Güvenlik Sertifikaları ve Uygunluk Merkez

Aralık 2021

İçindekiler

Apple güvenlik güvencesine giriş

Apple, güvenliğe bağlılığının bir parçası olarak Apple donanımlarının, yazılımlarının ve servislerinin güvenliğini onaylamak ve doğrulamak için üçüncü taraf kuruluşlarla düzenli olarak bağlantı kurar. Uluslararası tanınan bu kuruluşlar, Apple'a her büyük işletim sistemi sürümüyle uyumlu sertifikalar sağlar. Bu şekilde, sistemin güvenlik gereksinimlerinin karşılandığına dair bir güven (güvenlik güvencesi) sağlanmış olur. Apple, karşılıklı tanıma anlaşmaları (MRA'lar) çerçevesinde kabul edilmemiş veya gelişmiş güvenlik sertifikası standartlarına sahip olmayan bazı teknik alanlar için uygun güvenlik standartlarının geliştirilmesine katılmaktadır. Amacımız, tüm Apple donanımlarında, işletim sistemlerinde, uygulamalarında ve servislerinde tüm dünyada kabul gören, kapsamlı güvenlik sertifikalarını kullanmaktır.

Sertifikalar çoğunlukla mevzuat, düzenleme ve sektör standartları ile ilgili gereksinimleri karşılamak için gereklidir. Apple Okul Yönetimi ve Apple İşletme Yönetimi gibi servisler, Apple'ın ISO/IEC 27001 ve ISO/IEC 27018 sertifikaları kapsamındadır. Kamu kurumları, kurumsal şirketler ve eğitim kurumları da dahil olmak üzere Apple aygıtlarını dağıtan tüm müşteriler, uygunluğunu desteklemek için donanım, işletim sistemi, yazılım ve servis sertifikalarını kullanabilir.

Donanım sertifikaları

Güvenli yazılım, donanımda yerleşik güvenlik temelleri gerektirdiği için tüm Apple aygıtları (iOS, iPadOS, macOS, tvOS veya watchOS çalıştırması farketmeksizin), donanımları için tasarlanmış güvenlik yeteneklerine sahiptir. Bunlara, sistem güvenliği özelliklerine ve güvenlik işlevlerine ayrılmış donanımlara güç veren özel CPU yetenekleri de dahildir. En kritik bileşen, tüm modern iOS, iPadOS, watchOS ve tvOS aygıtlarında, Apple Silicon yongasına sahip tüm Mac bilgisayarlarında ve Apple T2 güvenlik yongasına sahip Intel tabanlı Mac bilgisayarlarında görünen Secure Enclave yardımcı işlemcisidir. Secure Enclave; aygıtta duran verileri şifreleme, macOS'te güvenli başlatma ve biyometrik işlevlerinin temelini oluşturur.

Apple'ın güvenlik güvencesine bağlılığı, donanım güven kökünden güvenli başlatma uygulamasına, güvenli anahtar deposu sunan Secure Enclave'e, Touch ID ve Face ID ile güvenli kimlik doğrulamaya varana dek donanımlarındaki temel güvenlik bileşenlerinin sertifikalarıyla başlar. Apple aygıtlarının güvenlik özellikleri, yalnızca Apple'ın sunduğu devre tasarımlarının, donanımların, yazılımların ve servislerin birleşimi sayesinde mümkün olmuştur. Bu bileşenlere yönelik sertifikalar, Apple'ın sunduğu güvenceyi doğrulamanın önemli bir parçasıdır.

Donanımlar ve ilişkili firmware bileşenleri ile ilgili herkese açık sertifikalar hakkında bilgi için şu sayfalara bakın:

- Apple T2 güvenlik yongası için güvenlik sertifikaları
- Secure Enclave işlemcisi için güvenlik sertifikaları

Yazılım ve uygulama sertifikaları

Apple, şifreleme modülleri için ABD Federal Bilgi İşleme Standardı (FIPS) 140-2/-3 ve işletim sistemleri, uygulamalar ve aygıt servisleri için Ortak Kriterler uygunluğuna göre işletim sistemleri ve uygulamaları ile ilgili bağımsız sertifikalara ve onaylara sahiptir. İşletim sistemleri kapsamına iOS, iPadOS, macOS, sepOS, T2 firmware, tvOS ve watchOS dahildir. Uygulamalar açısından, bağımsız sertifikalara başlangıçta Safari tarayıcısı ve Kişiler uygulaması dahil olmakla birlikte gelecekte daha fazla uygulamanın onaylanması planlanmaktadır.

Apple *işletim sistemleri* ile ilgili herkese açık sertifikalar hakkında bilgi için şu sayfalara bakın:

- iOS için güvenlik sertifikaları
- iPadOS için güvenlik sertifikaları
- macOS için güvenlik sertifikaları
- tvOS için güvenlik sertifikaları
- watchOS için güvenlik sertifikaları

Apple *uygulamaları* ile ilgili herkese açık sertifikalar hakkında bilgi için şu sayfalara bakın:

- Apple uygulamaları için güvenlik sertifikaları

Servis sertifikaları

Apple, ister kurumsal alanda ister eğitim alanında olsun tüm müşterilerini desteklemeye yönelik güvenlik sertifikalarına sahiptir. Bu sertifikalar, Apple müşterilerinin Apple donanımları ve yazılımları ile Apple servislerini kullanırken mevzuat ve sözleşme kaynaklı yükümlülüklerini yerine getirebilmelerini sağlar. Bu sertifikalar müşterilerimize, Apple sistemleri için Apple'ın bilgi güvenliği, çevre ve gizlilik uygulamaları ile ilgili bağımsız bir onay sağlar.

Apple *internet servisleri* ile ilgili herkese açık sertifikalar hakkında bilgi için şu sayfalara bakın:

- Apple internet servisleri için güvenlik sertifikaları

Apple'ın Güvenlik ve Gizlilik Sertifikaları ile ilgili sorular için security-certifications@apple.com ile iletişim kurun.

Donanım güvenliği sertifikaları

Apple donanım güvenliği sertifikalarına genel bakış

Apple, diğer sertifikaların yanı sıra sepOS ve T2 firmware için ABD Federal Bilgi İşleme Standardı (FIPS) 140-2/-3 uygunluk doğrulama sertifikalarına da sahiptir. Apple, uygun olduğunda kapsamlı bir biçimde birden fazla platforma uygulanan *sertifika yapı taşları* ile başlar. Bu yapı taşlarından biri, Apple tarafından geliştirilen işletim sistemlerindeki yazılım ve donanım şifreleme modülü dağıtımları için kullanılan corecrypto arşivi doğrulamasıdır. İkinci bir yapı taşı, birçok Apple aygıtında yerleşik olan Secure Enclave'dir. Üçüncüsü ise Apple'ın Touch ID'li aygıtlarında ve Face ID'li aygıtlarında bulunan Secure Element (SE) sertifikasıdır. Bu donanım sertifikası yapı taşları, daha geniş platform güvenliği sertifikaları için bir temel oluşturur.

Şifreleme algoritması doğrulamaları

Birçok şifreleme algoritmasının ve ilişkili güvenlik işlevinin uygulama doğruluğunun tasdiklenmesi, FIPS 140-3 doğrulamasının ön koşuludur ve diğer sertifikalar için de destekleyicidir. Doğrulama, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Şifreleme Algoritması Doğrulama Programı (CAVP) tarafından yönetilir. Apple uygulamalarının doğrulama sertifikaları CAVP arama özelliği kullanılarak bulunabilir. Daha fazla bilgi için Şifreleme Algoritması Doğrulama Programı (CAVP) web sitesine bakın.

Şifreleme modülü doğrulamaları: FIPS 140-2/3 (ISO/IEC 19790)

Apple'ın şifreleme modüllerinin, şifreleme modülleri için ABD Federal Bilgi İşleme Standardı (FIPS 140-2) ile uyumlu olduğu, Şifreleme Modülü Doğrulama Programı (CMVP) tarafından 2012'den beri işletim sistemlerinin her büyük sürümünden sonra yinelenerek doğrulanmıştır. Apple, her büyük sürümden sonra bu modülleri standarda uygunluğunun doğrulanması için CMVP'ye gönderir. Bu modüller, Apple işletim sistemleri ve uygulamaları tarafından kullanılmalarının yanı sıra Apple tarafından sunulan servisler için şifreleme işlevleri sağlar ve üçüncü parti uygulamalar tarafından da kullanılabilir.

Apple, macOS'e yönelik "Intel İçin Corecrypto Modülü" ve "Intel İçin Corecrypto Çekirdek Modülü" yazılım tabanlı modülleri için her yıl **Güvenlik Düzeyi 1** sertifikasını alır. Apple Silicon için, "ARM için Corecrypto modülü" ve "ARM için Corecrypto çekirdek modülü" adlı modüller iOS, iPadOS, tvOS, watchOS ve Mac bilgisayarlarındaki yerleşik Apple T2 güvenlik yongasında bulunan firmware için geçerlidir.

2019 yılında Apple, "Apple Corecrypto Modülü: Güvenli Anahtar Deposu" olarak tanımlanan ve Secure Enclave'de oluşturulan ve yönetilen anahtarların ABD hükümeti onaylı kullanımını etkinleştiren gömülü donanım şifreleme modülü için ilk FIPS 140-2 **Güvenlik Düzeyi 2**'yi elde etmiştir. Apple, birbirini izleyen her büyük işletim sistemi sürümünde donanım şifreleme modülü için doğrulamaları elde etmeye çalışır.

FIPS 140-3, ABD Ticaret Bakanlığı tarafından 2019 yılında onaylanmıştır. Standardın bu sürümündeki en belirgin değişiklik, ISO/IEC standartlarının (özellikle ISO/IEC 19790:2015'in ve ilişkili test standardı ISO/IEC 24759:2017'nin) belirtimidir. CMVP, bir geçiş programı başlattı ve 2020'den itibaren şifreleme modüllerinin FIPS 140-3 temel alınarak doğrulanmaya başlanacağını belirtti. Apple şifreleme modüllerinin en kısa sürede FIPS 140-3 standardına uygun hâle gelip bu standarda geçmesi hedeflenmektedir.

CMVP, şu an test ve doğrulama aşamasındaki şifreleme modüllerine yönelik iki ayrı liste tutar. Bu listeler, önerilen doğrulamalar hakkında bilgi içerebilir. Yetkili bir laboratuvarda test edilmekte olan şifreleme modülleri için Test Edilen Uygulama Listesi, modülü listeleyebilir. Laboratuvar, testleri tamamlayıp CMVP tarafından doğrulanmalarını önerdikten sonra Apple şifreleme modülleri, İşlenen Modüller listesinde görünür. Mevcut durumda laboratuvar testleri tamamlanmıştır ve testlerin CMVP tarafından doğrulanması beklenmektedir. Değerlendirme işleminin süresi değişebileceğinden, büyük işletim sistemi sürümünün çıkış tarihiyle CMVP tarafından doğrulama sertifikasının veriliş tarihi arasında Apple şifreleme modüllerinin güncel durumunu belirlemek için yukarıda belirtilen iki işlem listesine de bakın.

Ürün sertifikaları: Ortak Kriterler (ISO/IEC 15408)

Ortak Kriterler (ISO/IEC 15408), birçok kuruluş tarafından BT ürünlerinin güvenlik değerlendirmelerini gerçekleştirmede temel olarak kullanılan bir standarttır.

Uluslararası Ortak Kriterler Tanıma Anlaşması (CCRA) çerçevesinde karşılıklı olarak tanınan sertifikalar için Ortak Kriterler Portalı'na bakın. Ortak Kriterler standardı, CCRA dışında ulusal ve özel doğrulama programları tarafından da kullanılabilir. Avrupa'da karşılıklı tanıma, hem SOG-IS hem de CCRA anlaşmasına tabidir.

Bu girişimin amacı, Ortak Kriterler topluluğu tarafından belirtildiği şekilde, Bilgi Teknolojisi ürünlerinin anlaşılır ve güvenilir bir değerlendirmesini sunmak için uluslararası düzeyde onaylı güvenlik standartlarının oluşturulmasıdır. Ortak Kriterler Sertifikası ürünün, güvenlik standartlarını karşılayıp karşılamadığına ilişkin bağımsız bir değerlendirme sağlayarak müşterilerin Bilgi Teknolojisi ürünlerinin güvenliğinden emin olmasına ve daha bilinçli kararlar vermesine olanak tanır.

CCRA ile, üye ülkeler Bilgi Teknolojisi ürünlerine yönelik bu sertifikayı aynı güven düzeyinde tanımayı kabul etmiştir. Sertifikadan önce gereken kapsamlı değerlendirmeler şunları içerir:

- Koruma profilleri (PP)
- Güvenlik hedefleri (ST)
- Güvenlik işlev gereksinimleri (SFR)
- Güvenlik güvence gereksinimleri (SAR)
- Değerlendirme güvence düzeyleri (EAL)

Koruma profilleri (PP), bir aygıt türü sınıfı (Taşınabilirlik gibi) için güvenlik gereksinimlerini belirten ve aynı sınıftaki BT ürün değerlendirmelerini karşılaştırmak için kullanılan belgelerdir. CCRA üye sayısı ve giderek uzayan onaylı PP'lerin listesi yıllık bazda büyümeye devam etmektedir. Bu anlaşma, ürün geliştiricilerinin, herhangi bir sertifika yetkilendirme programı kapsamında tek bir sertifika almak için çalışmasına ve tüm sertifika kullanım imzacıları tarafından tanınmasını sağlamasına izin verir.

