TPM/블록체인

https://youtu.be/sZfSwLOVzsU

TPM(Trusted Platform Module)

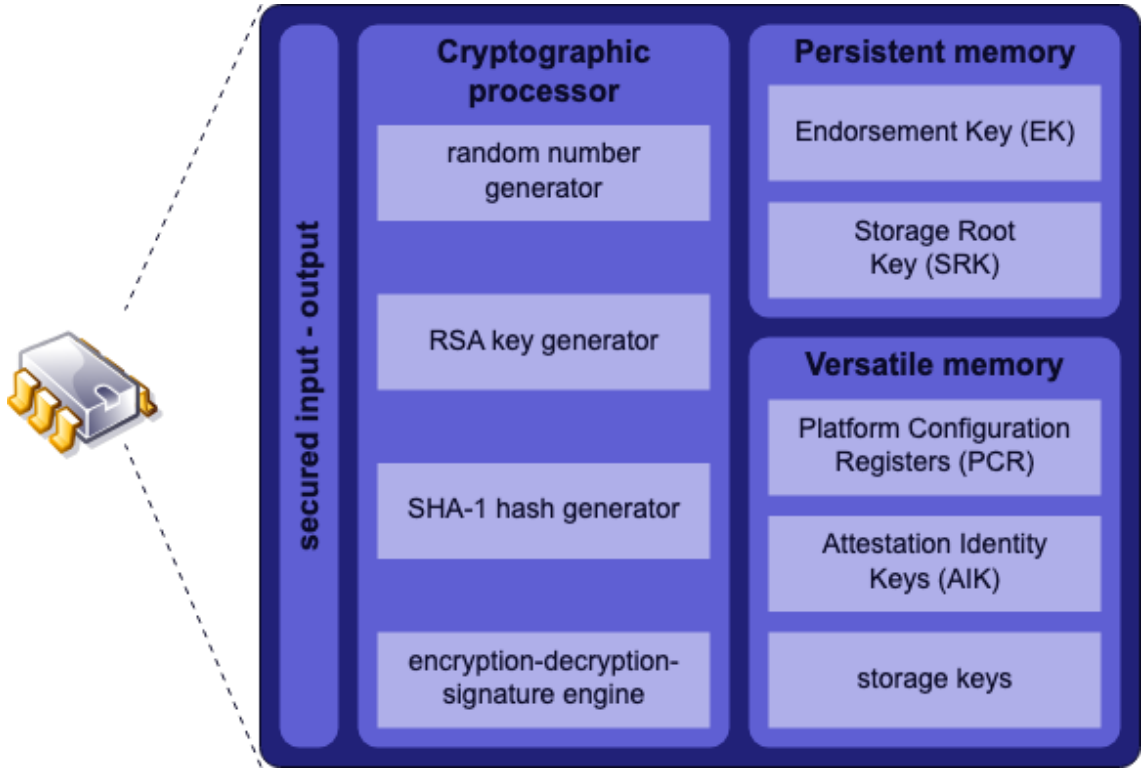
- 보안을 높은 수준으로 보장하기 위해 설계된 특수 보안 칩 또는 하드웨어
  - 소프트웨어 기반 공격으로부터 보호
  - 물리적 격리, 암호화, 키 관리, 인증, 위변조 감지

- 현대 컴퓨터와 장치에서 민감한 정보를 보호하고 시스템의 전반적인 보안 상태를 강화
  - 마이크로소프트는 Windows 11에서 TPM 2.0을 요구사항으로 지정

- 2003년에 설립된 산업 컨소시엄인 신뢰할 수 있는 컴퓨팅 그룹(TCG)의 작업
  IBM, 인텔, HP, 마이크로소프트 등 주요 기술 회사들이
  하드웨어 기반 보안에 대한 오픈 표준을 개발하기 위해 창설

- 버전 1.2(2009년 표준화), 버전 2.0(2015년 표준화)

