보안 인증 및 준수 센터

2021년 12월

목차

Apple 보안 보증 소개 **4**

하드웨어 인증 4

소프트웨어 및 앱 인증 5

서비스 인증 5

하드웨어 보안 인증 **6**

Apple 하드웨어 보안 인증 개요 6

Secure Enclave 프로세서의 보안 인증 9

Apple T2 보안 칩용 보안 인증 12

운영 체제 보안 인증 **16**

Apple 운영 체제 보안 인증 개요 16

iOS용 보안 인증 18

iPadOS용 보안 인증 24

macOS용 보안 인증 30

tvOS용 보안 인증 37

watchOS용 보안 인증 41

소프트웨어 보안 인증 **45**

Apple 소프트웨어 보안 인증 개요 45

Apple 앱의 보안 인증 47

Apple 인터넷 서비스의 보안 인증 **50**

ISO/IEC 27001 50

ISO/IEC 27018 51

ISO/IEC 27001 및 ISO/IEC 27018이 적용된 Apple 서비스 51

인증 52

macOS 보안 준수 프로젝트 53

문서 수정 내역 54

용어집 55

Apple 보안 보증 소개

Apple은 보안에 대한 노력의 일환으로 다른 인증 기관과 정기적으로 협력하여 Apple의 하드웨어, 소프트웨어 및 서비스 보안에 대해 인증하고 증명합니다. 전 세계적으로 인정되는 이러한 기관에서는 운영 체제의 주요 릴리즈마다 Apple에 인증을 제공합니다. 이러한 방식으로 시스템의 보안 요구에 부합하는 신뢰의 척도인 보안 보증을 제공합니다. MRA(상호 인정 협정)에 따라 인정되지 않거나 유효한 보안 인증 표준이 없는 기술 분야의 경우, Apple은 적합한 보안 표준 개발에 참여합니다. 이러한 사명은 Apple 하드웨어, 운영 체제, 앱 및 서비스 전반에서 전 세계적으로 인정되는 포괄적 보안 인증이 적용되도록 추진하는 것입니다.

법률, 규제 및 산업 표준의 요구 사항에 부합하기 위해 종종 인증이 필요합니다. Apple School Manager 및 Apple Business Manager와 같은 서비스는 Apple의 ISO/IEC 27001 및 ISO/IEC 27018 인증에 따라 적용됩니다. Apple 기기를 배포하는 정부 기관, 기업 및 교육 기관을 포함한 모든 고객은 하드웨어, 운영 체제, 소프트웨어 및 서비스 인증을 사용하여 준수 입증을 지원할 수 있습니다.

하드웨어 인증

하드웨어 수준에서 보안의 기반이 마련되어야 소프트웨어도 안전하게 사용할 수 있으므로 iOS, iPadOS, macOS, tvOS, watchOS 등을 실행하는 모든 Apple 기기에 보안 기능이 담긴 실리콘 칩이 탑재되어 있습니다. 여기에는 시스템 보안 특성을 제공하는 커스텀 CPU 기능과 보안 기능을 제공하는 전용 실리콘 칩이 포함됩니다. 가장 핵심이 되는 구성요소는 최근 출시되는 모든 iOS, iPadOS, watchOS 및 tvOS 기기, Apple Silicon이 장착된 모든 Mac 컴퓨터와 Apple T2 보안 칩이 탑재된 Intel 기반 Mac 컴퓨터에 지원되는 Secure Enclave 보조 프로세서입니다. Secure Enclave는 안전한 데이터 암호화, macOS의 보안 시동, 생체 인증에서 기반이 되는 역할을 수행합니다.

Apple의 보안 보증에 대한 노력은 하드웨어 신뢰 루트부터 보안 시동 적용, 보안 키 저장소를 제공하는 Secure Enclave, Touch ID 및 Face ID를 통한 보안 인증에 이르기까지 실리콘 칩의 기본적인 보안 구성요소의 인증에서 시작됩니다. Apple 기기의 보안 기능은 실리콘 칩 설계, 하드웨어, 소프트웨어, 그리고 오직 Apple에서만 제공할 수 있는 서비스의 조합으로 이루어집니다. 이러한 구성요소의 인증은 Apple이 제공하는 보증을 검증하는 데 중요한 부분을 차지합니다.

하드웨어 및 연계 펌웨어 구성요소에 관련된 공인 인증에 관한 정보는 다음을 참조하십시오.

- Apple T2 보안 칩용 보안 인증
- Secure Enclave 프로세서의 보안 인증

소프트웨어 및 앱 인증

Apple은 암호화 모듈에 대해 미국 FIPS(Federal Information Processing Standards) 140-2/-3을 준수하고, 운영 체제, 앱 및 기기 서비스에 대해 CC를 준수하여 운영 체제 및 앱에 대한 독자적 인증과 증명을 유지합니다. 운영 체제의 적용 범위는 iOS, iPadOS, macOS, sepOS, T2 펌웨어, tvOS 및 watchOS가 포함됩니다. 앱의 경우 독자적 인증에 Safari 브라우저 및 연락처 앱이 처음으로 포함되며 향후 더 많은 앱이 인증됩니다.

Apple **운영 체제**에 관련된 공인 인증에 관한 정보는 다음을 참조하십시오.

- iOS용 보안 인증
- iPadOS용 보안 인증
- macOS용 보안 인증
- tvOS용 보안 인증
- watchOS용 보안 인증

Apple **앱**에 관련된 공인 인증에 관한 정보는 다음을 참조하십시오.

- Apple 앱의 보안 인증

서비스 인증

Apple은 기업부터 교육 기관에 이르는 고객을 지원하기 위해 보안 인증을 유지합니다. 이러한 인증은 Apple 고객이 Apple 하드웨어 및 소프트웨어로 Apple 서비스를 사용할 때 규제 및 계약 의무를 이행할 수 있도록 합니다. 이러한 인증은 고객에게 Apple 시스템에 대한 Apple 정보 보안, 환경 및 개인 정보 보호 관행에 있어서 독자적 증명을 제공합니다.

Apple **인터넷 서비스**에 관련된 공인 인증에 관한 정보는 다음을 참조하십시오.

- Apple 인터넷 서비스의 보안 인증

Apple 보안 및 개인 정보 보호 인증에 관한 질문은 security-certifications@apple.com으로 문의하십시오.

하드웨어 보안 인증

Apple 하드웨어 보안 인증 개요

Apple은 sepOS 및 T2 펌웨어에 대한 미국 FIPS(Federal Information Processing Standard) 140-2/-3 준수 검증 인증 및 기타 인증을 유지합니다. Apple은 적합한 여러 플랫폼에 광범위하게 적용되는 **인증 빌딩 블록**으로 시작합니다. 첫 번째 빌딩 블록은 Apple에서 개발한 운영 체제 내 소프트웨어 및 하드웨어 암호화 모듈 배포에 사용되는 corecrypto 라이브러리 검증입니다. 두 번째 빌딩 블록은 많은 Apple 기기에 내장된 Secure Enclave 인증입니다. 세 번째는 Touch ID가 있는 Apple 기기 및 Face ID가 있는 기기에 적용된 Secure Element(SE) 인증입니다. 이러한 하드웨어 인증 빌딩 블록은 광범위한 플랫폼 보안 인증의 기반을 형성합니다.

암호화 알고리즘 검증

많은 암호화 알고리즘 및 관련 보안 기능의 구현 정확성을 검증하는 것은 FIPS 140-3 검증 및 지원되는 기타 인증의 필수 전제 조건입니다. 검증은 NIST(National Institute of Standards and Technology) CAVP(Cryptographic Algorithm Validation Program)에서 관리됩니다. Apple 구현에 대한 검증 인증서는 CAVP 검색 기능을 사용하여 찾을 수 있습니다. 추가 정보를 보려면 CAVP(Cryptographic Algorithm Validation Program) 웹 사이트를 참조하십시오.

암호화 모듈 검증: FIPS 140-2/3(ISO/IEC 19790)

Apple의 암호화 모듈은 2012년부터 운영 체제의 주요 릴리즈마다 암호화 모듈에 대한 미국 FIPS(Federal Information Processing Standard) 140-2에 따라 CMVP(Cryptographic Module Validation Program)를 통해 반복적으로 검증되었습니다. Apple은 매 주요 릴리즈 이후 CMVP에 모듈을 제출하여 표준 준수 검증을 실시합니다. 이 모듈은 Apple 운영 체제 및 앱에서 사용될 뿐 아니라 Apple 제공 서비스에 암호화 기능을 제공하며 타사 앱에서 사용할 수 있습니다.

Apple은 소프트웨어 기반 모듈인 macOS용 'Intel용 Corecrypto Module' 및 'Intel용 Corecrypto Kernel Module'에 대해 매년 **Security Level 1**을 받았습니다. Apple Silicon의 경우 'ARM용 Corecrypto Module' 및 'ARM용 Corecrypto Kernel Module' 모듈은 iOS, iPadOS, tvOS, watchOS 및 Mac 컴퓨터에 내장된 Apple T2 보안 칩의 펌웨어에 적용됩니다.

2019년에 Apple은 'Apple Corecrypto Module: Secure Key Store'로 명명된 내장 하드웨어 암호화 모듈에 대한 최초의 FIPS 140-2 **Security Level 2**를 획득하여 Secure Enclave로 생성 및 관리되는 키의 사용 승인을 미국 정부로부터 받았습니다. Apple은 각각의 주요 운영 체제 릴리즈에서 하드웨어 암호화 모듈의 검증을 진행합니다.

FIPS 140-3은 2019년 미국 상무부의 승인을 받았습니다. 이 표준 버전에서 가장 눈에 띄는 변화는 ISO/IEC 표준, 특히 ISO/IEC 19790:2015 및 관련 테스팅 표준 ISO/IEC 24759:2017의 사양입니다. CMVP는 전환 프로그램을 시작하고 2020년부터 FIPS 140-3의 기반으로 암호화 모듈을 검증할 것이라고 밝혔습니다. Apple은 Apple 암호화 모듈이 가능한 빠른 시일 내에 FIPS 140-3 표준을 충족하여 전환하는 것을 목표로 하고 있습니다.

현재 테스트 및 검증 절차에 있는 암호화 모듈의 경우, CMVP는 제안된 검증에 대한 정보를 포함할 수 있는 두 개의 별도 목록을 지닙니다. 공인 연구소에서 테스트 중인 암호화 모듈의 경우, Implementation Under Test List(테스트 중인 구현 목록)에 모듈이 표시될 수 있습니다. 연구소에서 테스트를 완료하고 CMVP의 검증을 권장한 후 Apple 암호화 모듈은 Modules in Process List(처리 중인 모듈 목록)에 표시됩니다. 현재 연구소의 테스트가 완료되어 CMVP의 테스트 검증을 대기 중입니다. 평가 프로세스의 기간은 가변적이므로 주요 운영 체제 릴리즈 날짜와 CMVP의 검증 인증서 발급 날짜 사이의 기간에 Apple 암호화 모듈의 현재 상태를 파악하려면 위의 두 프로세스 목록을 확인하십시오.

제품 인증: CC(ISO/IEC 15408)

CC(ISO/IEC 15408)는 여러 기관에서 IT 제품의 보안 평가의 기반으로 사용하는 표준입니다.

국제 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증에 대해서는 Common Criteria Portal을 참조하십시오. CC 표준은 국가 및 민간 검증 체계에 의해 CCRA 외부에서도 사용될 수 있습니다. 유럽에서 상호 인정은 SOG-IS 합의 및 CCRA를 따릅니다.

CC 커뮤니티에서 언급한 바와 같이, 국제적으로 승인된 보안 표준 집합을 사용하여 정보 기술 제품의 보안 기능에 대한 명확하고 신뢰할 수 있는 평가 방식을 제공하는 것이 목표입니다. CC는 제품의 보안 표준 준수 능력에 대한 독자적 평가를 제공함으로써 고객에게 정보 기술 제품의 보안에 대한 확신을 주며 더 많은 정보에 입각한 결정을 유도합니다.

CCRA를 통해 회원 국가는 동일한 수준의 신뢰도를 가진 정보 기술 제품의 인증을 인정하는 데 합의했습니다. 인증 전에 필요한 평가는 광범위하며 다음을 포함합니다.

