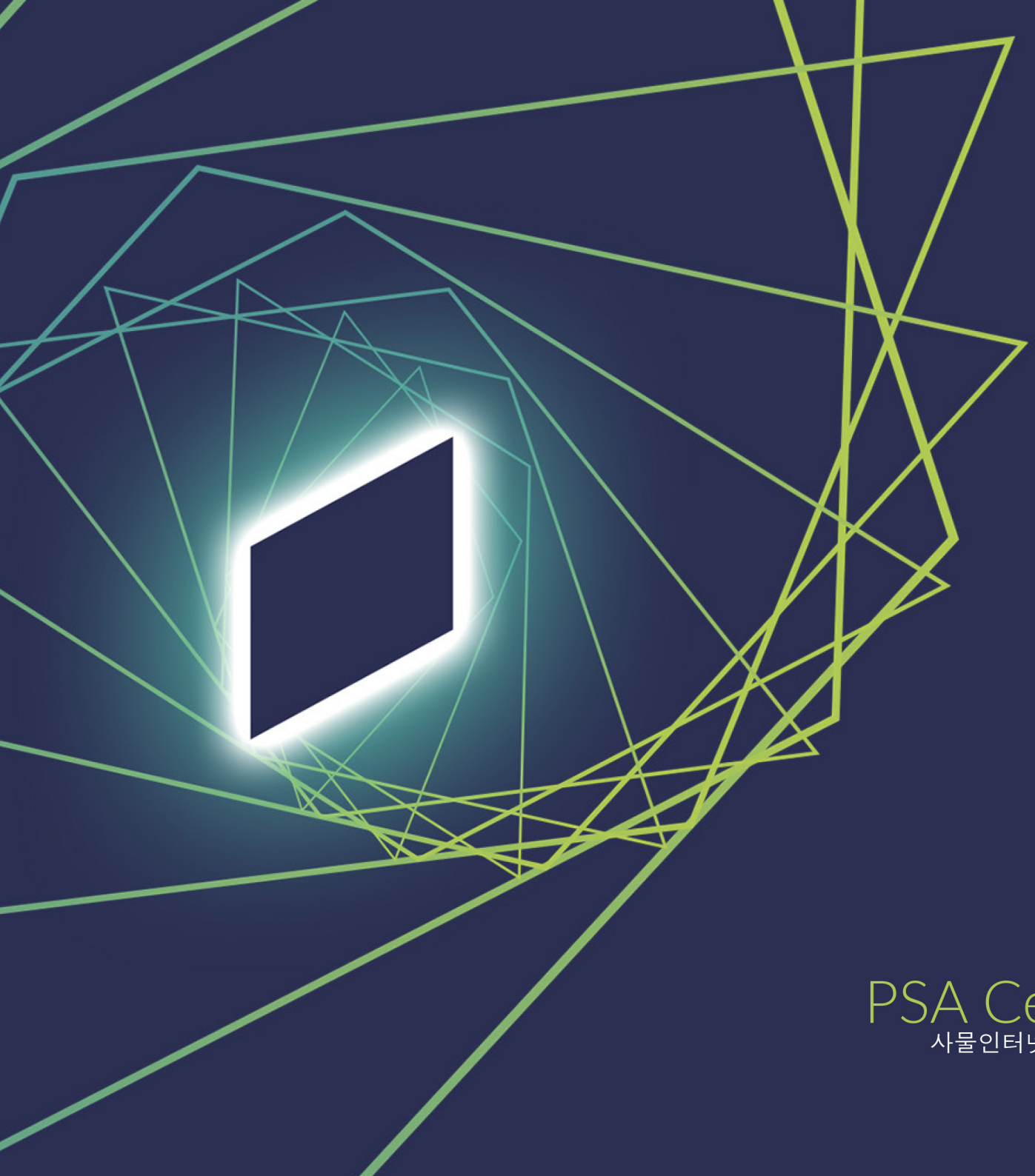


psacertified™

PSA Certified 프로그램 개요

사물인터넷(IoT)을 위한 업계 지원 보안 프레임워크 및 보증 제도

PSA Certified 프로그램 개요

사물인터넷(IoT)을 위한 업계 지원 보안 프레임워크 및 보증 제도

PSA Certified는 위협 모델, 보안 목표 및 전 세계 정부 및 산업 표준을 사용하여 체계적으로 개발된 범용 보증 제도입니다. 2017년에 발표된 프레임워크인 PSA(Platform Security Architecture)를 기반으로 구축되어 보안 전문가가 아니더라도 대규모로 보안을 쉽게 구현하고 관리할 수 있습니다

https://www.psacertified.org/

소개

매년 출하되고 있는 수십억 개의 커넥티드 디바이스는 집, 회사, 도시, 지역 및 국가 인프라 등 우리 주변 세계에 대한 탁월한 통찰력을 제공합니다. 놀랍고 혁신적인 기술은 디지털 전환을 가능하게 하지만, 궁극적으로는 신뢰에 기반하여 구축되어야 합니다.