기능 1



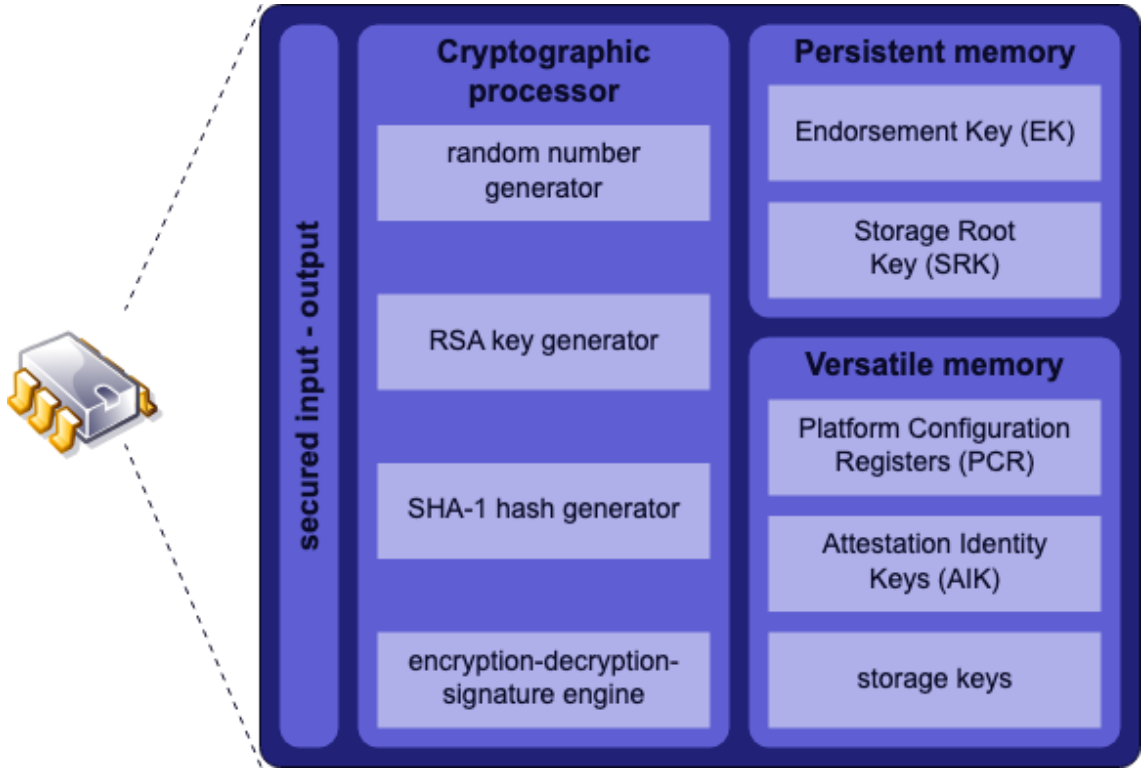
• 인증 키(EK):
EK는 TPM 제조 시 내장된 고유한 비대칭 키 쌍으로,
TPM의 신뢰의 루트 역할. 이 키는 플랫폼 신원 확인 및 인증에 사용.

• 루트 암호화 키
TPM의 **키 계층 구조**에서 최상위에 위치한 키로, TPM 내에서 생성된 다른 모든 키들을 보호하는 역할

• 증명 ID 키(AIK):
AIK는 증명을 위해 디지털 서명을 생성하는 데 사용
AIK는 EK에서 파생되며, EK를 직접 드러내지 않고
TPM이 특정 작업이나 측정을 수행했음을 증명

• 2.0
보증 계층(Endorsement Hierarchy, EH),
저장 계층(Storage Hierarchy, SH) ,
플랫폼 계층(Platform Hierarchy, PH)