- 보호 프로파일(PP)
- 보안 대상(ST)
- 보안 기능 요구 사항(SFR)
- 보안 보증 요구 사항(SAR)
- EAL(Evaluation Assurance Levels)

보호 프로파일(PP)은 휴대성과 같은 기기 유형의 클래스에 대한 보안 요구 사항을 명시하는 문서로, 동일한 클래스 내에서의 IT 제품 평가 간 비교 가능성을 제공하는 데 사용됩니다. 늘어나는 승인된 PP 목록과 더불어 CCRA 멤버십 수가 매년 계속해서 증가하고 있습니다. 이 협정은 제품 개발자가 인증서 인증 체계 중 하나에 따라 단일 인증을 실행할 수 있도록 허용하며, 제품 개발자는 인증서를 수용하는 합의국 중 어떤 국가에서든 인정을 받을 수 있습니다.

보안 대상(ST)은 IT 제품 인증 시 평가할 **항목**을 정의합니다. ST는 더 구체적으로 **보안 기능 요구 사항(SFR)**으로 변환되며, ST를 더 상세하게 평가하는 데 사용됩니다.

또한 CC(Common Criteria)는 **보안 보증 요구 사항**을 포함합니다. 일반적으로 식별되는 지표 중 하나는 **EAL(Evaluation Assurance Levels)**입니다. EAL은 자주 발생하는 일련의 SAR을 그룹화하고, 비교 가능성을 지원하기 위해 PP 및 ST에 명시될 수 있습니다.

대다수의 이전 PP는 보관소에 저장되었으며 특정 솔루션 및 환경에 중점을 두고 개발되는 대상 PP로 대체되고 있습니다. 모든 CCRA 회원들 간에 지속적인 상호 인정을 보장하기 위한 공동의 노력으로, iTC(국제 기술 커뮤니티)는 처음부터 CCRA 합의국 제도의 참여로 개발된 cPP(공동 보호 프로파일)를 개발하고 유지하기 위해 설립되었습니다. CCRA 외에 사용자 그룹 및 상호 인정 협정을 대상으로 하는 PP는 적합한 이해 당사자가 계속 개발하고 있습니다.

2015년 초부터 Apple은 업데이트된 CCRA하에 엄선된 cPP로 인증을 진행해 왔습니다. 그 이후로 Apple은 주요 iOS 릴리즈마다 CC 인증을 받아왔으며 적용 범위를 확대하여 새로운 PP가 제공하는 보안 보증을 포함시켰습니다.

Apple은 모바일 보안 기술 평가에 중점을 둔 기술 커뮤니티 내에서 적극적 역할을 수행합니다. 여기에는 cPP를 개발하고 업데이트하는 iTC가 포함됩니다. Apple은 현재 PP 및 cPP에 대해 평가하고 인증을 받기 위해 계속 노력하고 있습니다.

일반적으로 북미 시장에서의 Apple 플랫폼 인증은, 아직 인증되지 않았으나 현재 평가 중인 프로젝트 목록을 유지하는 NIAP(National Information Assurance Partnership)를 통해 수행됩니다.

나열된 일반 플랫폼 인증서 외에도 일부 시장에 대한 특정 보안 요구 사항을 입증하기 위해 다른 인증서가 발급되었습니다.

Secure Enclave 프로세서의 보안 인증

Secure Enclave 인증 배경

하드웨어 암호화 모듈**(Apple SEP 보안 키 저장소 암호화 모듈)**은 다음 제품에 포함된 Apple SoC에 내장되어 있습니다. iPhone 및 iPad용 Apple A 시리즈, Apple Silicon이 장착된 Mac 컴퓨터용 M 시리즈, Apple Watch용 S 시리즈 및 2017년 출시된 iMac Pro부터 Intel 기반 Mac 컴퓨터에 탑재된 T 시리즈 보안 칩이 해당됩니다.

2018년, Apple은 2017년에 출시된 운영 체제인 iOS 11, macOS 10.13, tvOS 11 및 watchOS 4를 소프트웨어 암호화 모듈의 검증과 동기화했습니다. Apple SEP 보안 키 저장소 암호화 모듈 v1.0으로 식별된 SEP 하드웨어 암호화 모듈은 처음에 FIPS 140-2 Security Level 1 요구 사항에 대해 검증되었습니다.

2019년, Apple은 해당하는 corecrypto 사용자 및 corecrypto 커널 모듈 검증 버전과 동기화하기 위해 FIPS 140-2 Security Level 2 요구 사항에 대해 하드웨어 모듈을 검증했고 모듈 버전 식별자를 v9.0으로 업데이트했습니다. 2019년, iOS 12, macOS 10.14, tvOS 12 및 watchOS 5가 포함되었습니다.

2020년 및 2021년, Apple은 FIPS 140-3 준수 여부 및 Apple Silicon(A13, A14, S6 및 M1 칩)용 물리적 보안 요구 사항의 보안 수준 3 추가 보증에 대한 검증을 추진하고 있습니다.

Apple은 또한 운영 체제의 주요 릴리즈마다 corecrypto 사용자 및 corecrypto 커널 모듈의 검증에 적극적으로 참여합니다. 준수 검증은 최종 릴리즈 버전을 대상으로만 수행할 수 있습니다.

암호화 모듈 검증 상태

CMVP(Cryptographic Module Validation Program)는 현재 상태에 따라 세 개의 개별 목록하에 암호화 모듈의 검증 상태를 유지합니다.

- CMVP Implementation Under Test List(테스트 중인 구현 목록)에 표시되려면 연구소는 Apple과 계약하여 테스트를 진행해야 합니다.
- 연구소의 테스트가 완료된 후 해당 연구소는 CMVP의 검증을 권장하고, CMVP 수수료를 지불한 다음 해당 모듈이 Modules in Process List(처리 중인 모듈 목록)에 추가됩니다. MIP 목록은 다음의 네 단계로 CMVP 검증 활동의 진행 상황을 추적합니다.
  - **Review Pending(검토 대기):** CMVP 담당자 할당을 기다리는 중입니다.
  - **In Review(검토 중):** CMVP 담당자가 검증 활동을 수행하는 중입니다.
  - **Coordination(조정):** 연구소와 CMVP가 발견된 문제를 해결하는 중입니다.
  - **Finalization(최종 승인):** 인증서 발급과 관련된 활동 및 절차입니다.
- CMVP의 검증 후 해당 모듈은 준수 인증서를 받고 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)에 추가되며, 여기에는 다음이 포함됩니다.
  - 검증된 모듈은 활성으로 표시됩니다.
  - 5년이 지나면 모듈이 이전으로 표시됩니다.
  - 어떤 이유에서든 모듈 인증서가 파기된 경우 파기로 표시됩니다.

2020년, CMVP는 FIPS 140-3의 기반으로 국제 표준인 ISO/IEC 19790을 채택했습니다.

FIPS 140-3 인증

현재 상태

아래 표에는 FIPS 140-3을 준수하여 현재 연구소에서 테스트 중인 2020년 및 2021년 암호화 모듈이 표시됩니다.

2020년 및 2021년에 출시된 운영 체제 관련 SKS(Secure Key Store)는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. 이는 Modules in Process List(처리 중인 모듈 목록)에 표시되어 있으며, 검증이 완료되면 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)로 이동됩니다.

iOS 15(2021년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 거치는 중이며, Implementation Under Test List(테스트 중인 구현 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** 2021년 출시된 iOS, iPadOS, macOS, tvOS, 및 watchOS와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14, T2, M1, S3-S6) **전반적인 보안 수준:** 2
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** 2021년 출시된 iOS, iPadOS, macOS, tvOS, 및 watchOS와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A13, A14, S6, M1) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** 2020년 출시된 iOS, iPadOS, macOS, tvOS, 및 watchOS와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14, T2, M1, S3-S6) **전반적인 보안 수준:** 2
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** 2020년 출시된 iOS, iPadOS, macOS, tvOS, 및 watchOS와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A13, A14, S6, M1) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3

FIPS 140-2 인증

아래 표에는 FIPS 140-2를 준수하여 연구소에서 테스트를 거친 암호화 모듈이 표시됩니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2019 **검증일:** 2021-02-05	**인증서:** 3811 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v10.0 **운영 체제:** macOS 10.15 Catalina용 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2018 **검증일:** 2019-09-10	**인증서:** 3523 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v9.0 **운영 체제:** macOS 10.14 Mojave용 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2017 **검증일:** 2019-09-10	**인증서:** 3223 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v1.0 **운영 체제:** macOS 10.13 High Sierra용 sepOS **유형:** 하드웨어 **보안 수준:** 2

CC(Common Criteria) 인증

Apple은 적합한 보호 프로파일로 Apple 기술의 보안 기능을 보장하는 CC 평가에 적극적으로 참여합니다.

CC(Common Criteria) 인증 상태

NIAP에서 운영하는 미국의 제도는 Products in Evaluation(평가 중인 제품) 목록을 유지합니다. 이 목록에는 현재 미국에서 NIAP의 승인을 받은 CCTL(Common Criteria Testing Laboratory)과 함께 평가가 진행 중인 제품 및 CCEVS 경영진이 공식적으로 제품 평가를 수락하는 평가 킥오프 미팅 또는 이에 준하는 회의를 완료한 제품이 포함됩니다.

NIAP는 제품이 인증된 후 Product Compliant list(제품 준수 목록)에 현재 유효한 인증을 추가합니다. 2년 후에 해당 인증이 현재 보증 유지 관리 정책을 준수하는지 검토합니다. NIAP는 보증 유지 관리 날짜가 만료된 후 인증 목록을 Archived Products list(저장된 제품 목록)로 이동시킵니다.

Common Criteria Portal에서는 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증을 나열합니다. CC Portal은 인증된 제품 목록에 5년 동안 제품을 유지할 수 있고, 기록은 CC Portal의 Archived Certifications(저장된 인증)로 보관됩니다.

아래 표에는 현재 연구소에서 평가 중인 인증, 또는 CC를 준수하는 것으로 인증된 인증이 표시됩니다.

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: sepOS **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple Secure Enclave[2020] **보호 프로파일:** CPP_DSC_V1.0 **하드웨어:** (A9-A14, M1, T2, S3-S6)용 Secure Enclave **소프트웨어:** iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7과 함께 배포된 sepOS

추가 인증

아래 표에는 CC 또는 FIPS 140-3을 사용하지 않는 Secure Enclave에 대한 인증이 표시됩니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2020 **검증일:** 2019-12-07부터 2022-12-26까지	**인증서:** CFNR201902910002 (P.R. China: Technology Certification of Mobile Financial Service) 중국어 버전 영어 버전	**제목:** Mobile Terminal Trusted Execution Environment(모바일 터미널 신뢰 실행 환경) **운영 체제:** iOS 13.5.1 **규격:** JR/T 0156-2017

Apple T2 보안 칩용 보안 인증

암호화 모듈 검증 배경

Apple은 운영 체제의 주요 릴리즈마다 Apple의 내장된 소프트웨어 및 하드웨어 모듈의 검증에 적극적으로 참여합니다. 준수 검증은 최종 모듈 릴리즈 버전을 대상으로만 수행할 수 있습니다.

2020년, CMVP는 미국 FIPS(Federal Information Processing Standard) 140-3의 기반으로 국제 표준인 ISO/IEC 19790을 채택했습니다.

또한 2017년부터 대부분의 Mac 컴퓨터는 Intel CPU 외에 Apple Silicon 기반 SoC(System on Chip)인 별도의 Apple T2 보안 칩을 탑재하고 있습니다. T2 칩이 탑재된 이러한 Mac 컴퓨터는 다양한 오프라인 서비스에 대해 모두 다섯 개의 암호화 모듈을 사용합니다.

- Intel용 Corecrypto 사용자 모듈(Intel 기반 Mac 컴퓨터의 macOS에서 사용)
- Intel용 Corecrypto 커널 모듈(Intel 기반 Mac 컴퓨터의 macOS에서 사용)
- ARM용 Corecrypto 사용자 모듈(T2 칩에서 사용)
- ARM용 Corecrypto 커널 모듈(T2 칩에서 사용)
- 보안 키 저장소 암호화 모듈(T2 칩의 내장된 Secure Enclave 보조 프로세서에서 사용)

참고: T2 칩에서 실행되는 Apple Silicon 기반 모듈은 Apple A 시리즈, S 시리즈 및 M 시리즈 등 다른 Apple Silicon에서 실행되는 모듈과 동일합니다.

