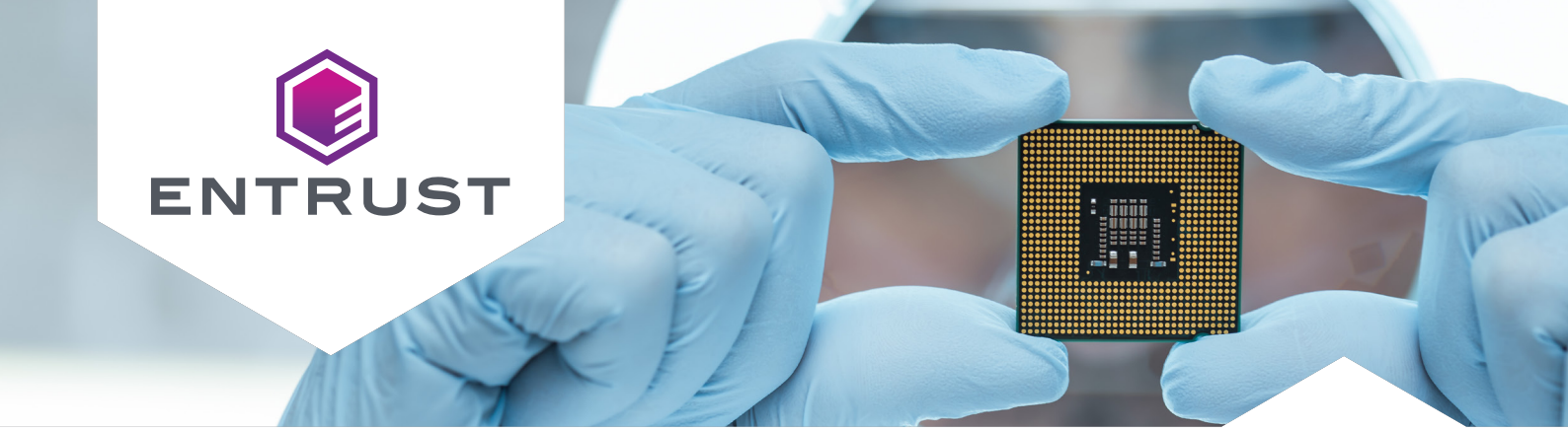

Microchip의 IoT 지원 SAM L11 마이크로 컨트롤러에 루트 ID를 프로비저닝하는 Entrust

사물 인터넷(IoT)은 멈출 수 없는 현상이 되었습니다. IDC는 모든 연결된 IoT 장치 수가 2025년까지 400억을 초과할 것으로 예측하며, 이마저도 많은 사람들은 매우 보수적인 숫자로 보고 있습니다.

그러나 자율 주행 차량에서 스마트 가전 제품, 의료 장비, 농업 기계에 이르기까지 IoT 관련 엔드포인트의 폭발적인 확산에 그 자체로 어려움이 없는 것은 아닙니다. 이 중 가장 중요한 것은 보안 문제로, 모든 장치가 손상되지 않도록 보호할 수 있어야 합니다.

비즈니스적 요구

Microchip Technology의 제품 마케팅 관리자인 Anand Rangarajan은 다음과 같이 설명했습니다. "IoT 세계에는 현재 보안에 대한 보편적인 표준이 없습니다. 제품에 적절한 보안 조치를 통합하는 데 따르는 복잡성은 많은 제조업체에게 어려운 제안입니다."

> **업계 최강의 보안이 임베디드 시스템에 통합되면 전체 IoT 시장의 진짜 판도가 바뀔 것입니다.**
>
> – Anand Rangarajan, Microchip Technology 제품 마케팅 관리자

ENTRUST.COM/HSM에서 자세히 보기

Microchip

지속적인 혁신과 선도적인 제품으로 유명한 Microchip Technology, Inc.는 마이크로 컨트롤러, 혼합 신호, 아날로그 및 플래시 IP 솔루션을 제공하는 세계 최고 공급업체 중 하나입니다. 회사의 최신 마이크로 컨트롤러 중 하나인 SAM L11은 ARM Techcon에서 최고의 IoT 보안 공헌으로 2018 혁신 어워드를 수상했으며, 구체적으로 IoT 노드 및 스마트 엔드 포인트 (예: 의료 기기, 센서, 카메라 및 자동차)의 특징, 기능 및 보안 요구 사항을 해결합니다.

애리조나 주 챈들러에 본사가 있는 Microchip 은 나스닥 거래소에 상장되어 있습니다. 이 회사는 전 세계 수십만 고객에게 수십억 개의 마이크로 컨트롤러와 마이크로 프로세서를 제공해 왔습니다.

기술적 요구

Rangarajan은 "마이크로 컨트롤러의 관점에서 볼 때, SAM L11에 대해 우리가 예상하는 사용 사례 유형은 고성능이지만 낮은 전력 소비에 대한 니즈 같은, 매우 독특한 설계 특성을 수반합니다"라고 설명합니다.

솔루션

SAM L11 보안 아키텍처의 핵심은 Microchip이 제조 중에 장치 고유 키를 삽입할 수 있도록 만든 RoT(신뢰 루트) 기능입니다. 중요한 작업을 관리하고 실행할 기술을 선택하는 것은 매우 간단합니다. "우리는 Entrust(구 nCipher)와 오랜 관계를 유지해 왔으며 개별 키를 생성하기 위해 HSM(하드웨어 보안 모듈)을 선택하는 것은 우리에게 명확한 선택이었습니다"라고 Rangarajan은 말했습니다.

