Enclave menyediakan fondasi bagi enkripsi data pada saat disimpan, boot aman di macOS, dan biometrik.

Komitmen Apple terhadap jaminan keamanan dimulai dengan sertifikasi komponen keamanan mendasar di silikon, dari dasar kepercayaan perangkat keras, ke pemberlakuan boot aman, ke Secure Enclave yang menyediakan penyimpanan kunci aman, ke pengesahan aman dengan Touch ID serta Face ID. Fitur keamanan perangkat Apple dimungkinkan oleh kombinasi desain silikon, perangkat keras, perangkat lunak, dan layanan yang hanya tersedia dari Apple. Sertifikasi komponen ini adalah bagian penting dalam memverifikasi jaminan yang disediakan oleh Apple.

Untuk informasi mengenai sertifikasi publik berkaitan dengan komponen perangkat keras dan firmware terkait, lihat:

- Sertifikasi keamanan untuk Keping Keamanan T2 Apple
- Sertifikasi keamanan untuk Prosesor Secure Enclave

Sertifikasi perangkat lunak dan app

Apple mempertahankan sertifikasi dan pengesahan independen bagi sistem operasi serta app-nya sesuai dengan Standar Pemrosesan Informasi Federal (FIPS) 140-2/-3 A.S. untuk modul kriptografis dan Common Criteria untuk sistem operasi, app, dan layanan perangkat. Cakupan sistem operasi termasuk iOS, iPadOS, macOS, sepOS, firmware T2, tvOS, dan watchOS. Untuk app, sertifikasi independen awalnya akan menyertakan app browser Safari dan Kontak, dengan app lainnya yang akan disertifikasi di masa mendatang.

Untuk informasi mengenai sertifikasi publik yang berkaitan dengan *sistem operasi* Apple, lihat:

- Sertifikasi keamanan untuk iOS
- Sertifikasi keamanan untuk iPadOS
- Sertifikasi keamanan untuk macOS
- Sertifikasi keamanan untuk tvOS
- Sertifikasi keamanan untuk watchOS

Untuk informasi mengenai sertifikasi publik yang berkaitan dengan *app* Apple, lihat:

- Sertifikasi keamanan untuk app Apple

Sertifikasi layanan

Apple mempertahankan sertifikasi keamanan untuk mendukung pelanggan kami, dari perusahaan hingga pendidikan. Sertifikasi ini memungkinkan pelanggan Apple untuk memahami peraturan dan kewajiban kontraknya saat menggunakan layanan Apple dengan perangkat keras serta perangkat lunak Apple. Sertifikasi ini memberikan pelanggan kami pengesahan independen atas praktik keamanan informasi, lingkungan, dan privasi Apple untuk sistem Apple.

Untuk informasi mengenai sertifikasi publik yang berkaitan dengan *layanan internet* Apple, lihat:

- Sertifikasi keamanan untuk layanan internet Apple

Untuk pertanyaan mengenai Sertifikasi Keamanan dan Privasi Apple, hubungi security-certifications@apple.com.

Sertifikasi keamanan perangkat keras

Tinjauan sertifikasi keamanan perangkat keras Apple

Apple mempertahankan Sertifikat Validasi Kepatuhan Standar Pemrosesan Informasi Federal (FIPS) 140-2/-3 A.S. untuk sepOS dan firmware T2 serta sertifikasi lainnya. Apple memulai dengan *blok pembuatan sertifikasi* yang diterapkan secara luas di beberapa platform yang sesuai. Blok pembuatan pertama adalah validasi perpustakaan corecrypto yang digunakan untuk penyebaran modul kriptografis perangkat lunak dan perangkat keras di dalam sistem operasi yang dikembangkan oleh Apple. Blok pembuatan kedua adalah sertifikasi Secure Enclave, yang disematkan di berbagai perangkat Apple. Blok pembuatan ketiga adalah sertifikasi Elemen Aman (SE) yang ditemukan di perangkat Apple dengan Touch ID dan perangkat dengan Face ID. Blok pembuatan sertifikasi perangkat keras ini membuat landasan untuk sertifikasi keamanan platform yang lebih luas.

Validasi algoritme kriptografis

Validasi ketepatan implementasi dari banyak algoritme kriptografis dan fungsi keamanan terkait adalah prasyarat untuk validasi FIPS 140-3 dan mendukung sertifikasi lain. Validasi dikelola oleh Cryptographic Algorithm Validation Program (CAVP) dari National Institute of Standards and Technology (NIST). Sertifikasi validasi untuk implementasi Apple dapat ditemukan menggunakan fasilitas pencarian CAVP. Untuk informasi lainnya, lihat situs web Cryptographic Algorithm Validation Program (CAVP).

Validasi modul kriptografis: FIPS 140-2/3 (ISO/IEC 19790)

Modul kriptografis Apple telah divalidasi berulang-ulang oleh Cryptographic Module Validation Program (CMVP) agar sesuai dengan modul kriptografis Standar Pemrosesan Informasi Federal (FIPS 140-2) A.S. menyusul setiap perilisan besar dari sistem operasi sejak tahun 2012. Setelah setiap perilisan besar, Apple mengirimkan modul ke CMVP untuk validasi kepatuhan dengan standar. Selain digunakan oleh sistem operasi dan app Apple, modul ini menyediakan fungsionalitas kriptografis untuk layanan yang disediakan oleh Apple dan tersedia untuk digunakan oleh app pihak ketiga.

Apple mendapatkan **Keamanan Level 1** setiap tahun untuk modul berbasis perangkat lunak "Modul Corecrypto untuk Intel" dan "Modul Kernel Corecrypto untuk Intel" untuk macOS. Untuk Apple Silicon, modul "Modul Corecrypto untuk ARM" serta "Modul Kernel Corecrypto untuk ARM" berlaku untuk iOS, iPadOS, tvOS, watchOS dan firmware di Keping Keamanan T2 Apple yang disematkan di komputer Mac.

Pada tahun 2019, Apple menerima **Keamanan Level 2** FIPS 140-2 pertama untuk modul kriptografis perangkat keras tersemat yang diidentifikasi sebagai "Modul Corecrypto Apple: Penyimpanan Kunci Aman", yang memungkinkan pemerintahan A.S. menyetujui penggunaan kunci yang dibuat dan dikelola di Secure Enclave. Apple terus mengupayakan validasi untuk modul kriptografis perangkat keras di setiap perilisan sistem operasi besar berikutnya.

FIPS 140-3 disetujui oleh Departemen Perdagangan A.S. pada tahun 2019. Perubahan yang paling jelas dalam versi standar ini adalah spesifikasi standar ISO/IEC—khususnya, ISO/IEC 19790:2015, dan standar pengujian terkait ISO/IEC 24759:2017. CMVP telah memulai program transisi dan telah mengindikasikan bahwa mulai tahun 2020, modul kriptografis akan mulai divalidasi menggunakan FIPS 140-3 sebagai basis. Modul kriptografis Apple akan bertujuan untuk memenuhi dan berpindah ke standar FIPS 140-3 sesegera mungkin.

Untuk modul kriptografis yang saat ini dalam proses pengujian dan validasi, CMVP mempertahankan dua daftar terpisah yang dapat berisi informasi mengenai validasi yang diajukan. Untuk modul kriptografis yang sedang diuji dengan laboratorium terakreditasi, Daftar Implementasi Sedang Diuji dapat mencantumkan modul tersebut. Setelah laboratorium menyelesaikan tes dan merekomendasikan validasi oleh CMVP, modul kriptografis Apple muncul di Daftar Modul dalam Proses. Saat ini, pengetesan laboratorium telah selesai dan menunggu validasi pengetesan oleh CMVP. Karena durasi proses evaluasi dapat bervariasi, lihat kedua daftar proses di atas untuk menentukan status modul kriptografis Apple saat ini antara tanggal perilisan sistem operasi besar dan penerbitan sertifikat validasi oleh CMVP.

Sertifikasi produk: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) adalah standar yang digunakan oleh berbagai organisasi sebagai dasar untuk melakukan evaluasi keamanan produk TI.

Untuk sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA) internasional, lihat Portal Common Criteria. Standar Common Criteria juga dapat digunakan di luar CCRA oleh skema validasi nasional dan swasta. Di Eropa, pengakuan bersama diatur berdasarkan persetujuan SOG-IS serta CCRA.

Tujuannya, sebagaimana dijelaskan oleh komunitas Common Criteria, adalah untuk kumpulan standar keamanan yang disetujui secara internasional untuk memberikan evaluasi yang jelas dan dapat diandalkan mengenai kemampuan keamanan produk Teknologi Informasi. Dengan memberikan penilaian independen atas kemampuan produk dalam memenuhi standar keamanan, Sertifikasi Common Criteria memberikan pelanggan kepercayaan lebih terhadap keamanan produk Teknologi Informasi dan menghasilkan keputusan yang lebih matang.

Melalui CCRA, negara anggota telah setuju untuk mengakui sertifikasi produk Teknologi Informasi dengan level kepercayaan yang sama. Evaluasi yang diperlukan sebelum sertifikasi bersifat ekstensif dan menyertakan:

- Profil Perlindungan (PP)
- Target Keamanan (ST)
- Persyaratan Fungsional Keamanan (SFR)
- Persyaratan Jaminan Keamanan (SAR)
- Level Jaminan Evaluasi (EAL)

Profil Perlindungan (PP) adalah dokumen yang menentukan persyaratan keamanan untuk kelas jenis perangkat (seperti Mobilitas) dan digunakan untuk menyediakan perbandingan antara evaluasi produk TI dalam kelas yang sama. Keanggotaan CCRA bersamaan dengan meningkatnya daftar PP yang disetujui, terus berkembang setiap tahunnya. Pengaturan ini memungkinkan pengembang produk untuk mengupayakan sertifikasi tunggal berdasarkan salah satu skema pengesahan sertifikat apa pun dan membuatnya dikenali oleh salah satu penanda tangan konsumen sertifikat.

Target Keamanan (ST) mendefinisikan *apa* yang akan dievaluasi saat produk TI sedang disertifikasi. ST diterjemahkan ke *Persyaratan Fungsional Keamanan (SFR)* yang lebih spesifik, yang digunakan untuk mengevaluasi ST secara lebih mendetail.

Common Criteria (CC) juga menyertakan *Persyaratan Jaminan Keamanan*. Satu metrik yang umum teridentifikasi adalah *Level Jaminan Evaluasi (EAL)*. EAL mengelompokkan kumpulan SAR yang sering terjadi dan dapat ditetapkan di PP serta ST untuk mendukung keterbandingan.

Banyak PP yang lebih lama telah diarsipkan dan sedang diganti dengan PP yang ditargetkan, yang sedang dikembangkan dan fokus pada solusi serta lingkungan tertentu. Dalam upaya selaras untuk memastikan pengenalan bersama berkelanjutan pada semua anggota CCRA, international Technical Community (iTC) telah dibangun untuk mengembangkan dan memelihara Profil Perlindungan kolaboratif (cPP) yang dikembangkan dari awal dengan keterlibatan dari beberapa skema penanda tangan CCRA. PP yang ditargetkan untuk grup pengguna dan pengaturan pengakuan bersama selain CCRA terus dikembangkan oleh pemegang saham yang sesuai.

Apple mulai mengupayakan sertifikasi berdasarkan CCRA yang diperbarui dengan cPP terpilih mulai awal 2015. Sejak saat itu, Apple telah mendapatkan sertifikasi Common Criteria untuk setiap perilisan iOS besar dan telah memperluas cakupannya untuk menyertakan jaminan keamanan yang diberikan oleh PP baru.

Apple berperan aktif dalam komunitas teknis yang fokus mengevaluasi teknologi keamanan seluler. Ini menyertakan iTC yang bertanggung jawab dalam mengembangkan dan memperbarui cPP. Apple terus mengevaluasi dan mengupayakan sertifikasi berdasarkan PP dan cPP saat ini.

Sertifikasi platform Apple untuk pasar Amerika Utara secara umum dilakukan dengan National Information Assurance Partnership (NIAP), yang mempertahankan daftar proyek yang saat ini dalam evaluasi namun belum disertifikasi.