암호화 모듈 검증 상태

CMVP(Cryptographic Module Validation Program)는 현재 상태에 따라 세 개의 개별 목록하에 암호화 모듈의 검증 상태를 유지합니다.

- CMVP Implementation Under Test List(테스트 중인 구현 목록)에 표시되려면 연구소는 Apple과 계약하여 테스트를 진행해야 합니다.
- 연구소의 테스트가 완료된 후 해당 연구소는 CMVP의 검증을 권장하고, CMVP 수수료를 지불한 다음 해당 모듈이 MIP(Modules in Process) List(처리 중인 모듈 목록)에 추가됩니다. MIP 목록은 다음의 4단계로 CMVP 검증 활동의 진행 상황을 추적합니다.
  - **Review Pending(검토 대기):** CMVP 담당자 할당을 기다리는 중입니다.
  - **In Review(검토 중):** CMVP 담당자가 검증 활동을 수행하는 중입니다.
  - **Coordination(조정):** 연구소와 CMVP가 발견된 문제를 해결하는 중입니다.
  - **Finalization(최종 승인):** 인증서 발급과 관련된 활동 및 절차입니다.
- CMVP의 검증 후 해당 모듈은 준수 인증서를 받고 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)에 추가되며, 여기에는 다음이 포함됩니다.
  - 검증된 모듈은 활성으로 표시됩니다.
  - 5년이 지나면 모듈이 이전으로 표시됩니다.
  - 어떤 이유에서든 모듈 인증서가 파기된 경우 파기로 표시됩니다.

FIPS 140-3 인증

현재 상태

사용자 공간, 커널 공간 및 보안 키 저장소용 2020년 모듈은 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

사용자 공간, 커널 공간 및 보안 키 저장소용 2021년 모듈은 연구소에서 테스트하는 중이며, Implementation Under Test List(테스트 중인 구현 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** macOS 12 Monterey용 sepOS **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** macOS 12 Monterey용 sepOS **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** macOS 12 Monterey용 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(T2) **보안 수준:** 2

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** macOS 11 Big Sur용 sepOS **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** macOS 11 Big Sur용 sepOS **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** Intel 기반 macOS 11 Big Sur용 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어 **보안 수준:** 2

FIPS 140-2 인증

아래 표에는 FIPS 140-2를 준수하여 연구소에서 테스트를 거친 암호화 모듈이 표시됩니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3856 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v10.0 **운영 체제:** macOS 10.15 Catalina 용 sepOS **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3855 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v10.0 **운영 체제:** macOS 10.15 Catalina 용 sepOS **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-02-05	**인증서:** 3811 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Secure Key Store Cryptographic Module v10.0 **운영 체제:** macOS 10.15 Catalina 용 sepOS **유형:** 하드웨어 **보안 수준:** 2

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2018 **검증일:** 2019-04-23	**인증서:** 3438 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v9.0 **운영 체제:** macOS 10.14 Mojave용 sepOS **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-04-11	**인증서:** 3433 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v9.0 **운영 체제:** macOS 10.14 Mojave용 sepOS **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-09-10	**인증서:** 3523 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v9.0 **운영 체제:** macOS 10.14 Mojave용 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-22, 2018-07-06	**인증서:** 3148 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v8.0 **운영 체제:** macOS 10.13 High Sierra용 sepOS **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-17, 2018-07-03	**인증서:** 3147 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v8.0 **운영 체제:** macOS 10.13 High Sierra용 sepOS **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2018-07-10	**인증서:** 3223 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v1.0 **운영 체제:** macOS 10.13 High Sierra용 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2016 **검증일:** 2017-02-01	**인증서:** 2828 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple iOS Corecrypto Kernel Module v7.0 **운영 체제:** macOS 10.12 Sierra용 sepOS **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2016 **검증일:** 2017-02-01	**인증서:** 2827 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple iOS Corecrypto Kernel Module v7.0 **운영 체제:** macOS 10.12 Sierra용 sepOS **유형:** 소프트웨어 **보안 수준:** 1

운영 체제 보안 인증

Apple 운영 체제 보안 인증 개요

Apple은 sepOS 및 T2 펌웨어에 대한 미국 FIPS(Federal Information Processing Standard) 140-2/-3 준수 검증 인증 및 기타 인증을 유지합니다. Apple은 적합한 여러 플랫폼에 광범위하게 적용되는 **인증 빌딩 블록**으로 시작합니다. 첫 번째 빌딩 블록은 Apple에서 개발한 운영 체제 내 소프트웨어 및 하드웨어 암호화 모듈 배포에 사용되는 corecrypto 검증입니다. 두 번째 빌딩 블록은 많은 Apple 기기에 내장된 Secure Enclave 인증입니다. 세 번째는 Touch ID가 있는 Apple 기기 및 Face ID가 있는 기기에 적용된 Secure Element(SE) 인증입니다. 이러한 하드웨어 인증 빌딩 블록은 광범위한 플랫폼 보안 인증의 기반을 형성합니다.

암호화 알고리즘 검증

많은 암호화 알고리즘 및 관련 보안 기능의 구현 정확성을 검증하는 것은 FIPS 140-3 검증 및 지원되는 기타 인증의 필수 전제 조건입니다. 검증은 NIST CAVP(암호화 알고리즘 검증 프로그램)에서 관리됩니다. Apple 구현에 대한 검증 인증서는 CAVP 검색 기능을 사용하여 찾을 수 있습니다.

암호화 모듈 검증: FIPS 140-2/3(ISO/IEC 19790)

Apple 운영 체제의 암호화 모듈은 2012년부터 운영 체제의 주요 릴리즈마다 미국 FIPS(Federal Information Processing Standards) 140-2에 따라 CMVP(Cryptographic Module Validation Program)를 통해 반복적으로 검증되었습니다. Apple은 매 주요 릴리즈 이후 모든 CMVP 모듈을 제출하여 전체 암호화 검증을 실시합니다. 이렇게 검증된 모듈은 Apple 제공 서비스에 암호화 작업을 제공하며 타사 앱에서 사용할 수 있습니다.

Apple은 소프트웨어 기반 모듈인 macOS용 'Intel용 Corecrypto Module' 및 'Intel용 Corecrypto Kernel Module'에 대해 매년 **Security Level 1**을 받았습니다. Apple Silicon의 경우 'ARM용 Corecrypto Module' 및 'ARM용 Corecrypto Kernel Module' 모듈은 iOS, iPadOS, tvOS, watchOS 및 Mac 컴퓨터에 내장된 Apple T2 보안 칩의 펌웨어에 적용됩니다.

2019년에 Apple은 'Apple Corecrypto Module: Secure Key Store'로 명명된 내장 하드웨어 암호화 모듈에 대한 최초의 FIPS 140-2 **Security Level 2**를 획득하여 Secure Enclave로 생성 및 관리되는 키의 사용 승인을 미국 정부로부터 받았습니다. Apple은 각각의 주요 운영 체제 릴리즈에서 하드웨어 암호화 모듈의 검증을 진행합니다.

FIPS 140-3은 2019년 미국 상무부의 승인을 받았습니다. 이 표준 버전에서 가장 눈에 띄는 변화는 ISO/IEC 표준, 특히 ISO/IEC 19790:2015 및 관련 테스팅 표준 ISO/IEC 24759:2017의 사양입니다. CMVP는 전환 프로그램을 시작하고 2020년부터 FIPS 140-3의 기반으로 암호화 모듈을 검증할 것이라고 밝혔습니다. Apple은 Apple 암호화 모듈이 가능한 빠른 시일 내에 FIPS 140-3 표준을 충족하여 전환하는 것을 목표로 하고 있습니다.

현재 테스트 및 검증 절차에 있는 암호화 모듈의 경우, CMVP는 제안된 검증에 대한 정보를 포함할 수 있는 두 개의 별도 목록을 지닙니다. 공인 연구소에서 테스트 중인 암호화 모듈의 경우, Implementation Under Test List(테스트 중인 구현 목록)에 모듈이 표시될 수 있습니다. 연구소에서 테스트를 완료하고 CMVP의 검증을 권장한 후 Apple 암호화 모듈은 Modules in Process List(처리 중인 모듈 목록)에 표시됩니다. 현재 연구소의 테스트가 완료되어 CMVP의 테스트 검증을 대기 중입니다. 평가 프로세스의 기간은 가변적이므로 주요 운영 체제 릴리즈 날짜와 CMVP의 검증 인증서 발급 날짜 사이의 기간에 Apple 암호화 모듈의 현재 상태를 파악하려면 위의 두 프로세스 목록을 확인하십시오.

제품 인증: CC(ISO/IEC 15408)

CC(ISO/IEC 15408)는 여러 기관에서 IT 제품의 보안 평가의 기반으로 사용하는 표준입니다.

국제 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증에 대해서는 Common Criteria Portal을 참조하십시오. CC 표준은 국가 및 민간 검증 체계에 의해 CCRA 외부에서도 사용될 수 있습니다. 유럽에서 상호 인정은 SOG-IS 합의 및 CCRA를 따릅니다.

CC 커뮤니티에서 언급한 바와 같이, 국제적으로 승인된 보안 표준 집합을 사용하여 정보 기술 제품의 보안 기능에 대한 명확하고 신뢰할 수 있는 평가 방식을 제공하는 것이 목표입니다. CC는 제품의 보안 표준 준수 능력에 대한 독자적 평가를 제공함으로써 고객에게 정보 기술 제품의 보안에 대한 확신을 주며 더 많은 정보에 입각한 결정을 유도합니다.

CCRA를 통해 회원 국가는 동일한 수준의 신뢰도를 가진 정보 기술 제품의 인증을 인정하는 데 합의했습니다. 인증 전에 필요한 평가는 광범위하며 다음을 포함합니다.

- 보호 프로파일(PP)
- 보안 대상(ST)
- 보안 기능 요구 사항(SFR)
- 보안 보증 요구 사항(SAR)
- EAL(Evaluation Assurance Levels)

보호 프로파일(PP)은 휴대성과 같은 기기 유형의 클래스에 대한 보안 요구 사항을 명시하는 문서로, 동일한 클래스 내에서의 IT 제품 평가 간 비교 가능성을 제공하는 데 사용됩니다. 늘어나는 승인된 PP 목록과 더불어 CCRA 멤버십 수가 매년 계속해서 증가하고 있습니다. 이 협정은 제품 개발자가 인증서 인증 체계 중 하나에 따라 단일 인증을 실행할 수 있도록 허용하며, 제품 개발자는 인증서를 수용하는 합의국 중 어떤 국가에서든 인정을 받을 수 있습니다.

보안 대상(ST)은 IT 제품 인증 시 평가할 **항목**을 정의합니다. ST는 더 구체적으로 **보안 기능 요구 사항(SFR)**으로 변환되며, ST를 더 상세하게 평가하는 데 사용됩니다.

또한 CC(Common Criteria)는 **보안 보증 요구 사항**을 포함합니다. 일반적으로 식별되는 지표 중 하나는 **EAL(Evaluation Assurance Levels)**입니다. EAL은 자주 발생하는 일련의 SAR을 그룹화하고, 비교 가능성을 지원하기 위해 PP 및 ST에 명시될 수 있습니다.

대다수의 이전 PP는 보관소에 저장되었으며 특정 솔루션 및 환경에 중점을 두고 개발되는 대상 PP로 대체되고 있습니다. 모든 CCRA 회원들 간에 지속적인 상호 인정을 보장하기 위한 공동의 노력으로, iTC(국제 기술 커뮤니티)는 처음부터 CCRA 합의국 제도의 참여로 개발된 **cPP(공동 보호 프로파일)**를 개발하고 유지하기 위해 설립되었습니다. CCRA 외에 사용자 그룹 및 상호 인정 협정을 대상으로 하는 PP는 적합한 이해 당사자가 계속 개발하고 있습니다.

2015년 초부터 Apple은 업데이트된 CCRA하에 엄선된 cPP로 인증을 진행해 왔습니다. 그 이후로 Apple은 주요 iOS 릴리즈마다 CC 인증을 받아왔으며 적용 범위를 확대하여 새로운 PP가 제공하는 보안 보증을 포함시켰습니다.

