Attestation in Client SSDs for Ensuring Data Security

David Yeh

Product Marketing Manager of Client SSD Controller

Silicon Motion Technology Corp.

Agenda

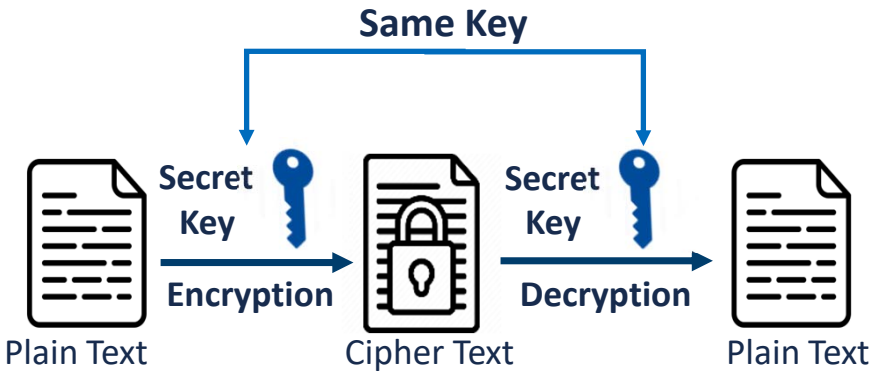
- Background
- HMAC (Hash-based Message Authentication Code) Algorithm
- RSA (Rivest-Shamir-Adleman) Algorithm
- Concept of Attestation
- DICS Attestation
- Summary

Background

- With escalating data breaches and security threats, ensuring the protection of sensitive data has become increasingly important, especially when it comes to storage.
- Client SSDs offer critical security features that play a crucial role in protecting data integrity and authenticity.
- Security implementations have continuously evolved in response to the increasing risks posed by data breaches and attacks. This evolution can be observed from the early methods like HMAC and RSA encryption to the modern approach of attestation.

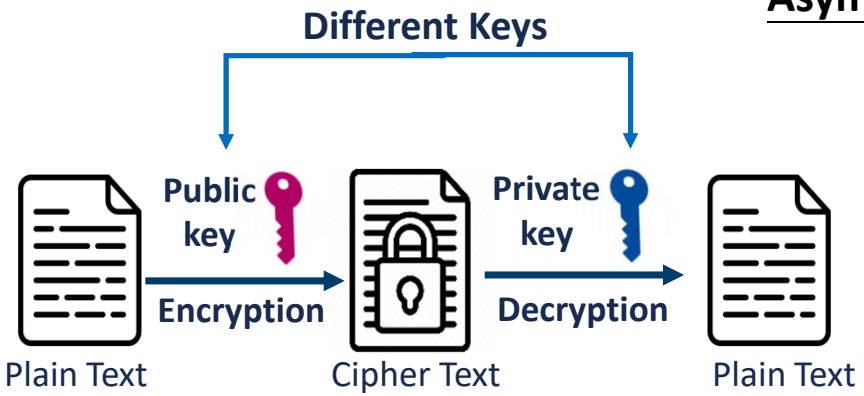
Symmetric and Asymmetric Cryptography

Symmetric Encryption



- Using the same key for encryption and decryption
- Ex. HMAC (Hash-based Message Authentication Code)

Asymmetric Encryption



- Using a key pair for separate encryption and decryption.
- Ex. RSA (Rivest-Shamir-Adleman)