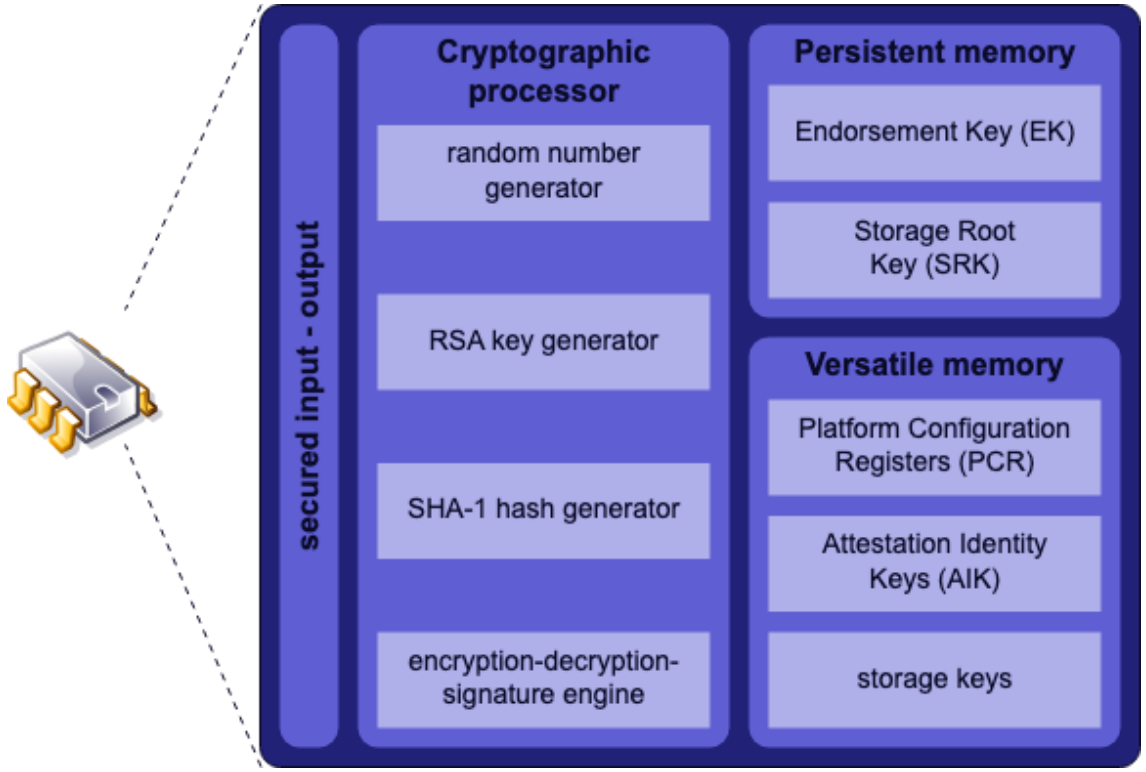
기능 2



- PCR :
시스템 구성 요소와 설정의 해시 측정값을 저장하는 특수 레지스터 펌웨어, 부트로더, 운영 체제 구성 요소 등이 측정 대상

부팅 과정에서 로드되는 각 구성 요소는 해시 측정되어 PCR에 저장.
이를 통해 펌웨어부터 운영 체제까지 "신뢰의 연쇄"가 형성.
구성 요소가 변경되면 PCR 값이 변경되어 무결성 위반

기능 3



• 증명(Attestation):
증명은 TPM이 장치가 특정 상태에 있거나 특정 작업이 수행되었음을 증명하는 과정
PCR 값 또는 기타 중요한 데이터를 TPM에 저장된 AIK(Attestation Identity Key)로 서명하여 수행

• 원격 증명:
원격 서버는 TPM이 서명한 증명 보고서를 요청해 장치의 무결성을 검증 가능
이는 장치가 네트워크 자원에 접근하기 전에 보안 상태임을 보장하기 위해 자주 사용