Güvenlik hedefleri (ST), bir BT ürününün onaylanması sürecinde *nelerin* değerlendirileceğini tanımlar. ST'ler, kendileriyle ilgili daha ayrıntılı değerlendirmelerde kullanılan *güvenlik işlev gereksinimlerine (SFR)* çevrilir.

Ortak Kriterler (CC), *güvenlik güvence gereksinimlerini* de içerir. En yaygın tanımlanan ölçümlerden biri *değerlendirme güvence düzeyidir (EAL)*. EAL'ler, en sık görülen SAR kümelerini gruplar ve karşılaştırılabilmelerini sağlamak için koruma profillerinde (PP) veya güvenlik hedeflerinde (ST) belirtilebilir.

Birçok eski koruma profili arşivlenmiş ve belirli çözümlere ve ortamlara odaklanması amacıyla geliştirilen hedefe yönelik koruma profilleri (PP) bunların yerini almıştır. Tüm CCRA üyelerinin devam eden karşılıklı tanıma konusunda ortak hareket edebilmesini sağlamak amacıyla sürecin başından beri CCRA imzacı programının katılımıyla geliştirilen iş birliğine dayalı koruma profilleri (cPP) geliştirmek ve sürekliliğini sağlamak için uluslararası teknik topluluklar (iTC) kurulmuştur. Hedefi CCRA dışındaki kullanıcı grupları ve karşılıklı tanıma anlaşmaları olan koruma profilleri (PP), uygun paydaşlar tarafından geliştirilmeye devam eder.

Apple, 2015 yılının başından itibaren belirli iş birliğine dayalı koruma profillerinde (cPP'ler) güncellenmiş CCRA kapsamındaki sertifikaları almak için gereken çalışmalara başlamıştır. O zamandan beri Apple, her büyük iOS sürümü için Ortak Kriterler sertifikalarını almış ve kapsamını yeni koruma profilleri (PP) tarafından sağlanan güvenlik güvencesini de içerecek şekilde genişletmiştir.

Apple, mobil güvenlik teknolojilerinin değerlendirilmesine odaklanan teknik topluluklarda aktif rol alır. Bunlara cPP'lerin geliştirilmesinden ve güncellenmesinden sorumlu iTC'ler de dahildir. Apple, güncel PP ve cPP sürümlerine uygun sertifikaları değerlendirmeyi ve uygulamayı sürdürmektedir.

Kuzey Amerika pazarı için Apple platform sertifikaları, genellikle şu an değerlendirme aşamasında olup henüz onaylanmamış projelerin listesini tutan Ulusal Bilgi Güvencesi Ortaklığı (NIAP) ile gerçekleştirilir.

Listelenen genel platform sertifikalarının yanı sıra bazı pazarlar için belirli güvenlik gereksinimlerini göstermek üzere başka sertifikalar da verilmiştir.

Secure Enclave işlemcisi için güvenlik sertifikaları

Secure Enclave sertifikası arka planı

Donanım Şifreleme Modülü (*Apple SEP Güvenli Anahtar Deposu Şifreleme Modülü*), şu ürünlerde bulunan Apple SOC'de yerleşik gelir: Apple'ın iPhone ve iPad için A serisi, Apple Silicon yongasına sahip Mac bilgisayarları için M serisi, Apple Watch için S serisi ve 2017 yılında tanıtılan iMac Pro ile başlayarak Intel tabanlı Mac bilgisayarlarında bulunan T serisi güvenlik yongası.

2018 yılında Apple, yazılım şifreleme modülleri doğrulamasını 2017'de çıkan şu işletim sistemleriyle eşzamanlamıştır: iOS 11, macOS 10.13, tvOS 11 ve watchOS 4. Apple SEP Güvenli Anahtar Deposu Şifreleme Modülü 1.0 olarak tanımlanan SEP donanım şifreleme modülünün FIPS 140-2 Güvenlik Düzeyi 1 gereksinimlerine uygunluğu doğrulanmıştır.

2019 yılında Apple, donanım modülünü FIPS 140-2 Güvenlik Düzeyi 2 gereksinimlerine uygunluk açısından doğrulamış ve modül sürümü tanıtıcısını, karşılık gelen corecrypto kullanıcı ve corecrypto çekirdek modülü doğrulamalarının sürümleriyle eşzamanlı olması için 9.0 olarak güncellemiştir. 2019 yılında bu kapsama iOS 12, macOS 10.14, tvOS 12 ve watchOS 5 dahil edilmiştir.

Apple 2020 ve 2021'de, Apple Silicon A13, A14, S6 ve M1 yongalarının fiziksel güvenlik gereksinimlerinin, FIPS 140-2 ve güvenlik düzeyi 3 ek güvencesi ile uygunluğunu doğrulama işlemlerine devam etmiştir.

Apple, her büyük işletim sistemi sürümünde bulunan corecrypto kullanıcı ve corecrypto çekirdek modüllerinin doğrulanmasında da etkin bir şekilde görev almaktadır. Uygunluk doğrulaması yalnızca en son çıkan sürümde gerçekleştirilebilir.

Şifreleme modülü doğrulama durumu

Şifreleme Modülü Doğrulama Programı (CMVP), şifreleme modüllerinin doğrulama durumunu, modüllerin mevcut durumlarına göre üç ayrı listede tutar:

- Laboratuvarın CMVP Test Edilen Uygulama listesinde listelenmesi için test yapma konusunda Apple ile sözleşme yapmış olması gerekir.
- Testler laboratuvar tarafından tamamlandıktan, laboratuvar CMVP tarafından doğrulanma önerdikten ve CMVP ücretleri ödendikten sonra modül, İşlenen Modüller listesine eklenir. İşlenen Modüller (MIP) Listesi, CMVP doğrulama çalışmaları ilerlemesini dört aşamada takip eder:
  - *İnceleme Bekleniyor:* CMVP kaynağının atanması bekleniyor.
  - *İncelemede:* CMVP kaynakları, doğrulama çalışmalarını gerçekleştiriyor.
  - *Koordinasyon:* Laboratuvar ve CMVP bulunan sorunların çözümü üzerinde çalışıyor.
  - *Sonlandırma:* Sertifika vermeye ilişkin çalışmalar ve formaliteler.
- Modüller, CMVP tarafından doğrulandıktan sonra bir uygunluk sertifikası alır ve doğrulanan şifreleme modülleri listesine eklenir. Bu liste şunları içerir:
  - Etkin olarak işaretlenmiş doğrulanmış modüller.
  - 5 yıl sonra modüller geçmiş olarak işaretlenir.
  - Modül sertifikası bir nedenden dolayı iptal edilirse modül iptal edilmiş olarak işaretlenir.

2020 yılında CMVP, FIPS 140-3 için temel olarak ISO/IEC 19790 uluslararası standardını benimsemiştir.

FIPS 140-3 sertifikaları

Şu anki durum

Aşağıdaki tablo, şu anda laboratuvar tarafından FIPS 140-3 uygunluğu konusunda test edilen 2020 ve 2021 şifreleme modüllerini gösterir.

2020 ve 2021 işletim sistemi sürümleriyle ilişkili güvenli anahtar deposu (SKS) için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller Listesi'nde listelenir ve doğrulandıktan sonra doğrulanan şifreleme modülleri listesine taşınır.

iOS 15 (2021) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu laboratuvar testlerine tabi tutulmaktadır. Bunlar, Test Edilen Uygulama listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple corecrypto Modülü 12 *İşletim sistemi:* iOS, iPadOS, macOS, tvOS ve watchOS 2021 sürümleriyle dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14, T2, M1, S3-S6) *Genel güvenlik düzeyi:* 2

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iOS, iPadOS, macOS, tvOS ve watchOS 2021 sürümleriyle dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A13, A14, S6, M1) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iOS, iPadOS, macOS, tvOS ve watchOS 2020 sürümleriyle dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14, T2, M1, S3-S6) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iOS, iPadOS, macOS, tvOS ve watchOS 2020 sürümleriyle dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A13, A14, S6, M1) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3

FIPS 140-2 sertifikaları

Aşağıdaki tablo, laboratuvar tarafından FIPS 140-2 uygunluğu konusunda testleri tamamlanmış olan şifreleme modüllerini gösterir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 05.02.2021	*Sertifikalar:* 3811 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 10.0 *İşletim sistemi:* macOS 10.15 Catalina için sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3523 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 9.0 *İşletim sistemi:* macOS 10.14 Mojave için sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3223 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 1.0 *İşletim sistemi:* macOS 10.13 High Sierra için sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2

Ortak Kriterler (CC) sertifikaları

Apple, uygun koruma profillerinin Apple teknolojilerinin güvenlik işlevini kapsadığı Ortak Kriterler değerlendirmelerinde etkin bir şekilde görev almaktadır.

Ortak Kriterler (CC) sertifika durumu

NIAP tarafından yürütülen ABD programı bir Değerlendirilen Ürünler listesi tutar. Bu liste, şu anda ABD'de NIAP onaylı bir Ortak Kriterler Test Laboratuvarı'nda (CCTL) teste tabi tutulan ürünleri ve CCEVS yönetiminin ürünü resmi olarak değerlendirmeye kabul ettiği Değerlendirme Başlangıcı Toplantısı'ndan (veya eşdeğeri) geçenleri listeler.

Ürünler onaylandıktan sonra NIAP, şu an geçerli doğrulamaları Uyumlu Ürünler listesine ekler. 2 yıldan sonra bu sertifikalar, güncel güvence bakım politikasına uygunluğu açısından incelenir. Güvence bakım tarihi geçtikten sonra NIAP, sertifika listesini kendi Arşivlenmiş Ürünler listesine taşır.

Ortak Kriterler Portalı, Ortak Kriterleri Tanıma Anlaşması (CCRA) kapsamında karşılıklı olarak tanınabilecek sertifikaları listeler. CC Portalı, ürünleri sertifikalı ürün listesinde 5 yıl saklayabilir. CC Portalı, arşivlenen sertifikaların kayıtlarını tutar.

Aşağıdaki tablo, şu an bir laboratuvar tarafından değerlendirilmekte olan veya Ortak Kriterler'e uygun olduğu onaylanmış sertifikaları gösterir.

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: sepOS *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple Secure Enclave [2020] *Koruma Profilleri:* CPP_DSC_V1.0 *Donanım:* (A9-A14, M1, T2, S3-S6) için Secure Enclave *Yazılım:* iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 ile dağıtılan sepOS

Ek sertifikalar

Aşağıdaki tablo, Secure Enclave için Ortak Kriterler'i ve FIPS 140-3'ü kullanmayan sertifikaları gösterir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* 07.12.2019 - 26.12.2022	*Sertifikalar:* CFNR201902910002 (P.R. Çin: Mobil Finansal Servisler İçin Teknoloji Sertifikası) Çince sürümü İngilizce sürümü	*Başlık:* Mobil Terminal Güvenilir Çalıştırma Ortamı *İşletim sistemi:* iOS 13.5.1 *Belirtim:* JR/T 0156-2017

Apple T2 güvenlik yongası için güvenlik sertifikaları

Şifreleme modülü doğrulaması arka planı

Apple, her büyük işletim sistemi sürümünde bulunan Apple yazılım ve donanım modüllerinin doğrulanmasında etkin bir şekilde görev almaktadır. Uygunluk doğrulaması yalnızca en son modül sürümünde gerçekleştirilebilir.

2020 yılında CMVP, ABD Federal Bilgi İşleme Standardı (FIPS) 140-3 için temel olarak ISO/IEC 19790 uluslararası standardını benimsemiştir.

Birçok Mac bilgisayarında Intel CPU bulunmasına ek olarak 2017 yılından beri Apple Silicon tabanlı bir yongadaki sistem (SoC) olan ayrı bir Apple T2 güvenlik yongası da bulunur. T2 yongalı bu Mac bilgisayarları, aygıttaki çeşitli servisler için beş şifreleme modülünün hepsini kullanır.

- Intel için corecrypto kullanıcı modülü (Intel tabanlı Mac bilgisayarlarında macOS tarafından kullanılır)
- Intel için corecrypto çekirdek modülü (Intel tabanlı Mac bilgisayarlarında macOS tarafından kullanılır)
- ARM için corecrypto kullanıcı modülü (T2 yongası tarafından kullanılır)
- ARM için corecrypto çekirdek modülü (T2 yongası tarafından kullanılır)
- Güvenli Anahtar Deposu Şifreleme Modülü (T2 yongasında yerleşik Secure Enclave yardımcı işlemcisi tarafından kullanılır)

Not: T2 yongasında çalışan Apple Silicon tabanlı modüller; Apple A serisi, S serisi ve M serisi gibi diğer Apple Silicon yongalarında çalışanlarla aynıdır.