Selain sertifikat platform umum yang tercantum, sertifikat lainnya telah diterbitkan untuk mendemonstrasikan persyaratan keamanan spesifik untuk beberapa pasar.

Sertifikasi keamanan untuk Prosesor Secure Enclave

Latar belakang sertifikasi Secure Enclave

Modul Kriptografis Perangkat Keras—*Modul Kriptografis Penyimpanan Kunci Aman SEP Apple*—disematkan di SOC Apple yang berada dalam produk berikut: Seri A Apple untuk iPhone dan iPad, seri M untuk komputer Mac dengan Apple Silicon, seri S untuk Apple Watch, dan keping keamanan seri T yang ditemukan di komputer Mac berbasis Intel dimulai dari iMac Pro yang diperkenalkan tahun 2017.

Pada tahun 2018, Apple menyelaraskan dengan validasi modul kriptografis perangkat lunak dengan sistem operasi yang dirilis pada tahun 2017: iOS 11, macOS 10.13, tvOS 11, dan watchOS 4. Modul kriptografis perangkat keras SEP yang diidentifikasi sebagai Modul Kriptografis Penyimpanan Kunci Aman Apple v1.0 awalnya disahkan dengan persyaratan Keamanan FIPS 140-2 Level 1.

Pada tahun 2019, Apple mengesahkan modul perangkat keras dengan persyaratan Keamanan FIPS 140-2 Level 2 dan memperbarui pengenal versi modul ke v9.0 untuk menyelaraskan dengan versi validasi modul Pengguna corecrypto dan Kernel corecrypto yang sesuai. Pada tahun 2019, penyelarasan ini meliputi iOS 12, macOS 10.14, tvOS 12, dan watchOS 5.

Pada tahun 2020 dan 2021, Apple mengupayakan validasi kepatuhan dengan FIPS 140-3 dan dengan jaminan tambahan untuk level keamanan 3 persyaratan keamanan fisik untuk Apple Silicon: Keping A13, A14, S6 dan M1.

Apple juga secara aktif ikut serta dalam validasi modul Pengguna corecrypto dan Kernel corecrypto untuk setiap perilisan sistem operasi besar. Validasi kepatuhan hanya dapat dijalankan untuk versi rilis final.

Status validasi modul kriptografis

Cryptographic Module Validation Program (CMVP) mempertahankan status validasi modul kriptografis di tiga daftar terpisah tergantung statusnya saat ini:

- Agar dapat dicantumkan di Daftar Implementasi Sedang Diuji CMVP, laboratorium harus membuat kontrak dengan Apple untuk menyediakan tes.
- Setelah tes diselesaikan oleh laboratorium, lab telah merekomendasikan validasi oleh CMVP, dan biaya CMVP telah dibayar, kemudian modul ditambahkan ke Daftar Modul dalam Proses. Daftar MIP melacak kemajuan upaya validasi CMVP dalam empat fase:
  - *Tinjauan Tertunda:* Menunggu sumber daya CMVP untuk ditetapkan.
  - *Dalam Tinjauan:* Sumber daya CMVP sedang melakukan aktivitas validasinya.
  - *Koordinasi:* Lab dan CMVP sedang menyelesaikan masalah apa pun yang ditemukan.
  - *Finalisasi:* Aktivitas dan formalitas yang terkait penerbitan sertifikat.
- Setelah validasi oleh CMVP, modul diberikan sertifikat kepatuhan dan ditambahkan ke daftar modul kriptografis yang disahkan. Ini meliputi:
  - Modul yang divalidasi ditandai sebagai aktif.
  - Setelah 5 tahun, modul akan ditandai sebagai historis.
  - Jika sertifikasi modul dicabut karena suatu alasan, modul akan ditandai sebagai dicabut.

Pada tahun 2020, CMVP mengadopsi standar internasional ISO/IEC 19790 sebagai dasar untuk FIPS 140-3.

Sertifikasi FIPS 140-3

Status saat ini

Tabel di bawah menampilkan modul kriptografis 2020 dan 2021 yang saat ini sedang diuji kepatuhannya oleh laboratorium dengan FIPS 140-3.

Penyimpanan Kunci Aman (SKS) yang terkait dengan rilis sistem operasi 2020 dan 2021 telah menyelesaikan pengujian laboratorium dan telah direkomendasikan oleh laboratorium kepada CMVP untuk validasi. Rilis tersebut tercantum di Daftar Modul dalam Proses dan setelah divalidasi akan dipindahkan ke daftar modul kriptografis yang divalidasi.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman iOS 15 (2021) sedang menjalani pengujian laboratorium. Item tersebut tercantum di Daftar Implementasi Sedang Diuji.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS, iPadOS, macOS, tvOS, dan watchOS rilisan 2021 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14, T2, M1, S3-S6) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS, iPadOS, macOS, tvOS, dan watchOS rilisan 2021 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A13, A14, S6, M1) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS, iPadOS, macOS, tvOS, dan watchOS rilisan 2020 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14, T2, M1, S3-S6) *Level keamanan keseluruhan:* 2

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS, iPadOS, macOS, tvOS, dan watchOS rilisan 2020 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A13, A14, S6, M1) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3

Sertifikasi FIPS 140-2

Tabel di bawah menampilkan modul kriptografis yang saat ini telah diuji kepatuhannya oleh laboratorium dengan FIPS 140-2.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 05/02/2021	*Sertifikat:* 3811 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v10.0 Apple *Sistem operasi:* sepOS untuk macOS 10.15 Catalina *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3523 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v9.0 Apple *Sistem operasi:* sepOS untuk macOS 10.14 Mojave *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3223 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v1.0 Apple *Sistem operasi:* sepOS untuk macOS 10.13 High Sierra *Jenis:* Perangkat keras *Level keamanan:* 2

Sertifikasi Common Criteria (CC)

Apple secara aktif terlibat dalam evaluasi Common Criteria yang Profil Perlindungannya yang sesuai mencakup fungsionalitas keamanan teknologi Apple.

Status sertifikasi Common Criteria (CC)

Skema A.S., yang dioperasikan oleh NIAP, memelihara daftar Produk dalam Evaluasi. Daftar ini menyertakan produk yang sedang dievaluasi di Amerika Serikat dengan Common Criteria Testing Laboratory (CCTL) yang disetujui NIAP dan yang telah menyelesaikan Rapat Pertama Evaluasi (atau setara) tempat manajemen CCEVS menerima produk ke evaluasi secara resmi.

Setelah produk disertifikasi, NIAP memasukkan sertifikasi yang saat ini valid di daftar Produk yang Sesuai. Setelah 2 tahun, sertifikasi ini ditinjau kesesuaiannya dengan kebijakan pemeliharaan jaminan saat ini. Setelah tanggal pemeliharaan jaminan kedaluwarsa, NIAP memindahkan sertifikasi yang tercantum ke daftar Produk yang Diarsipkan miliknya.

Portal Common Criteria mencantumkan sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA). Portal CC dapat mempertahankan produk di daftar produk besertifikasi selama 5 tahun. Catatan disimpan oleh Portal CC untuk sertifikasi yang diarsipkan.

Tabel di bawah menampilkan sertifikasi yang saat ini sedang dievaluasi oleh laboratorium, atau yang telah disertifikasi sebagai sesuai dengan Common Criteria.

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem operasi: sepOS *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* Secure Enclave Apple [2020] *Profil Perlindungan:* CPP_DSC_V1.0 *Perangkat keras:* Secure Enclave untuk (A9-A14, M1, T2, S3-S6) *Perangkat lunak:* sepOS yang didistribusikan dengan iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7

Sertifikasi tambahan

Tabel di bawah menampilkan sertifikasi untuk Secure Enclave yang tidak menggunakan Common Criteria maupun FIPS 140-3.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* 07-12-2019 hingga 26-12-2022	*Sertifikat:* CFNR201902910002 (P.R. China: Technology Certification of Mobile Financial Service) Versi bahasa Tionghoa Versi bahasa Inggris	*Judul:* Lingkungan Eksekusi Tepercaya Terminal Bergerak *Sistem operasi:* iOS 13.5.1 *Spesifikasi:* JR/T 0156-2017

Sertifikasi keamanan untuk Keping Keamanan T2 Apple

Latar belakang validasi modul kriptografis

Apple secara aktif ikut serta dalam validasi modul perangkat lunak dan perangkat keras yang disematkan Apple untuk setiap perilisan sistem operasi besar. Validasi kepatuhan hanya dapat dijalankan untuk versi rilis modul final.

Pada tahun 2020, CMVP mengadopsi standar internasional ISO/IEC 19790, sebagai dasar untuk Standar Pemrosesan Informasi Federal (FIPS) 140-3 A.S.

Selain memiliki CPU Intel, sebagian besar komputer Mac sejak 2017 juga memiliki Keping Keamanan T2 Apple terpisah yang merupakan sistem pada keping (SoC) berbasis Apple Silicon. Komputer Mac dengan keping T2 ini menggunakan lima modul kriptografis untuk berbagai layanan pada perangkat.

- Modul pengguna Corecrypto untuk Intel (digunakan oleh macOS pada komputer Mac berbasis Intel)
- Modul kernel Corecrypto untuk Intel (digunakan oleh macOS pada komputer Mac berbasis Intel)
- Modul pengguna Corecrypto untuk ARM (digunakan oleh keping T2)
- Modul kernel Corecrypto untuk ARM (digunakan oleh keping T2)
- Modul Kriptografis Penyimpanan Kunci Aman (digunakan oleh koprosesor Secure Enclave yang disematkan di keping T2)

Catatan: Modul berbasis Apple Silicon yang berjalan pada keping T2 sama dengan modul yang berjalan pada keping Apple Silicon lainnya seperti seri A, seri S, dan seri M Apple.

Status validasi modul kriptografis

Cryptographic Module Validation Program (CMVP) mempertahankan status validasi modul kriptografis di tiga daftar terpisah tergantung statusnya saat ini:

- Agar dapat dicantumkan di Daftar Implementasi Sedang Diuji CMVP, laboratorium harus membuat kontrak dengan Apple untuk menyediakan tes.
- Setelah tes diselesaikan oleh laboratorium, lab telah merekomendasikan validasi oleh CMVP, dan biaya CMVP telah dibayar, kemudian modul ditambahkan ke Daftar Modul dalam Proses (MIP). Daftar MIP melacak kemajuan upaya validasi CMVP dalam empat fase:
  - *Tinjauan Tertunda:* Menunggu sumber daya CMVP untuk ditetapkan.
  - *Dalam Tinjauan:* Sumber daya CMVP sedang melakukan aktivitas validasinya.
  - *Koordinasi:* Lab dan CMVP sedang menyelesaikan masalah apa pun yang ditemukan.
  - *Finalisasi:* Aktivitas dan formalitas yang terkait penerbitan sertifikat.
- Setelah validasi oleh CMVP, modul diberikan sertifikat kepatuhan dan ditambahkan ke daftar modul kriptografis yang disahkan. Ini meliputi:
  - Modul yang divalidasi ditandai sebagai aktif.
  - Setelah 5 tahun, modul akan ditandai sebagai historis.
  - Jika sertifikasi modul dicabut karena suatu alasan, modul akan ditandai sebagai dicabut.