의사 결정의 기반이 되는 데이터와 이를 생성하는 디바이스에 대한 신뢰가 있어야만 광범위한 디지털화의 이점이 실현될 수 있기 때문입니다. 그렇다면, 고객이 신뢰할 수 있는 제품의 설계, 개발 및 제조를 어떻게 보증할 수 있을까요?



사물인터넷(IoT) 디바이스에 대한 신뢰를 구축하는 유일한 방법은 여정의 시작 단계인 반도체에서부터 보안을 설계하는 것입니다. 허술하게 만들어진 제품들은 범죄자들의 쉬운 표적이 되며 해킹은 점점 더 간단하고 저렴해지고 있습니다. 몇 가지 유명한 사례들은 기본 보안의 취약함으로 인해 어떤 피해가 발생할 수 있지 보여줬을 뿐만 아니라, 디지털 전환에서 보안 문제가 최상위 과제로 떠오르는 계기가 되었습니다. 전 세계 정부와 업계는 이제 사용자들을 보호하기 위해 새로운 보안 규정을 수립하고 있습니다.

보다 엄중한 잣대의 필요성과 중요성이 높아지고 있지만, 유럽, 영국, 미국을 포함한 전 세계의 다양한 표준은 여러분이 어디에서부터 보안 여정을 시작해야 하는지, 그리고 전 세계적으로 제품을 확장하는 시기에 어떻게 수요를 충족해야 할지를 알기 어렵게 만듭니다. 이게 바로 Arm이 범용 보안 프레임워크 및 보증 제도인 PSA Certified를 개발한 이유입니다.

PSA Certified는 신뢰할 수 있는 디바이스 구축에 수반되는 시간, 비용 및 위험을 줄여주며 주요 산업 표준 및 정부 규정을 준수합니다. 또한 디바이스에 적절한 수준의 보안을 구현할 수 있도록 하고, 독립적인 다단계 평가 및 인증을 통해 고객에게 보안성에 대한 확신을 보여줄 수 있습니다. 특히, 산업 전반에 걸친 수년간의 연구와 모범 사례를 바탕으로 정립된 본 제도는 실리콘 공급사, 디바이스 제조사, 클라우드 공급업체 및 소비자를 포함한 IoT 생태계 내의 모든 사람들이 제품의 보안성을 이해하고 평가할 수 있도록 하는 공통의 언어로서 역할을 할 것으로 기대됩니다.

이 문서는 PSA Certified의 주요 기능을 설명하고 IoT 디바이스의 보안성을 구축하고 인증하기 위해 수행해야 할 단계를 요약합니다. 더 자세한 사항은 이어지는 내용을 통해 확인해 보실 수 있습니다.

PSA Certified란 무엇인가?

PSA Certified는 디지털 전환의 핵심인 수십억 개의 커넥티드 디바이스에 대한 신뢰를 구축하는 데 도움을 주는 IoT 보증 제도로, 업계의 지지를 받고 있습니다. 이는 범용 프레임워크와 기술 자원을 제공하는 유일한 보증 프로그램이며, 적합한 다단계 인증제도와 동급 최고의 산업 지원을 제공합니다.

해당 프로그램은 기업이 제품을 신속하게 출시하는 데 있어 보안 문제가 걸림돌이 되지 않도록 하기 위해 설계되었습니다. 이는 기업들이 요구사항에부합하는 적절한 보안 수준을 확보하고 고객에게 보안의 견고성을 보여주는 데 도움이 될 것입니다.

https://www.psacertified.org/what-is-psa-certified/our-approach/

PSA Certified 는 쉽게 이해할 수 있는 4 단계로 구성되어 있습니다.

1 분석

공개되고 편집 가능한 위협 모델과 다양한 일반 IoT 사용 사례에서 도출한 보안 분석을 통해 장치 및 보안 요구사항에 대한 위협을 식별합니다.