Şifreleme modülü doğrulama durumu

Şifreleme Modülü Doğrulama Programı (CMVP), şifreleme modüllerinin doğrulama durumunu, modüllerin mevcut durumlarına göre üç ayrı listede tutar:

- Laboratuvarın CMVP Test Edilen Uygulama listesinde listelenmesi için test yapma konusunda Apple ile sözleşme yapmış olması gerekir.
- Testler laboratuvar tarafından tamamlandıktan, laboratuvar CMVP tarafından doğrulanma önerdikten ve CMVP ücretleri ödendikten sonra modül, İşlenen Modüller (MIP) listesine eklenir. İşlenen Modüller (MIP) Listesi, CMVP doğrulama çalışmaları ilerlemesini dört aşamada takip eder:
  - *İnceleme Bekleniyor:* CMVP kaynağının atanması bekleniyor.
  - *İncelemede:* CMVP kaynakları, doğrulama çalışmalarını gerçekleştiriyor.
  - *Koordinasyon:* Laboratuvar ve CMVP bulunan sorunların çözümü üzerinde çalışıyor.
  - *Sonlandırma:* Sertifika vermeye ilişkin çalışmalar ve formaliteler.
- Modüller, CMVP tarafından doğrulandıktan sonra bir uygunluk sertifikası alır ve doğrulanan şifreleme modülleri listesine eklenir. Bu liste şunları içerir:
  - Etkin olarak işaretlenmiş doğrulanmış modüller.
  - 5 yıl sonra modüller geçmiş olarak işaretlenir.
  - Modül sertifikası bir nedenden dolayı iptal edilirse modül iptal edilmiş olarak işaretlenir.

FIPS 140-3 sertifikaları

Şu anki durum

Kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için olan 2020 modüllerinin laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

Kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için olan 2021 modülleri laboratuvar testlerine tabi tutulmaktadır. Bunlar, Test Edilen Uygulama listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* macOS 12 Monterey için sepOS *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* macOS 12 Monterey için sepOS *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* macOS 12 Monterey için sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (T2) *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* macOS 11 Big Sur için sepOS *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* macOS 11 Big Sur için sepOS *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* Intel'de macOS 11 Big Sur için sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım *Güvenlik düzeyi:* 2

FIPS 140-2 sertifikaları

Aşağıdaki tablo, laboratuvar tarafından FIPS 140-2 uygunluğu konusunda testleri tamamlanmış olan şifreleme modüllerini gösterir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3856 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 10.0 *İşletim sistemi:* macOS 10.15 Catalina için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3855 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 10.0 *İşletim sistemi:* macOS 10.15 Catalina için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 05.02.2021	*Sertifikalar:* 3811 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Güvenli Anahtar Deposu Şifreleme Modülü 10.0 *İşletim sistemi:* macOS 10.15 Catalina için sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 23.04.2019	*Sertifikalar:* 3438 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 9.0 *İşletim sistemi:* macOS 10.14 Mojave için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 11.04.2019	*Sertifikalar:* 3433 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 9.0 *İşletim sistemi:* macOS 10.14 Mojave için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3523 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 9.0 *İşletim sistemi:* macOS 10.14 Mojave için sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikalar:* 3148 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 8.0 *İşletim sistemi:* macOS 10.13 High Sierra için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikalar:* 3147 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 8.0 *İşletim sistemi:* macOS 10.13 High Sierra için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 10.07.2018	*Sertifikalar:* 3223 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 1.0 *İşletim sistemi:* macOS 10.13 High Sierra için sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2016 *Doğrulama tarihleri:* 01.02.2017	*Sertifikalar:* 2828 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple iOS Corecrypto Çekirdek Modülü 7.0 *İşletim sistemi:* macOS 10.12 Sierra için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2016 *Doğrulama tarihleri:* 01.02.2017	*Sertifikalar:* 2827 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple iOS Corecrypto Çekirdek Modülü 7.0 *İşletim sistemi:* macOS 10.12 Sierra için sepOS *Tür:* Yazılım *Güvenlik düzeyi:* 1

İşletim sistemi güvenlik sertifikaları

Apple işletim sistemi güvenlik sertifikalarına genel bakış

Apple, diğer sertifikaların yanı sıra sepOS ve T2 firmware için ABD Federal Bilgi İşleme Standardı (FIPS) 140-2/-3 uygunluk doğrulama sertifikalarına da sahiptir. Apple, uygun olduğunda kapsamlı bir biçimde birden fazla platforma uygulanan *sertifika yapı taşları* ile başlar. Bu yapı taşlarından biri, Apple tarafından geliştirilen işletim sistemlerindeki yazılım ve donanım şifreleme modülü dağıtımları için kullanılan corecrypto doğrulamasıdır. İkinci bir yapı taşı, birçok Apple aygıtında yerleşik olan Secure Enclave'dir. Üçüncüsü ise Apple'ın Touch ID'li aygıtlarında ve Face ID'li aygıtlarında bulunan Secure Element (SE) sertifikasıdır. Bu donanım sertifikası yapı taşları, daha geniş platform güvenliği sertifikaları için bir temel oluşturur.

Şifreleme algoritması doğrulamaları

Birçok şifreleme algoritmasının ve ilişkili güvenlik işlevinin uygulama doğruluğunun tasdiklenmesi, FIPS 140-3 doğrulamasının ön koşuludur ve diğer sertifikalar için de destekleyicidir. Doğrulama, NIST Şifreleme Algoritması Doğrulama Programı (CAVP) tarafından yönetilir. Apple uygulamalarının doğrulama sertifikaları CAVP arama özelliği kullanılarak bulunabilir.

Şifreleme modülü doğrulamaları: FIPS 140-2/3 (ISO/IEC 19790)

Apple işletim sistemlerindeki şifreleme modüllerinin ABD Federal Bilgi İşleme Standartları (FIPS) 140-2 ile uyumlu olduğu, Şifreleme Modülü Doğrulama Programı (CMVP) tarafından 2012'den beri işletim sistemlerinin her büyük sürümünden sonra yinelenerek doğrulanmıştır. Apple, her büyük sürümden sonra tüm modülleri tam şifreleme doğrulaması için CMVP'ye gönderir. Bu doğrulanan modüller, Apple tarafından verilen servisler için şifreleme işlemleri sunar ve üçüncü parti uygulamalar tarafından kullanılabilir.

Apple, macOS'e yönelik "Intel İçin Corecrypto Modülü" ve "Intel İçin Corecrypto Çekirdek Modülü" yazılım tabanlı modülleri için her yıl **Güvenlik Düzeyi 1** sertifikasını alır. Apple Silicon için, "ARM için Corecrypto modülü" ve "ARM için Corecrypto çekirdek modülü" adlı modüller iOS, iPadOS, tvOS, watchOS ve Mac bilgisayarlarındaki yerleşik Apple T2 güvenlik yongasında bulunan firmware için geçerlidir.

2019 yılında Apple, "Apple Corecrypto Modülü: Güvenli Anahtar Deposu" olarak tanımlanan ve Secure Enclave'de oluşturulan ve yönetilen anahtarların ABD hükümeti onaylı kullanımını etkinleştiren gömülü donanım şifreleme modülü için ilk FIPS 140-2 **Güvenlik Düzeyi 2**'yi elde etmiştir. Apple, birbirini izleyen her büyük işletim sistemi sürümünde donanım şifreleme modülü için doğrulamaları elde etmeye çalışır.

FIPS 140-3, ABD Ticaret Bakanlığı tarafından 2019 yılında onaylanmıştır. Standardın bu sürümündeki en belirgin değişiklik, ISO/IEC standartlarının (özellikle ISO/IEC 19790:2015'in ve ilişkili test standardı ISO/IEC 24759:2017'nin) belirtimidir. CMVP, bir geçiş programı başlattı ve 2020'den itibaren şifreleme modüllerinin FIPS 140-3 temel alınarak doğrulanmaya başlanacağını belirtti. Apple şifreleme modüllerinin en kısa sürede FIPS 140-3 standardına uygun hâle gelip bu standarda geçmesi hedeflenmektedir.

CMVP, şu an test ve doğrulama aşamasındaki şifreleme modüllerine yönelik iki ayrı liste tutar. Bu listeler, önerilen doğrulamalar hakkında bilgi içerebilir. Yetkili bir laboratuvarda test edilmekte olan şifreleme modülleri için Test Edilen Uygulama Listesi, modülü listeleyebilir. Laboratuvar, testleri tamamlayıp CMVP tarafından doğrulanmalarını önerdikten sonra Apple şifreleme modülleri, İşlenen Modüller listesinde görünür. Mevcut durumda laboratuvar testleri tamamlanmıştır ve testlerin CMVP tarafından doğrulanması beklenmektedir. Değerlendirme işleminin süresi değişebileceğinden, büyük işletim sistemi sürümünün çıkış tarihiyle CMVP tarafından doğrulama sertifikasının veriliş tarihi arasında Apple şifreleme modüllerinin güncel durumunu belirlemek için yukarıda belirtilen iki işlem listesine de bakın.

Ürün sertifikaları: Ortak Kriterler (ISO/IEC 15408)

Ortak Kriterler (ISO/IEC 15408), birçok kuruluş tarafından BT ürünlerinin güvenlik değerlendirmelerini gerçekleştirmede temel olarak kullanılan bir standarttır.

Uluslararası Ortak Kriterler Tanıma Anlaşması (CCRA) çerçevesinde karşılıklı olarak tanınan sertifikalar için Ortak Kriterler Portalı'na bakın. Ortak Kriterler standardı, CCRA dışında ulusal ve özel doğrulama programları tarafından da kullanılabilir. Avrupa'da karşılıklı tanıma, hem SOG-IS hem de CCRA anlaşmasına tabidir.

Bu girişimin amacı, Ortak Kriterler topluluğu tarafından belirtildiği şekilde, Bilgi Teknolojisi ürünlerinin anlaşılır ve güvenilir bir değerlendirmesini sunmak için uluslararası düzeyde onaylı güvenlik standartlarının oluşturulmasıdır. Ortak Kriterler Sertifikası ürünün, güvenlik standartlarını karşılayıp karşılamadığına ilişkin bağımsız bir değerlendirme sağlayarak müşterilerin Bilgi Teknolojisi ürünlerinin güvenliğinden emin olmasına ve daha bilinçli kararlar vermesine olanak tanır.

CCRA ile, üye ülkeler Bilgi Teknolojisi ürünlerine yönelik bu sertifikayı aynı güven düzeyinde tanımayı kabul etmiştir. Sertifikadan önce gereken kapsamlı değerlendirmeler şunları içerir:

- Koruma profilleri (PP)
- Güvenlik hedefleri (ST)
- Güvenlik işlev gereksinimleri (SFR)
- Güvenlik güvence gereksinimleri (SAR)
- Değerlendirme güvence düzeyleri (EAL)

Koruma profilleri (PP), bir aygıt türü sınıfı (Taşınabilirlik gibi) için güvenlik gereksinimlerini belirten ve aynı sınıftaki BT ürün değerlendirmelerini karşılaştırmak için kullanılan belgelerdir. CCRA üye sayısı ve giderek uzayan onaylı PP'lerin listesi yıllık bazda büyümeye devam etmektedir. Bu anlaşma, ürün geliştiricilerinin, herhangi bir sertifika yetkilendirme programı kapsamında tek bir sertifika almak için çalışmasına ve tüm sertifika kullanım imzacıları tarafından tanınmasını sağlamasına izin verir.

Güvenlik hedefleri (ST), bir BT ürününün onaylanması sürecinde *nelerin* değerlendirileceğini tanımlar. ST'ler, kendileriyle ilgili daha ayrıntılı değerlendirmelerde kullanılan *güvenlik işlev gereksinimlerine (SFR)* çevrilir.

Ortak Kriterler (CC), *güvenlik güvence gereksinimlerini* de içerir. En yaygın tanımlanan ölçümlerden biri *değerlendirme güvence düzeyidir (EAL)*. EAL'ler, en sık görülen SAR kümelerini gruplar ve karşılaştırılabilmelerini sağlamak için koruma profillerinde (PP) veya güvenlik hedeflerinde (ST) belirtilebilir.

Birçok eski koruma profili arşivlenmiş ve belirli çözümlere ve ortamlara odaklanması amacıyla geliştirilen hedefe yönelik koruma profilleri (PP) bunların yerini almıştır. Tüm CCRA üyelerinin devam eden karşılıklı tanıma konusunda ortak hareket edebilmesini sağlamak amacıyla sürecin başından beri CCRA imzacı programının katılımıyla geliştirilen *iş birliğine dayalı koruma profilleri (cPP)* geliştirmek ve sürekliliğini sağlamak için uluslararası teknik topluluklar (iTC) kurulmuştur. Hedefi CCRA dışındaki kullanıcı grupları ve karşılıklı tanıma anlaşmaları olan koruma profilleri (PP), uygun paydaşlar tarafından geliştirilmeye devam eder.

Apple, 2015 yılının başından itibaren belirli iş birliğine dayalı koruma profillerinde (cPP'ler) güncellenmiş CCRA kapsamındaki sertifikaları almak için gereken çalışmalara başlamıştır. O zamandan beri Apple, her büyük iOS sürümü için Ortak Kriterler sertifikalarını almış ve kapsamını yeni koruma profilleri (PP) tarafından sağlanan güvenlik güvencesini de içerecek şekilde genişletmiştir.

Apple, mobil güvenlik teknolojilerinin değerlendirilmesine odaklanan teknik topluluklarda aktif rol alır. Bunlara cPP'lerin geliştirilmesinden ve güncellenmesinden sorumlu iTC'ler de dahildir. Apple, güncel PP ve cPP sürümlerine uygun sertifikaları değerlendirmeyi ve uygulamayı sürdürmektedir.

Kuzey Amerika pazarı için Apple platform sertifikaları, genellikle şu an değerlendirme aşamasında olup henüz onaylanmamış projelerin listesini tutan Ulusal Bilgi Güvencesi Ortaklığı (NIAP) ile gerçekleştirilir.