기능 4

- 모노토닉 카운터(Monotonic Counter):
  시간이 지나도 줄어들지 않고 계속 증가하는 카운터로,
  이벤트의 순서를 추적하고 재사용 공격을 방지하는 데 사용
  - 증가만 가능: 모노토닉 카운터는 외부의 요청이나 이벤트에 의해 증가하지만, 감소하거나 초기화 불가
  - 이벤트 추적: 특정 작업(예: 데이터의 서명, 암호화된 트랜잭션의 수 등)이 발생할 때마다 카운터 값이 증가하며,
    이 값을 이용해 특정 이벤트가 일어난 순서를 보장 가능

- Trusted Timestamp :
  외부 신뢰 시간 소스와 연동하여 이벤트가 발생한 정확한 시간을 기록하고, 그 시간 기록의 무결성을 보장하는 기능
  - 외부 시간 소스 연동: TPM 자체는 시계 기능을 가지고 있지 않기 때문에, 신뢰할 수 있는 타임스탬프를 제공하기 위해 외부의 신뢰할 수 있는 시간 소스(예: NTP 서버, GPS 시간 정보 등)와 통합
  - 타임스탬프 생성: 특정 이벤트(예: 데이터 서명, 파일 생성 등)가 발생할 때, TPM은 이 이벤트를 신뢰할 수 있는 외부 시간 소스로부터 받은 시간과 연관시켜 타임스탬프를 생성

TEE 비교

- **TEE**는 CPU 내에서 **안전한 실행 환경**을 제공하여 메인 OS와 격리된 신뢰할 수 있는 애플리케이션을 실행하는 데 중점

➢ TEE는 일반적인 보안 실행을 위해 설계

- **TPM**은 **하드웨어 기반 보안** 및 **암호화 키 관리**를 제공하여 시스템의 무결성과 보안을 특히 부팅 시점에서 보장하고 민감한 데이터를 안전하게 저장하는 데 중점.

➢ TPM은 하드웨어 부팅 프로세스의 보안, 플랫폼 무결성 보장, 및 키의 안전한 저장에 중점

	TEE	TPM
주요 목적	안전한 실행 환경 제공	하드웨어 기반 보안 및 암호화 키 관리
보호되는 공간	CPU 내의 격리된 실행 환경	독립적인 하드웨어 칩
기능	- 안전한 코드 실행 - 민감한 데이터 보호 - 원격 증명 지원 - DRM, 결제, 사용자 인증 등	- 암호화 키 생성 및 저장 - 시스템 부팅 무결성 검증 - 플랫폼 인증 및 증명 - 보안 기능 (예: 암호화, 해싱)

TEE 기반 블록체인 합의 알고리즘

- PoET
  - TEE를 활용하여 무작위로 부여된 대기 시간을 통해 블록 생성자를 선택하는 방식
  - PoET의 핵심 기능인 무작위 대기 시간 생성과 그 무결성을 보장하는 역할
- PoL
  - PoL에서는 각 노드가 무작위로 생성된 운(luck) 값을 사용하여 블록을 생성하고, 가장 운이 좋은(즉, luck 값이 높은) 노드가 블록을 채굴
    TEE는 이 운의 값을 공정하게 생성하고, 이를 기반으로 블록 생성 과정을 보호

- 대기 시간
- 블록 생성 과정의 무결성 보장
- 무작위 수 생성
- Monotonic Counter 사용 무결성 검증
- 원격 인증(Remote Attestation)

진행사항

- TPM 조사
  - 기능
  - TEE와 차이
  - 블록체인 관련

  ➢TEE와 유사하게 적용은 가능하나 어플리케이션 실행의 무결성은 보장 X

  ➢표준 O, 개별 하드웨어 모듈-IoT 적용의 장점

  ➢블록체인의 보안 요소를 강화하는데 사용 적합

- 보유 환경에서 tpm2-tss 라이브러리 c코드 테스트

Q & A