Entrust nShield® HSM은 중요한 암호화, 디지털 서명 및 키 생성 기능을 실행하는 인증된 하드웨어 보안 어플라이언스입니다. 강화된 네트워크 플랫폼은 확장성이 뛰어나며 업계 최고의 암호화 트랜잭션 속도를 제공할 수 있는 독특하고 유연한 아키텍처를 사용합니다.

결과

Rangarajan은 "nShield HSM의 고유 키를 각 SAM L11 마이크로 컨트롤러에 삽입할 수 있는 기능을 통해 장치를 개별적으로 식별, 확인 및 원격 관리할 수 있습니다. 이는 IoT 장치와 기타 연결된 엔드 포인트간에 신뢰를 다시 설정해야 할 때 특히 중요합니다." 제조업체는 이제 클라우드를 최대한 활용하여 각 노드 간에 안전하고 광범위한 연결을 제공할 수 있습니다. 무선 센서 보안, 핸드헬드 의료 기기의 데이터 암호화, 클라우드 연결 시스템의 원격 인증과 같은 애플리케이션에 이상적입니다"라고 말했습니다.

Microchip SAM L11 마이크로 컨트롤러의 매우 매력적인 가치 제안의 일부는 전 세계적으로 15억 개 이상의 보호 장치를 배포한 장치 보안 시장의 리더 Trustonic과의 파트너십의 결과입니다.

가장 큰 돌파구 중 하나는 Trustonic이 하나의 소프트웨어 개발 키트에 인증, 보안 부팅, 변조 감지, AES 및 SHA 암호화, 보안 키 저장을 포함한 보안 기능 라이브러리를 생성하여 통합한 것입니다.

Microchip

> **Entrust nShield HSM을 선택하여 개별 키를 생성하는 것은 우리에게 명확한 선택이었습니다.**
>
> – Anand Rangarajan, Microchip Technology 제품 마케팅 관리자

Rangarajan은 "설계자는 이제 모듈식 보안 프레임워크를 이용해 간단한 API 호출만 하면 우리가 구축한 매우 정교한 보안 기능 세트에 액세스할 수 있습니다. 칩 수준 프로토콜에 대한 심층적인 전문 지식은 더 이상 필요하지 않습니다. 이는 개발 기간을 크게 단축하고 전통적으로 IoT 장치 보안과 관련된 오버 헤드를 크게 줄입니다"라고 말했습니다.

보안 모듈 라이브러리는 크기가 제한된 IoT 칩셋을 위해 Trustonic에서 사용자 정의한 모듈식 하드웨어 보안 운영 환경인 Kinibi-M을 기반으로 구축되었습니다. Kinibi-M 하에서, 하드웨어 추상화 계층은 암호화된 Entrust nShield 생성 키 사용 관리를 포함하여 SAM L11과의 직접 통신을 용이하게 합니다.

Rangarajan은 "Microchip의 SAM L11 개발자들은 자체 실사를 통해 Entrust nShield HSM이 우리에게 최적의 선택이라고 결정했지만, 이와는 별도로 Trustonic 역시 우리에게 Entrust HSM을 사용해야 한다고 권장했습니다. 우리의 결정에 대해 완전히 독립적인 지지를 받는 것은 매우 큰 타당성을 부여해 주었습니다"라고 회상했습니다.

판도를 바꾸는 칩으로 보안을 단순화하다

SAM L11은 Arm Cortex-M23 프로세서와 Arm TrustZone 내장 보안 기술을 활용하는 업계 최초의 마이크로 컨트롤러로서, 신뢰할 수 있는 리소스와 신뢰할 수 없는 리소스를 하드웨어로 별도 격리합니다. Rangarajan은 "보안 아키텍처의 정교하고 포괄적인 기능에도 불구하고 Kinibi-M을 사용하면 여전히 SAM L11의 보안 기능과 완전하게 통합된 펌웨어로 보안 애플리케이션을 더 간단하게 개발할 수 있으며, 관련 IoT 사용 사례를 해결할 수 있는 코드 예제를 제공하기 때문에 SAM L11과 같은 기기로부터 이점을 얻을 수 있습니다"라고 말합니다.

Entrust nShield® HSM에서 생성된 키를 활용하여 IoT 장치 개발자에게 세계적 수준의 신뢰 루트 기반을 제공하는 기능은 전 세계적으로 상당한 영향을 미치고 있습니다. Rangarajan은 "우리가 취한 접근 방식이 시사하는 바는, 이제 우리가 전력 소비가 극히 낮은 고성능 패키지에 보안을 통합할 수 있다는 것입니다. 업계 최강의 보안이 임베디드 시스템에 통합되면 전체 IoT 시장의 진짜 판도가 바뀔 것입니다"라고 말했습니다.

Microchip

IoT 전반에 걸친 보안 혁신

비즈니스적 요구

- IoT 노드 및 엔드 포인트를 보호하기 위한 솔루션 생성
- IoT 장치에 보안을 통합하는 복잡성과 비용 감소
- 칩 수준의 전문 프로그래밍 기술에 대한 필요성 제거

기술적 요구

- 강력한 보안 기능을 빠르고 전력 효율적인 마이크로 컨트롤러에 통합
- 메모리 집약적인 애플리케이션과 함께 사용할 수 있는 소형 공간 설계
- 신뢰 루트 설정

솔루션

- Entrust nShield HSM

결과

- 업계 최고의 기능과 성능을 갖춘 SAM L11 마이크로 컨트롤러 출시
- 간단한 API로 정교한 보안 기능에 액세스할 수 있는 소프트웨어 개발 키트
- IoT 장치 제조업체의 출시 시간 단축
- IoT 장치와 여기에서 생성되는 데이터에 대한 신뢰 가능

ENTRUST 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500 명이 넘는 동료 및 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com