Listelenen genel platform sertifikalarının yanı sıra bazı pazarlar için belirli güvenlik gereksinimlerini göstermek üzere başka sertifikalar da verilmiştir.

iOS için güvenlik sertifikaları

iOS sertifikası arka planı

Apple, her büyük işletim sistemi sürümünde bulunan Apple yazılım ve donanım modüllerinin doğrulanmasında etkin bir şekilde görev almaktadır. Uygunluk doğrulaması yalnızca en son çıkan sürümde gerçekleştirilebilir.

iOS şifreleme modülü doğrulama durumu

Şifreleme Modülü Doğrulama Programı (CMVP), şifreleme modüllerinin doğrulama durumunu, modüllerin mevcut durumlarına göre üç ayrı listede tutar:

- Laboratuvarın CMVP Test Edilen Uygulama listesinde listelenmesi için test yapma konusunda Apple ile sözleşme yapmış olması gerekir.
- Testler laboratuvar tarafından tamamlandıktan, laboratuvar CMVP tarafından doğrulanma önerdikten ve CMVP ücretleri ödendikten sonra modül, İşlenen Modüller (MIP) listesine eklenir. İşlenen Modüller (MIP) Listesi, CMVP doğrulama çalışmaları ilerlemesini dört aşamada takip eder:
  - *İnceleme Bekleniyor:* CMVP kaynağının atanması bekleniyor.
  - *İncelemede:* CMVP kaynakları, doğrulama çalışmalarını gerçekleştiriyor.
  - *Koordinasyon:* Laboratuvar ve CMVP bulunan sorunların çözümü üzerinde çalışıyor.
  - *Sonlandırma:* Sertifika vermeye ilişkin çalışmalar ve formaliteler.
- Modüller, CMVP tarafından doğrulandıktan sonra bir uygunluk sertifikası alır ve doğrulanan şifreleme modülleri listesine eklenir. Bu liste şunları içerir:
  - Etkin olarak işaretlenmiş doğrulanmış modüller.
  - 5 yıl sonra modüller geçmiş olarak işaretlenir.
  - Modül sertifikası bir nedenden dolayı iptal edilirse modül iptal edilmiş olarak işaretlenir.

2020 yılında CMVP, FIPS 140-3 için temel olarak ISO/IEC 19790 uluslararası standardını benimsemiştir.

FIPS 140-3 sertifikaları

Şu anki durum

iOS 14 (2020) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

iOS 15 (2021) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu laboratuvar testlerine tabi tutulmaktadır. Bunlar, Test Edilen Uygulama listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iOS 15 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iOS 15 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iOS 15 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iOS 15 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A13, A14, A15) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iOS 14 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iOS 14 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iOS 14 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iOS 14 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A13-A14) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3

FIPS 140-2 sertifikaları

Aşağıdaki tablo, laboratuvar tarafından FIPS 140-2 uygunluğu konusunda şu an test edilen ve testleri tamamlanmış olan şifreleme modüllerini gösterir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3856 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 10.0 *İşletim sistemi:* iOS 13 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3855 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 10.0 *İşletim sistemi:* iOS 13 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 05.02.2021	*Sertifikalar:* 3811 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 10.0 *İşletim sistemi:* iOS 13 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 23.04.2019	*Sertifikalar:* 3438 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 9.0 *İşletim sistemi:* iOS 12 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 11.04.2019	*Sertifikalar:* 3433 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 9.0 *İşletim sistemi:* iOS 12 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3523 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 9.0 *İşletim sistemi:* iOS 12 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikalar:* 3148 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 8.0 *İşletim sistemi:* iOS 11 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikalar:* 3147 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 8.0 *İşletim sistemi:* iOS 11 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3223 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 1.0 *İşletim sistemi:* iOS 11 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2016 *Doğrulama tarihleri:* 01.02.2017	*Sertifikalar:* 2828 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple iOS Corecrypto Çekirdek Modülü 7.0 *İşletim sistemi:* iOS 10 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2016 *Doğrulama tarihleri:* 01.02.2017	*Sertifikalar:* 2827 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple iOS Corecrypto Çekirdek Modülü 7.0 *İşletim sistemi:* iOS 10 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Önceki sürümler

5 yıldan eski sertifikalar CMVP tarafından geçmiş durumu ile listelenir: Şu önceki iOS sürümleri şifreleme modülü doğrulamalarına sahiptir:

- iOS 9 (corecrypto modülleri 6.0)
- iOS 8 (corecrypto modülleri 5.0)
- iOS 7 (corecrypto modülleri 4.0)
- iOS 6 (corecrypto modülleri 3.0)

Ortak Kriterler (CC) sertifikası arka planı

Apple, her büyük iOS işletim sistemi sürümü değerlendirmesinde etkin bir şekilde görev almaktadır. Değerlendirme işlemi yalnızca işletim sisteminin en son genel kullanıma sunulan sürümünde gerçekleştirilebilir. iPadOS 13.1'den önce iPadOS, iOS olarak adlandırılırdı.

Ortak Kriterler (CC) sertifika durumu

NIAP tarafından yürütülen ABD programı bir Değerlendirilen Ürünler listesi tutar. Bu liste, şu anda ABD'de NIAP onaylı bir Ortak Kriterler Test Laboratuvarı'nda (CCTL) teste tabi tutulan ürünleri ve CCEVS yönetiminin ürünü resmi olarak değerlendirmeye kabul ettiği Değerlendirme Başlangıcı Toplantısı'ndan (veya eşdeğeri) geçenleri listeler.

Ürünler onaylandıktan sonra NIAP, şu an geçerli doğrulamaları Uyumlu Ürünler listesine ekler. 2 yıldan sonra bu sertifikalar, güncel güvence bakım politikasına uygunluğu açısından incelenir. Güvence bakım tarihi geçtikten sonra NIAP, sertifika listesini kendi Arşivlenmiş Ürünler listesine taşır.

Ortak Kriterler Portalı, Ortak Kriterleri Tanıma Anlaşması (CCRA) kapsamında karşılıklı olarak tanınabilecek sertifikaları listeler. CC Portalı, ürünleri sertifikalı ürün listesinde 5 yıl saklayabilir. CC Portalı, arşivlenen sertifikaların kayıtlarını tutar.

Aşağıdaki tablo, şu an bir laboratuvar tarafından değerlendirilmekte olan veya Ortak Kriterler'e uygun olduğu onaylanmış sertifikaları gösterir.

Şu anki durum

iOS 15 için NIAP değerlendirmelerinin laboratuvar testleri devam etmektedir. En son bilgiler için Değerlendirilen Ürünler (NIAP) ve Uyumlu Ürünler Listesi sayfasına bakın.

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: iOS 15 *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* —	*Başlık:* Apple iOS 15: iPhone'lar *Koruma Profilleri:* Mobil Aygıt Esasları (PP Modülleri doğrulanacak)
İşletim sistemi: iOS 14 *Sertifika tarihi:* 01.09.2021	*Program kimliği:* 11146 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple iOS 14: iPhone'lar *Koruma Profilleri:* Mobil Aygıt Esasları, VPN İstemcisi modülü, WLAN İstemcileri PP Modülü, MDM Aracısı EP

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: iOS 13 *Sertifika tarihi:* 06.11.2020	*Program kimliği:* 11036 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* iPhone'da Apple iOS 13 *Koruma Profilleri:* Mobil Aygıt Esasları, VPN İstemcisi modülü, WLAN İstemcileri EP, MDM Aracısı EP

iOS için arşivlenmiş Ortak Kriterler sertifikaları

Şu önceki iOS sürümleri Ortak Kriterler doğrulamalarına sahiptir. Bunlar, NIAP politikasına göre NIAP tarafından arşivlenir:

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: iOS 12 *Sertifika tarihi:* 14.03.2019	*Program kimliği:* 10937 *Belgeler:* Güvenlik Hedefi Yönergeler	*Başlık:* iOS 12 yüklü iPhone *Koruma Profilleri:* Mobil Aygıt Esasları, VPN İstemcisi modülü, Kablosuz LAN İstemcisi EP, MDM Aracısı EP
İşletim sistemi: iOS 11 *Sertifika tarihi:* 17.07.2018	*Program kimliği:* 10851 *Belgeler:* Güvenlik Hedefi Yönergeler	*Başlık:* Apple iOS 11 *Koruma Profilleri:* Mobil Aygıt Esasları, Kablosuz LAN İstemcisi EP, MDM Aracısı EP
İşletim sistemi: iOS 10 *Sertifika tarihi:* 27.07.2017	*Program kimliği:* 10782 *Belgeler:* Güvenlik Hedefi, Yönergeler	*Başlık:* iPhone ve iPad Aygıtlarında iOS 10.2 *Koruma Profilleri:* Mobil Aygıt Esasları, Kablosuz LAN İstemcisi EP, MDM Aracısı EP
İşletim sistemi: iOS 10 *Sertifika tarihi:* 27.07.2017	*Program kimliği:* 10792 *Belgeler:* Güvenlik Hedefi, Yönergeler	*Başlık:* iPhone ve iPad Üzerinde iOS 10.2 VPN İstemcisi *Koruma Profilleri:* VPN İstemcisi PP
İşletim sistemi: iOS 9 *Sertifika tarihi:* 14.10.2016	*Program kimliği:* 10725 *Belgeler:* Güvenlik Hedefi, Yönergeler	*Başlık:* MDM Aracısı ile iOS 9.3.2 *Koruma Profilleri:* Mobil Aygıt Esasları, MDM Aracısı EP
İşletim sistemi: iOS 9 *Sertifika tarihi:* 13.10.2016	*Program kimliği:* 10714 *Belgeler:* Güvenlik Hedefi, Yönergeler	*Başlık:* iPhone ve iPad üzerinde işletim sistemi VPN istemcisi *Koruma Profilleri:* VPN İstemcisi PP
İşletim sistemi: iOS 9 *Sertifika tarihi:* 28.01.2016	*Program kimliği:* 10695 *Belgeler:* Güvenlik Hedefi, Yönergeler	*Başlık:* iOS 9 *Koruma Profilleri:* Mobil Aygıt Esasları

iPadOS için güvenlik sertifikaları

iPadOS sertifikası arka planı

Apple, iş birliğine dayalı koruma profillerini ve FIPS 140-3 güvenlik düzeylerini kullanarak her büyük işletim sistemi sürümü için Apple işletim sistemlerinin doğrulanmasında etkin bir şekilde görev almaktadır. Uygunluk doğrulaması yalnızca en son çıkan sürümde gerçekleştirilebilir.

Not: 2019 yılında, iPad aygıtlarının işletim sisteminin yeni adı iPadOS oldu. iPadOS 13.1'den önce iPadOS, iOS olarak adlandırılırdı.

iPadOS şifreleme modülü doğrulama durumu

Şifreleme Modülü Doğrulama Programı (CMVP), şifreleme modüllerinin doğrulama durumunu, modüllerin mevcut durumlarına göre üç ayrı listede tutar:

- Laboratuvarın CMVP Test Edilen Uygulama listesinde listelenmesi için test yapma konusunda Apple ile sözleşme yapmış olması gerekir.
- Testler laboratuvar tarafından tamamlandıktan, laboratuvar CMVP tarafından doğrulanma önerdikten ve CMVP ücretleri ödendikten sonra modül, İşlenen Modüller (MIP) listesine eklenir. İşlenen Modüller (MIP) listesi, CMVP doğrulama çalışmaları ilerlemesini dört aşamada takip eder:
  - *İnceleme Bekleniyor:* CMVP kaynağının atanması bekleniyor.
  - *İncelemede:* CMVP kaynakları, doğrulama çalışmalarını gerçekleştiriyor.
  - *Koordinasyon:* Laboratuvar ve CMVP bulunan sorunların çözümü üzerinde çalışıyor.
  - *Sonlandırma:* Sertifika vermeye ilişkin çalışmalar ve formaliteler.
- Modüller, CMVP tarafından doğrulandıktan sonra bir uygunluk sertifikası alır ve doğrulanan şifreleme modülleri listesine eklenir. Bu liste şunları içerir:
  - Etkin olarak işaretlenmiş doğrulanmış modüller.
  - 5 yıl sonra modüller geçmiş olarak işaretlenir.
  - Modül sertifikası bir nedenden dolayı iptal edilirse modül iptal edilmiş olarak işaretlenir.

2020 yılında CMVP, FIPS 140-3 için temel olarak ISO/IEC 19790 uluslararası standardını benimsemiştir.