Sertifikasi FIPS 140-3

Status saat ini

Modul 2020 ruang pengguna, ruang kernel, dan penyimpanan kunci aman telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Modul 2021 untuk ruang pengguna, ruang kernel, dan penyimpanan kunci aman sedang menjalani pengujian laboratorium. Item tersebut tercantum di Daftar Implementasi Sedang Diuji.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* sepOS untuk macOS 12 Monterey *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* sepOS untuk macOS 12 Monterey *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* sepOS untuk macOS 12 Monterey *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (T2) *Level keamanan:* 2
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS untuk macOS 11 Big Sur *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS untuk macOS 11 Big Sur *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS untuk macOS 11 Big Sur di Intel *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat keras *Level keamanan:* 2

Sertifikasi FIPS 140-2

Tabel di bawah menampilkan modul kriptografis yang saat ini telah diuji kepatuhannya oleh laboratorium dengan FIPS 140-2.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3856 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* sepOS untuk macOS 10.15 Catalina *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3855 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* sepOS untuk macOS 10.15 Catalina *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 05/02/2021	*Sertifikat:* 3811 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman Corecrypto v10.0 Apple *Sistem operasi:* sepOS untuk macOS 10.15 Catalina *Jenis:* Perangkat keras *Level keamanan:* 2

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 23/04/2019	*Sertifikat:* 3438 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v9.0 Apple untuk ARM *Sistem operasi:* sepOS untuk macOS 10.14 Mojave *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 11/04/2019	*Sertifikat:* 3433 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v9.0 Apple untuk ARM *Sistem operasi:* sepOS untuk macOS 10.14 Mojave *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3523 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v9.0 Apple *Sistem operasi:* sepOS untuk macOS 10.14 Mojave *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 22/05/2018, 06/07/2018	*Sertifikat:* 3148 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v8.0 Apple untuk ARM *Sistem operasi:* sepOS untuk macOS 10.13 High Sierra *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 17/05/2018, 03/07/2018	*Sertifikat:* 3147 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v8.0 Apple untuk ARM *Sistem operasi:* sepOS untuk macOS 10.13 High Sierra *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 10-07-2018	*Sertifikat:* 3223 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v1.0 Apple *Sistem operasi:* sepOS untuk macOS 10.13 High Sierra *Jenis:* Perangkat keras *Level keamanan:* 2

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2016 *Tanggal validasi:* 01/02/2017	*Sertifikat:* 2828 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto iOS v7.0 Apple *Sistem operasi:* sepOS untuk macOS 10.12 Sierra *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2016 *Tanggal validasi:* 01/02/2017	*Sertifikat:* 2827 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto iOS v7.0 Apple *Sistem operasi:* sepOS untuk macOS 10.12 Sierra *Jenis:* Perangkat lunak *Level keamanan:* 1

Sertifikasi keamanan sistem operasi

Tinjauan sertifikasi keamanan sistem operasi Apple

Apple mempertahankan Sertifikat Validasi Kepatuhan Standar Pemrosesan Informasi Federal (FIPS) 140-2/-3 A.S. untuk sepOS dan firmware T2 serta sertifikasi lainnya. Apple memulai dengan *blok pembuatan sertifikasi* yang diterapkan secara luas di beberapa platform yang sesuai. Blok pembuatan pertama adalah validasi corecrypto yang digunakan untuk penyebaran modul kriptografis perangkat lunak dan perangkat keras di dalam sistem operasi yang dikembangkan oleh Apple. Blok pembuatan kedua adalah sertifikasi Secure Enclave, yang disematkan di berbagai perangkat Apple. Blok pembuatan ketiga adalah sertifikasi Elemen Aman (SE) yang ditemukan di perangkat Apple dengan Touch ID dan perangkat dengan Face ID. Blok pembuatan sertifikasi perangkat keras ini membuat landasan untuk sertifikasi keamanan platform yang lebih luas.

Validasi algoritme kriptografis

Validasi ketepatan implementasi dari banyak algoritme kriptografis dan fungsi keamanan terkait adalah prasyarat untuk validasi FIPS 140-3 dan mendukung sertifikasi lain. Validasi dikelola oleh Cryptographic Algorithm Validation Program (CAVP) dari NIST. Sertifikasi validasi untuk implementasi Apple dapat ditemukan menggunakan fasilitas pencarian CAVP.

Validasi modul kriptografis: FIPS 140-2/3 (ISO/IEC 19790)

Modul kriptografis dalam sistem operasi Apple telah divalidasi berulang-ulang oleh Cryptographic Module Validation Program (CMVP) agar sesuai dengan Standar Pemrosesan Informasi Federal (FIPS) 140-2 A.S. menyusul setiap rilis besar dari sistem operasi sejak tahun 2012. Setelah setiap perilisan besar, Apple mengirimkan semua modul ke CMVP untuk validasi kriptografis penuh. Modul yang divalidasi ini memberikan operasi kriptografis untuk layanan yang disediakan oleh Apple dan tersedia untuk digunakan oleh app pihak ketiga.

Apple mendapatkan **Keamanan Level 1** setiap tahun untuk modul berbasis perangkat lunak "Modul Corecrypto untuk Intel" dan "Modul Kernel Corecrypto untuk Intel" untuk macOS. Untuk Apple Silicon, modul "Modul Corecrypto untuk ARM" serta "Modul Kernel Corecrypto untuk ARM" berlaku untuk iOS, iPadOS, tvOS, watchOS dan firmware di Keping Keamanan T2 Apple yang disematkan di komputer Mac.

Pada tahun 2019, Apple menerima **Keamanan Level 2** FIPS 140-2 pertama untuk modul kriptografis perangkat keras tersemat yang diidentifikasi sebagai "Modul Corecrypto Apple: Penyimpanan Kunci Aman", yang memungkinkan pemerintahan A.S. menyetujui penggunaan kunci yang dibuat dan dikelola di Secure Enclave. Apple terus mengupayakan validasi untuk modul kriptografis perangkat keras di setiap perilisan sistem operasi besar berikutnya.

FIPS 140-3 disetujui oleh Departemen Perdagangan A.S. pada tahun 2019. Perubahan yang paling jelas dalam versi standar ini adalah spesifikasi standar ISO/IEC—khususnya, ISO/IEC 19790:2015, dan standar pengujian terkait ISO/IEC 24759:2017. CMVP telah memulai program transisi dan telah mengindikasikan bahwa mulai tahun 2020, modul kriptografis akan mulai divalidasi menggunakan FIPS 140-3 sebagai basis. Modul kriptografis Apple akan bertujuan untuk memenuhi dan berpindah ke standar FIPS 140-3 sesegera mungkin.

Untuk modul kriptografis yang saat ini dalam proses pengujian dan validasi, CMVP mempertahankan dua daftar terpisah yang dapat berisi informasi mengenai validasi yang diajukan. Untuk modul kriptografis yang sedang diuji dengan laboratorium terakreditasi, Daftar Implementasi Sedang Diuji dapat mencantumkan modul tersebut. Setelah laboratorium menyelesaikan tes dan merekomendasikan validasi oleh CMVP, modul kriptografis Apple muncul di Daftar Modul dalam Proses. Saat ini, pengetesan laboratorium telah selesai dan menunggu validasi pengetesan oleh CMVP. Karena durasi proses evaluasi dapat bervariasi, lihat kedua daftar proses di atas untuk menentukan status modul kriptografis Apple saat ini antara tanggal perilisan sistem operasi besar dan penerbitan sertifikat validasi oleh CMVP.

Sertifikasi produk: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) adalah standar yang digunakan oleh berbagai organisasi sebagai dasar untuk melakukan evaluasi keamanan produk TI.

Untuk sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA) internasional, lihat Portal Common Criteria. Standar Common Criteria juga dapat digunakan di luar CCRA oleh skema validasi nasional dan swasta. Di Eropa, pengakuan bersama diatur berdasarkan persetujuan SOG-IS serta CCRA.

Tujuannya, sebagaimana dijelaskan oleh komunitas Common Criteria, adalah untuk kumpulan standar keamanan yang disetujui secara internasional untuk memberikan evaluasi yang jelas dan dapat diandalkan mengenai kemampuan keamanan produk Teknologi Informasi. Dengan memberikan penilaian independen atas kemampuan produk dalam memenuhi standar keamanan, Sertifikasi Common Criteria memberikan pelanggan kepercayaan lebih terhadap keamanan produk Teknologi Informasi dan menghasilkan keputusan yang lebih matang.

Melalui CCRA, negara anggota telah setuju untuk mengakui sertifikasi produk Teknologi Informasi dengan level kepercayaan yang sama. Evaluasi yang diperlukan sebelum sertifikasi bersifat ekstensif dan menyertakan:

- Profil Perlindungan (PP)
- Target Keamanan (ST)
- Persyaratan Fungsional Keamanan (SFR)
- Persyaratan Jaminan Keamanan (SAR)
- Level Jaminan Evaluasi (EAL)

Profil Perlindungan (PP) adalah dokumen yang menentukan persyaratan keamanan untuk kelas jenis perangkat (seperti Mobilitas) dan digunakan untuk menyediakan perbandingan antara evaluasi produk TI dalam kelas yang sama. Keanggotaan CCRA bersamaan dengan meningkatnya daftar PP yang disetujui, terus berkembang setiap tahunnya. Pengaturan ini memungkinkan pengembang produk untuk mengupayakan sertifikasi tunggal berdasarkan salah satu skema pengesahan sertifikat apa pun dan membuatnya dikenali oleh salah satu penanda tangan konsumen sertifikat.

Target Keamanan (ST) mendefinisikan *apa* yang akan dievaluasi saat produk TI sedang disertifikasi. ST diterjemahkan ke *Persyaratan Fungsional Keamanan (SFR)* yang lebih spesifik, yang digunakan untuk mengevaluasi ST secara lebih mendetail.

Common Criteria (CC) juga menyertakan *Persyaratan Jaminan Keamanan*. Satu metrik yang umum teridentifikasi adalah *Level Jaminan Evaluasi (EAL)*. EAL mengelompokkan kumpulan SAR yang sering terjadi dan dapat ditetapkan di PP serta ST untuk mendukung keterbandingan.

Banyak PP yang lebih lama telah diarsipkan dan sedang diganti dengan PP yang ditargetkan, yang sedang dikembangkan dan fokus pada solusi serta lingkungan tertentu. Dalam upaya selaras untuk memastikan pengenalan bersama berkelanjutan pada semua anggota CCRA, international Technical Community (iTC) telah dibangun untuk mengembangkan dan memelihara *Profil Perlindungan kolaboratif (cPP)* yang dikembangkan dari awal dengan keterlibatan dari beberapa skema penanda tangan CCRA. PP yang ditargetkan untuk grup pengguna dan pengaturan pengakuan bersama selain CCRA terus dikembangkan oleh pemegang saham yang sesuai.

Apple mulai mengupayakan sertifikasi berdasarkan CCRA yang diperbarui dengan cPP terpilih mulai awal 2015. Sejak saat itu, Apple telah mendapatkan sertifikasi Common Criteria untuk setiap perilisan iOS besar dan telah memperluas cakupannya untuk menyertakan jaminan keamanan yang diberikan oleh PP baru.

Apple berperan aktif dalam komunitas teknis yang fokus mengevaluasi teknologi keamanan seluler. Ini menyertakan iTC yang bertanggung jawab dalam mengembangkan dan memperbarui cPP. Apple terus mengevaluasi dan mengupayakan sertifikasi berdasarkan PP dan cPP saat ini.

Sertifikasi platform Apple untuk pasar Amerika Utara secara umum dilakukan dengan National Information Assurance Partnership (NIAP), yang mempertahankan daftar proyek yang saat ini dalam evaluasi namun belum disertifikasi.

Selain sertifikat platform umum yang tercantum, sertifikat lainnya telah diterbitkan untuk mendemonstrasikan persyaratan keamanan spesifik untuk beberapa pasar.

Sertifikasi keamanan untuk iOS

Latar belakang sertifikasi iOS

Apple secara aktif ikut serta dalam validasi modul perangkat lunak dan perangkat keras yang disematkan Apple untuk setiap perilisan sistem operasi besar. Validasi kepatuhan hanya dapat dijalankan untuk versi rilis final.

Status validasi modul kriptografis iOS

Cryptographic Module Validation Program (CMVP) mempertahankan status validasi modul kriptografis di tiga daftar terpisah tergantung statusnya saat ini:

- Agar dapat dicantumkan di Daftar Implementasi Sedang Diuji CMVP, laboratorium harus membuat kontrak dengan Apple untuk menyediakan tes.
- Setelah tes diselesaikan oleh laboratorium, lab telah merekomendasikan validasi oleh CMVP, dan biaya CMVP telah dibayar, kemudian modul ditambahkan ke Daftar Modul dalam Proses (MIP). Daftar MIP melacak kemajuan upaya validasi CMVP dalam empat fase:
  - *Tinjauan Tertunda:* Menunggu sumber daya CMVP untuk ditetapkan.
  - *Dalam Tinjauan:* Sumber daya CMVP sedang melakukan aktivitas validasinya.
  - *Koordinasi:* Lab dan CMVP sedang menyelesaikan masalah apa pun yang ditemukan.
  - *Finalisasi:* Aktivitas dan formalitas yang terkait penerbitan sertifikat.
- Setelah validasi oleh CMVP, modul diberikan sertifikat kepatuhan dan ditambahkan ke daftar modul kriptografis yang disahkan. Ini meliputi:
  - Modul yang divalidasi ditandai sebagai aktif.
  - Setelah 5 tahun, modul akan ditandai sebagai historis.
  - Jika sertifikasi modul dicabut karena suatu alasan, modul akan ditandai sebagai dicabut.