2 설계

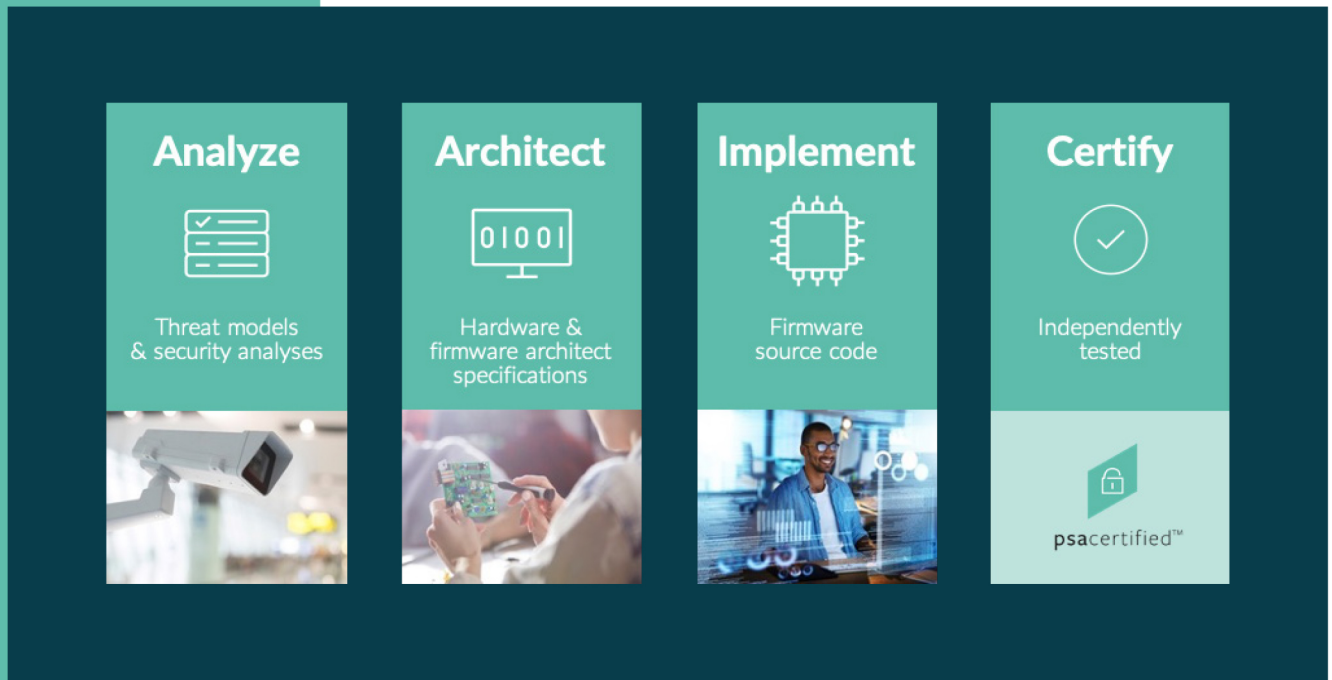
설계단계에 보안을 포함시켜 신뢰를 구축할 수 있도록 돕기 위해 PSA Certified 에코시스템에서 펌웨어 및 하드웨어 아키텍처 사양을 무료로 제공합니다.

3 구현

펌웨어 아키텍처 사양, API, 그리고 보안 기능에 대한 신뢰할 수 있는 코드 기반 및 인터페이스를 제공하는 API 테스트 스위트의 오픈소스 참조 구현에 액세스할 수 있습니다.

4 인증

고객에게 보증을 제공하기 위한 칩, 디바이스 및 소프트웨어 플랫폼에 대한 독립적 평가 제도로, 3 단계의 강화된 견고성과 인증을 통해 IoT 칩에 적절한 수준의 보안을 구축합니다.



PSA Certified에 왜 참여해야 하는가?

보안 전문가가 개발: PSA Certified는 7개의 업계 최고 파트너사에 의해 설립되었습니다. IoT 보안 시장 내 단편화를 줄이기 위해 명확하고 공통된 언어와 표준 접근법을 제공하고자 만들어졌습니다.

시장 요구사항에 부합: 본 프로그램은 광범위한 지역의 주요 산업 표준 및 정부 규정에 부합합니다.

보안 견고성 입증: 독립적인 다단계 평가 절차는 공정한 인증 기관 뿐만 아니라 전세계적인 역량을 보유한 신뢰할 수 있는 시험기관의 감사를 받습니다.

에코시스템 전반에 대한 보안: 본 제도는 칩 설계자부터, 소프트웨어 공급업체 및 디바이스 개발사까지 전 생태계에 적용 가능하도록 설계되어 클라우드 및 네트워크 인프라 공급사와 IoT 애플리케이션 개발사들에게 보안의 명확성을 제공합니다.

세계 최고 수준의 보안 전문지식에 대한 액세스: PSA Certified는 보안 전문가 팀에 의해 지속적으로 검토되고 정기적으로 업데이트되어 끊임없이 진화하고 있습니다.

오픈소스 소프트웨어 및 리소스 지원: 체계적으로 구축된 프레임워크와 리소스가 PSA Certified 생태계를 통해 공유됩니다. 위협 모델, 보안 목표 및 다양한 세계 표준을 비롯하여 이해하기 쉬운 지침 및 문서를 자유롭게 이용할 수 있습니다.

NORDIC SEMICONDUCTOR

"PSA Certified는 '이 디바이스는 필요한 수준의 보안을 제공한다'는 인증을 표시하는 스탬프와 같기 때문에 노르딕 세미컨덕터(Nordic Semiconductor)에게 중요합니다."