Apple은 모바일 보안 기술 평가에 중점을 둔 기술 커뮤니티 내에서 적극적 역할을 수행합니다. 여기에는 cPP를 개발하고 업데이트하는 iTC가 포함됩니다. Apple은 현재 PP 및 cPP에 대해 평가하고 인증을 받기 위해 계속 노력하고 있습니다.

일반적으로 북미 시장에서의 Apple 플랫폼 인증은, 아직 인증되지 않았으나 현재 평가 중인 프로젝트 목록을 유지하는 NIAP(National Information Assurance Partnership)를 통해 수행됩니다.

나열된 일반 플랫폼 인증서 외에도 일부 시장에 대한 특정 보안 요구 사항을 입증하기 위해 다른 인증서가 발급되었습니다.

iOS용 보안 인증

iOS 인증 배경

Apple은 운영 체제의 주요 릴리즈마다 Apple의 내장된 소프트웨어 및 하드웨어 모듈의 검증에 적극적으로 참여합니다. 준수 검증은 최종 릴리즈 버전을 대상으로만 수행할 수 있습니다.

iOS 암호화 모듈 검증 상태

CMVP(Cryptographic Module Validation Program)는 현재 상태에 따라 세 개의 개별 목록하에 암호화 모듈의 검증 상태를 유지합니다.

- CMVP Implementation Under Test List(테스트 중인 구현 목록)에 표시되려면 연구소는 Apple과 계약하여 테스트를 진행해야 합니다.
- 연구소의 테스트가 완료된 후 해당 연구소는 CMVP의 검증을 권장하고, CMVP 수수료를 지불한 다음 해당 모듈이 MIP(Modules in Process) List(처리 중인 모듈 목록)에 추가됩니다. MIP 목록은 다음의 4단계로 CMVP 검증 활동의 진행 상황을 추적합니다.
  - **Review Pending(검토 대기):** CMVP 담당자 할당을 기다리는 중입니다.
  - **In Review(검토 중):** CMVP 담당자가 검증 활동을 수행하는 중입니다.
  - **Coordination(조정):** 연구소와 CMVP가 발견된 문제를 해결하는 중입니다.
  - **Finalization(최종 승인):** 인증서 발급과 관련된 활동 및 절차입니다.
- CMVP의 검증 후 해당 모듈은 준수 인증서를 받고 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)에 추가되며, 여기에는 다음이 포함됩니다.
  - 검증된 모듈은 활성으로 표시됩니다.
  - 5년이 지나면 모듈이 이전으로 표시됩니다.
  - 어떤 이유에서든 모듈 인증서가 파기된 경우 파기로 표시됩니다.

2020년, CMVP는 FIPS 140-3의 기반으로 국제 표준인 ISO/IEC 19790을 채택했습니다.

FIPS 140-3 인증

현재 상태

iOS 14(2020년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

iOS 15(2021년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 거치는 중이며, Implementation Under Test List(테스트 중인 구현 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iOS 15 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iOS 15 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iOS 15와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14) **전반적인 보안 수준:** 2
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iOS 15와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A13, A14, A15) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iOS 14 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iOS 14 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iOS 14와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14) **전반적인 보안 수준:** 2
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iOS 14와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A13-A14) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3

FIPS 140-2 인증

아래 표에는 FIPS 140-2를 준수하여 현재 연구소에서 테스트 중이거나 테스트가 완료된 암호화 모듈이 표시됩니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3856 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v10.0 **운영 체제:** iOS 13 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3855 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v10.0 **운영 체제:** iOS 13 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-02-05	**인증서:** 3811 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v10.0 **운영 체제:** iOS 13과 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2018 **검증일:** 2019-04-23	**인증서:** 3438 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v9.0 **운영 체제:** iOS 12 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-04-11	**인증서:** 3433 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v9.0 **운영 체제:** iOS 12 **유형:** 소프트웨어 **보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2018 **검증일:** 2019-09-10	**인증서:** 3523 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v9.0 **운영 체제:** iOS 12와 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-22, 2018-07-06	**인증서:** 3148 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v8.0 **운영 체제:** iOS 11 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-17, 2018-07-03	**인증서:** 3147 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v8.0 **운영 체제:** iOS 11 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2019-09-10	**인증서:** 3223 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v1.0 **운영 체제:** iOS 11과 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2016 **검증일:** 2017-02-01	**인증서:** 2828 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple iOS Corecrypto Kernel Module v7.0 **운영 체제:** iOS 10 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2016 **검증일:** 2017-02-01	**인증서:** 2827 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple iOS Corecrypto Kernel Module v7.0 **운영 체제:** iOS 10 **유형:** 소프트웨어 **보안 수준:** 1

이전 버전

5년이 지난 인증서는 CMVP에 다음과 같이 이전 상태로 표시됩니다. 아래와 같은 이전 iOS 버전은 암호화 모듈 검증을 거쳤습니다.

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

CC(Common Criteria) 인증 배경

Apple은 운영 체제의 주요 릴리즈마다 iOS 평가에 적극적으로 참여합니다. 평가는 공개적으로 릴리즈된 운영 체제의 최종 버전에 대해서만 수행할 수 있습니다. iPadOS 13.1 이전에는 iPadOS의 이름이 iOS였습니다.

CC(Common Criteria) 인증 상태

NIAP에서 운영하는 미국의 제도는 Products in Evaluation(평가 중인 제품) 목록을 유지합니다. 이 목록에는 현재 미국에서 NIAP의 승인을 받은 CCTL(Common Criteria Testing Laboratory)과 함께 평가가 진행 중인 제품 및 CCEVS 경영진이 공식적으로 제품 평가를 수락하는 평가 킥오프 미팅 또는 이에 준하는 회의를 완료한 제품이 포함됩니다.

NIAP는 제품이 인증된 후 Product Compliant list(제품 준수 목록)에 현재 유효한 인증을 추가합니다. 2년 후에 해당 인증이 현재 보증 유지 관리 정책을 준수하는지 검토합니다. NIAP는 보증 유지 관리 날짜가 만료된 후 인증 목록을 Archived Products list(저장된 제품 목록)로 이동시킵니다.

Common Criteria Portal에서는 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증을 나열합니다. CC Portal은 인증된 제품 목록에 5년 동안 제품을 유지할 수 있고, 기록은 CC Portal의 Archived Certifications(저장된 인증)로 보관됩니다.

아래 표에는 현재 연구소에서 평가 중인 인증, 또는 CC를 준수하는 것으로 인증된 인증이 표시됩니다.

현재 상태

NIAP와 함께 iOS 15에 대한 연구소 테스트가 진행 중입니다. 최신 정보는 NIAP의 Products in Evaluation(평가 중인 제품) 및 Product Compliant List(제품 준수 목록)를 참조하십시오.

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: iOS 15 **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** —	**제목:** Apple iOS 15: iPhone **보호 프로파일:** 모바일 기기 기본 기능 (PP-모듈 확인 예정)
운영 체제: iOS 14 **인증 날짜:** 2021-09-01	**스키마 ID:** 11146 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple iOS 14: iPhone **보호 프로파일:** 모바일 기기 기본 기능, vPN 클라이언트 모듈, WLAN 클라이언트 PP 모듈, MDM Agent EP
운영 체제: iOS 13 **인증 날짜:** 2020-11-06	**스키마 ID:** 11036 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** iPhone에 설치된 Apple iOS 13 **보호 프로파일:** 모바일 기기 기본 기능, vPN 클라이언트 모듈, WLAN 클라이언트 EP, MDM Agent EP

iOS용 저장된 CC 인증

아래와 같은 이전 iOS 버전은 CC 검증을 거쳤습니다. 해당 버전은 NIAP 정책에 따라 NIAP에서 보관합니다.

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: iOS 12 **인증 날짜:** 2019-03-14	**스키마 ID:** 10937 **문서:** 보안 대상 지침	**제목:** iOS 12가 설치된 iPhone **보호 프로파일:** 모바일 기기 기본 기능, vPN 클라이언트 모듈, 무선 LAN 클라이언트 EP, MDM Agent EP
운영 체제: iOS 11 **인증 날짜:** 2018-07-17	**스키마 ID:** 10851 **문서:** 보안 대상 지침	**제목:** Apple iOS 11 **보호 프로파일:** 모바일 기기 기본 기능, 무선 LAN 클라이언트 EP, MDM Agent EP
운영 체제: iOS 10 **인증 날짜:** 2017-07-27	**스키마 ID:** 10782 **문서:** 보안 대상, 지침	**제목:** iPhone 및 iPad 기기의 iOS 10.2 **보호 프로파일:** 모바일 기기 기본 기능, 무선 LAN 클라이언트 EP, MDM Agent EP
운영 체제: iOS 10 **인증 날짜:** 2017-07-27	**스키마 ID:** 10792 **문서:** 보안 대상, 지침	**제목:** iPhone 및 iPad의 iOS 10.2 vPN 클라이언트 **보호 프로파일:** vPN 클라이언트 PP
운영 체제: iOS 9 **인증 날짜:** 2016-10-14	**스키마 ID:** 10725 **문서:** 보안 대상, 지침	**제목:** MDM Agent가 설치된 iOS 9.3.2 **보호 프로파일:** 모바일 기기 기본 기능, MDM Agent EP
운영 체제: iOS 9 **인증 날짜:** 2016-10-13	**스키마 ID:** 10714 **문서:** 보안 대상, 지침	**제목:** iPhone 및 iPad의 OS vPN 클라이언트 **보호 프로파일:** vPN 클라이언트 PP
운영 체제: iOS 9 **인증 날짜:** 2016-01-28	**스키마 ID:** 10695 **문서:** 보안 대상, 지침	**제목:** iOS 9 **보호 프로파일:** 모바일 기기 기본 기능

iPadOS용 보안 인증

iPadOS 인증 배경

Apple은 적합한 협업 보호 프로파일 및 FIPS 140-3 보안 수준을 사용하여 운영 체제의 주요 릴리즈마다 Apple 운영 체제 검증을 적극적으로 수행합니다. 준수 검증은 최종 릴리즈 버전을 대상으로만 수행할 수 있습니다.

참고: 2019년, iPad 기기의 운영 체제가 iPadOS로 새롭게 변경되었습니다. iPadOS 13.1 이전에는 iPadOS의 이름이 iOS였습니다.

iPadOS 암호화 모듈 검증 상태

CMVP(Cryptographic Module Validation Program)는 현재 상태에 따라 세 개의 개별 목록하에 암호화 모듈의 검증 상태를 유지합니다.

- CMVP Implementation Under Test List(테스트 중인 구현 목록)에 표시되려면 연구소는 Apple과 계약하여 테스트를 진행해야 합니다.
- 연구소의 테스트가 완료된 후 해당 연구소는 CMVP의 검증을 권장하고, CMVP 수수료를 지불한 다음 해당 모듈이 MIP(Modules in Process) List(처리 중인 모듈 목록)에 추가됩니다. MIP 목록은 다음의 4단계로 CMVP 검증 활동의 진행 상황을 추적합니다.
  - **Review Pending(검토 대기):** CMVP 담당자 할당을 기다리는 중입니다.
  - **In Review(검토 중):** CMVP 담당자가 검증 활동을 수행하는 중입니다.
  - **Coordination(조정):** 연구소와 CMVP가 발견된 문제를 해결하는 중입니다.
  - **Finalization(최종 승인):** 인증서 발급과 관련된 활동 및 절차입니다.
- CMVP의 검증 후 해당 모듈은 준수 인증서를 받고 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)에 추가되며, 여기에는 다음이 포함됩니다.
  - 검증된 모듈은 활성으로 표시됩니다.
  - 5년이 지나면 모듈이 이전으로 표시됩니다.
  - 어떤 이유에서든 모듈 인증서가 파기된 경우 파기로 표시됩니다.

2020년, CMVP는 FIPS 140-3의 기반으로 국제 표준인 ISO/IEC 19790을 채택했습니다.