Pada tahun 2020, CMVP mengadopsi standar internasional ISO/IEC 19790 sebagai dasar untuk FIPS 140-3.

Sertifikasi FIPS 140-3

Status saat ini

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman iOS 14 (2020) telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman iOS 15 (2021) sedang menjalani pengujian laboratorium. Item tersebut tercantum di Daftar Implementasi Sedang Diuji.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem Operasi:* iOS 15 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem Operasi:* iOS 15 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 15 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 15 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A13, A14, A15) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem Operasi:* iOS 14 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem Operasi:* iOS 14 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 14 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 14 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A13-A14) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3

Sertifikasi FIPS 140-2

Tabel di bawah menampilkan modul kriptografis yang saat ini sedang diuji dan telah diuji kepatuhannya oleh laboratorium dengan FIPS 140-2.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3856 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v10.0 Apple untuk ARM *Sistem Operasi:* iOS 13 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3855 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v10.0 Apple untuk ARM *Sistem Operasi:* iOS 13 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 05/02/2021	*Sertifikat:* 3811 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v10.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 13 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 23/04/2019	*Sertifikat:* 3438 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v9.0 Apple untuk ARM *Sistem Operasi:* iOS 12 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 11/04/2019	*Sertifikat:* 3433 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v9.0 Apple untuk ARM *Sistem Operasi:* iOS 12 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3523 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v9.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 12 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 22/05/2018, 06/07/2018	*Sertifikat:* 3148 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v8.0 Apple untuk ARM *Sistem Operasi:* iOS 11 *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 17/05/2018, 03/07/2018	*Sertifikat:* 3147 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v8.0 Apple untuk ARM *Sistem Operasi:* iOS 11 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3223 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v1.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 11 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2016 *Tanggal validasi:* 01/02/2017	*Sertifikat:* 2828 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto iOS v7.0 Apple *Sistem Operasi:* iOS 10 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2016 *Tanggal validasi:* 01/02/2017	*Sertifikat:* 2827 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto iOS v7.0 Apple *Sistem Operasi:* iOS 10 *Jenis:* Perangkat lunak *Level keamanan:* 1

Versi sebelumnya

Sertifikasi yang lebih lama dari 5 tahun dicantumkan oleh CMVP dengan status historis. Versi iOS lama berikut ini memiliki validasi modul kriptografis:

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

Latar belakang sertifikasi Common Criteria (CC)

Apple secara aktif ikut serta dalam evaluasi iOS untuk setiap perilisan sistem operasi besar. Evaluasi hanya dapat dilakukan dengan versi final sistem operasi yang dirilis secara publik. Sebelum iPadOS 13.1, iPadOS bernama iOS.

Status sertifikasi Common Criteria (CC)

Skema A.S., yang dioperasikan oleh NIAP, memelihara daftar Produk dalam Evaluasi. Daftar ini menyertakan produk yang sedang dievaluasi di Amerika Serikat dengan Common Criteria Testing Laboratory (CCTL) yang disetujui NIAP dan yang telah menyelesaikan Rapat Pertama Evaluasi (atau setara) tempat manajemen CCEVS menerima produk ke evaluasi secara resmi.

Setelah produk disertifikasi, NIAP memasukkan sertifikasi yang saat ini valid di daftar Produk yang Sesuai. Setelah 2 tahun, sertifikasi ini ditinjau kesesuaiannya dengan kebijakan pemeliharaan jaminan saat ini. Setelah tanggal pemeliharaan jaminan kedaluwarsa, NIAP memindahkan sertifikasi yang tercantum ke daftar Produk yang Diarsipkan miliknya.

Portal Common Criteria mencantumkan sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA). Portal CC dapat mempertahankan produk di daftar produk besertifikasi selama 5 tahun. Catatan disimpan oleh Portal CC untuk sertifikasi yang diarsipkan.

Tabel di bawah menampilkan sertifikasi yang saat ini sedang dievaluasi oleh laboratorium, atau yang telah disertifikasi sebagai sesuai dengan Common Criteria.

Status saat ini

Pengujian laboratorium untuk evaluasi dengan NIAP untuk iOS 15 sedang berlangsung. Untuk informasi terbaru, lihat Produk sedang dievaluasi (NIAP) dan Daftar Kepatuhan Produk.

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem Operasi: iOS 15 *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* —	*Judul:* iOS 15 Apple: iPhone *Profil Perlindungan:* Fundamental Perangkat Bergerak (PP-Module akan dikonfirmasi)
Sistem Operasi: iOS 14 *Tanggal sertifikasi:* 01/09/2021	*ID Skema:* 11146 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iOS 14 Apple: iPhone *Profil Perlindungan:* Fundamental Perangkat Bergerak, modul Klien VPN, Modul PP Klien WLAN, EP Agen MDM
Sistem Operasi: iOS 13 *Tanggal sertifikasi:* 06/11/2020	*ID Skema:* 11036 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iOS 13 Apple di iPhone *Profil Perlindungan:* Fundamental Perangkat Bergerak, modul Klien VPN, EP Klien WLAN, EP Agen MDM

Sertifikasi Common Criteria yang diarsipkan untuk iOS

Versi iOS lama berikut ini memiliki validasi Common Criteria. Versi iOS sebelumnya diarsipkan oleh NIAP menurut kebijakan NIAP:

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem Operasi: iOS 12 *Tanggal sertifikasi:* 14/03/2019	*ID Skema:* 10937 *Dokumen:* Target Keamanan Panduan	*Judul:* iPhone dengan iOS 12 *Profil Perlindungan:* Fundamental Perangkat Bergerak, modul Klien VPN, EP klien LAN nirkabel, EP Agen MDM
Sistem Operasi: iOS 11 *Tanggal sertifikasi:* 17/07/2018	*ID Skema:* 10851 *Dokumen:* Target Keamanan Panduan	*Judul:* iOS 11 Apple *Profil Perlindungan:* Fundamental Perangkat Bergerak, EP klien LAN nirkabel, EP Agen MDM
Sistem Operasi: iOS 10 *Tanggal sertifikasi:* 27/07/2017	*ID Skema:* 10782 *Dokumen:* Target Keamanan, Panduan	*Judul:* iOS 10.2 di Perangkat åiPhone dan iPad *Profil Perlindungan:* Fundamental Perangkat Bergerak, EP klien LAN nirkabel, EP Agen MDM
Sistem Operasi: iOS 10 *Tanggal sertifikasi:* 27/07/2017	*ID Skema:* 10792 *Dokumen:* Target Keamanan, Panduan	*Judul: Klien VPN* iOS 10.2 di iPhone dan iPad *Profil Perlindungan:* PP Klien VPN
Sistem Operasi: iOS 9 *Tanggal sertifikasi:* 14/10/2016	*ID Skema:* 10725 *Dokumen:* Target Keamanan, Panduan	*Judul:* iOS 9.3.2 dengan Agen MDM *Profil Perlindungan:* Fundamental Perangkat Bergerak, EP Agen MDM
Sistem Operasi: iOS 9 *Tanggal sertifikasi:* 13/10/2016	*ID Skema:* 10714 *Dokumen:* Target Keamanan, Panduan	*Judul:* Klien VPN OS di iPhone dan iPad *Profil Perlindungan:* PP Klien VPN
Sistem Operasi: iOS 9 *Tanggal sertifikasi:* 28/01/2016	*ID Skema:* 10695 *Dokumen:* Target Keamanan, Panduan	*Judul:* iOS 9 *Profil Perlindungan:* Fundamental Perangkat Bergerak

Sertifikasi keamanan untuk iPadOS

Latar belakang sertifikasi iPadOS

Apple secara aktif terlibat dalam validasi sistem operasi Apple untuk setiap rilis besar sistem operasi, menggunakan Profil Perlindungan kolaboratif yang sesuai, dan level keamanan FIPS 140-3. Validasi kepatuhan hanya dapat dijalankan untuk versi rilis final.

Catatan: Pada tahun 2019, sistem operasi untuk perangkat iPad diubah menjadi iPadOS. Sebelum iPadOS 13.1, iPadOS bernama iOS.

Status validasi modul kriptografis iPadOS

Cryptographic Module Validation Program (CMVP) mempertahankan status validasi modul kriptografis di tiga daftar terpisah tergantung statusnya saat ini:

- Agar dapat dicantumkan di Daftar Implementasi Sedang Diuji CMVP, laboratorium harus membuat kontrak dengan Apple untuk menyediakan tes.
- Setelah tes diselesaikan oleh laboratorium, lab telah merekomendasikan validasi oleh CMVP, dan biaya CMVP telah dibayar, kemudian modul ditambahkan ke Daftar Modul dalam Proses (MIP). Daftar MIP melacak kemajuan upaya validasi CMVP dalam empat fase:
  - *Tinjauan Tertunda:* Menunggu sumber daya CMVP untuk ditetapkan.
  - *Dalam Tinjauan:* Sumber daya CMVP sedang melakukan aktivitas validasinya.
  - *Koordinasi:* Lab dan CMVP sedang menyelesaikan masalah apa pun yang ditemukan.
  - *Finalisasi:* Aktivitas dan formalitas yang terkait penerbitan sertifikat.
- Setelah validasi oleh CMVP, modul diberikan sertifikat kepatuhan dan ditambahkan ke daftar modul kriptografis yang disahkan. Ini meliputi:
  - Modul yang divalidasi ditandai sebagai aktif.
  - Setelah 5 tahun, modul akan ditandai sebagai historis.
  - Jika sertifikasi modul dicabut karena suatu alasan, modul akan ditandai sebagai dicabut.

Pada tahun 2020, CMVP mengadopsi standar internasional ISO/IEC 19790 sebagai dasar untuk FIPS 140-3.

Sertifikasi FIPS 140-3

Status saat ini

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman iPadOS 14 (2020) telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman iPadOS 15 (2021) sedang menjalani pengujian laboratorium. Item tersebut tercantum di Daftar Implementasi Sedang Diuji.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* iPadOS 15 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* iPadOS 15 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iPadOS 15 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14, M1) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iPadOS 15 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14, M1) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* iPadOS 14 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* iPadOS 14 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iPadOS 14 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14, M1) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iPadOS 14 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A9-A14, M1) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3

Sertifikasi FIPS 140-2

Tabel di bawah menampilkan modul kriptografis yang saat ini sedang diuji dan telah diuji kepatuhannya oleh laboratorium dengan FIPS 140-2.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3856 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* iPadOS 13 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3855 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* iPadOS 13 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 05/02/2021	*Sertifikat:* 3811 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman Corecrypto v10.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iPadOS 13 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 23/04/2019	*Sertifikat:* 3438 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v9.0 Apple untuk ARM *Sistem Operasi:* iOS 12 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 11/04/2019	*Sertifikat:* 3433 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v9.0 Apple untuk ARM *Sistem Operasi:* iOS 12 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3523 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v9.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 12 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 22/05/2018, 06/07/2018	*Sertifikat:* 3148 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v8.0 Apple untuk ARM *Sistem Operasi:* iOS 11 *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 17/05/2018, 03/07/2018	*Sertifikat:* 3147 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v8.0 Apple untuk ARM *Sistem Operasi:* iOS 11 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3223 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v1.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan iOS 11 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2016 *Tanggal validasi:* 01/02/2017	*Sertifikat:* 2828 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto iOS v7.0 Apple *Sistem Operasi:* iOS 10 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2016 *Tanggal validasi:* 01/02/2017	*Sertifikat:* 2827 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto iOS v7.0 Apple *Sistem Operasi:* iOS 10 *Jenis:* Perangkat lunak *Level keamanan:* 1

Versi sebelumnya

Sertifikasi yang lebih lama dari 5 tahun dicantumkan oleh CMVP dengan status historis. Versi iOS lama berikut ini memiliki validasi modul kriptografis:

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

Latar belakang sertifikasi Common Criteria (CC)

Apple secara aktif ikut serta dalam evaluasi iPadOS untuk setiap perilisan sistem operasi besar. Evaluasi hanya dapat dilakukan dengan versi final sistem operasi yang dirilis secara publik.