스베인-에질 닐슨(Svein-Egil Nielsen) | 노르딕 세미컨덕터 최고기술책임자(CTO)

PSA Certified의 혜택

"PSA Certified를 통해 칩 제조사, 소프트웨어 플랫폼 및 디바이스 제조사들은 '적절한 보안 원칙을 적용했으니 믿어주십시오'라고 말하는 것 대신 '이 제품은 독립 시험기관의 평가를 받았으며 여기에 그 증거가 있습니다'라고 이야기할 수 있게 되었습니다.

롭 쿰스(Rob Coombs)
Arm 비즈니스 개발 디렉터 겸
PSA Certified 창립멤버



범용 프레임워크 및 보증 제도가 보안 구축을 용이하게 하는 5가지 방법은 다음과 같습니다.

1. 보안 경제성 향상: PSA Certified는 보안 설계를 더 빠르고 쉽게 만들어 초기 보안 비용을 획기적으로 절감합니다. 인증 제도는 물론 포괄적 프레임워크와 기술 지원을 제공합니다. 보안 전문가에 의해 선별되고 정부 표준 및 법률에 부합하기 때문에 프레임워크는 총소유비용(TCO)을 낮추는 동시에 리스크를 줄여줍니다.

2. 적절한 규모의 보안: PSA Certified는 제품 또는 디바이스에 대한 적절한 보안 수준을 식별하기 위해 필요한 도구를 제공합니다. 즉, 요구 사항을 충족하지 않는 옵션을 필터링하여 출시 기간을 단축할 수 있습니다.

3. 복잡성 감소: PSA Certified는 사용하기 쉬운 보안 프레임워크와 세계 유수 조직들이 제공하는 API와 같은 공통 보안 구성요소로 구성되어 보안 구현을 쉽게 만듭니다. 또한 적절하게 수행되고 있는지 확인을 돕고 감사 추적을 생성합니다.

4. IoT 보안 단편화 방지: IoT의 다양성은 혁신가들에게 큰 기회를 제공하지만 커넥티드 디바이스 보안을 더 복잡하게 만들기도 합니다. PSA Certified는 다양한 보안 수준과 이해하기 쉬운 공통 언어로 명확성을 높입니다. 기술의 잠재력을 제한하지 않으면서 일상의 보안 문제를 해결하도록 도움을 주고 있습니다.

5. 확실성: 대부분의 칩과 제품은 독립적으로 테스트되지 않고 않지만 PSA Certified는 공정한 평가 및 인증을 제공합니다.

"PSA Certified는 업계 전반의 파트너들과 쉽게 소통할 수 있도록 도와줍니다. 어떠한 수준의 보안이 필요한지 물어볼 수 있으며, 따라서 칩에 어떤 보호 기능이 포함되어야 하는지 파악할 수 있습니다. 또한 소비자에게는 확실성을 제공합니다. 소비자들은 각 디바이스가 어떤 종류의 보안을 제공하는지 알 수 있습니다."

제이슨 린(Jason Lin) 반도체 기업 누보톤 (Nuvoton) MCU 사업부 부사장



brightsight®
the number one security lab in the world

오늘날의 IoT 보안 문제는 기술과 위협 두 가지 모두가 계속 변화되고 급속히 발전하는 환경 속에서 발생하며, 운영되는 디바이스 수와 공공 및 민간 조직의 보안 프레임워크 증가로 인해 배가되고 있습니다. PSA Certified는 이러한 문제의 해결을 위해 설계를 통해 보안에 대한 기대를 충족시키도록 돕고 있습니다.

카를로스 세라토스(Carlos Serratos), 브라이트사이트(Brightsight) 전략 및 정책 홍보 부문 시니어 디렉터

life.augmented

"소프트웨어와 하드웨어 사이에 매치가 잘 되어 구현을 용이하게 해 주고 둘 사이의 보안 격차를 더 쉽게 해소할 수 있습니다."

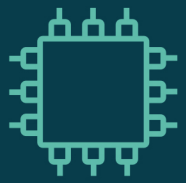
드라고스 다비데스쿠(Dragos Davidescu) ST마이크로일렉트로닉스 (STMicroelectronics) 수석 시스템 아키텍트 겸 펠로우

PSA Certified의 수혜자는 누구인가?

본 프레임워크와 보증 제도는 가치 사슬을 전체적으로 지원하도록 설계되었습니다.



미들웨어/디바이스 애플리케이션 개발자
특정 보안 전문 지식 없이도 출시 기간을 단축하고 복잡한 보안을 구축할 수 있도록 재사용 가능한 키 코드를 제공합니다.



실리콘 업체
PSA Certified는 제품에 잘 설계된 Root of Trust (RoT)가 있음을 입증하고 보안에 대한 투자 증거를 제공할 수 있도록 도와줍니다.