FIPS 140-3 인증

현재 상태

iPadOS 14(2020년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

iPadOS 15(2021년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 거치는 중이며, Implementation Under Test List(테스트 중인 구현 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iPadOS 15 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iPadOS 15 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iPadOS 15와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14, M1) **전반적인 보안 수준:** 2
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** iPadOS 15와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14, M1) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iPadOS 14 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iPadOS 14 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iPadOS 14와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14, M1) **전반적인 보안 수준:** 2
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** iPadOS 14와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(A9-A14, M1) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3

FIPS 140-2 인증

아래 표에는 FIPS 140-2를 준수하여 현재 연구소에서 테스트 중이거나 테스트가 완료된 암호화 모듈이 표시됩니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3856 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v10.0 **운영 체제:** iPadOS 13 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3855 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v10.0 **운영 체제:** iPadOS 13 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-02-05	**인증서:** 3811 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Secure Key Store Cryptographic Module v10.0 **운영 체제:** iPadOS 13과 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2018 **검증일:** 2019-04-23	**인증서:** 3438 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v9.0 **운영 체제:** iOS 12 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-04-11	**인증서:** 3433 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v9.0 **운영 체제:** iOS 12 **유형:** 소프트웨어 **보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2018 **검증일:** 2019-09-10	**인증서:** 3523 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v9.0 **운영 체제:** iOS 12와 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-22, 2018-07-06	**인증서:** 3148 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v8.0 **운영 체제:** iOS 11 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-17, 2018-07-03	**인증서:** 3147 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v8.0 **운영 체제:** iOS 11 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2019-09-10	**인증서:** 3223 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v1.0 **운영 체제:** iOS 11과 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2016 **검증일:** 2017-02-01	**인증서:** 2828 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple iOS Corecrypto Kernel Module v7.0 **운영 체제:** iOS 10 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2016 **검증일:** 2017-02-01	**인증서:** 2827 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple iOS Corecrypto Kernel Module v7.0 **운영 체제:** iOS 10 **유형:** 소프트웨어 **보안 수준:** 1

이전 버전

5년이 지난 인증서는 CMVP에 다음과 같이 이전 상태로 표시됩니다. 아래와 같은 이전 iOS 버전은 암호화 모듈 검증을 거쳤습니다.

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

CC(Common Criteria) 인증 배경

Apple은 운영 체제의 주요 릴리즈마다 iPadOS 평가에 적극적으로 참여합니다. 평가는 공개적으로 릴리즈된 운영 체제의 최종 버전에 대해서만 수행할 수 있습니다.

CC(Common Criteria) 인증 상태

NIAP에서 운영하는 미국의 제도는 Products in Evaluation(평가 중인 제품) 목록을 유지합니다. 이 목록에는 현재 미국에서 NIAP의 승인을 받은 CCTL(Common Criteria Testing Laboratory)과 함께 평가가 진행 중인 제품 및 CCEVS 경영진이 공식적으로 제품 평가를 수락하는 평가 킥오프 미팅 또는 이에 준하는 회의를 완료한 제품이 포함됩니다.

NIAP는 제품이 인증된 후 Product Compliant list(제품 준수 목록)에 현재 유효한 인증을 추가합니다. 2년 후에 해당 인증이 현재 보증 유지 관리 정책을 준수하는지 검토합니다. NIAP는 보증 유지 관리 날짜가 만료된 후 인증 목록을 Archived Products list(저장된 제품 목록)로 이동시킵니다.

Common Criteria Portal에서는 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증을 나열합니다. CC Portal은 인증된 제품 목록에 5년 동안 제품을 유지할 수 있고, 기록은 CC Portal의 Archived Certifications(저장된 인증)로 보관됩니다.

아래 표에는 현재 연구소에서 평가 중인 인증, 또는 CC를 준수하는 것으로 인증된 인증이 표시됩니다.

현재 상태

NIAP와 함께 iPadOS 15에 대한 연구소 테스트가 진행 중입니다. 최신 정보는 NIAP의 Products in Evaluation(평가 중인 제품) 및 Product Compliant List(제품 준수 목록)를 참조하십시오.

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: iPadOS 15 **인증 날짜:** 2019-03-14	**스키마 ID:** — **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** iOS 12가 설치된 iPad **보호 프로파일:** 모바일 기기 기본 기능, vPN 클라이언트 모듈, 무선 LAN 클라이언트 EP, MDM Agent EP
운영 체제: iPadOS 14 **인증 날짜:** 2021-09-01	**스키마 ID:** 11147 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple iPadOS 14: iPad **보호 프로파일:** 모바일 기기 기본 기능, vPN 클라이언트 모듈, 무선 LAN 클라이언트 EP, MDM Agent EP
운영 체제: iPadOS 13 **인증 날짜:** 2020-11-06	**스키마 ID:** 11036 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** iPad 모바일 기기에 설치된 iPadOS 13 **보호 프로파일:** 모바일 기기 기본 기능, vPN 클라이언트 모듈, 무선 LAN 클라이언트 EP, MDM Agent EP

이전 버전

아래와 같은 이전 iOS 버전은 CC 검증을 거쳤습니다. 해당 버전은 NIAP 정책에 따라 NIAP에서 보관합니다.

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

macOS용 보안 인증

macOS 인증 배경

Apple은 적합한 협업 보호 프로파일 및 FIPS 140-3 보안 수준을 사용하여 운영 체제의 주요 릴리즈마다 Apple 운영 체제 검증을 적극적으로 수행합니다. 준수 검증은 최종 릴리즈 버전을 대상으로만 수행할 수 있습니다.

macOS 암호화 모듈 검증 상태

CMVP(Cryptographic Module Validation Program)는 현재 상태에 따라 세 개의 개별 목록하에 암호화 모듈의 검증 상태를 유지합니다.

- CMVP Implementation Under Test List(테스트 중인 구현 목록)에 표시되려면 연구소는 Apple과 계약하여 테스트를 진행해야 합니다.
- 연구소의 테스트가 완료된 후 해당 연구소는 CMVP의 검증을 권장하고, CMVP 수수료를 지불한 다음 해당 모듈이 MIP(Modules in Process) List(처리 중인 모듈 목록)에 추가됩니다. MIP 목록은 다음의 4단계로 CMVP 검증 활동의 진행 상황을 추적합니다.
  - **Review Pending(검토 대기):** CMVP 담당자 할당을 기다리는 중입니다.
  - **In Review(검토 중):** CMVP 담당자가 검증 활동을 수행하는 중입니다.
  - **Coordination(조정):** 연구소와 CMVP가 발견된 문제를 해결하는 중입니다.
  - **Finalization(최종 승인):** 인증서 발급과 관련된 활동 및 절차입니다.
- CMVP의 검증 후 해당 모듈은 준수 인증서를 받고 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)에 추가되며, 여기에는 다음이 포함됩니다.
  - 검증된 모듈은 활성으로 표시됩니다.
  - 5년이 지나면 모듈이 이전으로 표시됩니다.
  - 어떤 이유에서든 모듈 인증서가 파기된 경우 파기로 표시됩니다.

2020년, CMVP는 FIPS 140-3의 기반으로 국제 표준인 ISO/IEC 19790을 채택했습니다.

Apple Mac 컴퓨터와 관련하여 아래 표에는 Mac 기술에 적용 가능한 암호화 모듈이 표시됩니다.

암호화 모듈	Apple Silicon이 장착된 Mac 컴퓨터	Apple T2 보안 칩이 장착된 Mac 컴퓨터	Apple T2 보안 칩이 장착되지 않은 Intel 기반 Mac 컴퓨터
Apple Silicon User Space	✓		
Apple Silicon Kernel	✓		
Intel User Space		✓	✓
Intel Kernel		✓	✓
Secure Key Store	✓	✓	

FIPS 140-3 인증

2020년, Apple은 Apple Silicon을 기반으로 하는 Mac 컴퓨터를 출시했습니다. Apple Silicon 또는 Intel 기반 Mac 컴퓨터에 대한 암호화 모듈의 적용 가능성은 아래 표의 모듈 정보 열에 표시됩니다.

참고: Apple T2 보안 칩은 여러 Intel 기반 Mac 컴퓨터에 탑재되었습니다. T2 칩 인증에 대한 자세한 정보는 Apple T2 보안 칩용 보안 인증을 참조하십시오.

macOS ssh 클라이언트

선택된 FIPS 140-3 알고리즘과 대응하는 FIPS 140-3 검증 모듈을 사용하기 위해 OpenSSH를 구성할 수 있습니다. 기관은 서명되고 공증된 설치 프로그램(Apple에서 제공)을 비밀번호 **FIPS140Mode**로 실행할 수 있습니다. 설치 프로그램이 Mac에 다음의 두 파일을 설치합니다.

- **fips_ssh_config:** /Private/etc/ssh/ssh_config.d/에 위치함
- **fips_sshd_config:** /Private/etc/ssh/sshd_config.d/에 위치함

그런 다음 macOS는 이 파일들을 사용해 오직 NIST가 검증한 암호만을 OpenSSH에서 사용 가능하도록 제한하고, OpenSSH 클라이언트가 플랫폼에서 제공되고 확인된 암호화 모듈을 사용하도록 보장합니다. 관리자는 스스로 파일을 만들 수도 있습니다. 더 많은 정보를 보려면 macOS 12.0 이상의 `apple_ssh_and_fips` 매뉴얼 페이지를 참조하십시오.

현재 상태

macOS 11 Big Sur 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

macOS 12 Monterey 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 거치는 중이며, Implementation Under Test List(테스트 중인 구현 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** Apple Silicon 기반 macOS 12 Monterey **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** Apple Silicon 기반 macOS 12 Monterey **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** Intel 기반 macOS 12 Monterey **환경:** Intel, 사용자, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** Intel 기반 macOS 12 Monterey **환경:** Intel, 커널, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** Apple Silicon 기반에서 macOS 12 Monterey와 함께 배포된 sepOS, T2 칩 및 Intel 기반에서 macOS 12 Monterey와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(M1 및 T2) **보안 수준:** 2
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12.0 **운영 체제:** Apple Silicon 기반에서 macOS 12 Monterey와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(M1) **보안 수준:** 2 **물리적 보안 수준:** 3
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** Intel 기반 macOS 11 Big Sur **환경:** Intel, 사용자, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** Intel 기반 macOS 11 Big Sur **환경:** Intel, 커널, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** Apple Silicon 기반 macOS 11 Big Sur **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** Apple Silicon 기반 macOS 11 Big Sur **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** Apple Silicon 기반에서 macOS 11 Big Sur와 함께 배포된 sepOS, Intel 기반에서 macOS 11 Big Sur와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(M1) **보안 수준:** 2
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** Apple Silicon 기반에서 macOS 11 Big Sur와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(M1) **보안 수준:** 2 **물리적 보안 수준:** 3

FIPS 140-2 인증

아래 표에는 FIPS 140-2를 준수하여 현재 연구소에서 테스트 중이거나 테스트가 완료된 암호화 모듈이 표시됩니다.

macOS 10.15 Catalina 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

참고: Apple T2 보안 칩은 여러 Intel 기반 Mac 컴퓨터에 탑재되었습니다. T2 칩 인증에 대한 자세한 정보는 Apple T2 보안 칩용 보안 인증을 참조하십시오.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2019 **검증일:** 2021-03-24	**인증서:** 3859 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Intel용 Apple Corecrypto User Space Module(ccv10) **운영 체제:** macOS 10.15 Catalina **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-03-24	**인증서:** 3858 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Intel용 Apple Corecrypto Kernel Module v10.0(ccv10) **운영 체제:** macOS 10.15 Catalina **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-04-12	**인증서:** 3402 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Intel용 Apple Corecrypto User Module v9.0 **운영 체제:** macOS 10.14 Mojave **유형:** 소프트웨어 **보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2018 **검증일:** 2019-04-12	**인증서:** 3431 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Intel용 Apple Corecrypto Kernel Module v9.0 **운영 체제:** macOS 10.14 Mojave **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2018-03-22	**인증서:** 3155 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Intel용 Apple Corecrypto User Module v8.0 **운영 체제:** macOS 10.13 High Sierra **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2018-03-22	**인증서:** 3156 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Intel용 Apple Corecrypto Kernel Module v8.0 **운영 체제:** macOS 10.13 High Sierra **유형:** 소프트웨어 **보안 수준:** 1

이전 버전

이들 이전 OS X 및 macOS 버전은 암호화 모듈 검증이 있었습니다. 5년이 지난 암호화 모듈 검증은 CMVP에 다음과 같이 이전 상태로 표시됩니다.