Status sertifikasi Common Criteria (CC)

Skema A.S., yang dioperasikan oleh NIAP, memelihara daftar Produk dalam Evaluasi. Daftar ini menyertakan produk yang sedang dievaluasi di Amerika Serikat dengan Common Criteria Testing Laboratory (CCTL) yang disetujui NIAP dan yang telah menyelesaikan Rapat Pertama Evaluasi (atau setara) tempat manajemen CCEVS menerima produk ke evaluasi secara resmi.

Setelah produk disertifikasi, NIAP memasukkan sertifikasi yang saat ini valid di daftar Produk yang Sesuai. Setelah 2 tahun, sertifikasi ini ditinjau kesesuaiannya dengan kebijakan pemeliharaan jaminan saat ini. Setelah tanggal pemeliharaan jaminan kedaluwarsa, NIAP memindahkan sertifikasi yang tercantum ke daftar Produk yang Diarsipkan miliknya.

Portal Common Criteria mencantumkan sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA). Portal CC dapat mempertahankan produk di daftar produk besertifikasi selama 5 tahun. Catatan disimpan oleh Portal CC untuk sertifikasi yang diarsipkan.

Tabel di bawah menampilkan sertifikasi yang saat ini sedang dievaluasi oleh laboratorium, atau yang telah disertifikasi sebagai sesuai dengan Common Criteria.

Status saat ini

Pengujian laboratorium untuk evaluasi dengan NIAP untuk iPadOS 15 sedang berlangsung. Untuk informasi terbaru, lihat Produk sedang dievaluasi (NIAP) dan Daftar Kepatuhan Produk.

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem operasi: iPadOS 15 *Tanggal sertifikasi:* 14/03/2019	*ID Skema:* — *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iPad dengan iOS 12 *Profil Perlindungan:* Fundamental Perangkat Bergerak, modul Klien VPN, EP klien LAN nirkabel, EP Agen MDM
Sistem operasi: iPadOS 14 *Tanggal sertifikasi:* 01/09/2021	*ID Skema:* 11147 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iPadOS 14 Apple: iPad *Profil Perlindungan:* Fundamental Perangkat Bergerak, modul Klien VPN, EP klien LAN nirkabel, EP Agen MDM

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem operasi: iPadOS 13 *Tanggal sertifikasi:* 06/11/2020	*ID Skema:* 11036 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iPadOS 13 di Perangkat Bergerak iPad *Profil Perlindungan:* Fundamental Perangkat Bergerak, modul Klien VPN, EP klien LAN nirkabel, EP Agen MDM

Versi sebelumnya

Versi iOS lama berikut ini memiliki validasi Common Criteria. Versi iOS sebelumnya diarsipkan oleh NIAP menurut kebijakan NIAP:

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

Sertifikasi keamanan untuk macOS

Latar belakang sertifikasi macOS

Apple secara aktif terlibat dalam validasi sistem operasi Apple untuk setiap rilis besar sistem operasi, menggunakan Profil Perlindungan kolaboratif yang sesuai, dan level keamanan FIPS 140-3. Validasi kepatuhan hanya dapat dijalankan untuk versi rilis final.

Status validasi modul kriptografis macOS

Cryptographic Module Validation Program (CMVP) mempertahankan status validasi modul kriptografis di tiga daftar terpisah tergantung statusnya saat ini:

- Agar dapat dicantumkan di Daftar Implementasi Sedang Diuji CMVP, laboratorium harus membuat kontrak dengan Apple untuk menyediakan tes.
- Setelah tes diselesaikan oleh laboratorium, lab telah merekomendasikan validasi oleh CMVP, dan biaya CMVP telah dibayar, kemudian modul ditambahkan ke Daftar Modul dalam Proses (MIP). Daftar MIP melacak kemajuan upaya validasi CMVP dalam empat fase:
  - *Tinjauan Tertunda:* Menunggu sumber daya CMVP untuk ditetapkan.
  - *Dalam Tinjauan:* Sumber daya CMVP sedang melakukan aktivitas validasinya.
  - *Koordinasi:* Lab dan CMVP sedang menyelesaikan masalah apa pun yang ditemukan.
  - *Finalisasi:* Aktivitas dan formalitas yang terkait penerbitan sertifikat.
- Setelah validasi oleh CMVP, modul diberikan sertifikat kepatuhan dan ditambahkan ke daftar modul kriptografis yang disahkan. Ini meliputi:
  - Modul yang divalidasi ditandai sebagai aktif.
  - Setelah 5 tahun, modul akan ditandai sebagai historis.
  - Jika sertifikasi modul dicabut karena suatu alasan, modul akan ditandai sebagai dicabut.

Pada tahun 2020, CMVP mengadopsi standar internasional ISO/IEC 19790 sebagai dasar untuk FIPS 140-3.

Untuk komputer Mac Apple, tabel berikut menampilkan pasangan modul kriptografis dengan teknologi Mac.

Modul kriptografis	Komputer Mac dengan Apple silicon	Komputer Mac dengan Keping Keamanan T2 Apple	Komputer Mac berbasis Intel tanpa Keping Keamanan T2 Apple
Ruang Pengguna Apple silicon	✓		
Kernel Apple silicon	✓		
Ruang Pengguna Intel		✓	✓
Kernel Intel		✓	✓
Penyimpanan Kunci Aman	✓	✓	

Sertifikasi FIPS 140-3

Pada tahun 2020, Apple merilis komputer Mac berbasis Apple Silicon. Penerapan modul kriptografis ke komputer Mac berbasis Apple Silicon atau Intel diindikasikan di kolom Info Modul di tabel di bawah.

Catatan: Keping Keamanan T2 Apple disertakan di banyak komputer Mac berbasis Intel. Untuk informasi mengenai sertifikasi keping T2, lihat Sertifikasi keamanan untuk Keping Keamanan T2 Apple.

Klien ssh macOS

OpenSSH dapat dikonfigurasi untuk menggunakan modul yang divalidasi FIPS 140-3 untuk algoritme FIPS 140-3 tertentu. Organisasi dapat menjalankan penginstal yang ditandatangani dan disahkan yang tersedia dari Apple dengan kata sandi *FIPS140Mode*. Penginstal meletakkan dua file di Mac:

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

Lalu macOS menggunakan file ini untuk membatasi sandi yang tersedia ke OpenSSH hanya untuk yang telah divalidasi oleh NIST dan memastikan bahwa klien OpenSSH menggunakan modul kriptografis yang disediakan oleh platform dan divalidasi. Administrator juga dapat membuat filenya sendiri. Untuk informasi lainnya, lihat halaman man `apple_ssh_and_fips` di macOS 12.0.1 atau lebih baru.

Status saat ini

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman macOS 11 Big Sur telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman macOS 12 Monterey sedang menjalani pengujian laboratorium. Item tersebut tercantum di Daftar Implementasi Sedang Diuji.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* macOS 12 Monterey di Apple Silicon *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* macOS 12 Monterey di Apple Silicon *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* macOS 12 Monterey di Intel *Lingkungan:* Intel, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* macOS 12 Monterey di Intel *Lingkungan:* Intel, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan macOS 12 Monterey pada Apple silicon, sep OS yang didistribusikan dengan macOS 12 Monterey pada Intel dengan T2 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (M1 dan T2) *Level keamanan:* 2
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan macOS 12 Monterey di Apple silicon *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (M1) *Level keamanan:* 2 *Level keamanan fisik:* 3
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* macOS 11 Big Sur pada Intel *Lingkungan:* Intel, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* macOS 11 Big Sur pada Intel *Lingkungan:* Intel, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* macOS 11 Big Sur pada Apple silicon *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* macOS 11 Big Sur pada Apple silicon *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan macOS 11 Big Sur pada Apple silicon, sep OS yang didistribusikan dengan macOS 11 Big Sur pada Intel *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (M1) *Level keamanan:* 2
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan macOS 11 Big Sur di Apple silicon *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (M1) *Level keamanan:* 2 *Level keamanan fisik:* 3

Sertifikasi FIPS 140-2

Tabel di bawah menampilkan modul kriptografis yang saat ini sedang diuji dan telah diuji kepatuhannya oleh laboratorium dengan FIPS 140-2.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman macOS 10.15 Catalina telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Catatan: Keping Keamanan T2 Apple disertakan di banyak komputer Mac berbasis Intel. Untuk informasi mengenai sertifikasi keping T2, lihat Sertifikasi keamanan untuk Keping Keamanan T2 Apple.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 24-03-2021	*Sertifikat:* 3859 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Ruang Pengguna Corecrypto Apple untuk Intel (ccv10) *Sistem operasi:* macOS 10.15 Catalina *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 24-03-2021	*Sertifikat:* 3858 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v10.0 Apple untuk Intel (ccv10) *Sistem operasi:* macOS 10.15 Catalina *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 12-04-2019	*Sertifikat:* 3402 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v9.0 Apple untuk Intel *Sistem operasi:* macOS 10.14 Mojave *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 12-04-2019	*Sertifikat:* 3431 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v9.0 Apple untuk Intel *Sistem operasi:* macOS 10.14 Mojave *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 22-03-2018	*Sertifikat:* 3155 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v8.0 Apple untuk Intel *Sistem operasi:* macOS 10.13 High Sierra *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 22-03-2018	*Sertifikat:* 3156 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v8.0 Apple untuk Intel *Sistem operasi:* macOS 10.13 High Sierra *Jenis:* Perangkat lunak *Level keamanan:* 1

Versi sebelumnya

Versi OS X dan macOS lama berikut ini memiliki validasi modul kriptografis. Versi yang lebih lama dari 5 tahun dicantumkan oleh CMVP dengan status historis:

- macOS 10.12 Sierra
- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks
- OS X 10.8 Mountain Lion
- OS X 10.7 Lion
- OS X 10.6 Snow Leopard

Latar belakang sertifikasi Common Criteria (CC)

Apple secara aktif ikut serta dalam evaluasi macOS untuk setiap perilisan sistem operasi besar. Evaluasi hanya dapat dilakukan dengan versi final sistem operasi yang dirilis secara publik.

Status sertifikasi Common Criteria (CC)

Skema A.S., yang dioperasikan oleh NIAP, memelihara daftar Produk dalam Evaluasi. Daftar ini menyertakan produk yang sedang dievaluasi di Amerika Serikat dengan Common Criteria Testing Laboratory (CCTL) yang disetujui NIAP dan yang telah menyelesaikan Rapat Pertama Evaluasi (atau setara) tempat manajemen CCEVS menerima produk ke evaluasi secara resmi.

Setelah produk disertifikasi, NIAP memasukkan sertifikasi yang saat ini valid di daftar Produk yang Sesuai. Setelah 2 tahun, sertifikasi ini ditinjau kesesuaiannya dengan kebijakan pemeliharaan jaminan saat ini. Setelah tanggal pemeliharaan jaminan kedaluwarsa, NIAP memindahkan sertifikasi yang tercantum ke Daftar Produk yang Diarsipkan miliknya.

Portal Common Criteria mencantumkan sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA). Portal CC dapat mempertahankan produk di daftar produk besertifikasi selama 5 tahun. Catatan disimpan oleh Portal CC untuk sertifikasi yang diarsipkan.

Tabel di bawah menampilkan sertifikasi yang saat ini sedang dievaluasi oleh laboratorium, atau yang telah disertifikasi sebagai sesuai dengan Common Criteria.

Status saat ini

Evaluasi dengan NIAP untuk macOS 11 dan macOS 12 menggunakan Profil Perlindungan Sistem Operasi Tujuan Umum dan Enkripsi Disk Penuh (FDE) (AA dan EE) sedang berlangsung.