SiliconMotion

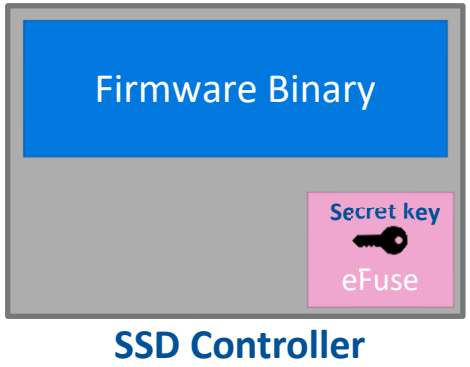
Introduction of HMAC

Flash Memory Summit

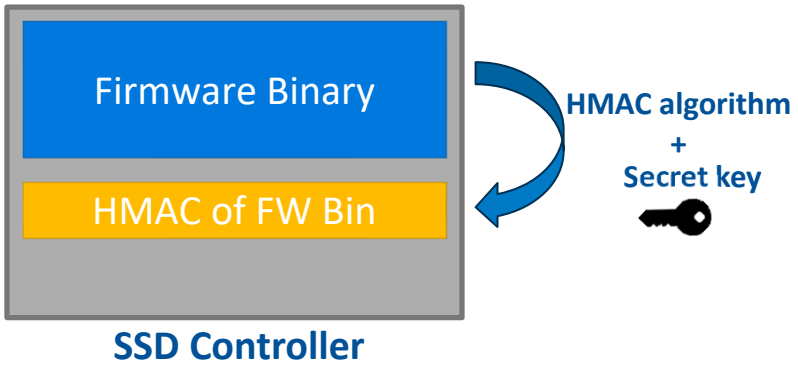
- HMAC (Hash-based Message Authentication Code) is a cryptographic mechanism for message authentication.
- It combines a hash function and a secret key(root key) to generate an authentication code.
- The receiver can verify the integrity of the message by recalculating the HMAC using the shared secret key and comparing it to the received HMAC.
- HMAC provides tampering resistance and detects even minor changes in the message.

Firmware Protection from HMAC

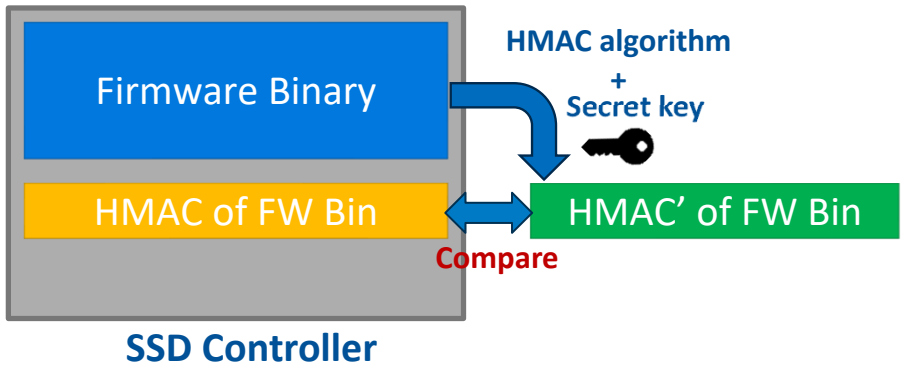
1. Generate a random key and store it in the eFuse.



2. During the production process, the FW Binary is processed using the HMAC algorithm with a secret key, and the output is stored into the drive.



3. During the power-on flow, the FW binary will use the HMAC algorithm with a secret key, and the output is then compared with the stored result in the drive to verify the consistency.



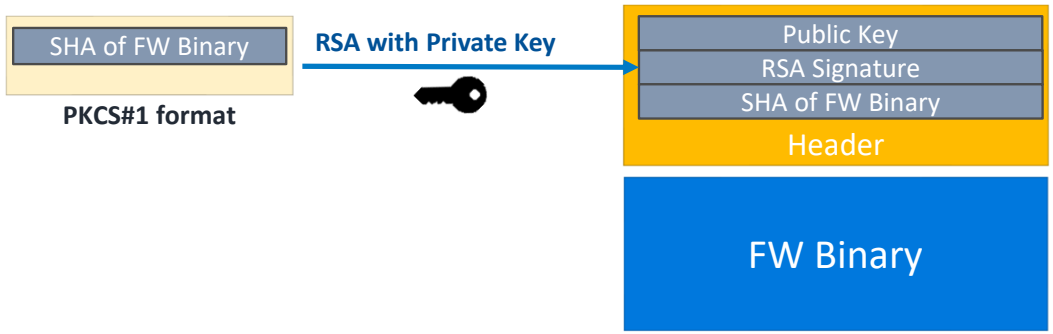
Pros and Cons of HMAC

- Pros:
  - Efficiency: HMAC offers fast computation and verification due to its use of hash functions.
  - Flexibility: HMAC can utilize different hash functions (such as SHA-256, SHA-512, etc.) and keys to meet various security requirements.
- Cons:
  - One-way authentication: HMAC only provides message integrity verification and does not offer digital signature.