기업
PSA Certified는 기업이 사업을 위해 확보하는 디바이스와 해당 디바이스의 보안 수준에 대한 이해를 높여줍니다.



OEM 업체
PSA Certified는 주요 정부 요구 사항에 부합하므로 신규 법률 및 표준도 선제적으로 준수하고 보안에 대한 투자 증거를 제공할 수 있도록 도와줍니다.



클라우드 서비스 공급자 및 모바일 네트워크 사업자 엔티티 증명 토큰(Entity Attestation Tokens)을 통해 귀사의 네트워크에 연결하기 전 디바이스 보안 자격증명을 쉽게 파악할 수 있습니다.



시스템 소프트웨어 공급업체
칩 보안 기능에 대한 효율적인 액세스와 보안성에 대한 증거를 제공합니다. 보안 규정을 준수하고 보안 전문성을 보여줄 수 있습니다.



정부
PSA Certified는 업계 전문가들이 기존에 잘 구축해 놓은 제도이므로 불필요한 시간을 소모하거나 새로운 연구에 투자할 필요가 없습니다.

숫자로 보는 IoT 보안의 중요성



60

신뢰할 수 있는 디바이스에 대해 상당한 추가금을 기꺼이 지불할 의향이 있다고 답한 설문조사 응답자의 비율



5,200

매달 IoT 허니팟을 겨냥한 평균 공격 수



15

커넥티드 카메라를 겨냥한 공격 비율로, 전년도의 3.5%보다 증가함



3.92 백만

최근 보고서에 따른 데이터 침해로 발생하는 평균 비용(단위: 달러)



76

한 설문조사에서 기업이디바이스 보안을 위해 더많은 노력을 해야 한다고응답한 비율



28

최근 설문조사에서 스마트디바이스를 소유하고 있지않은 사람의 28%가 보안에대한 우려 때문에구매하지 않을 것이라고응답



70

상위 10개 소비자 IoT제품을 대상으로 한 연구에서 '심각한 취약성'이 발견된 디바이스 비율



<30

보안 전문가가 스마트락을 해제하는 데 걸린 시간(초)



123456

한 연구를 통해 발견했던 2018년 대부분의 공격자가 IoT 디바이스에 액세스하기 위해 사용한 암호



프로그램의 핵심 요소

IoT는 커넥티드 디바이스 수(2035년까지 1조 개 예상)와 그 잠재력 측면에서 계속 성장하고 있습니다. 실제로 최근 설문 조사에 참여한 제조, 의료, 에너지, IT 및 자동차 등 다양한 분야의 기업의 2/3는 IoT가 '자사 디지털 전략의 근간'이라고 답했습니다.

그러나 이는 업계에 도전을 야기합니다. IoT디바이스 수가 1조 개 규모에 달한다고 상상해 보면 완전히 판도가 바뀝니다. 더 이상 가정이나 사무실에서 소규모의 안전한 네트워크를 관리하는 수준이 아닙니다. 이것은 모든 것이 연결되었다는 것을 의미하며, 한 네트워크의 약점 하나가 전체 시스템에 위협이 된다는 뜻입니다.

PSA Certified는 모든 커넥티드 디바이스를 구축할 수 있는 보안 기반을 확보하기 위해 개발되었습니다. 개발자와 디바이스 제조사가 보다 쉽고 비용 효율적으로 더 안전한 장치를 구축할 수 있게 해주는 4단계 프레임워크로 시작했으며 이제 생태계 참여자들의 귀중한 공헌을 통해 산업 전체의 모범 사례를 포함하는 범용 보증 제도로 발전하였으며 주요 산업 및 정부 표준을 준수합니다.

프레임워크 및 보증 제도는 다음과 같은 6가지 핵심 보안 요소로 구성됩니다.

위협 모델링 및 보안 분석

위협 모델링과 보안 분석(TMSA) 또는 영어 보호 프로파일(English Language Protection Profile)은 보안의 시작점입니다. 다음과 같은 예시의 식별 프로세스를 통해 디바이스에 대해 단계별로 적절한 보호 수준을 갖출 수 있도록 도와줍니다.

보호되어야 할 자산

디바이스에 대한 모든 잠재 위협

잠재 위협의 범위와 심각성

공격자 유형 및 디바이스를 손상시키는 데 사용될 수 있는 방법

구현 가능한 대책

이러한 프로세스의 일부로 작성하는 문서는 보안에 대한 접근법을 안내하고 일련의 보안 목표를 통해 강조되는 업계 모범 사례 수준에 맞추어 요구사항을 충족할 수 있게 합니다.