FIPS 140-3 sertifikaları

Şu anki durum

iPadOS 14 (2020) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

iPadOS 15 (2021) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu laboratuvar testlerine tabi tutulmaktadır. Bunlar, Test Edilen Uygulama listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iPadOS 15 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iPadOS 15 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iPadOS 15 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14, M1) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* iPadOS 15 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14, M1) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iPadOS 14 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iPadOS 14 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iPadOS 14 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14, M1) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* iPadOS 14 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A9-A14, M1) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3

FIPS 140-2 sertifikaları

Aşağıdaki tablo, laboratuvar tarafından FIPS 140-2 uygunluğu konusunda şu an test edilen ve testleri tamamlanmış olan şifreleme modüllerini gösterir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3856 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 10.0 *İşletim sistemi:* iPadOS 13 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3855 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 10.0 *İşletim sistemi:* iPadOS 13 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 05.02.2021	*Sertifikalar:* 3811 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Güvenli Anahtar Deposu Şifreleme Modülü 10.0 *İşletim sistemi:* iPadOS 13 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 23.04.2019	*Sertifikalar:* 3438 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 9.0 *İşletim sistemi:* iOS 12 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 11.04.2019	*Sertifikalar:* 3433 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 9.0 *İşletim sistemi:* iOS 12 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3523 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 9.0 *İşletim sistemi:* iOS 12 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikalar:* 3148 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 8.0 *İşletim sistemi:* iOS 11 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikalar:* 3147 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 8.0 *İşletim sistemi:* iOS 11 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3223 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 1.0 *İşletim sistemi:* iOS 11 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2016 *Doğrulama tarihleri:* 01.02.2017	*Sertifikalar:* 2828 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple iOS Corecrypto Çekirdek Modülü 7.0 *İşletim sistemi:* iOS 10 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2016 *Doğrulama tarihleri:* 01.02.2017	*Sertifikalar:* 2827 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple iOS Corecrypto Çekirdek Modülü 7.0 *İşletim sistemi:* iOS 10 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Önceki sürümler

5 yıldan eski sertifikalar CMVP tarafından geçmiş durumu ile listelenir: Şu önceki iOS sürümleri şifreleme modülü doğrulamalarına sahiptir:

- iOS 9 (corecrypto modülleri 6.0)
- iOS 8 (corecrypto modülleri 5.0)
- iOS 7 (corecrypto modülleri 4.0)
- iOS 6 (corecrypto modülleri 3.0)

Ortak Kriterler (CC) sertifikası arka planı

Apple, her büyük iPadOS işletim sistemi sürümü değerlendirmesinde etkin bir şekilde görev almaktadır. Değerlendirme işlemi yalnızca işletim sisteminin en son genel kullanıma sunulan sürümünde gerçekleştirilebilir.

Ortak Kriterler (CC) sertifika durumu

NIAP tarafından yürütülen ABD programı bir Değerlendirilen Ürünler listesi tutar. Bu liste, şu anda ABD'de NIAP onaylı bir Ortak Kriterler Test Laboratuvarı'nda (CCTL) teste tabi tutulan ürünleri ve CCEVS yönetiminin ürünü resmi olarak değerlendirmeye kabul ettiği Değerlendirme Başlangıcı Toplantısı'ndan (veya eşdeğeri) geçenleri listeler.

Ürünler onaylandıktan sonra NIAP, şu an geçerli doğrulamaları Uyumlu Ürünler listesine ekler. 2 yıldan sonra bu sertifikalar, güncel güvence bakım politikasına uygunluğu açısından incelenir. Güvence bakım tarihi geçtikten sonra NIAP, sertifika listesini kendi Arşivlenmiş Ürünler listesine taşır.

Ortak Kriterler Portalı, Ortak Kriterleri Tanıma Anlaşması (CCRA) kapsamında karşılıklı olarak tanınabilecek sertifikaları listeler. CC Portalı, ürünleri sertifikalı ürün listesinde 5 yıl saklayabilir. CC Portalı, arşivlenen sertifikaların kayıtlarını tutar.

Aşağıdaki tablo, şu an bir laboratuvar tarafından değerlendirilmekte olan veya Ortak Kriterler'e uygun olduğu onaylanmış sertifikaları gösterir.

Şu anki durum

iPadOS 15 için NIAP değerlendirmelerinin laboratuvar testleri devam etmektedir. En son bilgiler için Değerlendirilen Ürünler (NIAP) ve Uyumlu Ürünler Listesi sayfasına bakın.

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: iPadOS 15 *Sertifika tarihi:* 14.03.2019	*Program kimliği:* — *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* iOS 12 yüklü iPad *Koruma Profilleri:* Mobil Aygıt Esasları, VPN İstemcisi Modülü, Kablosuz LAN İstemcisi EP, MDM Aracısı EP
İşletim sistemi: iPadOS 14 *Sertifika tarihi:* 01.09.2021	*Program kimliği:* 11147 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple iPadOS 14: iPad'ler *Koruma Profilleri:* Mobil Aygıt Esasları, VPN İstemcisi Modülü, Kablosuz LAN İstemcisi EP, MDM Aracısı EP
İşletim sistemi: iPadOS 13 *Sertifika tarihi:* 06.11.2020	*Program kimliği:* 11036 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* iPad Mobil Aygıtlarında iPadOS 13 *Koruma Profilleri:* Mobil Aygıt Esasları, VPN İstemcisi Modülü, Kablosuz LAN İstemcisi EP, MDM Aracısı EP

Önceki sürümler

Şu önceki iOS sürümleri Ortak Kriterler doğrulamalarına sahiptir. Bunlar, NIAP politikasına göre NIAP tarafından arşivlenir:

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

macOS için güvenlik sertifikaları

macOS sertifikası arka planı

Apple, iş birliğine dayalı koruma profillerini ve FIPS 140-3 güvenlik düzeylerini kullanarak her büyük işletim sistemi sürümü için Apple işletim sistemlerinin doğrulanmasında etkin bir şekilde görev almaktadır. Uygunluk doğrulaması yalnızca en son çıkan sürümde gerçekleştirilebilir.

macOS şifreleme modülü doğrulama durumu

Şifreleme Modülü Doğrulama Programı (CMVP), şifreleme modüllerinin doğrulama durumunu, modüllerin mevcut durumlarına göre üç ayrı listede tutar:

- Laboratuvarın CMVP Test Edilen Uygulama listesinde listelenmesi için test yapma konusunda Apple ile sözleşme yapmış olması gerekir.
- Testler laboratuvar tarafından tamamlandıktan, laboratuvar CMVP tarafından doğrulanma önerdikten ve CMVP ücretleri ödendikten sonra modül, İşlenen Modüller (MIP) listesine eklenir. İşlenen Modüller (MIP) Listesi, CMVP doğrulama çalışmaları ilerlemesini dört aşamada takip eder:
  - *İnceleme Bekleniyor:* CMVP kaynağının atanması bekleniyor.
  - *İncelemede:* CMVP kaynakları, doğrulama çalışmalarını gerçekleştiriyor.
  - *Koordinasyon:* Laboratuvar ve CMVP bulunan sorunların çözümü üzerinde çalışıyor.
  - *Sonlandırma:* Sertifika vermeye ilişkin çalışmalar ve formaliteler.
- Modüller, CMVP tarafından doğrulandıktan sonra bir uygunluk sertifikası alır ve doğrulanan şifreleme modülleri listesine eklenir. Bu liste şunları içerir:
  - Etkin olarak işaretlenmiş doğrulanmış modüller.
  - 5 yıl sonra modüller geçmiş olarak işaretlenir.
  - Modül sertifikası bir nedenden dolayı iptal edilirse modül iptal edilmiş olarak işaretlenir.

2020 yılında CMVP, FIPS 140-3 için temel olarak ISO/IEC 19790 uluslararası standardını benimsemiştir.

Apple Mac bilgisayarları için aşağıdaki tablo hangi şifreleme modülünün hangi Mac teknolojisi için geçerli olduğunu gösterir.

Şifreleme modülü	Apple Silicon yongasına sahip Mac bilgisayarları	Apple T2 güvenlik yongasına sahip Mac bilgisayarları	Apple T2 güvenlik yongasına sahip olmayan Intel tabanlı Mac bilgisayarları
Apple Silicon Kullanıcı Alanı	✓		
Apple Silicon Çekirdeği	✓		
Intel Kullanıcı Alanı		✓	✓
Intel Çekirdeği		✓	✓
Güvenli Anahtar Deposu	✓	✓	

FIPS 140-3 sertifikaları

2020 yılında Apple, Apple Silicon'u taban alan Mac bilgisayarlarını kullanıma sunmuştur. Şifreleme modüllerinin Apple Silicon veya Intel tabanlı Mac bilgisayarlarına uygulanabilirliği aşağıdaki tablonun Modül Bilgisi sütununda belirtilir.

Not: Apple T2 güvenlik yongaları birçok Intel tabanlı Mac bilgisayarında bulunur. T2 yongası sertifikaları hakkında bilgi için Apple T2 güvenlik yongası için güvenlik sertifikaları bölümüne bakın.

macOS ssh istemcisi

OpenSSH, belirli FIPS 140-3 algoritmaları için doğrulanan FIPS 140-3 modüllerini kullanacak şekilde ayarlanabilir. Kurumlar, Apple'dan edinebilecekleri imzalı ve onaylı bir yükleyiciyi *FIPS140Mode* parolası ile çalıştırabilir. Yükleyici Mac'e iki dosya yerleştirir:

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

macOS bundan sonra OpenSSH tarafından kullanılan şifreleri yalnızca NIST tarafından onaylananlarla sınırlar ve OpenSSH istemcisinin platform tarafından sağlanan onaylanmış şifreleme modülünü kullanmasını sağlar. Yöneticiler de kendi dosyalarını yaratabilir. Daha fazla bilgi için macOS 12.0.1 veya daha yenisinde `apple_ssh_and_fips` man sayfasına bakın.

Şu anki durum

macOS 11 Big Sur kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

macOS 12 Monterey kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu laboratuvar testlerine tabi tutulmaktadır. Bunlar, Test Edilen Uygulama listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* Apple Silicon'da macOS 12 Monterey *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* Apple Silicon'da macOS 12 Monterey *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* Intel'de macOS 12 Monterey *Ortam:* Intel, Kullanıcı, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* Intel'de macOS 12 Monterey *Ortam:* Intel, Çekirdek, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* Apple Silicon'da macOS 12 Monterey ile dağıtılan sep OS, T2 yongalı Intel'de macOS 12 Monterey ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (M1 ve T2) *Güvenlik düzeyi:* 2

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12.0 *İşletim sistemi:* Apple Silicon'da macOS 12 Monterey ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (M1) *Güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* Intel'de macOS 11 Big Sur *Ortam:* Intel, Kullanıcı, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* Intel'de macOS 11 Big Sur *Ortam:* Intel, Çekirdek, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* Apple Silicon'da macOS 11 Big Sur *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* Apple Silicon'da macOS 11 Big Sur *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* Apple Silicon'da macOS 11 Big Sur ile dağıtılan sepOS, Intel'de macOS 11 Big Sur ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (M1) *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* Apple Silicon'da macOS 11 Big Sur ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (M1) *Güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3

FIPS 140-2 sertifikaları

Aşağıdaki tablo, laboratuvar tarafından FIPS 140-2 uygunluğu konusunda şu an test edilen ve testleri tamamlanmış olan şifreleme modüllerini gösterir.

macOS 10.15 Catalina kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

Not: Apple T2 güvenlik yongaları birçok Intel tabanlı Mac bilgisayarında bulunur. T2 yongası sertifikaları hakkında bilgi için Apple T2 güvenlik yongası için güvenlik sertifikaları bölümüne bakın.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 24.03.2021	*Sertifikalar:* 3859 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Intel İçin Apple Corecrypto Kullanıcı Alanı Modülü (ccv10) *İşletim sistemi:* macOS 10.15 Catalina *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 24.03.2021	*Sertifikalar:* 3858 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Intel İçin Apple Corecrypto Çekirdek Modülü 10.0 (ccv10) *İşletim sistemi:* macOS 10.15 Catalina *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 12.04.2019	*Sertifikalar:* 3402 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Intel İçin Apple Corecrypto Kullanıcı Modülü 9.0 *İşletim sistemi:* macOS 10.14 Mojave *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 12.04.2019	*Sertifikalar:* 3431 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Intel İçin Apple Corecrypto Çekirdek Modülü 9.0 *İşletim sistemi:* macOS 10.14 Mojave *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 22.03.2018	*Sertifikalar:* 3155 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Intel İçin Apple Corecrypto Kullanıcı Modülü 8.0 *İşletim sistemi:* macOS 10.13 High Sierra *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 22.03.2018	*Sertifikalar:* 3156 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Intel İçin Apple Corecrypto Çekirdek Modülü 8.0 *İşletim sistemi:* macOS 10.13 High Sierra *Tür:* Yazılım *Güvenlik düzeyi:* 1

Önceki sürümler

Şu önceki OS X ve macOS sürümleri, şifreleme modülü doğrulamalarına sahiptir. 5 yıldan eski olanlar CMVP tarafından geçmiş durumu ile listelenir:

- 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

Ortak Kriterler (CC) sertifikası arka planı

Apple, her büyük macOS işletim sistemi sürümü değerlendirmesinde etkin bir şekilde görev almaktadır. Değerlendirme işlemi yalnızca işletim sisteminin en son genel kullanıma sunulan sürümünde gerçekleştirilebilir.

Ortak Kriterler (CC) sertifika durumu

NIAP tarafından yürütülen ABD programı bir Değerlendirilen Ürünler listesi tutar. Bu liste, şu anda ABD'de NIAP onaylı bir Ortak Kriterler Test Laboratuvarı'nda (CCTL) teste tabi tutulan ürünleri ve CCEVS yönetiminin ürünü resmi olarak değerlendirmeye kabul ettiği Değerlendirme Başlangıcı Toplantısı'ndan (veya eşdeğeri) geçenleri listeler.

Ürünler onaylandıktan sonra NIAP, şu an geçerli doğrulamaları Uyumlu Ürünler listesine ekler. 2 yıldan sonra bu sertifikalar, güncel güvence bakım politikasına uygunluğu açısından incelenir. Güvence bakım tarihi geçtikten sonra NIAP, sertifika listesini kendi Arşivlenmiş Ürünler Listesi'ne taşır.