Untuk informasi terbaru, lihat Produk sedang dievaluasi (NIAP) dan Daftar Kepatuhan Produk.

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem operasi: macOS 12 Monterey *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* —	*Judul:* Apple FileVault 2 dengan macOS 12 Monterey *Profil Perlindungan:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP akan dikonfirmasi)
Sistem operasi: macOS 12 Monterey *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* —	*Judul:* macOS 12 Monterey *Profil Perlindungan:* PP_OS_V4.21 (PP akan dikonfirmasi)
Sistem operasi: macOS 11 Big Sur *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* Apple FileVault 2 dengan macOS 11 Big Sur *Profil Perlindungan:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Sistem operasi: macOS 11 Big Sur *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* macOS 11 Big Sur Apple *Profil Perlindungan:* PP_OS_V4.21
Sistem operasi: macOS 10.15 Catalina *Tanggal sertifikasi:* 29/04/2021	*ID Skema:* 11078 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* FileVault 2 Apple pada komputer T2 yang menjalankan macOS 10.15 Catalina *Profil Perlindungan:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Sistem operasi: macOS 10.15 Catalina *Tanggal sertifikasi:* 23/09/2020	*ID Skema:* 11077 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* macOS 10.15 Catalina *Profil Perlindungan:* PP_OS_V4.21

Sertifikasi keamanan untuk tvOS

Latar belakang sertifikasi tvOS

Apple secara aktif terlibat dalam validasi modul kriptografis yang terkait dengan setiap rilis besar tvOS. Validasi kepatuhan hanya dapat dijalankan untuk versi rilis final.

Status validasi modul kriptografis tvOS

Cryptographic Module Validation Program (CMVP) mempertahankan status validasi modul kriptografis di tiga daftar terpisah tergantung statusnya saat ini:

- Agar dapat dicantumkan di Daftar Implementasi Sedang Diuji CMVP, laboratorium harus membuat kontrak dengan Apple untuk menyediakan tes.
- Setelah tes diselesaikan oleh laboratorium, lab telah merekomendasikan validasi oleh CMVP, dan biaya CMVP telah dibayar, kemudian modul ditambahkan ke Daftar Modul dalam Proses (MIP). Daftar MIP melacak kemajuan upaya validasi CMVP dalam empat fase:
  - *Tinjauan Tertunda:* Menunggu sumber daya CMVP untuk ditetapkan.
  - *Dalam Tinjauan:* Sumber daya CMVP sedang melakukan aktivitas validasinya.
  - *Koordinasi:* Lab dan CMVP sedang menyelesaikan masalah apa pun yang ditemukan.
  - *Finalisasi:* Aktivitas dan formalitas yang terkait penerbitan sertifikat.
- Setelah validasi oleh CMVP, modul diberikan sertifikat kepatuhan dan ditambahkan ke daftar modul kriptografis yang disahkan. Ini meliputi:
  - Modul yang divalidasi ditandai sebagai aktif.
  - Setelah 5 tahun, modul akan ditandai sebagai historis.
  - Jika sertifikasi modul dicabut karena suatu alasan, modul akan ditandai sebagai dicabut.

Pada tahun 2020, CMVP mengadopsi standar internasional ISO/IEC 19790 sebagai dasar untuk FIPS 140-3.

Sertifikasi FIPS 140-3

Status saat ini

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman tvOS 14 (2020) telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman tvOS 15 (2021) sedang menjalani pengujian laboratorium. Item tersebut tercantum di Daftar Implementasi Sedang Diuji.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* tvOS 15 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* tvOS 15 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan tvOS 15 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A10, A12) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* tvOS 14 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* tvOS 14 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan tvOS 14 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (A10, A12) *Level keamanan keseluruhan:* 2

Sertifikasi FIPS 140-2

Tabel di bawah menampilkan modul kriptografis yang saat ini sedang diuji dan telah diuji kepatuhannya oleh laboratorium dengan FIPS 140-2.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman tvOS 13 (2019) telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3856 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* tvOS 13 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 23/03/2021	*Sertifikat:* 3855 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* tvOS 13 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 05/02/2021	*Sertifikat:* 3811 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v10.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan tvOS 13 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 23/04/2019	*Sertifikat:* 3438 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v9.0 Apple untuk ARM *Sistem operasi:* tvOS 12 *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 11/04/2019	*Sertifikat:* 3433 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v9.0 Apple untuk ARM *Sistem operasi:* tvOS 12 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3523 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v9.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan tvOS 12 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 22/05/2018, 06/07/2018	*Sertifikat:* 3148 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v8.0 Apple untuk ARM *Sistem operasi:* tvOS 11 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 17/05/2018, 03/07/2018	*Sertifikat:* 3147 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v8.0 Apple untuk ARM *Sistem operasi:* tvOS 11 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3223 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v1.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan tvOS 11 *Jenis:* Perangkat keras *Level keamanan:* 2

Sertifikasi keamanan untuk watchOS

Latar belakang sertifikasi watchOS

Apple secara aktif terlibat dalam validasi modul kriptografis yang terkait dengan setiap rilis besar watchOS. Validasi kepatuhan hanya dapat dijalankan untuk versi rilis final.

Status validasi modul kriptografis watchOS

Cryptographic Module Validation Program (CMVP) mempertahankan status validasi modul kriptografis di tiga daftar terpisah tergantung statusnya saat ini:

- Agar dapat dicantumkan di Daftar Implementasi Sedang Diuji CMVP, laboratorium harus membuat kontrak dengan Apple untuk menyediakan tes.
- Setelah tes diselesaikan oleh laboratorium, lab telah merekomendasikan validasi oleh CMVP, dan biaya CMVP telah dibayar, kemudian modul ditambahkan ke Daftar Modul dalam Proses (MIP). Daftar MIP melacak kemajuan upaya validasi CMVP dalam empat fase:
  - *Tinjauan Tertunda:* Menunggu sumber daya CMVP untuk ditetapkan.
  - *Dalam Tinjauan:* Sumber daya CMVP sedang melakukan aktivitas validasinya.
  - *Koordinasi:* Lab dan CMVP sedang menyelesaikan masalah apa pun yang ditemukan.
  - *Finalisasi:* Aktivitas dan formalitas yang terkait penerbitan sertifikat.
- Setelah validasi oleh CMVP, modul diberikan sertifikat kepatuhan dan ditambahkan ke daftar modul kriptografis yang disahkan. Ini meliputi:
  - Modul yang divalidasi ditandai sebagai aktif.
  - Setelah 5 tahun, modul akan ditandai sebagai historis.
  - Jika sertifikasi modul dicabut karena suatu alasan, modul akan ditandai sebagai dicabut.

Pada tahun 2020, CMVP mengadopsi standar internasional ISO/IEC 19790 sebagai dasar untuk FIPS 140-3.

Sertifikasi FIPS 140-3

Status saat ini

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman watchOS 7 (2020) telah selesai diuji laboratorium dan telah direkomendasikan oleh laboratorium ke CMVP untuk validasi. Item tersebut tercantum di Daftar Modul dalam Proses.

Ruang pengguna, ruang kernel, dan penyimpanan kunci aman watchOS 8 (2021) sedang menjalani pengujian laboratorium. Item tersebut tercantum di Daftar Implementasi Sedang Diuji.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* watchOS 8 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* watchOS 8 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan watchOS 8 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (S3, S4, S5, S6) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2021 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v12 Apple *Sistem operasi:* sepOS yang didistribusikan dengan watchOS 8 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (S6) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* watchOS 7 *Lingkungan:* Apple Silicon, Pengguna, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* watchOS 7 *Lingkungan:* Apple Silicon, Kernel, Perangkat Lunak *Jenis:* Perangkat lunak *Level keamanan keseluruhan:* 1
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan watchOS 7 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (S3, S4, S5, S6) *Level keamanan keseluruhan:* 2
Tanggal rilis sistem operasi: 2020 *Tanggal validasi:* —	*Sertifikat:* Belum disertifikasi *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Corecrypto v11.1 Apple *Sistem operasi:* sepOS yang didistribusikan dengan watchOS 7 *Lingkungan:* Apple Silicon, Penyimpanan Kunci Aman, Perangkat keras *Jenis:* Perangkat Keras (S6) *Level keamanan keseluruhan:* 2 *Level keamanan fisik:* 3

Sertifikasi FIPS 140-2

Tabel di bawah menampilkan modul kriptografis yang saat ini sedang diuji dan telah diuji kepatuhannya oleh laboratorium dengan FIPS 140-2.

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* —	*Sertifikat:* 3856 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* watchOS 6 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* —	*Sertifikat:* 3855 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v10.0 Apple untuk ARM *Sistem operasi:* watchOS 6 *Jenis:* Perangkat lunak *Level keamanan:* 1

Tanggal	Sertifikat/Dokumen	Info modul
Tanggal rilis sistem operasi: 2019 *Tanggal validasi:* 05/02/2021	*Sertifikat:* 3811 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v10.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan watchOS 6 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 23/04/2019	*Sertifikat:* 3438 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v9.0 Apple untuk ARM *Sistem operasi:* watchOS 5 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 11/04/2019	*Sertifikat:* 3433 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v9.0 Apple untuk ARM *Sistem operasi:* watchOS 5 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2018 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3523 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v9.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan watchOS 5 *Jenis:* Perangkat keras *Level keamanan:* 2
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 22/05/2018, 06/07/2018	*Sertifikat:* 3148 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Pengguna Corecrypto v8.0 Apple untuk ARM *Sistem operasi:* watchOS 4 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 09/03/2018, 17/05/2018, 03/07/2018	*Sertifikat:* 3147 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kernel Corecrypto v8.0 Apple untuk ARM *Sistem operasi:* watchOS 4 *Jenis:* Perangkat lunak *Level keamanan:* 1
Tanggal rilis sistem operasi: 2017 *Tanggal validasi:* 10/09/2019	*Sertifikat:* 3223 *Dokumen:* Sertifikat Kebijakan Keamanan Panduan Pejabat Kriptografis	*Judul:* Modul Kriptografis Penyimpanan Kunci Aman v1.0 Apple *Sistem operasi:* sepOS yang didistribusikan dengan watchOS 4 *Jenis:* Perangkat keras *Level keamanan:* 2

Sertifikasi keamanan perangkat lunak

Tinjauan sertifikasi keamanan perangkat lunak Apple

Apple mempertahankan Sertifikat Validasi Kepatuhan Standar Pemrosesan Informasi Federal (FIPS) 140-2/-3 A.S. untuk sepOS dan firmware T2 serta sertifikasi lainnya. Apple memulai dengan *blok pembuatan sertifikasi* yang diterapkan secara luas di beberapa platform yang sesuai. Blok pembuatan pertama adalah validasi corecrypto yang digunakan untuk penyebaran modul kriptografis perangkat lunak dan perangkat keras di dalam sistem operasi yang dikembangkan oleh Apple. Blok pembuatan kedua adalah sertifikasi Secure Enclave, yang disematkan di berbagai perangkat Apple. Blok pembuatan ketiga adalah sertifikasi Elemen Aman (SE) yang ditemukan di perangkat Apple dengan Touch ID dan perangkat dengan Face ID. Blok pembuatan sertifikasi perangkat keras ini membuat landasan untuk sertifikasi keamanan platform yang lebih luas.

Sertifikasi produk: Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) adalah standar yang digunakan oleh berbagai organisasi sebagai dasar untuk melakukan evaluasi keamanan produk TI.

Untuk sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA) internasional, lihat Portal Common Criteria. Standar Common Criteria juga dapat digunakan di luar CCRA oleh skema validasi nasional dan swasta. Di Eropa, pengakuan bersama diatur berdasarkan persetujuan SOG-IS serta CCRA.

Tujuannya, sebagaimana dijelaskan oleh komunitas Common Criteria, adalah untuk kumpulan standar keamanan yang disetujui secara internasional untuk memberikan evaluasi yang jelas dan dapat diandalkan mengenai kemampuan keamanan produk Teknologi Informasi. Dengan memberikan penilaian independen atas kemampuan produk dalam memenuhi standar keamanan, Sertifikasi Common Criteria memberikan pelanggan kepercayaan lebih terhadap keamanan produk Teknologi Informasi dan menghasilkan keputusan yang lebih matang.