위협 모델링에 대한 더욱 자세한 내용은 웹사이트 에서 확인해 보실 수 있습니다.

www.psacertified.org/development-resources/building-in-security/threat-models/

PSA Certified 의 10 가지 보안 목표

세계 최고의 보안 전문가들이 모든 칩, 운영 체제(OS) 및 IoT 디바이스에 구현되어야 하는 10가지 보안 요구사항 또는 목표를 정의했는데, 이는 모범 사례를 보여주고 보안 시스템의 기반을 마련하려는 개발자들에게 체크리스트와 같은 역할을 합니다.

보안 목표는 PSA Certified 프레임워크 및 보증 제도의 핵심입니다. 따라서 (다른 보안 요구사항과 함께) PSA Certified 레벨 1에서 평가받습니다. 이러한 기본 보안 목표는 또한 전 세계적으로 인정받는 표준 및 규정에도 적용되어 있습니다.

www.psacertified.org/blog/psa-certified-10-security-goals-explained/

1 고유 ID: 모든 디바이스는 고유 ID가 필요하며 증명할 수 있어야 한다. 이는 데이터 교환 및 디바이스 관리처럼 디바이스와 신뢰할 수 있는 상호작용을 용이하게 한다.

2 보안 라이프사이클: 디바이스는 개발 및 제조 단계부터 디버그 및 수리에 이르는 보안 라이프사이클을 지원해야 한다. 또한 각 보안 상태도 증명할 수 있어야 한다.

3 증명: 모든 디바이스는 증명을 지원해야 한다. 즉, 상기에 기술된 목표와 마찬가지로 디바이스 속성에 대한 증거를 제공해야 한다.

4 보안 부팅: 인증된 소프트웨어만 디바이스에서 실행되도록 해야 하며 보안 부팅 및 보안 로딩 프로세스를 사용하여 초기부터 시스템에 무결성을 구축해야 한다.

5 보안 업데이트: 모든 디바이스는 보안을 강화하거나 새로운 기능을 제공하기 위해 보안 업데이트를 지원해야 한다. 프로세스는 견고해야 하며 장치의 무결성을 손상시키지 않아야 한다.

6 롤백 방지: 디바이스는 취약할 수 있는 이전 버전으로의 무단 롤백을 방지해야 한다. 롤백은 복구 목적으로 승인된 경우에만 가능해야 한다.

7 격리: 격리는 항상 가능해야 하며 최소한 비(非)보안 애플리케이션 소프트웨어와 RoT 소프트웨어 간의 격리는 언제나 가능해야 한다. 또한, 이상적으로 격리는 시스템의 신뢰할 수 있는 부분을 보호할 수 있도록 하드웨어 기반이어야 한다.

8 상호작용: 디바이스는 경계를 넘어 신뢰할 수 있는 상호작용을 가능하게 해야 한다. 디바이스 내부에서 이루어지는 상호작용과 디바이스와 외부 세계 간에 이루어지는 상호작용까지 고려되야 한다.

9 보안 스토리지: 예) 키 또는 인증서. 신뢰할 수 있는 서비스 또는 디바이스 외부에서 개인 데이터가 복제되거나 공개되지 않도록 고유하게 묶여 있어야 한다.

10 암호화/신뢰할 수 있는 서비스: 최대로 신뢰할 수 있는 시스템 수준에서 최소한의 암호 운영 세트를 구현해야 한다. 보안 라이프사이클, 격리, 보안 스토리지, 증명, 보안 부팅, 보안 로딩 및 데이터 바인딩 등의 주요 기능을 지원해야 한다.

https://www.psacertified.org/blog/psa-certified-10-security-goals-explained/



전 세계 표준 및 규정 준수

주요 세계 시장에서의 정부 및 업계의 요구사항을 모니터링하고 검토함으로써, 실리콘 업체, 소프트웨어 개발자 및 OEM업체들이, 특히 제품을 전 세계적으로 확장하려는 경우, 보다 쉽게 컴플라이언스를 보장할 수 있도록 합니다.

PSA Certified 창립자들은 ETSI 303 645, NIST 8259v2, 캘리포니아 주법 SB-327과 영국 디지털·문화·미디어·스포츠부(Department for Digital, Culture, Media & Sport, DCMS)의 신규 법률에 맞게 보안 매핑을 시행하였습니다.

기본 보안 기준을 충족하는지 확인하기 위해 PSA Certified 레벨 1 설문지 버전 2.0은 이 규정들에 맞추어 작성되었습니다.

첫 세 가지 핵심 요소는 함께 강력한 보안 접근법을 만들고 기본 요구사항을 평가할 수 있도록 도와줍니다. 그 다음 이어지는 보안 기반 요소들은 전체 생태계의 지원을 통해서만 달성할 수 있는 확장 가능한 보증을 제공하는 것을 목표로 합니다.

https://publications.psacertified.org/iot-security-standards-and-regulations/welcome/



"디바이스 제조업체들은 우리 플랫폼이 최고의 글로벌 표준에 맞추어 인증되었음을 알고 있습니다. 이는 제조사들이 이러한 표준을 따를 수 있다는 것은 물론, 확인을 위해 우리가 제품 소스 코드를 공개하거나 여러 문서를 제공할 필요가 없다는 걸 의미합니다."