Ortak Kriterler Portalı, Ortak Kriterleri Tanıma Anlaşması (CCRA) kapsamında karşılıklı olarak tanınabilecek sertifikaları listeler. CC Portalı, ürünleri sertifikalı ürün listesinde 5 yıl saklayabilir. CC Portalı, arşivlenen sertifikaların kayıtlarını tutar.

Aşağıdaki tablo, şu an bir laboratuvar tarafından değerlendirilmekte olan veya Ortak Kriterler'e uygun olduğu onaylanmış sertifikaları gösterir.

Şu anki durum

macOS 11 ve macOS 12 için Genel Amaçlı İşletim Sistemi ve Tam Disk Şifreleme (FDE) (AA ve EE) koruma profilleri kullanılarak NIAP ile değerlendirmeler devam etmektedir.

En son bilgiler için Değerlendirilen Ürünler (NIAP) ve Uyumlu Ürünler Listesi sayfasına bakın.

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: macOS 12 Monterey *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* —	*Başlık:* macOS 12 Monterey ile Apple FileVault 2 *Koruma Profilleri:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP'ler doğrulanacak)
İşletim sistemi: macOS 12 Monterey *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* —	*Başlık:* macOS 12 Monterey *Koruma Profilleri:* PP_OS_V4.21 (PP'ler doğrulanacak)
İşletim sistemi: macOS 11 Big Sur *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* macOS 11 Big Sur ile Apple FileVault 2 *Koruma Profilleri:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: macOS 11 Big Sur *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple macOS 11 Big Sur *Koruma Profilleri:* PP_OS_V4.21
İşletim sistemi: macOS 10.15 Catalina *Sertifika tarihi:* 29.04.2021	*Program kimliği:* 11078 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* macOS 10.15 Catalina çalıştıran T2 bilgisayarında Apple FileVault 2 *Koruma Profilleri:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
İşletim sistemi: macOS 10.15 Catalina *Sertifika tarihi:* 23.09.2020	*Program kimliği:* 11077 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* macOS 10.15 Catalina *Koruma Profilleri:* PP_OS_V4.21

tvOS için güvenlik sertifikaları

tvOS sertifikası arka planı

Apple, her büyük tvOS sürümüyle ilişkili şifreleme modüllerinin doğrulanmasında etkin bir şekilde görev almaktadır. Uygunluk doğrulaması yalnızca en son çıkan sürümde gerçekleştirilebilir.

tvOS şifreleme modülü doğrulama durumu

Şifreleme Modülü Doğrulama Programı (CMVP), şifreleme modüllerinin doğrulama durumunu, modüllerin mevcut durumlarına göre üç ayrı listede tutar:

- Laboratuvarın CMVP Test Edilen Uygulama listesinde listelenmesi için test yapma konusunda Apple ile sözleşme yapmış olması gerekir.
- Testler laboratuvar tarafından tamamlandıktan, laboratuvar CMVP tarafından doğrulanma önerdikten ve CMVP ücretleri ödendikten sonra modül, İşlenen Modüller (MIP) listesine eklenir. İşlenen Modüller (MIP) Listesi, CMVP doğrulama çalışmaları ilerlemesini dört aşamada takip eder:
  - *İnceleme Bekleniyor:* CMVP kaynağının atanması bekleniyor.
  - *İncelemede:* CMVP kaynakları, doğrulama çalışmalarını gerçekleştiriyor.
  - *Koordinasyon:* Laboratuvar ve CMVP bulunan sorunların çözümü üzerinde çalışıyor.
  - *Sonlandırma:* Sertifika vermeye ilişkin çalışmalar ve formaliteler.
- Modüller, CMVP tarafından doğrulandıktan sonra bir uygunluk sertifikası alır ve doğrulanan şifreleme modülleri listesine eklenir. Bu liste şunları içerir:
  - Etkin olarak işaretlenmiş doğrulanmış modüller.
  - 5 yıl sonra modüller geçmiş olarak işaretlenir.
  - Modül sertifikası bir nedenden dolayı iptal edilirse modül iptal edilmiş olarak işaretlenir.

2020 yılında CMVP, FIPS 140-3 için temel olarak ISO/IEC 19790 uluslararası standardını benimsemiştir.

FIPS 140-3 sertifikaları

Şu anki durum

tvOS 14 (2020) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

tvOS 15 (2021) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu laboratuvar testlerine tabi tutulmaktadır. Bunlar, Test Edilen Uygulama listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* tvOS 15 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* tvOS 15 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* tvOS 15 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A10, A12) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* tvOS 14 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* tvOS 14 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* tvOS 14 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (A10, A12) *Genel güvenlik düzeyi:* 2

FIPS 140-2 sertifikaları

Aşağıdaki tablo, laboratuvar tarafından FIPS 140-2 uygunluğu konusunda şu an test edilen ve testleri tamamlanmış olan şifreleme modüllerini gösterir.

tvOS 13 (2019) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3856 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 10.0 *İşletim sistemi:* tvOS 13 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 23.03.2021	*Sertifikalar:* 3855 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 10.0 *İşletim sistemi:* tvOS 13 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 05.02.2021	*Sertifikalar:* 3811 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 10.0 *İşletim sistemi:* tvOS 13 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 23.04.2019	*Sertifikalar:* 3438 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 9.0 *İşletim sistemi:* tvOS 12 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 11.04.2019	*Sertifikalar:* 3433 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 9.0 *İşletim sistemi:* tvOS 12 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3523 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 9.0 *İşletim sistemi:* tvOS 12 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikalar:* 3148 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 8.0 *İşletim sistemi:* tvOS 11 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikalar:* 3147 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 8.0 *İşletim sistemi:* tvOS 11 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3223 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 1.0 *İşletim sistemi:* tvOS 11 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2

watchOS için güvenlik sertifikaları

watchOS sertifikası arka planı

Apple, her büyük watchOS sürümüyle ilişkili şifreleme modüllerinin doğrulanmasında etkin bir şekilde görev almaktadır. Uygunluk doğrulaması yalnızca en son çıkan sürümde gerçekleştirilebilir.

watchOS şifreleme modülü doğrulama durumu

Şifreleme Modülü Doğrulama Programı (CMVP), şifreleme modüllerinin doğrulama durumunu, modüllerin mevcut durumlarına göre üç ayrı listede tutar:

- Laboratuvarın CMVP Test Edilen Uygulama listesinde listelenmesi için test yapma konusunda Apple ile sözleşme yapmış olması gerekir.
- Testler laboratuvar tarafından tamamlandıktan, laboratuvar CMVP tarafından doğrulanma önerdikten ve CMVP ücretleri ödendikten sonra modül, İşlenen Modüller (MIP) listesine eklenir. İşlenen Modüller (MIP) Listesi, CMVP doğrulama çalışmaları ilerlemesini dört aşamada takip eder:
  - *İnceleme Bekleniyor:* CMVP kaynağının atanması bekleniyor.
  - *İncelemede:* CMVP kaynakları, doğrulama çalışmalarını gerçekleştiriyor.
  - *Koordinasyon:* Laboratuvar ve CMVP bulunan sorunların çözümü üzerinde çalışıyor.
  - *Sonlandırma:* Sertifika vermeye ilişkin çalışmalar ve formaliteler.
- Modüller, CMVP tarafından doğrulandıktan sonra bir uygunluk sertifikası alır ve doğrulanan şifreleme modülleri listesine eklenir. Bu liste şunları içerir:
  - Etkin olarak işaretlenmiş doğrulanmış modüller.
  - 5 yıl sonra modüller geçmiş olarak işaretlenir.
  - Modül sertifikası bir nedenden dolayı iptal edilirse modül iptal edilmiş olarak işaretlenir.

2020 yılında CMVP, FIPS 140-3 için temel olarak ISO/IEC 19790 uluslararası standardını benimsemiştir.

FIPS 140-3 sertifikaları

Şu anki durum

watchOS 7 (2020) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu için laboratuvar testleri tamamlanmış ve doğrulanmaları için laboratuvar tarafından CMVP'ye önerilmiştir. Bunlar, İşlenen Modüller listesinde listelenmektedir.

watchOS 8 (2021) kullanıcı alanı, çekirdek alanı ve güvenli anahtar deposu laboratuvar testlerine tabi tutulmaktadır. Bunlar, Test Edilen Uygulama listesinde listelenmektedir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* watchOS 8 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* watchOS 8 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* watchOS 8 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (S3, S4, S5, S6) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2021 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 12 *İşletim sistemi:* watchOS 8 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (S6) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* watchOS 7 *Ortam:* Apple Silicon, Kullanıcı, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* watchOS 7 *Ortam:* Apple Silicon, Çekirdek, Yazılım *Tür:* Yazılım *Genel güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* watchOS 7 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (S3, S4, S5, S6) *Genel güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2020 *Doğrulama tarihleri:* —	*Sertifikalar:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Corecrypto Modülü 11.1 *İşletim sistemi:* watchOS 7 ile dağıtılan sepOS *Ortam:* Apple Silicon, Güvenli Anahtar Deposu, Donanım *Tür:* Donanım (S6) *Genel güvenlik düzeyi:* 2 *Fiziksel güvenlik düzeyi:* 3

FIPS 140-2 sertifikaları

Aşağıdaki tablo, laboratuvar tarafından FIPS 140-2 uygunluğu konusunda şu an test edilen ve testleri tamamlanmış olan şifreleme modüllerini gösterir.

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* —	*Sertifikalar:* 3856 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 10.0 *İşletim sistemi:* watchOS 6 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* —	*Sertifikalar:* 3855 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 10.0 *İşletim sistemi:* watchOS 6 *Tür:* Yazılım *Güvenlik düzeyi:* 1

Tarihler	Sertifikalar / Belgeler	Modül bilgisi
İşletim sistemi çıkış tarihi: 2019 *Doğrulama tarihleri:* 05.02.2021	*Sertifikalar:* 3811 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 10.0 *İşletim sistemi:* watchOS 6 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 23.04.2019	*Sertifikalar:* 3438 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 9.0 *İşletim sistemi:* watchOS 5 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 11.04.2019	*Sertifikalar:* 3433 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 9.0 *İşletim sistemi:* watchOS 5 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2018 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3523 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 9.0 *İşletim sistemi:* watchOS 5 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 22.05.2018, 06.07.2018	*Sertifikalar:* 3148 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Kullanıcı Modülü 8.0 *İşletim sistemi:* watchOS 4 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 09.03.2018, 17.05.2018, 03.07.2018	*Sertifikalar:* 3147 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* ARM İçin Apple Corecrypto Çekirdek Modülü 8.0 *İşletim sistemi:* watchOS 4 *Tür:* Yazılım *Güvenlik düzeyi:* 1
İşletim sistemi çıkış tarihi: 2017 *Doğrulama tarihleri:* 10.09.2019	*Sertifikalar:* 3223 *Belgeler:* Sertifika Güvenlik Politikası Şifreleme Görevlisi Kılavuzu	*Başlık:* Apple Güvenli Anahtar Deposu Şifreleme Modülü 1.0 *İşletim sistemi:* watchOS 4 ile dağıtılan sepOS *Tür:* Donanım *Güvenlik düzeyi:* 2

Yazılım güvenliği sertifikaları

Apple yazılım güvenliği sertifikalarına genel bakış

Apple, diğer sertifikaların yanı sıra sepOS ve T2 firmware için ABD Federal Bilgi İşleme Standardı (FIPS) 140-2/-3 uygunluk doğrulama sertifikalarına da sahiptir. Apple, uygun olduğunda kapsamlı bir biçimde birden fazla platforma uygulanan *sertifika yapı taşları* ile başlar. Bu yapı taşlarından biri, Apple tarafından geliştirilen işletim sistemlerindeki yazılım ve donanım şifreleme modülü dağıtımları için kullanılan corecrypto doğrulamasıdır. İkinci bir yapı taşı, birçok Apple aygıtında yerleşik olan Secure Enclave'dir. Üçüncüsü ise Apple'ın Touch ID'li aygıtlarında ve Face ID'li aygıtlarında bulunan Secure Element (SE) sertifikasıdır. Bu donanım sertifikası yapı taşları, daha geniş platform güvenliği sertifikaları için bir temel oluşturur.

Ürün sertifikaları: Ortak Kriterler (ISO/IEC 15408)

Ortak Kriterler (ISO/IEC 15408), birçok kuruluş tarafından BT ürünlerinin güvenlik değerlendirmelerini gerçekleştirmede temel olarak kullanılan bir standarttır.

Uluslararası Ortak Kriterler Tanıma Anlaşması (CCRA) çerçevesinde karşılıklı olarak tanınan sertifikalar için Ortak Kriterler Portalı'na bakın. Ortak Kriterler standardı, CCRA dışında ulusal ve özel doğrulama programları tarafından da kullanılabilir. Avrupa'da karşılıklı tanıma, hem SOG-IS hem de CCRA anlaşmasına tabidir.

Bu girişimin amacı, Ortak Kriterler topluluğu tarafından belirtildiği şekilde, Bilgi Teknolojisi ürünlerinin anlaşılır ve güvenilir bir değerlendirmesini sunmak için uluslararası düzeyde onaylı güvenlik standartlarının oluşturulmasıdır. Ortak Kriterler Sertifikası ürünün, güvenlik standartlarını karşılayıp karşılamadığına ilişkin bağımsız bir değerlendirme sağlayarak müşterilerin Bilgi Teknolojisi ürünlerinin güvenliğinden emin olmasına ve daha bilinçli kararlar vermesine olanak tanır.