Melalui CCRA, negara anggota telah setuju untuk mengakui sertifikasi produk Teknologi Informasi dengan level kepercayaan yang sama. Evaluasi yang diperlukan sebelum sertifikasi bersifat ekstensif dan menyertakan:

- Profil Perlindungan (PP)
- Target Keamanan (ST)
- Persyaratan Fungsional Keamanan (SFR)
- Persyaratan Jaminan Keamanan (SAR)
- Level Jaminan Evaluasi (EAL)

Profil Perlindungan (PP) adalah dokumen yang menentukan persyaratan keamanan untuk kelas jenis perangkat (seperti Mobilitas) dan digunakan untuk menyediakan perbandingan antara evaluasi produk TI dalam kelas yang sama. Keanggotaan CCRA bersamaan dengan meningkatnya daftar PP yang disetujui, terus berkembang setiap tahunnya. Pengaturan ini memungkinkan pengembang produk untuk mengupayakan sertifikasi tunggal berdasarkan salah satu skema pengesahan sertifikat apa pun dan membuatnya dikenali oleh salah satu penanda tangan konsumen sertifikat.

Target Keamanan (ST) mendefinisikan *apa* yang akan dievaluasi saat produk TI sedang disertifikasi. ST diterjemahkan ke *Persyaratan Fungsional Keamanan (SFR)* yang lebih spesifik, yang digunakan untuk mengevaluasi ST secara lebih mendetail.

Common Criteria (CC) juga menyertakan *Persyaratan Jaminan Keamanan*. Satu metrik yang umum teridentifikasi adalah *Level Jaminan Evaluasi (EAL)*. EAL mengelompokkan kumpulan SAR yang sering terjadi dan dapat ditetapkan di PP serta ST untuk mendukung keterbandingan.

Banyak PP yang lebih lama telah diarsipkan dan sedang diganti dengan PP yang ditargetkan, yang sedang dikembangkan dan fokus pada solusi serta lingkungan tertentu. Dalam upaya selaras untuk memastikan pengenalan bersama berkelanjutan pada semua anggota CCRA, international Technical Community (iTC) telah dibangun untuk mengembangkan dan memelihara Profil Perlindungan kolaboratif (cPP) yang dikembangkan dari awal dengan keterlibatan dari beberapa skema penanda tangan CCRA. PP yang ditargetkan untuk grup pengguna dan pengaturan pengakuan bersama selain CCRA terus dikembangkan oleh pemegang saham yang sesuai.

Apple mulai mengupayakan sertifikasi berdasarkan CCRA yang diperbarui dengan cPP terpilih mulai awal 2015. Sejak saat itu, Apple telah mendapatkan sertifikasi Common Criteria untuk setiap perilisan iOS besar dan telah memperluas cakupannya untuk menyertakan jaminan keamanan yang diberikan oleh PP baru.

Apple berperan aktif dalam komunitas teknis yang fokus mengevaluasi teknologi keamanan seluler. Ini menyertakan iTC yang bertanggung jawab dalam mengembangkan dan memperbarui cPP. Apple terus mengevaluasi dan mengupayakan sertifikasi berdasarkan PP dan cPP saat ini.

Sertifikasi platform Apple untuk pasar Amerika Utara secara umum dilakukan dengan National Information Assurance Partnership (NIAP), yang mempertahankan daftar proyek yang saat ini dalam evaluasi namun belum disertifikasi.

Selain sertifikat platform umum yang tercantum, sertifikat lainnya telah diterbitkan untuk mendemonstrasikan persyaratan keamanan spesifik untuk beberapa pasar.

Sertifikasi keamanan untuk app Apple

Latar belakang sertifikasi app Apple

Apple secara aktif berpartisipasi dalam sertifikasi keamanan app Apple menggunakan Profil Perlindungan (PP) Common Criteria yang sesuai. Evaluasi ini dibuat berdasarkan sertifikasi perangkat keras dan sistem operasi yang telah diperoleh Apple.

Pada tahun 2018, Apple memulai evaluasi keamanan aplikasi untuk aplikasi utama yang dijalankan di iOS 11 dengan app browser Safari dan Kontak. Apple melanjutkan evaluasi ini di app yang dijalankan di iOS 12, iOS 13 serta iPadOS 13.1. Pada tahun 2021, cakupan untuk app yang dijalankan di macOS 11 sedang ditambahkan.

Status sertifikasi modul kriptografis

App Apple yang tercantum di sini menggunakan modul kriptografis untuk sistem operasi yang berlaku. Untuk informasi lainnya, lihat Sertifikasi keamanan untuk iOS, Sertifikasi keamanan untuk iPadOS, dan Sertifikasi keamanan untuk macOS.

Status sertifikasi Common Criteria (CC)

Skema A.S., yang dioperasikan oleh NIAP, memelihara daftar Produk dalam Evaluasi. Daftar ini menyertakan produk yang sedang dievaluasi di Amerika Serikat dengan Common Criteria Testing Laboratory (CCTL) yang disetujui NIAP dan yang telah menyelesaikan Rapat Pertama Evaluasi (atau setara) tempat manajemen CCEVS menerima produk ke evaluasi secara resmi.

Setelah produk disertifikasi, NIAP memasukkan sertifikasi yang saat ini valid di daftar Produk yang Sesuai. Setelah 2 tahun, sertifikasi ini ditinjau kesesuaiannya dengan kebijakan pemeliharaan jaminan saat ini. Setelah tanggal pemeliharaan jaminan kedaluwarsa, NIAP memindahkan sertifikasi yang tercantum ke daftar Produk yang Diarsipkan miliknya.

Portal Common Criteria mencantumkan sertifikasi yang dapat sama-sama dikenali di Common Criteria Recognition Arrangement (CCRA). Portal CC dapat mempertahankan produk di daftar produk besertifikasi selama 5 tahun. Catatan disimpan oleh Portal CC untuk sertifikasi yang diarsipkan.

Tabel di bawah menampilkan sertifikasi yang saat ini sedang dievaluasi oleh laboratorium, atau yang telah disertifikasi sebagai sesuai dengan Common Criteria.

Status saat ini

- Evaluasi dengan NIAP yang diterbitkan sebagai sedang berlangsung tercantum di Produk dalam evaluasi (NIAP).
- Evaluasi yang telah selesai dan divalidasi tercantum di Daftar Kepatuhan Produk NIAP.

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem operasi: macOS 11 Big Sur *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* macOS 11 Big Sur: Kontak *Profil Perlindungan:* PP untuk SW Aplikasi, EP untuk Browser Web
Sistem operasi: macOS 11 Big Sur *Tanggal sertifikasi:* —	*ID Skema:* Belum disertifikasi *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* macOS 11 Big Sur: Safari *Profil Perlindungan:* PP untuk SW Aplikasi, EP untuk Browser Web
Sistem operasi: iOS 14, iPadOS 14 *Tanggal sertifikasi:* 20/08/2021	*ID Skema:* 11191 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iOS 14 dan iPadOS 14 Apple: Kontak *Profil Perlindungan:* PP untuk SW Aplikasi, EP untuk Browser Web
Sistem operasi: iOS 14, iPadOS 14 *Tanggal sertifikasi:* —	*ID Skema:* 11192 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iOS 14 dan iPadOS 14 Apple: Safari *Profil Perlindungan:* PP untuk SW Aplikasi, EP untuk Browser Web
Sistem operasi: iOS 13, iPadOS 13 *Tanggal sertifikasi:* 05/06/2020	*ID Skema:* 11060 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iOS 13 dan iPadOS 13 Apple: Safari *Profil Perlindungan:* PP untuk SW Aplikasi, EP untuk Browser Web

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem operasi: iOS 13, iPadOS 13 *Tanggal sertifikasi:* 05/06/2020	*ID Skema:* 11050 *Dokumen:* Sertifikat Target Keamanan Panduan Laporan Validasi Laporan Aktivitas Jaminan	*Judul:* iOS 13 dan iPadOS 13 Apple: Kontak *Profil Perlindungan:* PP untuk SW Aplikasi

Sertifikasi Common Criteria yang Diarsipkan untuk app Apple

Sistem operasi/Tanggal sertifikasi	ID Skema/Dokumen	Judul/Profil Perlindungan
Sistem Operasi: iOS 12 *Tanggal sertifikasi:* 12/06/2019	*ID Skema:* 10960 *Dokumen:* Target Keamanan Panduan	*Judul:* Safari iOS 12 *Profil Perlindungan:* PP untuk SW Aplikasi, EP untuk Browser Web
Sistem Operasi: iOS 12 *Tanggal sertifikasi:* 28/02/2019	*ID Skema:* 10961 *Dokumen:* Target Keamanan Panduan	*Judul:* Kontak iOS 12 *Profil Perlindungan:* PP untuk SW Aplikasi
Sistem Operasi: iOS 11 *Tanggal sertifikasi:* 09/11/2018	*ID Skema:* 10916 *Dokumen:* Target Keamanan Panduan	*Judul:* Safari iOS 11 *Profil Perlindungan:* PP untuk SW Aplikasi, EP untuk Browser Web
Sistem Operasi: iOS 11 *Tanggal sertifikasi:* 13/09/2018	*ID Skema:* 10915 *Dokumen:* Target Keamanan Panduan	*Judul:* Kontak iOS 11 *Profil Perlindungan:* PP untuk SW Aplikasi

Sertifikasi keamanan untuk layanan internet Apple

Apple mempertahankan sertifikasi sesuai dengan standar ISO/IEC 27001 dan ISO/IEC 27018 untuk memungkinkan pelanggan Apple menangani peraturan dan kewajiban kontraknya. Sertifikasi ini memberikan pengesahan independen pada pelaksanaan Keamanan dan Privasi Informasi Apple untuk sistem dalam lingkup.

ISO/IEC 27001 dan ISO/IEC 27018 adalah bagian dari standar Sistem Manajemen Keamanan Informasi (ISMS) yang diterbitkan oleh International Organization for Standardization (ISO). Sebagai bagian dari ISMS Apple, semua persyaratan kontrol Lampiran A telah disertakan di Pernyataan Keberterapan sebagaimana didefinisikan dalam standar ISO/IEC 27001 dan ISO/IEC 27018. Apple menjalani pengesahan independen oleh pencatat terakreditasi setiap tahun.

ISO/IEC 27001

ISO/IEC 27001 adalah standar Sistem Manajemen Keamanan Informasi yang menentukan persyaratan untuk membuat, mengimplementasikan, memelihara, dan secara terus-menerus meningkatkan Sistem Manajemen Keamanan Informasi organisasi. Standar ISO/IEC 27001 disertai dengan domain keamanan berikut yang dicakup oleh sertifikasi ISO/IEC Apple:

- Kebijakan keamanan informasi
- Organisasi keamanan informasi
- Manajemen aset
- Keamanan sumber daya manusia
- Keamanan fisik dan lingkungan
- Manajemen komunikasi dan operasi
- Kontrol akses
- Akuisisi, pengembangan, dan pemeliharaan sistem informasi
- Manajemen insiden keamanan informasi
- Manajemen berkelanjutan bisnis
- Kepatuhan

ISO/IEC 27018

ISO/IEC 27018 adalah kode praktik untuk perlindungan informasi yang dapat diidentifikasi secara pribadi (PII) di lingkungan awan publik. Standar ISO/IEC 27018 disertai dengan domain keamanan berikut yang dicakup oleh sertifikasi ISO/IEC Apple:

- Persetujuan dan pilihan
- Legitimasi dan spesifikasi tujuan
- Batasan pengumpulan
- Minimalisasi data
- Batasan penggunaan, retensi, dan pengungkapan
- Keakuratan dan kualitas
- Keterbukaan, transparansi, dan pemberitahuan
- Partisipasi dan akses individu
- Akuntabilitas
- Keamanan informasi
- Kepatuhan privasi

Layanan Apple yang dicakup oleh ISO/IEC 27001 dan ISO/IEC 27018

Sertifikasi ISO/IEC 27001 dan ISO/IEC 27018 Apple mencakup layanan berikut:

- Obrolan Bisnis Apple
- Apple Business Manager
- Layanan Pemberitahuan Push Apple (APN)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- Layanan iWork
- ID Apple yang Dikelola
- Schoolwork
- Siri

Sertifikasi

Bukti sertifikasi ISO/IEC 27001 dan 27018 Apple tersedia di pencatat kami.