- 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

CC(Common Criteria) 인증 배경

Apple은 운영 체제의 주요 릴리즈마다 macOS 평가에 적극적으로 참여합니다. 평가는 공개적으로 릴리즈된 운영 체제의 최종 버전에 대해서만 수행할 수 있습니다.

CC(Common Criteria) 인증 상태

NIAP에서 운영하는 미국의 제도는 Products in Evaluation(평가 중인 제품) 목록을 유지합니다. 이 목록에는 현재 미국에서 NIAP의 승인을 받은 CCTL(Common Criteria Testing Laboratory)과 함께 평가가 진행 중인 제품 및 CCEVS 경영진이 공식적으로 제품 평가를 수락하는 평가 킥오프 미팅 또는 이에 준하는 회의를 완료한 제품이 포함됩니다.

NIAP는 제품이 인증된 후 Product Compliant list(제품 준수 목록)에 현재 유효한 인증을 추가합니다. 2년 후에 해당 인증이 현재 보증 유지 관리 정책을 준수하는지 검토합니다. NIAP는 보증 유지 관리 날짜가 만료된 후 인증 목록을 Archived Products List(저장된 제품 목록)로 이동시킵니다.

Common Criteria Portal에서는 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증을 나열합니다. CC Portal은 인증된 제품 목록에 5년 동안 제품을 유지할 수 있고, 기록은 CC Portal의 Archived Certifications(저장된 인증)로 보관됩니다.

아래 표에는 현재 연구소에서 평가 중인 인증, 또는 CC를 준수하는 것으로 인증된 인증이 표시됩니다.

현재 상태

NIAP와 함께 General Purpose Operating System 및 전체 디스크 암호화(FDE)(AA 및 EE) 보호 프로파일을 사용하는 macOS 11 및 macOS 12 평가가 진행 중입니다.

최신 정보는 NIAP의 Products in Evaluation(평가 중인 제품) 및 Product Compliant List(제품 준수 목록)를 참조하십시오.

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: macOS 12 Monterey **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** —	**제목:** macOS 12 Monterey를 실행하는 Apple FileVault 2 **보호 프로파일:** CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E(PP 확인 예정)
운영 체제: macOS 12 Monterey **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** —	**제목:** macOS 12 Monterey **보호 프로파일:** PP_OS_V4.21(PP 확인 예정)
운영 체제: macOS 11 Big Sur **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** macOS 11 Big Sur를 실행하는 Apple FileVault 2 **보호 프로파일:** CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
운영 체제: macOS 11 Big Sur **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple macOS 11 Big Sur **보호 프로파일:** PP_OS_V4.21

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: macOS 10.15 Catalina **인증 날짜:** 2021-04-29	**스키마 ID:** 11078 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** macOS 10.15 Catalina를 실행하는 T2 컴퓨터의 Apple FileVault 2 **보호 프로파일:** CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
운영 체제: macOS 10.15 Catalina **인증 날짜:** 2020-09-23	**스키마 ID:** 11077 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** macOS 10.15 Catalina **보호 프로파일:** PP_OS_V4.21

tvOS용 보안 인증

tvOS 인증 배경

Apple은 주요 tvOS 릴리즈마다 암호화 모듈 검증을 적극적으로 수행합니다. 준수 검증은 최종 릴리즈 버전을 대상으로만 수행할 수 있습니다.

tvOS 암호화 모듈 검증 상태

CMVP(Cryptographic Module Validation Program)는 현재 상태에 따라 세 개의 개별 목록하에 암호화 모듈의 검증 상태를 유지합니다.

- CMVP Implementation Under Test List(테스트 중인 구현 목록)에 표시되려면 연구소는 Apple과 계약하여 테스트를 진행해야 합니다.
- 연구소의 테스트가 완료된 후 해당 연구소는 CMVP의 검증을 권장하고, CMVP 수수료를 지불한 다음 해당 모듈이 MIP(Modules in Process) List(처리 중인 모듈 목록)에 추가됩니다. MIP 목록은 다음의 4단계로 CMVP 검증 활동의 진행 상황을 추적합니다.
  - **Review Pending(검토 대기):** CMVP 담당자 할당을 기다리는 중입니다.
  - **In Review(검토 중):** CMVP 담당자가 검증 활동을 수행하는 중입니다.
  - **Coordination(조정):** 연구소와 CMVP가 발견된 문제를 해결하는 중입니다.
  - **Finalization(최종 승인):** 인증서 발급과 관련된 활동 및 절차입니다.
- CMVP의 검증 후 해당 모듈은 준수 인증서를 받고 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)에 추가되며, 여기에는 다음이 포함됩니다.
  - 검증된 모듈은 활성으로 표시됩니다.
  - 5년이 지나면 모듈이 이전으로 표시됩니다.
  - 어떤 이유에서든 모듈 인증서가 파기된 경우 파기로 표시됩니다.

2020년, CMVP는 FIPS 140-3의 기반으로 국제 표준인 ISO/IEC 19790을 채택했습니다.

FIPS 140-3 인증

현재 상태

tvOS 14(2020년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

tvOS 15(2021년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 거치는 중이며, Implementation Under Test List(테스트 중인 구현 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** tvOS 15 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** tvOS 15 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** tvOS 15와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** Hardware (A10, A12) **전반적인 보안 수준:** 2
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** tvOS 14 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** tvOS 14 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** tvOS 14와 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** Hardware (A10, A12) **전반적인 보안 수준:** 2

FIPS 140-2 인증

아래 표에는 FIPS 140-2를 준수하여 현재 연구소에서 테스트 중이거나 테스트가 완료된 암호화 모듈이 표시됩니다.

tvOS 13(2019년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3856 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v10.0 **운영 체제:** tvOS 13 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-03-23	**인증서:** 3855 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v10.0 **운영 체제:** tvOS 13 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-02-05	**인증서:** 3811 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v10.0 **운영 체제:** tvOS 13과 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2018 **검증일:** 2019-04-23	**인증서:** 3438 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v9.0 **운영 체제:** tvOS 12 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-04-11	**인증서:** 3433 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v9.0 **운영 체제:** tvOS 12 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-09-10	**인증서:** 3523 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v9.0 **운영 체제:** tvOS 12와 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-22, 2018-07-06	**인증서:** 3148 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v8.0 **운영 체제:** tvOS 11 **유형:** 소프트웨어 **보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-17, 2018-07-03	**인증서:** 3147 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v8.0 **운영 체제:** tvOS 11 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2019-09-10	**인증서:** 3223 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v1.0 **운영 체제:** tvOS 11과 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2

watchOS용 보안 인증

watchOS 인증 배경

Apple은 주요 watchOS 릴리즈마다 암호화 모듈 검증을 적극적으로 수행합니다. 준수 검증은 최종 릴리즈 버전을 대상으로만 수행할 수 있습니다.

watchOS 암호화 모듈 검증 상태

CMVP(Cryptographic Module Validation Program)는 현재 상태에 따라 세 개의 개별 목록하에 암호화 모듈의 검증 상태를 유지합니다.

- CMVP Implementation Under Test List(테스트 중인 구현 목록)에 표시되려면 연구소는 Apple과 계약하여 테스트를 진행해야 합니다.
- 연구소의 테스트가 완료된 후 해당 연구소는 CMVP의 검증을 권장하고, CMVP 수수료를 지불한 다음 해당 모듈이 MIP(Modules in Process) List(처리 중인 모듈 목록)에 추가됩니다. MIP 목록은 다음의 4단계로 CMVP 검증 활동의 진행 상황을 추적합니다.
  - **Review Pending(검토 대기):** CMVP 담당자 할당을 기다리는 중입니다.
  - **In Review(검토 중):** CMVP 담당자가 검증 활동을 수행하는 중입니다.
  - **Coordination(조정):** 연구소와 CMVP가 발견된 문제를 해결하는 중입니다.
  - **Finalization(최종 승인):** 인증서 발급과 관련된 활동 및 절차입니다.
- CMVP의 검증 후 해당 모듈은 준수 인증서를 받고 Validated Cryptographic Modules List(검증된 암호화 모듈 목록)에 추가되며, 여기에는 다음이 포함됩니다.
  - 검증된 모듈은 활성으로 표시됩니다.
  - 5년이 지나면 모듈이 이전으로 표시됩니다.
  - 어떤 이유에서든 모듈 인증서가 파기된 경우 파기로 표시됩니다.

2020년, CMVP는 FIPS 140-3의 기반으로 국제 표준인 ISO/IEC 19790을 채택했습니다.

FIPS 140-3 인증

현재 상태

watchOS 7(2020년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 완료했고 CMVP의 검증을 받도록 권장되었습니다. Modules in Process List(처리 중인 모듈 목록)에 표시되어 있습니다.

watchOS 8(2021년) 사용자 공간, 커널 공간 및 보안 키 저장소는 연구소에서 테스트를 거치는 중이며, Implementation Under Test List(테스트 중인 구현 목록)에 표시되어 있습니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** watchOS 8 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** watchOS 8 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** watchOS 8과 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(S3, S4, S5, S6) **전반적인 보안 수준:** 2
운영 체제 출시일: 2021 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v12 **운영 체제:** watchOS 8과 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(S6) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** watchOS 7 **환경:** Apple Silicon, 사용자, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** watchOS 7 **환경:** Apple Silicon, 커널, 소프트웨어 **유형:** 소프트웨어 **전반적인 보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** watchOS 7과 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(S3, S4, S5, S6) **전반적인 보안 수준:** 2
운영 체제 출시일: 2020 **검증일:** —	**인증서:** 인증받지 않음 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Corecrypto Module v11.1 **운영 체제:** watchOS 7과 함께 배포된 sepOS **환경:** Apple Silicon, 보안 키 저장소, 하드웨어 **유형:** 하드웨어(S6) **전반적인 보안 수준:** 2 **물리적 보안 수준:** 3

FIPS 140-2 인증

아래 표에는 FIPS 140-2를 준수하여 현재 연구소에서 테스트 중이거나 테스트가 완료된 암호화 모듈이 표시됩니다.

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2019 **검증일:** —	**인증서:** 3856 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v10.0 **운영 체제:** watchOS 6 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** —	**인증서:** 3855 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v10.0 **운영 체제:** watchOS 6 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2019 **검증일:** 2021-02-05	**인증서:** 3811 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v10.0 **운영 체제:** watchOS 6와 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2018 **검증일:** 2019-04-23	**인증서:** 3438 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v9.0 **운영 체제:** watchOS 5 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2018 **검증일:** 2019-04-11	**인증서:** 3433 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v9.0 **운영 체제:** watchOS 5 **유형:** 소프트웨어 **보안 수준:** 1

날짜	인증서 / 문서	모듈 정보
운영 체제 출시일: 2018 **검증일:** 2019-09-10	**인증서:** 3523 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v9.0 **운영 체제:** watchOS 5와 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-22, 2018-07-06	**인증서:** 3148 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto User Module v8.0 **운영 체제:** watchOS 4 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2018-03-09, 2018-05-17, 2018-07-03	**인증서:** 3147 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** ARM용 Apple Corecrypto Kernel Module v8.0 **운영 체제:** watchOS 4 **유형:** 소프트웨어 **보안 수준:** 1
운영 체제 출시일: 2017 **검증일:** 2019-09-10	**인증서:** 3223 **문서:** 인증서 보안 정책 암호화 책임자 지침	**제목:** Apple Secure Key Store Cryptographic Module v1.0 **운영 체제:** watchOS 4와 함께 배포된 sepOS **유형:** 하드웨어 **보안 수준:** 2

소프트웨어 보안 인증

Apple 소프트웨어 보안 인증 개요

Apple은 sepOS 및 T2 펌웨어에 대한 미국 FIPS(Federal Information Processing Standard) 140-2/-3 준수 검증 인증 및 기타 인증을 유지합니다. Apple은 적합한 여러 플랫폼에 광범위하게 적용되는 **인증 빌딩 블록**으로 시작합니다. 첫 번째 빌딩 블록은 Apple에서 개발한 운영 체제 내 소프트웨어 및 하드웨어 암호화 모듈 배포에 사용되는 corecrypto 검증입니다. 두 번째 빌딩 블록은 많은 Apple 기기에 내장된 Secure Enclave 인증입니다. 세 번째는 Touch ID가 있는 Apple 기기 및 Face ID가 있는 기기에 적용된 Secure Element(SE) 인증입니다. 이러한 하드웨어 인증 빌딩 블록은 광범위한 플랫폼 보안 인증의 기반을 형성합니다.