CCRA ile, üye ülkeler Bilgi Teknolojisi ürünlerine yönelik bu sertifikayı aynı güven düzeyinde tanımayı kabul etmiştir. Sertifikadan önce gereken kapsamlı değerlendirmeler şunları içerir:

- Koruma profilleri (PP)
- Güvenlik hedefleri (ST)
- Güvenlik işlev gereksinimleri (SFR)
- Güvenlik güvence gereksinimleri (SAR)
- Değerlendirme güvence düzeyleri (EAL)

Koruma profilleri (PP), bir aygıt türü sınıfı (Taşınabilirlik gibi) için güvenlik gereksinimlerini belirten ve aynı sınıftaki BT ürün değerlendirmelerini karşılaştırmak için kullanılan belgelerdir. CCRA üye sayısı ve giderek uzayan onaylı PP'lerin listesi yıllık bazda büyümeye devam etmektedir. Bu anlaşma, ürün geliştiricilerinin, herhangi bir sertifika yetkilendirme programı kapsamında tek bir sertifika almak için çalışmasına ve tüm sertifika kullanım imzacıları tarafından tanınmasını sağlamasına izin verir.

Güvenlik hedefleri (ST), bir BT ürününün onaylanması sürecinde *nelerin* değerlendirileceğini tanımlar. ST'ler, kendileriyle ilgili daha ayrıntılı değerlendirmelerde kullanılan *güvenlik işlev gereksinimlerine (SFR)* çevrilir.

Ortak Kriterler (CC), *güvenlik güvence gereksinimlerini* de içerir. En yaygın tanımlanan ölçümlerden biri *değerlendirme güvence düzeyidir (EAL)*. EAL'ler, en sık görülen SAR kümelerini gruplar ve karşılaştırılabilmelerini sağlamak için koruma profillerinde (PP) veya güvenlik hedeflerinde (ST) belirtilebilir.

Birçok eski koruma profili arşivlenmiş ve belirli çözümlere ve ortamlara odaklanması amacıyla geliştirilen hedefe yönelik koruma profilleri (PP) bunların yerini almıştır. Tüm CCRA üyelerinin devam eden karşılıklı tanıma konusunda ortak hareket edebilmesini sağlamak amacıyla sürecin başından beri CCRA imzacı programının katılımıyla geliştirilen iş birliğine dayalı koruma profilleri (cPP) geliştirmek ve sürekliliğini sağlamak için uluslararası teknik topluluklar (iTC) kurulmuştur. Hedefi CCRA dışındaki kullanıcı grupları ve karşılıklı tanıma anlaşmaları olan koruma profilleri (PP), uygun paydaşlar tarafından geliştirilmeye devam eder.

Apple, 2015 yılının başından itibaren belirli iş birliğine dayalı koruma profillerinde (cPP'ler) güncellenmiş CCRA kapsamındaki sertifikaları almak için gereken çalışmalara başlamıştır. O zamandan beri Apple, her büyük iOS sürümü için Ortak Kriterler sertifikalarını almış ve kapsamını yeni koruma profilleri (PP) tarafından sağlanan güvenlik güvencesini de içerecek şekilde genişletmiştir.

Apple, mobil güvenlik teknolojilerinin değerlendirilmesine odaklanan teknik topluluklarda aktif rol alır. Bunlara cPP'lerin geliştirilmesinden ve güncellenmesinden sorumlu iTC'ler de dahildir. Apple, güncel PP ve cPP sürümlerine uygun sertifikaları değerlendirmeyi ve uygulamayı sürdürmektedir.

Kuzey Amerika pazarı için Apple platform sertifikaları, genellikle şu an değerlendirme aşamasında olup henüz onaylanmamış projelerin listesini tutan Ulusal Bilgi Güvencesi Ortaklığı (NIAP) ile gerçekleştirilir.

Listelenen genel platform sertifikalarının yanı sıra bazı pazarlar için belirli güvenlik gereksinimlerini göstermek üzere başka sertifikalar da verilmiştir.

Apple uygulamaları için güvenlik sertifikaları

Apple uygulamalarının sertifika arka planı

Apple, uygun Ortak Kriterler Koruma Profillerini (PP) kullanarak Apple uygulamalarının güvenlik sertifikası çalışmalarında etkin bir şekilde görev almaktadır. Bu değerlendirmeler, Apple'ın edinmiş olduğu donanım ve işletim sistemi sertifikaları üzerine kurulmuştur.

2018 yılında Apple, iOS 11'de çalışan en önemli uygulamalar için uygulama güvenliği değerlendirmelerini Safari tarayıcısı ve Kişiler uygulaması ile başlatmıştır. Apple, bu değerlendirmeleri iOS 12'de, iOS 13'te ve iPadOS 13.1'de çalışan uygulamalarla sürdürmüştür. 2021'de macOS 11'de çalışan uygulamalar da kapsama eklenmektedir.

Şifreleme modülü sertifika durumu

Burada listelenen Apple uygulamaları, uygun işletim sistemine yönelik şifreleme modüllerini kullanır. Daha fazla bilgi için iOS için güvenlik sertifikaları, iPadOS için güvenlik sertifikaları ve macOS için güvenlik sertifikaları bölümlerine bakın.

Ortak Kriterler (CC) sertifika durumu

NIAP tarafından yürütülen ABD programı bir Değerlendirilen Ürünler listesi tutar. Bu liste, şu anda ABD'de NIAP onaylı bir Ortak Kriterler Test Laboratuvarı'nda (CCTL) teste tabi tutulan ürünleri ve CCEVS yönetiminin ürünü resmi olarak değerlendirmeye kabul ettiği Değerlendirme Başlangıcı Toplantısı'ndan (veya eşdeğeri) geçenleri listeler.

Ürünler onaylandıktan sonra NIAP, şu an geçerli doğrulamaları Uyumlu Ürünler listesine ekler. 2 yıldan sonra bu sertifikalar, güncel güvence bakım politikasına uygunluğu açısından incelenir. Güvence bakım tarihi geçtikten sonra NIAP, sertifika listesini kendi Arşivlenmiş Ürünler listesine taşır.

Ortak Kriterler Portalı, Ortak Kriterleri Tanıma Anlaşması (CCRA) kapsamında karşılıklı olarak tanınabilecek sertifikaları listeler. CC Portalı, ürünleri sertifikalı ürün listesinde 5 yıl saklayabilir. CC Portalı, arşivlenen sertifikaların kayıtlarını tutar.

Aşağıdaki tablo, şu an bir laboratuvar tarafından değerlendirilmekte olan veya Ortak Kriterler'e uygun olduğu onaylanmış sertifikaları gösterir.

Şu anki durum

- Çalışmaların devam ettiği bilgisiyle yayımlanan NIAP değerlendirmeleri Değerlendirilen Ürünler (NIAP) sayfasında listelenir.
- Tamamlanan ve doğrulanan değerlendirmeler NIAP Uyumlu Ürünler Listesi'nde listelenir.

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: macOS 11 Big Sur *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* macOS 11 Big Sur: Kişiler *Koruma Profilleri:* Uygulama Yazılımları İçin PP, Web Tarayıcılar İçin EP
İşletim sistemi: macOS 11 Big Sur *Sertifika tarihi:* —	*Program kimliği:* Henüz sertifikası yok *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* macOS 11 Big Sur: Safari *Koruma Profilleri:* Uygulama Yazılımları İçin PP, Web Tarayıcılar İçin EP
İşletim sistemi: iOS 14, iPadOS 14 *Sertifika tarihi:* 20.08.2021	*Program kimliği:* 11191 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple iOS 14 ve iPadOS 14: Kişiler *Koruma Profilleri:* Uygulama Yazılımları İçin PP, Web Tarayıcılar İçin EP
İşletim sistemi: iOS 14, iPadOS 14 *Sertifika tarihi:* —	*Program kimliği:* 11192 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple iOS 14 ve iPadOS 14: Safari *Koruma Profilleri:* Uygulama Yazılımları İçin PP, Web Tarayıcılar İçin EP
İşletim sistemi: iOS 13, iPadOS 13 *Sertifika tarihi:* 05.06.2020	*Program kimliği:* 11060 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple iOS 13 ve iPadOS 13: Safari *Koruma Profilleri:* Uygulama Yazılımları İçin PP, Web Tarayıcılar İçin EP

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: iOS 13, iPadOS 13 *Sertifika tarihi:* 05.06.2020	*Program kimliği:* 11050 *Belgeler:* Sertifika Güvenlik Hedefi Yönergeler Doğrulama Raporu Güvence Aktivite Raporu	*Başlık:* Apple iOS 13 ve iPadOS 13: Kişiler *Koruma Profilleri:* Uygulama Yazılımları İçin PP

Apple uygulamaları için arşivlenmiş Ortak Kriterler sertifikaları

İşletim sistemi / Sertifika tarihi	Program kimliği / Belgeler	Başlık / Koruma Profilleri
İşletim sistemi: iOS 12 *Sertifika tarihi:* 12.06.2019	*Program kimliği:* 10960 *Belgeler:* Güvenlik Hedefi Yönergeler	*Başlık:* iOS 12 Safari *Koruma Profilleri:* Uygulama Yazılımları İçin PP, Web Tarayıcılar İçin EP
İşletim sistemi: iOS 12 *Sertifika tarihi:* 28.02.2019	*Program kimliği:* 10961 *Belgeler:* Güvenlik Hedefi Yönergeler	*Başlık:* iOS 12 Kişiler *Koruma Profilleri:* Uygulama Yazılımları İçin PP
İşletim sistemi: iOS 11 *Sertifika tarihi:* 09.11.2018	*Program kimliği:* 10916 *Belgeler:* Güvenlik Hedefi Yönergeler	*Başlık:* iOS 11 Safari *Koruma Profilleri:* Uygulama Yazılımları İçin PP, Web Tarayıcılar İçin EP
İşletim sistemi: iOS 11 *Sertifika tarihi:* 13.09.2018	*Program kimliği:* 10915 *Belgeler:* Güvenlik Hedefi Yönergeler	*Başlık:* iOS 11 Kişiler *Koruma Profilleri:* Uygulama Yazılımları İçin PP

Apple internet servisleri için güvenlik sertifikaları

Apple, müşterilerinin mevzuat ve sözleşme kaynaklı yükümlülüklerini yerine getirebilmelerini sağlamak üzere ISO/IEC 27001 ve ISO/IEC 27018 standartlarına uygunluk sertifikalarına sahiptir. Bu sertifikalar müşterilerimize, kapsama dahil sistemler için Apple'ın Bilgi Güvenliği ve Gizliliği uygulamaları ile ilgili bağımsız bir onay sağlar.

ISO/IEC 27001 ve ISO/IEC 27018, Uluslararası Standardizasyon Teşkilatı (ISO) tarafından yayımlanan Bilgi Güvenliği Yönetimi Sistemi (ISMS) standartları ailesinin bir parçasıdır. Apple'ın ISMS'sinin bir parçası olarak, tüm Ek A denetim gereksinimleri, ISO/IEC 27001 ve ISO/IEC 27018 standartlarında tanımlandığı gibi Uygulanabilirlik Beyanı'na dahil edilmiştir. Apple, her yıl yetkili bir kayıt sitesinden bağımsız bir onay alır.

ISO/IEC 27001

ISO/IEC 27001, bir kuruluşun Bilgi Güvenliği Yönetimi Sistemi'ni kurma, uygulama, sürdürme ve sürekli olarak geliştirme gereksinimlerini belirten bir Bilgi Güvenliği Yönetimi Sistemi standardıdır. ISO/IEC 27001 standardı, Apple'ın ISO/IEC sertifikaları kapsamındaki şu güvenlik alanlarını içerir:

- Bilgi güvenliği politikaları
- Bilgi güvenliği organizasyonu
- Varlık yönetimi
- İnsan kaynakları güvenliği
- Fiziksel ve çevresel güvenlik
- İletişim ve işlem yönetimi
- Erişim denetimi
- Bilgi sistemlerinin alımı, geliştirilmesi ve bakımı
- Bilgi güvenliği olay yönetimi
- İş sürekliliği yönetimi
- Uygunluk

ISO/IEC 27018

ISO/IEC 27018, herkese açık bulut ortamlarında kişisel verilerin (PII) korunmasına yönelik bir uygulama kodudur. ISO/IEC 27018 standardı, Apple'ın ISO/IEC sertifikaları kapsamındaki şu güvenlik alanlarını içerir:

- Onay verme ve seçme
- Amacın yasalara uygunluğu ve belirtimler
- Bilgi toplama sınırlaması
- Verileri en aza indirme
- Kullanma, saklama ve açıklama sınırlaması
- Doğruluk ve kalite
- Açıklık, şeffaflık ve bildirme
- Bireysel katılım ve erişim
- Sorumluluk
- Bilgi güvenliği
- Gizlilik uyumluluğu

ISO/IEC 27001 ve ISO/IEC 27018 kapsamındaki Apple servisleri

Apple'ın ISO/IEC 27001 ve ISO/IEC 27018 sertifikaları şu servisleri kapsar:

- Apple İş Yeriyle Sohbet
- Apple İşletme Yönetimi
- Apple Anında İletme Bildirim servisi (APNs)
- Apple Okul Yönetimi
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork servisleri
- Yönetilen Apple Kimlikleri
- Okul
- Siri

Sertifikalar

Apple'ın ISO/IEC 27001 ve 27018 sertifikalarının kanıtları kayıt sitemizde bulunabilir.