Untuk melihat sertifikasi Apple, buka Certificate and Client Directory search di situs web British Standards Institution (BSI), masukkan Apple di bidang pencarian Company, klik tombol Search, lalu pilih hasil pencarian untuk melihat sertifikat.

Catatan: Informasi mengenai produk yang tidak diproduksi oleh Apple, atau situs web independen yang tidak dikontrol atau diuji oleh Apple, disediakan tanpa rekomendasi atau dukungan. Apple tidak bertanggung jawab atas pilihan, kinerja, atau penggunaan situs web atau produk pihak ketiga. Apple tidak memberikan pernyataan terkait keakuratan atau keandalan situs web pihak ketiga. Hubungi vendor untuk informasi tambahan.

Proyek Kepatuhan Keamanan macOS

Proyek Kepatuhan Keamanan macOS (mSCP) adalah upaya sumber terbuka untuk menyediakan pendekatan programatis untuk membuat panduan keamanan. Ini adalah proyek gabungan staf Keamanan TI operasional federal dari National Institute of Standards and Technology (NIST), National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA), dan Los Alamos National Laboratory (LANL). Proyek ini menggunakan kumpulan kontrol yang telah diuji dan disahkan untuk macOS dan memetakan kontrol ini terhadap panduan keamanan mana pun yang didukung oleh proyek. Selain itu, proyek ini dapat digunakan sebagai sumber daya untuk dengan mudah membuat basis keamanan yang disesuaikan dari kontrol keamanan teknis dengan memanfaatkan perpustakaan tindakan atomis yang telah diuji dan disahkan (pengaturan konfigurasi). Proyek ini menghasilkan dokumentasi, skrip, profil konfigurasi, dan daftar centang audit yang disesuaikan berdasarkan basis yang digunakan.

mSCP dapat menghasilkan konten output untuk digunakan bersama dengan alat pengelolaan dan keamanan untuk mencapai kepatuhan. Pengaturan konfigurasi di proyek ini mendukung basis panduan berikut:

Organisasi	Basis yang didukung
Publikasi Khusus (SP) 800-53 National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems and Organizations, Revision 5	800-53 Tinggi, 800-53 Sedang, 800-53 Rendah
Publikasi Khusus (SP) 800-171 National Institute of Standards and Technology (NIST), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Rev.2	800-171
Agen Sistem Informasi Keamanan (DISA) macOS 11 STIG, Panduan Implementasi Teknis Keamanan macOS 11 Apple	STIG
Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems	1253

Informasi tambahan:

- Basis untuk meninjau semua aturan di proyek tersedia di sini.
- Untuk mempelajari lebih lanjut mengenai proyek dan penggunaan, lihat wiki Proyek Kepatuhan Keamanan macOS.
- Untuk mengatur proyek yang akan digunakan, lihat: Mengenali Proyek Kepatuhan Keamanan macOS, Bagian 1 dan Mengenali Proyek Kepatuhan Keamanan macOS, Bagian 2.
- Jika Anda berminat untuk mendukung pengembangan proyek, lihat panduan kontributor.

Riwayat revisi dokumen

Tanggal	Ringkasan
27 Oktober 2021	Topik yang diperbarui: • Sertifikasi keamanan untuk Prosesor Secure Enclave • Sertifikasi keamanan untuk iOS • Sertifikasi keamanan untuk macOS
17 Agustus 2021	Topik yang diperbarui: • Sertifikasi keamanan untuk Prosesor Secure Enclave • Sertifikasi keamanan untuk Keping Keamanan T2 Apple • Sertifikasi keamanan untuk iOS • Sertifikasi keamanan untuk iPadOS • Sertifikasi keamanan untuk macOS • Sertifikasi keamanan untuk tvOS • Sertifikasi keamanan untuk watchOS • Sertifikasi keamanan untuk app Apple • Sertifikasi keamanan • Proyek Kepatuhan Keamanan macOS
26 April 2021	Topik yang ditambahkan: • Proyek Kepatuhan Keamanan macOS Topik yang diperbarui: • Sertifikasi keamanan untuk Keping Keamanan T2 Apple: Sertifikasi FIPS 140-2 baru, 3811 • Sertifikasi keamanan untuk Prosesor Secure Enclave: Sertifikasi FIPS 140-2 baru, 3811 dan tabel baru untuk sertifikasi tambahan. • Sertifikasi keamanan untuk iOS: Sertifikasi FIPS 140-2 baru, 3811, iOS 14 ID Skema 11146 dalam evaluasi • Sertifikasi keamanan untuk iPadOS: Sertifikasi FIPS 140-2 baru, 3811, iPadOS 14 ID Skema 11147 dalam evaluasi • Sertifikasi keamanan untuk macOS: Sertifikasi FIPS 140-2 baru, 3811. • Sertifikasi keamanan untuk tvOS: Sertifikasi FIPS 140-2 baru, 3811. • Sertifikasi keamanan untuk watchOS: Sertifikasi FIPS 140-2 baru, 3811. • Sertifikasi keamanan untuk app Apple: Pembaruan ke status Common Criteria, dan tabel baru untuk sertifikasi Common Criteria yang diarsipkan.

Glosarium

Apple Business Manager Portal sederhana berbasis web untuk administrator TI yang menyediakan cara yang cepat dan sederhana bagi organisasi untuk menyebarkan perangkat Apple yang telah mereka beli secara langsung dari Apple atau dari Penjual Resmi Apple dan Operator yang berpartisipasi. Mereka dapat secara otomatis mendaftarkan perangkat di solusi mobile device management (MDM) tanpa harus secara fisik menyentuh atau menyiapkan perangkat sebelum pengguna mendapatkannya.

Apple School Manager Portal sederhana berbasis web untuk administrator TI yang menyediakan cara yang cepat dan sederhana bagi organisasi untuk menyebarkan perangkat Apple yang telah mereka beli secara langsung dari Apple atau dari Penjual Resmi Apple dan Operator yang berpartisipasi. Mereka dapat secara otomatis mendaftarkan perangkat di solusi mobile device management (MDM) tanpa harus secara fisik menyentuh atau menyiapkan perangkat sebelum pengguna mendapatkannya.

Common Criteria (CC) Standar yang membangun konsep umum dan prinsip evaluasi keamanan TI serta menetapkan model evaluasi umum. Ini menyertakan katalog persyaratan keamanan dalam bahasa standar.

Common Criteria Recognition Arrangement (CCRA) Pengaturan pengakuan bersama yang membangun kebijakan dan persyaratan untuk pengakuan internasional terhadap sertifikat yang diterbitkan sesuai dengan ISO/IEC seri 15408 atau standar Common Criteria.

corecrypto Library yang menyediakan implementasi primitif kriptografis level rendah. Harap diperhatikan bahwa corecrypto tidak menyediakan antarmuka pemrograman secara langsung untuk pengembang dan digunakan melalui API yang disediakan oleh pengembang. Kode sumber corecrypto tersedia secara publik agar kebenaran fungsi dan karakteristik keamanannya dapat diverifikasi.

Cryptographic Algorithm Validation Program (CAVP) Organisasi yang dioperasikan oleh NIST untuk menyediakan pengujian validasi dari algoritme kriptografis yang Disetujui (misalnya, yang disetujui FIPS dan yang dianjurkan NIST) serta komponennya masing-masing.

Cryptographic Module Validation Program (CMVP) Organisasi yang dioperasikan oleh pemerintahan A.S. dan Kanada untuk memvalidasi kepatuhan terhadap standar FIPS 140-3.

Elemen Aman (SE) Keping silikon yang disematkan di banyak perangkat Apple yang mendukung fungsi seperti Apple Pay.

Enkripsi Disk Penuh (FDE) Pengenkripsian semua data di volume penyimpanan.

Implementasi yang sedang Diuji (IUT) Modul kriptografis yang sedang diuji oleh laboratorium.

international Technical Community (iTC) Grup yang bertanggung jawab dalam mengembangkan Profil Perlindungan atau Profil Perlindungan kolaboratif di bawah ßnaungan Common Criteria Recognition Arrangement (CCRA).

Klien VPN IPsec Di Profil Perlindungan, klien yang menyediakan koneksi IPsec aman antara platform host fisik atau virtual dan lokasi jarak jauh.

Layanan Pemberitahuan Push Apple (APN) Layanan global dari Apple yang mengirimkan pemberitahuan push ke perangkat Apple.

Level keamanan (SL) Empat level keamanan secara keseluruhan (1–4) yang didefinisikan dalam ISO/IEC 19790 untuk menjelaskan kumpulan persyaratan keamanan yang berlaku. Level 4 adalah yang paling ketat.

mobile device management (MDM) Layanan yang memungkinkan pengguna mengelola perangkat yang didaftarkan dari jarak jauh. Setelah perangkat didaftarkan, pengguna dapat menggunakan layanan MDM melalui jaringan untuk mengonfigurasi pengaturan dan melakukan tugas lainnya di perangkat tanpa interaksi pengguna.

Modul dalam Proses (MIP) Daftar yang dikelola oleh Cryptographic Module Validation Program (CMVP) dari modul kriptografis yang saat ini dalam proses validasi CMVP.

modul kriptografis Perangkat keras, perangkat lunak, dan/atau firmware yang menyediakan fungsi kriptografis dan memenuhi persyaratan standar modul kriptografis yang dinyatakan.

National Information Assurance Partnership (NIAP) Organisasi pemerintahan A.S. yang bertanggung jawab dalam mengoperasikan implementasi A.S. terhadap standar Common Criteria dan mengelola Skema Evaluasi dan Validasi Common Criteria (CCEVS) NIAP.

National Institute of Standards and Technology (NIST) Bagian dari Kementerian Perdagangan A.S. yang bertanggung jawab dalam memajukan sains, standar, dan teknologi pengukuran.

Pernyataan Keberterapan (SOA) Dokumen yang menjelaskan kontrol keamanan yang diimplementasikan dalam cakupan ISMS, yang diproduksi untuk mendukung sertifikasi ISO/IEC 27001.

Profil Perlindungan (PP) Dokumen yang menentukan masalah keamanan dan persyaratan keamanan untuk kelas produk tertentu.

Profil Perlindungan kolaboratif (cPP) Profil Perlindungan yang dikembangkan oleh international Technical Community, sekelompok pakar yang bertanggung jawab dalam pembuatan cPP.

Prosesor Secure Enclave (SEP) Koprosesor yang dibuat dalam sistem pada keping (SoC).

Senior Officials Group Information Systems Security (SOG-IS) Grup yang mengelola persetujuan pengakuan bersama antara beberapa negara Eropa.

sepOS Firmware Secure Enclave, berdasarkan versi mikrokernel L4 khusus Apple.

Sistem Manajemen Keamanan Informasi (ISMS) Sekumpulan kebijakan dan prosedur keamanan informasi yang mengatur batasan program keamanan yang dirancang untuk melindungi cakupan informasi dan sistem dengan mengelola keamanan informasi secara sistematis pada seluruh informasi dan atau siklus proses sistem.

sistem pada keping (SoC) Sirkuit terpadu (IC) yang menggabungkan beberapa komponen ke dalam satu keping.

Standar Pemrosesan Informasi Federal (FIPS) Publikasi yang dikembangkan oleh National Institute of Standards and Technology, baik saat diwajibkan oleh undang-undang, atau saat terdapat persyaratan pemerintahan federal yang berlaku untuk keamanan siber, atau keduanya.

T2 Keping keamanan Apple yang disertakan di beberapa komputer Mac berbasis Intel sejak tahun 2017.

Target Keamanan (ST) Dokumen yang menentukan masalah keamanan dan persyaratan keamanan untuk produk tertentu.

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

ID028-00499-B