황수익
시큐리티플랫폼(주) 대표



PSA Root of Trust

앞서 소개에서 강조했듯이 강력한 보안은 실리콘에서 시작됩니다. 세계 유수의 실리콘 업체 중 상당수가 이미 PSA Certified를 채택했으며 PSA-RoT(PSA Root of Trust)라는 새로운 보안 구성 요소를 제공하게 된 것을 기쁘게 생각합니다.

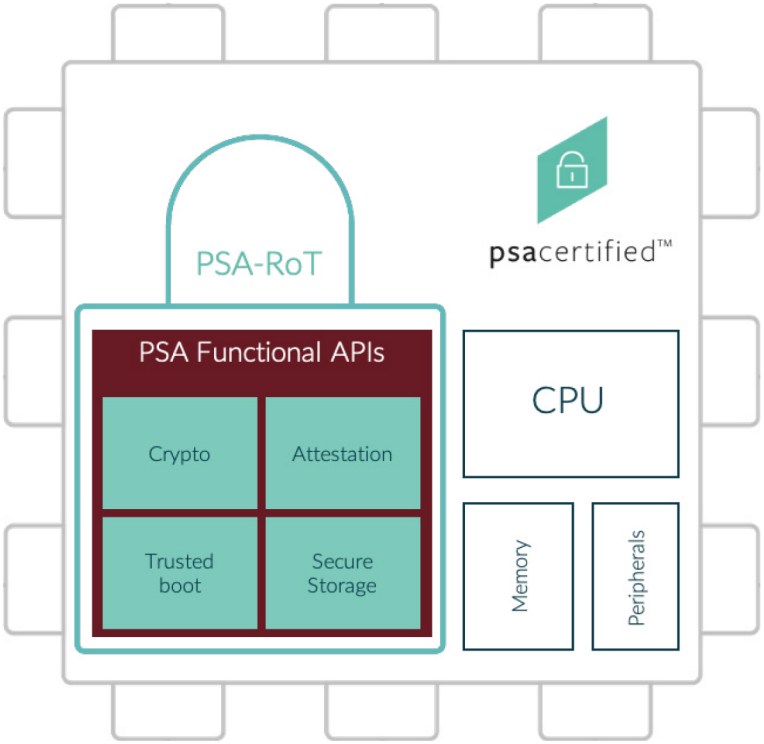
RoT는 시스템온칩(SoC)의 핵심이며 나머지 시스템이 의존하는 보안 기능을 제공합니다. PSA-RoT는 IoT 용으로 설계된 표준화되고 사용하기 쉬운 온칩 구성요소입니다.

PSA-RoT는 격리되고 신뢰할 수 있는 하드웨어와, 안전한 프로세싱 환경에서 일반적으로 암호화, 증명, 신뢰할 수 있는 부팅 및 보안 스토리지와 같은 필수 보안 기능을 제공하는 소량의 신뢰할 수 있는 펌웨어로 구성됩니다.

이를 통해 실리콘 업체는 칩의 보안 기능을 입증하고, OEM 업체는 디바이스에 적합한 보안 수준을 선택할 수 있으며, 클라우드 서비스 공급자와 이동통신사는 디바이스가 얼마나 안전한지 파악하고 해당 디바이스가 갖춰야 할 신뢰 수준에 대해 리스크에 기반한 판단을 내릴 수 있습니다.

도입을 장려하기 위해 무료 엔지니어링 제품 패키지가 준비되어 있습니다.

https://www.psacertified.org/blog/what-is-a-root-of-trust/



PSA Functional API

PSA-RoT를 사용하여 칩에 신뢰를 구축한 후 다음 단계는 개발자가 보안 프로세싱 환경 내에서 중요한 보안 기능에 액세스할 수 있도록 하는 것입니다. PSA Functional API는높은 수준의 인터페이스를 제공하고 모든 사람이 보안에 접근할 수 있게 합니다.

이는 다양한 칩과 실리콘 업체에서 PSA-RoT를 일관되게 활용하는 방법을 제공하기 때문에 가능하며 다음이 보장됩니다.

세 가지 기본 및 무료 API에는 암호화, 증명 및 보안 스토리지가 포함됩니다.

암호화
이 서비스는 대칭 및 비대칭 키 사용과 키 스토리지를 포함합니다. 암호화 API는 개발자가 설계를 보호할 수 있도록사용이 간편합니다.