제품 인증: CC(ISO/IEC 15408)

CC(ISO/IEC 15408)는 여러 기관에서 IT 제품의 보안 평가의 기반으로 사용하는 표준입니다.

국제 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증에 대해서는 Common Criteria Portal을 참조하십시오. CC 표준은 국가 및 민간 검증 체계에 의해 CCRA 외부에서도 사용될 수 있습니다. 유럽에서 상호 인정은 SOG-IS 합의 및 CCRA를 따릅니다.

CC 커뮤니티에서 언급한 바와 같이, 국제적으로 승인된 보안 표준 집합을 사용하여 정보 기술 제품의 보안 기능에 대한 명확하고 신뢰할 수 있는 평가 방식을 제공하는 것이 목표입니다. CC는 제품의 보안 표준 준수 능력에 대한 독자적 평가를 제공함으로써 고객에게 정보 기술 제품의 보안에 대한 확신을 주며 더 많은 정보에 입각한 결정을 유도합니다.

CCRA를 통해 회원 국가는 동일한 수준의 신뢰도를 가진 정보 기술 제품의 인증을 인정하는 데 합의했습니다. 인증 전에 필요한 평가는 광범위하며 다음을 포함합니다.

- 보호 프로파일(PP)
- 보안 대상(ST)
- 보안 기능 요구 사항(SFR)
- 보안 보증 요구 사항(SAR)
- EAL(Evaluation Assurance Levels)

보호 프로파일(PP)은 휴대성과 같은 기기 유형의 클래스에 대한 보안 요구 사항을 명시하는 문서로, 동일한 클래스 내에서의 IT 제품 평가 간 비교 가능성을 제공하는 데 사용됩니다. 늘어나는 승인된 PP 목록과 더불어 CCRA 멤버십 수가 매년 계속해서 증가하고 있습니다. 이 협정은 제품 개발자가 인증서 인증 체계 중 하나에 따라 단일 인증을 실행할 수 있도록 허용하며, 제품 개발자는 인증서를 수용하는 합의국 중 어떤 국가에서든 인정을 받을 수 있습니다.

보안 대상(ST)은 IT 제품 인증 시 평가할 **항목**을 정의합니다. ST는 더 구체적으로 **보안 기능 요구 사항(SFR)**으로 변환되며, ST를 더 상세하게 평가하는 데 사용됩니다.

또한 CC(Common Criteria)는 **보안 보증 요구 사항**을 포함합니다. 일반적으로 식별되는 지표 중 하나는 **EAL(Evaluation Assurance Levels)**입니다. EAL은 자주 발생하는 일련의 SAR을 그룹화하고, 비교 가능성을 지원하기 위해 PP 및 ST에 명시될 수 있습니다.

대다수의 이전 PP는 보관소에 저장되었으며 특정 솔루션 및 환경에 중점을 두고 개발되는 대상 PP로 대체되고 있습니다. 모든 CCRA 회원들 간에 지속적인 상호 인정을 보장하기 위한 공동의 노력으로, iTC(국제 기술 커뮤니티)는 처음부터 CCRA 합의국 제도의 참여로 개발된 cPP(공동 보호 프로파일)를 개발하고 유지하기 위해 설립되었습니다. CCRA 외에 사용자 그룹 및 상호 인정 협정을 대상으로 하는 PP는 적합한 이해 당사자가 계속 개발하고 있습니다.

2015년 초부터 Apple은 업데이트된 CCRA하에 엄선된 cPP로 인증을 진행해 왔습니다. 그 이후로 Apple은 주요 iOS 릴리즈마다 CC 인증을 받아왔으며 적용 범위를 확대하여 새로운 PP가 제공하는 보안 보증을 포함시켰습니다.

Apple은 모바일 보안 기술 평가에 중점을 둔 기술 커뮤니티 내에서 적극적 역할을 수행합니다. 여기에는 cPP를 개발하고 업데이트하는 iTC가 포함됩니다. Apple은 현재 PP 및 cPP에 대해 평가하고 인증을 받기 위해 계속 노력하고 있습니다.

일반적으로 북미 시장에서의 Apple 플랫폼 인증은, 아직 인증되지 않았으나 현재 평가 중인 프로젝트 목록을 유지하는 NIAP(National Information Assurance Partnership)를 통해 수행됩니다.

나열된 일반 플랫폼 인증서 외에도 일부 시장에 대한 특정 보안 요구 사항을 입증하기 위해 다른 인증서가 발급되었습니다.

Apple 앱의 보안 인증

Apple 앱 인증 배경

Apple은 적합한 CCPP(국제 공통 보호 프로파일)를 사용하여 Apple 앱의 보안 인증에 적극적으로 참여합니다. 이 평가는 Apple이 얻은 하드웨어 및 운영 체제 인증을 기반으로 합니다.

2018년, Apple은 Safari 브라우저 및 연락처 앱과 함께 iOS 11에서 실행되는 주요 응용 프로그램에 대한 보안 평가를 시작했습니다. Apple은 iOS 12, iOS 13 및 iPadOS 13.1에서 실행되는 앱을 대상으로 해당 평가를 계속해 왔습니다. 2021년에는 macOS 11에서 실행되는 앱이 평가 대상에 포함됩니다.

암호화 모듈 인증 상태

이 목록에 있는 Apple 앱은 해당 운영 체제의 암호화 모듈을 사용합니다. 추가 정보를 보려면 iOS용 보안 인증, iPadOS용 보안 인증 및 macOS용 보안 인증을 참조하십시오.

CC(Common Criteria) 인증 상태

NIAP에서 운영하는 미국의 제도는 Products in Evaluation(평가 중인 제품) 목록을 유지합니다. 이 목록에는 현재 미국에서 NIAP의 승인을 받은 CCTL(Common Criteria Testing Laboratory)과 함께 평가가 진행 중인 제품 및 CCEVS 경영진이 공식적으로 제품 평가를 수락하는 평가 킥오프 미팅 또는 이에 준하는 회의를 완료한 제품이 포함됩니다.

NIAP는 제품이 인증된 후 Product Compliant list(제품 준수 목록)에 현재 유효한 인증을 추가합니다. 2년 후에 해당 인증이 현재 보증 유지 관리 정책을 준수하는지 검토합니다. NIAP는 보증 유지 관리 날짜가 만료된 후 인증 목록을 Archived Products list(저장된 제품 목록)로 이동시킵니다.

Common Criteria Portal에서는 CCRA(국제상호인정협정)에 따라 상호 인정될 수 있는 인증을 나열합니다. CC Portal은 인증된 제품 목록에 5년 동안 제품을 유지할 수 있고, 기록은 CC Portal의 Archived Certifications(저장된 인증)로 보관됩니다.

아래 표에는 현재 연구소에서 평가 중인 인증, 또는 CC를 준수하는 것으로 인증된 인증이 표시됩니다.

현재 상태

- NIAP와 함께 평가가 진행 중인 경우 NIAP의 Products in Evaluation(평가 중인 제품)에 나열됩니다.
- 완료되고 검증을 마친 평가는 NIAP의 Product Compliant List(제품 준수 목록)에 나열됩니다.

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: macOS 11 Big Sur **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** macOS 11 Big Sur: 연락처 **보호 프로파일:** 응용 프로그램 소프트웨어용 PP, 웹 브라우저용 EP
운영 체제: macOS 11 Big Sur **인증 날짜:** —	**스키마 ID:** 인증받지 않음 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** macOS 11 Big Sur: Safari **보호 프로파일:** 응용 프로그램 소프트웨어용 PP, 웹 브라우저용 EP

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: iOS 14, iPadOS 14 **인증 날짜:** 2021-08-20	**스키마 ID:** 11191 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple iOS 14 및 iPadOS 14: 연락처 **보호 프로파일:** 응용 프로그램 소프트웨어용 PP, 웹 브라우저용 EP
운영 체제: iOS 14, iPadOS 14 **인증 날짜:** —	**스키마 ID:** 11192 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple iOS 14 및 iPadOS 14: Safari **보호 프로파일:** 응용 프로그램 소프트웨어용 PP, 웹 브라우저용 EP
운영 체제: iOS 13, iPadOS 13 **인증 날짜:** 2020-06-05	**스키마 ID:** 11060 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple iOS 13 및 iPadOS 13: Safari **보호 프로파일:** 응용 프로그램 소프트웨어용 PP, 웹 브라우저용 EP
운영 체제: iOS 13, iPadOS 13 **인증 날짜:** 2020-06-05	**스키마 ID:** 11050 **문서:** 인증서 보안 대상 지침 유효성 확인 리포트 보증 활동 리포트	**제목:** Apple iOS 13 및 iPadOS 13: 연락처 **보호 프로파일:** 응용 프로그램 소프트웨어용 PP

Apple 앱의 저장된 CC 인증

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: iOS 12 **인증 날짜:** 2019-06-12	**스키마 ID:** 10960 **문서:** 보안 대상 지침	**제목:** iOS 12 Safari **보호 프로파일:** 응용 프로그램 소프트웨어용 PP, 웹 브라우저용 EP
운영 체제: iOS 12 **인증 날짜:** 2019-02-28	**스키마 ID:** 10961 **문서:** 보안 대상 지침	**제목:** iOS 12 연락처 **보호 프로파일:** 응용 프로그램 소프트웨어용 PP

운영 체제 / 인증 날짜	스키마 ID / 문서	제목 / 보호 프로파일
운영 체제: iOS 11 **인증 날짜:** 2018-11-09	**스키마 ID:** 10916 **문서:** 보안 대상 지침	**제목:** iOS 11 Safari **보호 프로파일:** 응용 프로그램 소프트웨어용 PP, 웹 브라우저용 EP
운영 체제: iOS 11 **인증 날짜:** 2018-09-13	**스키마 ID:** 10915 **문서:** 보안 대상 지침	**제목:** iOS 11 연락처 **보호 프로파일:** 응용 프로그램 소프트웨어용 PP

Apple 인터넷 서비스의 보안 인증

Apple은 ISO/IEC 27001 및 ISO/IEC 27018 표준을 준수하는 인증을 유지하여 Apple 고객이 규제 및 계약 의무를 이행할 수 있도록 합니다. 이러한 인증은 고객에게 범위 내의 시스템에 대한 Apple 정보 보안 및 개인 정보 보호 관행에 있어서 독자적 증명을 제공합니다.

ISO/IEC 27001 및 ISO/IEC 27018은 ISO(International Organization for Standardization)에서 발행된 ISMS(Information Security Management System) 표준의 제품군 일부입니다. Apple ISMS의 일부로써, ISO/IEC 27001 및 ISO/IEC 27018 표준 내에 정의된 대로 모든 Annex A 제어 요구 사항이 적용성 보고서(Statement of Applicability)에 포함되었습니다. Apple은 매년 공인 기관에서 독자적 증명을 받습니다.

ISO/IEC 27001

IISO/IEC 27001은 조직의 정보 보안 관리 시스템을 구축하고, 구현하며, 유지하고, 지속적으로 개선하기 위한 요구 사항을 규정하는 정보 보안 관리 시스템 표준입니다. ISO/IEC 27001 표준은 Apple의 ISO/IEC 인증이 적용된 다음의 보안 도메인을 포함합니다.

- 정보 보안 정책
- 정보 보안 조직
- 자산 관리
- 인적 자원 보안
- 물리적 보안 및 환경적 보안
- 통신 및 작업 관리
- 접근 제어
- 정보 시스템 획득, 개발 및 유지 관리
- 정보 보안 사고 관리
- 비즈니스 연속성 관리
- 준수

ISO/IEC 27018

ISO/IEC 27018은 공용 클라우드 환경에서 PII(개인 식별 정보)를 보호하기 위한 행동 강령입니다. ISO/IEC 27018 표준은 Apple의 ISO/IEC 인증이 적용된 다음의 보안 도메인을 포함합니다.