Apple'ın sertifikalarını görüntülemek için İngiliz Standartları Enstitüsü (BSI) web sitesindeki Certificate and Client Directory (Sertifika ve Müşteri Dizini) arama bölümüne gidin, Company (Şirket) arama alanına Apple girin, Search (Ara) düğmesini tıklayın, sonra sertifikaları görüntülemek için arama sonuçlarını seçin.

Not: Apple tarafından üretilmeyen ürünler veya Apple tarafından denetlenmeyen veya test edilmeyen bağımsız web siteleri hakkındaki bilgiler bir öneri veya onay niteliği taşımadan sunulmuştur. Apple, üçüncü taraf web sitelerinin veya ürünlerinin seçimi, performansı veya kullanımıyla ilgili hiçbir sorumluluk kabul etmez. Apple, üçüncü taraf web sitelerinin doğruluğu veya güvenilirliğiyle ilgili herhangi bir beyanda bulunmamaktadır. Ek bilgi için satıcıyla iletişim kurun.

macOS Güvenlik Uygunluğu Projesi

macOS Güvenlik Uygunluğu Projesi (mSCP), güvenlik yönergeleri oluşturmayla ilgili programlı bir yaklaşım sunmayı hedefleyen bir açık kaynak girişimidir. Bu girişim, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Ulusal Havacılık ve Uzay Dairesi (NASA), Savunma Bilgi Sistemleri Ajansı (DISA) ve Los Alamos Ulusal Laboratuvarı (LANL) federal operasyonlarla ilgili BT Güvenliği personelinin ortak projesidir. Proje, macOS için bir grup test edilip doğrulanmış denetimi kullanır ve bu denetimleri proje tarafından desteklenen güvenlik yönergelerine eşler. Ayrıca bu proje, test edilip doğrulanmış işlem birimleri arşivinden (konfigürasyon ayarları) yararlanarak teknik güvenlik denetimlerine yönelik özel güvenlik temellerini kolayca yaratmak için bir kaynak olarak da kullanılabilir. Proje çıktısında, kullanılan temeli taban alan özel belgeler, betikler, konfigürasyon profilleri ve bir denetim kontrol listesi bulunur.

mSCP, uygunluğu elde etmek için yönetim ve güvenlik araçlarıyla birlikte kullanılacak çıktı içeriği üretebilir. Bu projedeki konfigürasyon ayarları şu yönerge temellerini destekler:

Kuruluş	Desteklenen temeller
Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Özel Yayını (SP) 800-53, Federal Bilgi Sistemleri ve Organizasyonları İçin Önerilen Güvenlik Denetimleri, Sürüm 5	800-53 Yüksek, 800-53 Normal, 800-53 Düşük
Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Özel Yayını (SP) 800-171, Federal Olmayan Sistemlerde ve Organizasyonlarda Denetimli Sınıflandırılmamış Bilgileri Koruma Sürüm 2	800-171
Savunma Bilgi Sistemleri Ajansı (DISA) macOS 11 STIG, Apple macOS 11 Güvenlik Teknik Uygulama Kılavuzu	STIG
Ulusal Güvenlik Sistemleri Yönerge Komitesi (CNSSI) 1253, Ulusal Güvenlik Sistemleri İçin Güvenlik Sınıflandırması ve Denetimi	1253

Ek bilgiler:

- Projedeki tüm kuralların gözden geçirilebileceği bir temel burada bulunabilir.
- Proje ve kullanım hakkında daha fazla bilgi edinmek için macOS Güvenlik Uygunluğu Projesi wiki sayfasına bakın.
- Projeyi kullanım için ayarlamak istiyorsanız şu sayfaya bakın: macOS Güvenlik Uygunluğu Projesi'ne Giriş, Bölüm 1 ve macOS Güvenlik Uygunluğu Projesi'ne Giriş, Bölüm 2.
- Bu projenin geliştirilmesini desteklemeyle ilgileniyorsanız katılımcı yönergelerine bakın.

Belge gözden geçirme geçmişi

Tarih	Özet
27 Ekim 2021	Güncellenen konular: • Secure Enclave işlemcisi için güvenlik sertifikaları • iOS için güvenlik sertifikaları • macOS için güvenlik sertifikaları
17 Ağustos 2021	Güncellenen konular: • Secure Enclave işlemcisi için güvenlik sertifikaları • Apple T2 güvenlik yongası için güvenlik sertifikaları • iOS için güvenlik sertifikaları • iPadOS için güvenlik sertifikaları • macOS için güvenlik sertifikaları • tvOS için güvenlik sertifikaları • watchOS için güvenlik sertifikaları • Apple uygulamaları için güvenlik sertifikaları • Güvenlik sertifikaları • macOS Güvenlik Uygunluğu Projesi
26 Nisan 2021	Eklenen konu: • macOS Güvenlik Uygunluğu Projesi Güncellenen konular: • Apple T2 güvenlik yongası için güvenlik sertifikaları: Yeni FIPS 140-2 sertifikası, 3811 • Secure Enclave işlemcisi için güvenlik sertifikaları: Yeni FIPS 140-2 sertifikası, 3811 ve ek sertifikalar için yeni bir tablo. • iOS için güvenlik sertifikaları: Yeni FIPS 140-2 sertifikaları, 3811, değerlendirme aşamasında olan iOS 14 program kimliği 11146 • iPadOS için güvenlik sertifikaları: Yeni FIPS 140-2 sertifikaları, 3811, değerlendirme aşamasında olan iPadOS 14 program kimliği 11147 • macOS için güvenlik sertifikaları: Yeni FIPS 140-2 sertifikası, 3811. • tvOS için güvenlik sertifikaları: Yeni FIPS 140-2 sertifikaları, 3811. • watchOS için güvenlik sertifikaları: Yeni FIPS 140-2 sertifikaları, 3811. • Apple uygulamaları için güvenlik sertifikaları: Ortak Kriterler durum güncellemeleri ve arşivlenen Ortak Kriterler sertifikaları için yeni bir tablo.

Sözlük

Apple Anında İletme Bildirim servisi (APNs) Apple tarafından sağlanan ve Apple aygıtlarına anında iletilen bildirimler gönderen dünya çapında bir servis.

Apple İşletme Yönetimi Kuruluşların doğrudan Apple'dan veya katılımcı bir Apple Yetkili Satıcısı'ndan ya da operatöründen satın aldığı Apple aygıtlarını dağıtması için hızlı ve kolay bir yol sunan, BT yöneticilerine yönelik web tabanlı basit bir portal. Kuruluşlar, aygıtları kullanıcılara vermeden önce hazırlamak veya fiziksel olarak onlara dokunmak zorunda kalmadan mobil aygıt yönetimi (MDM) çözümlerine otomatik olarak kaydettirebilir.

Apple Okul Yönetimi Kuruluşların doğrudan Apple'dan veya katılımcı bir Apple Yetkili Satıcısı'ndan ya da operatöründen satın aldığı Apple aygıtlarını dağıtması için hızlı ve kolay bir yol sunan, BT yöneticilerine yönelik web tabanlı basit bir portal. Kuruluşlar, aygıtları kullanıcılara vermeden önce hazırlamak veya fiziksel olarak onlara dokunmak zorunda kalmadan mobil aygıt yönetimi (MDM) çözümlerine otomatik olarak kaydettirebilir.

Bilgi Güvenliği Yönetimi Sistemi (ISMS) Bilgilerin ve/veya sistemin yaşam döngüsü boyunca bilgi güvenliğini sistemli bir şekilde yöneterek bu içerikleri korumak amacıyla tasarlanmış bir güvenlik programının sınırlarını yöneten bilgi güvenliği politikaları ve prosedürleri grubu.

corecrypto Alt düzey şifreleme temelleri uygulamalarını sağlayan bir kitaplık. corecrypto'nun geliştiriciler için programlama arayüzlerini doğrudan sunmadığını, geliştiricilere sağlanan API'ler aracılığıyla kullanıldığını unutmayın. corecrypto kaynak kodu, güvenlik özelliklerinin ve doğru bir şekilde çalıştığının doğrulanmasına olanak tanımak için herkese açıktır.

Federal Bilgi İşleme Standardı (FIPS) Yasa gereği veya siber güvenlik için zorunlu federal hükümet şartları olması durumunda ya da her iki nedenden ötürü Ulusal Standartlar ve Teknoloji Enstitüsü tarafından geliştirilen yayınlar.

Güvenlik Düzeyi (SL) Uygun güvenlik gereksinimi kümesini açıklamak için ISO/IEC 19790 içinde tanımlanan dört genel güvenlik düzeyi (1–4). En sıkı güvenlik düzeyi 4. düzeydir.

Güvenlik Hedefi (ST) Belirli bir ürün için güvenlik sorununu ve güvenlik gereksinimlerini belirten bir belge.

IPsec VPN İstemcisi Bir koruma profilinde, fiziksel veya sanal sunucu platformu ile uzaktaki konum arasında güvenli bir IPsec bağlantısı sağlayan bir istemci.

İşlenen Modüller (MIP) Şu an CMVP doğrulama sürecindeki şifreleme modüllerinin, Şifreleme Modülü Doğrulama Programı (CMVP) tarafından tutulan listesi.

Koruma profili (PP) Belirli bir ürün sınıfı için güvenlik sorununu ve güvenlik gereksinimlerini belirten bir belge.

mobil aygıt yönetimi (MDM) Kullanıcının kayıtlı aygıtları uzaktan yönetmesini sağlayan bir servis. Aygıt kaydolduktan sonra, kullanıcı herhangi bir kullanıcı etkileşimi olmadan ayarları yapmak ve aygıtta başka görevler gerçekleştirmek için ağ üzerinden MDM servisini kullanabilir.

ortak çalışmaya dayalı koruma profili (cPP) cPP'lerin yaratılmasından sorumlu uzman grubu olan uluslararası teknik topluluk tarafından geliştirilen bir koruma profili.

Ortak Kriterler (CC) BT güvenlik değerlendirmesinin genel kavramlarını ve ilkelerini belirleyen ve genel bir değerlendirme modeli belirten bir standart. Güvenlik gereksinimi kataloglarını standart bir dilde sunar.

Ortak Kriterleri Tanıma Anlaşması (CCRA) ISO/IEC 15408 serisi veya Ortak Kriterler standartlarına uygun olarak verilen sertifikaların uluslararası tanınması için politikaları ve gereksinimleri belirleyen bir karşılıklı tanıma anlaşması.

Secure Element (SE) Birçok Apple aygıtında yerleşik olan ve Apple Pay gibi işlevleri destekleyen bir Silicon yonga.

Secure Enclave işlemcisi (SEP) Yongadaki sistemde (SoC) yerleşik olarak üretilen bir yardımcı işlemci.

sepOS L4 mikro çekirdeğinin Apple tarafından özelleştirilmiş sürümünü baz alan Secure Enclave firmware'i.

Şifreleme Algoritması Doğrulama Programı (CAVP) NIST tarafından yönetilen ve onaylı (örneğin FIPS onaylı ve NIST tarafından önerilen) şifreleme algoritmalarının ve bunlara ait ayrı ayrı bileşenlerin doğrulama testlerini yapan bir kuruluş.

şifreleme modülü Şifreleme işlevleri sunan ve belirtilen şifreleme modülü standardına yönelik gereksinimleri karşılayan donanım, yazılım ve/veya firmware.

Şifreleme Modülü Doğrulama Programı (CMVP) ABD ve Kanada hükümetleri tarafından yönetilen ve FIPS 140-3 standardına uygunluk doğrulamasını gerçekleştiren bir kuruluş.

T2 2017 yılından beri bazı Intel tabanlı Mac bilgisayarlarında bulunan Apple güvenlik yongası.

Tam Disk Şifreleme (FDE) Bir depolama disk bölümündeki tüm verilerin şifrelenmesi.

Test Edilen Uygulama (IUT) Laboratuvar tarafından test edilen şifreleme modülü.

Ulusal Bilgi Güvencesi Ortaklığı (NIAP) Ortak Kriterler standardının ABD'de uygulanmasından ve NIAP Ortak Kriterler Değerlendirme ve Doğrulama Programı (CCEVS) yönetiminden sorumlu bir ABD hükümeti kuruluşu.

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ABD Ticaret Bakanlığı'nın ölçü bilimini, standartlarını ve teknolojisini geliştirmekten sorumlu bölümü.

uluslararası teknik topluluk (iTC) Ortak Kriterleri Tanıma Anlaşması (CCRA) denetiminde, koruma profillerinin veya iş birliğine dayalı koruma profillerinin geliştirilmesinden sorumlu bir grup.

Uygulanabilirlik Beyanı (SOA) ISO/IEC 27001 sertifikasını desteklemek amacıyla üretilen ve ISMS kapsamında uygulanan güvenlik denetimlerini açıklayan bir belge.

Üst Düzey Yetkililer Grubu Bilgi Sistemleri Güvenliği (SOG-IS) Birçok Avrupa ülkesi arasında karşılıklı tanıma anlaşmalarını yöneten bir grup.

yongadaki sistem (SoC) Tek bir yongada birden fazla bileşen içeren bir tümleşik devre (IC).

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

TU028-00499-B