증명
이 서비스는 디바이스의 ID 및 상태에 대한 클레임을포함하는 서명된 메시지를 제공합니다. 예를 들어 엔드포인트와 서비스 제공자 간의 신뢰를 구축하는 데 사용할수 있습니다. 또한 라이프사이클 정보 또는 서명된 보안 감사 로그를 공급자에게 제공하는 데 사용할 수도 있습니다.
PSA Certified는 국제 인터넷 표준화 기구(Internet Engineering Task Force, IETF)와 같은 표준 기관에서 정의한 엔티티 증명 토큰(EAT)를 사용하고 있습니다. 이는 전력이 제한된 IoT 디바이스에 최적화되어 있기 때문입니다.

보안 스토리지
디바이스에 저장된 데이터는 보안이 중요하기 때문에 데이터의 기밀성과 무결성을 유지하고 롤백을 방지하는 서비스를 제공합니다. 동일한 API에 의해 수행되는 기능은 두 가지가 있는데, 하나는 디바이스 내부 스토리지와 관련된 것이고 다른 하나는 외부 스토리지를 위한 것입니다.

https://www.psacertified.org/development-resources/



보증 수준 선택하기

PSA Certified는 IoT의 다양성을 고려하여 설계되었습니다. PSA Certified는 각 디바이스에는 자체 보안 요구사항이 있으며 비용과 보안 사이의 균형이 애플리케이션과 생태계에 따라 다를 것임을 인지하고 있습니다. 따라서 프레임워크와 제도는 IoT 제품에 다양한 수준의 보안을 구축할 수 있도록 설계되었습니다.

칩 업체는 위협 모델링 프로세스 중 수집한 정보를 사용하여 얼마나 강력한 보안을 필요로 하는지, 그에 따라 어떤 수준의 보안 인증을 추구해야 하는지를 파악할 수 있습니다.

OEM업체들에게 위협모델은 얼마나 강력한 보안을 필요로 하는지에 대한 판단을 내리고 보호가 필요한 취약점을 파악하는 데 도움이 될 것이며, 이를 통해 칩이 어떤 수준의 보안과 보증을 인증 받아 제공해야 하는지 알 수 있습니다.

요구사항을 충족하는 보안 솔루션을 선택하여 관련성이 낮은 옵션에 시간과 비용을 소비해 개발 속도가 늦어지는 것을 방지할 수 있습니다.다단계 보안 인증

다단계 보증 제도는 보안 요구사항이 디바이스에 대한 위협 분석에서 비롯된다는 것을 파악하여(자세한 내용은 1단계 '분석' 참조) 적절한 수준의 보안이 구축되었는지 확인하는 데 도움을 줍니다.

보안 인증에는 세 가지의 점진적 단계가 있습니다.







PSA Certified 레벨1
보안 설문지를 통한 보안 원칙 기반 설계 평가
칩 업체, OS 업체, OEM업체에 적용 가능
IoT 위협 모델, 보안 목표 및 전 세계 주요 정부 및 산업 규제와 표준에 기반한 체계적 개발
간결한 설문지 – 50문항 미만, 시험기관의 검토
칩 업체, OS 업체, OEM업체를 위한 별도 섹션을 포함한 복합 포맷
https://www.psacertified.org/getting-certified/device-manufacturer/

PSA Certified 레벨2
시험기관의 칩 PSA-RoT 보안 구성요소 평가
확장 가능한 원격 소프트웨어 공격에 대한 보호 증거 제공
칩 업체에 적용 가능
PSA Certified 레벨2 PSA-RoT 보호 프로파일 기반 에그노스틱 기술 구현
25일 이내의 평가 기간으로 시간과 비용 절감
https://www.psacertified.org/getting-certified/silicon-vendor/overview/level-2/

PSA Certified 레벨3 (개발 중)
시험기관의 칩 PSA-RoT 평가
상당한 보안성 보증 및 견고성 입증(휴대폰의 신뢰실행환경(TEE)과 유사)
물리적 공격과 소프트웨어 공격에 대한 보호 증거 제공
https://www.psacertified.org/getting-certified/silicon-vendor/overview/level-3/

PSA Functional API 인증
PSA Functional API 인증은 API를 사용할 수 있으며 올바르게 사용되고 있음을 입증하는 별도의 인증입니다. 실리콘 및 RTOS 업체는 인증을 통해 해당 분야에서 모범 사례를 유지하고 있음을 보여줄 수 있습니다.
https://www.psacertified.org/getting-certified/functional-api-certification/

시작하기: PSA Certified 프레임워크

PSA Certified는 유수의 실리콘 업체에서 OEM 및 RTOS 업체에 이르기까지 다양한 파트너를 보유하고 있습니다. 또한 IoT 디바이스를 개발 중인 기업들이 마음의 평화를 얻기 위해 이용할 수 있는 PSA Certified솔루션의 범위는 점점 더 확대되고 있습니다.

더 안전한 디바이스를 구축하거나 인증을 받을 준비가 되었다면 아래 또는 PSA Certified웹사이트에서 필요한 모든 정보를 찾으실 수 있습니다.

www.psacertified.org