- 동의 및 선택
- 목적 적합성 및 기준
- 수집 제한
- 데이터 최소화
- 사용, 유지 및 공개 제한
- 정확성 및 품질
- 개방성, 투명성 및 알림
- 개별 참여 및 접근
- 책임성
- 정보 보안
- 개인 정보 보호 준수

ISO/IEC 27001 및 ISO/IEC 27018이 적용된 Apple 서비스

Apple의 ISO/IEC 27001 및 ISO/IEC 27018 인증은 다음의 서비스에 적용됩니다.

- Apple 비즈니스 채팅
- Apple Business Manager
- APNS(Apple 푸시 알림 서비스)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork 서비스
- 관리형 Apple ID
- 스쿨워크
- Siri

인증

Apple의 ISO/IEC 27001 및 27018 인증에 대한 증빙은 등록 기관에서 확인할 수 있습니다.

Apple의 인증을 확인하려면 BSI(British Standards Institution) 웹 사이트의 Certificate and Client Directory search 페이지로 이동하여 Company(기업) 검색 필드에 Apple을 입력하고, Search(검색) 버튼을 클릭한 다음, 검색 결과를 선택하여 인증서를 보십시오.

참고: Apple이 제조하지 않은 제품에 관한 정보 또는 Apple의 관리 또는 테스트 대상이 아닌 독립적인 웹 사이트는 권장 또는 보증 없이 제공되는 것입니다. Apple은 타사 웹 사이트 또는 제품에 대한 선택, 성능, 사용과 관련하여 발생하는 결과에 대해 책임을 지지 않습니다. Apple은 타사 웹 사이트의 정확성 또는 신뢰도에 대해 어떠한 언급도 하지 않습니다. 자세한 내용은 공급업체에 문의하십시오.

macOS 보안 준수 프로젝트

mSCP(macOS 보안 준수 프로젝트)는 보안 지침을 만드는 데 프로그래밍적인 접근 방법을 제공하기 위한 오픈 소스 작업입니다. 이는 NIST(미국 국립표준기술원), NASA(미국 항공우주국), DISA(미국 국방 정보 시스템 기구) 및 LANL(로스앨러모스 국립 연구소) 소속 연합 운영 IT 보안 전문가의 공동 프로젝트입니다. 본 프로젝트는 테스트를 거치고 검증된 macOS용 제어 모음을 사용하며, 프로젝트가 지원하는 모든 보안 지침에 대해 해당 제어의 세부 정보를 명시합니다. 또한 테스트를 거치고 검증된 원자 동작(구성 설정) 라이브러리를 활용하여 기술 보안 제어의 맞춤형 보안 기준을 쉽게 만들기 위한 리소스로 이 프로젝트를 사용할 수 있습니다. 본 프로젝트는 맞춤형 문서, 스크립트, 구성 프로파일 및 사용 기준에 기반한 검사 확인 목록을 산출합니다.

mSCP는 규정 준수를 목적으로 관리 및 보안 도구와 함께 사용할 출력 콘텐츠를 제작할 수 있습니다. 이 프로젝트의 구성 설정은 다음의 지침 기준을 지원합니다.

기관	지원되는 기준
NIST(미국 국립표준기술원) SP(특별 출판) 800-53, Recommended Security Controls for Federal Information Systems and Organizations(연방 정보 시스템 및 조직에 대한 권장 보안 제어), Revision 5	800-53 높음(High), 800-53 중간(Moderate), 800-53 낮음(Low)
NIST(미국 국립표준기술원) SP(특별 출판) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations(비연방 시스템 및 조직에서 제어되는 미분류 정보 보호) Rev.2	800-171
DISA(미국 국방 정보 시스템 기구) macOS 11 STIG, Apple macOS 11 보안 기술 구현 설명서	STIG
CNSSI(국가 보안 시스템 지침 위원회) 1253, Security Categorization and Control Selection for National Security Systems(비연방 시스템 및 조직에서 제어되는 미분류 정보 보호)	1253

추가 정보:

- 본 프로젝트의 모든 규정을 검토하기 위한 기준은 여기에서 찾아볼 수 있습니다.
- 본 프로젝트 및 사용법에 관해 더 알아보려면 macOS Security Compliance Project wiki를 참조하십시오.
- 본 프로젝트를 설정해 사용하려면 Getting to Know the macOS Security Compliance Project, Part 1 및 Getting to Know the macOS Security Compliance Project, Part 2를 참조하십시오.
- 본 프로젝트의 개발 지원에 관심이 있는 경우 기여자 지침을 참조하십시오.

문서 수정 내역

날짜	요약
2021년 10월 27일	업데이트된 주제: • Secure Enclave 프로세서의 보안 인증 • iOS용 보안 인증 • macOS용 보안 인증
2021년 8월 17일	업데이트된 주제: • Secure Enclave 프로세서의 보안 인증 • Apple T2 보안 칩용 보안 인증 • iOS용 보안 인증 • iPadOS용 보안 인증 • macOS용 보안 인증 • tvOS용 보안 인증 • watchOS용 보안 인증 • Apple 앱의 보안 인증 • 보안 인증 • macOS 보안 준수 프로젝트
2021년 4월 26일	추가된 주제: • macOS 보안 준수 프로젝트 업데이트된 주제: • Apple T2 보안 칩용 보안 인증: 새로운 FIPS 140-2 인증, 3811 • Secure Enclave 프로세서용 보안 인증: 새로운 FIPS 140-2 인증, 3811 및 추가 인증에 대한 새로운 표 • iOS용 보안 인증: 새로운 FIPS 140-2 인증, 3811, 평가 중인 iOS 14 스키마 ID 11146 • iPadOS용 보안 인증: 새로운 FIPS 140-2 인증, 3811, 평가 중인 iPadOS 14 스키마 ID 11147 • macOS용 보안 인증: 새로운 FIPS 140-2 인증, 3811. • tvOS용 보안 인증: 새로운 FIPS 140-2 인증, 3811. • watchOS용 보안 인증: 새로운 FIPS 140-2 인증, 3811. • Apple 앱의 보안 인증: CC 상태 관련 업데이트 및 저장된 CC 인증에 대한 새로운 표

용어집

보안 대상(ST) 특정 제품의 보안 문제 및 보안 요구 사항을 명시하는 문서.

보안 수준(SL) 적용 가능한 일련의 보안 요구 사항을 설명하기 위해 ISO/IEC 19790 내에 정의된 4개의 전체 보안 수준(1–4). 4수준은 가장 강력한 수준입니다.

보호 프로파일(PP) 특정 제품 클래스의 보안 문제 및 보안 요구 사항을 명시하는 문서.

암호화 모듈 암호화 기능을 제공하고 명시된 암호화 모듈 표준의 요구 사항에 부합하는 하드웨어, 소프트웨어 및/또는 펌웨어.

APNS(Apple 푸시 알림 서비스) 푸시 알림을 Apple 기기에 전달하는 Apple이 제공하는 전 세계적인 서비스.

Apple Business Manager 간편한 웹 기반의 IT 관리자용 포털로, Apple이나 프로그램에 참여하는 Apple 공인 대리점 또는 이동통신사를 통해 조직이 직접 구입한 Apple 기기를 빠르고 원활하게 배포할 수 있는 방법을 제공합니다. 사용자에게 기기를 할당하기 전에 조직은 기기를 직접 조작하거나 먼저 준비할 필요 없이 자동으로 MDM(Mobile Device Management) 솔루션에 기기를 등록할 수 있습니다.

Apple School Manager 간편한 웹 기반의 IT 관리자용 포털로, Apple이나 프로그램에 참여하는 Apple 공인 대리점 또는 이동통신사를 통해 조직이 직접 구입한 Apple 기기를 빠르고 원활하게 배포할 수 있는 방법을 제공합니다. 사용자에게 기기를 할당하기 전에 조직은 기기를 직접 조작하거나 먼저 준비할 필요 없이 자동으로 MDM(Mobile Device Management) 솔루션에 기기를 등록할 수 있습니다.

CAVP(Cryptographic Algorithm Validation Program) 승인된(예: FIPS 승인 및 NIST 권장) 암호화 알고리즘 및 개별 구성요소의 검증 테스트를 제공하기 위해 NIST에서 운영하는 조직.

CC(Common Criteria) IT 보안 평가의 일반적인 개념 및 원칙을 설정하고 일반 평가 모델을 명시하는 표준. 표준화된 언어로 된 보안 요구 사항 카탈로그가 포함되어 있습니다.

CCRA(국제상호인정협정) ISO/IEC 15408 시리즈 또는 CC 표준에 따라 발급된 인증서의 국제적 인정을 위해 정책 및 요구 사항을 설정하는 상호 인정 협정.

CMVP(Cryptographic Module Validation Program) FIPS 140-3 표준 준수를 검증하기 위해 미국 및 캐나다 정부에서 운영하는 조직.

corecrypto 낮은 수준의 암호화 프리미티브 구현을 제공하는 라이브러리. corecrypto는 개발자를 위한 프로그래밍 인터페이스를 직접 제공하지 않고 개발자에게 제공된 API를 통해 사용됩니다. corecrypto 소스 코드는 보안 특징 및 올바른 기능의 검증을 허용하기 위해 공개적으로 사용할 수 있습니다.

cPP(공동 보호 프로파일) cPP 생성을 담당한 전문가 그룹인 국제 기술 커뮤니티에서 개발한 보호 프로파일.

FDE(전체 디스크 암호화) 저장 장치 볼륨의 모든 데이터 암호화.

FIPS(Federal Information Processing Standard) 법령에서 요구하는 경우, 또는 사이버 보안에 대해 연방 정부의 강력한 요구 사항이 있는 경우, 또는 둘 다에 따라 미국 국립표준기술연구소가 개발한 발행물.

IPsec VPN 클라이언트 보호 프로파일에서 물리적 호스트 또는 가상 호스트 플랫폼과 원격 위치 간에 보안 IPsec 연결을 제공하는 클라이언트.

ISMS(정보 보안 관리 시스템) 정보 및/또는 시스템의 수명 주기 전반에 걸쳐 정보 보안을 체계적으로 관리하여 정보 및 시스템의 범위를 보호하도록 설계된 보안 프로그램의 경계를 통제하는 일련의 정보 보안 정책 및 절차.

iTC(국제 기술 커뮤니티) CCRA(국제상호인정협정)의 주최로 보호 프로파일 또는 공동 보호 프로파일 개발을 담당하는 단체.

IUT(Implementation under Test) 연구소에서 테스트 중인 암호화 모듈.

MDM(Mobile Device Management) 사용자가 등록된 기기를 원격으로 관리할 수 있는 서비스. 기기가 등록되면 사용자는 네트워크를 통해 MDM 서비스를 사용하여 사용자 상호 작용 없이 기기의 설정을 구성하고 다른 작업을 수행할 수 있습니다.

MIP(Modules in Process) CMVP(Cryptographic Module Validation Program)에서 유지하는, 현재 CMVP 검증 절차에 있는 암호화 모듈 목록.

NIAP(National Information Assurance Partnership) 미국 내 CC 표준을 구현하고 NIAP CCEVS(Common Criteria Evaluation and Validation Scheme) 관리를 담당하는 미국 정부 기관.

NIST(National Institute of Standards and Technology) 측정 과학, 표준 및 기술 발전을 담당하는 미국 상무부 산하 부서.

Secure Element(SE) 많은 Apple 기기에 내장되어 있으며 Apple Pay와 같은 기능을 지원하는 실리콘 칩.

Secure Enclave 프로세서(SEP) SoC(System On Chip)에 내장된 보조 프로세서.

sepOS L4 마이크로커널의 Apple 맞춤형 버전을 기반으로 하는 Secure Enclave 펌웨어.

SOA(적용성 보고서) ISO/IEC 27001 인증을 지원하여 제작된, ISMS의 범위에서 구현된 보안 제어를 설명하는 문서.

SoC(System On Chip) 여러 구성요소를 단일 칩으로 통합한 집적 회로(IC).

SOG-IS(Senior Officials Group Information Systems Security) 여러 유럽 국가 간에 상호 인정 협정을 관리하는 단체.

T2 2017년부터 일부 Intel 기반 Mac 컴퓨터에 포함된 Apple 보안 칩.

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

KH028-00499-B