Introduction of RSA

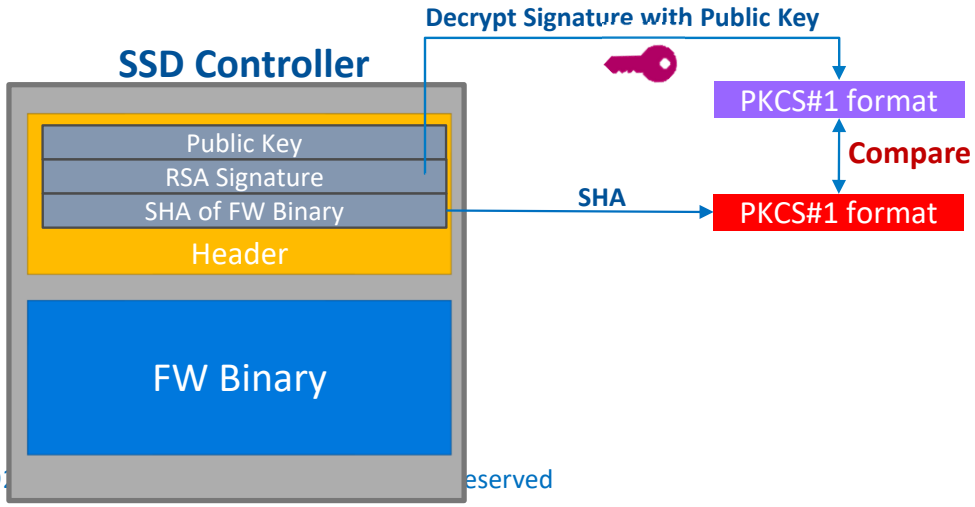
- RSA (Rivest-Shamir-Adleman) is an asymmetric encryption algorithm.
- It involves a pair of related keys: a public key for encryption and a private key for decryption.
- The applications in digital signatures, key exchange, and secure communication.

Firmware Protection – RSA



Generation

- The client (partner) will generate a key pair consisting of a private key and a public key.
- To generate an RSA signature using the private key in PKCS format for the SHA of FW Binary
- To include the public key, RSA signature, and SHA of the FW Binary in the header



Verification

- During boot or FFU process, the RSA signature can be decrypted using the public key into a PKCS format.
- The decrypted output can be compared with the FW information which stored in the NAND for verification.

Pros and Cons of RSA

- Pros:
  - Digital signatures: RSA enables the generation of digital signatures using the private key to verify the integrity and authenticity of firmware.
  - Public-private key combination: RSA employs public key encryption for verification and private key decryption, offering the advantages of asymmetric encryption.
- Cons:
  - Computational complexity: RSA encryption and verification operations are relatively complex and require more computational resources and time.
  - Key management: Proper management and protection of the private key are essential, and ensuring that only trusted entities access the private key.

Concept of Attestation

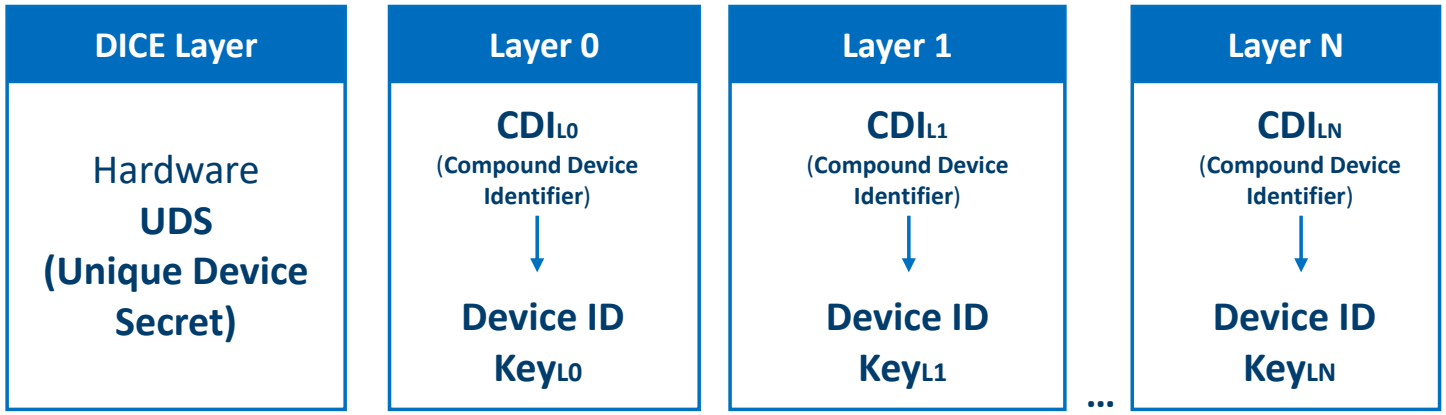
- HMAC and RSA primarily focus on verifying the integrity and authenticity of firmware, while attestation is more concerned with verifying the security state and trustworthiness of the system.

Attestation

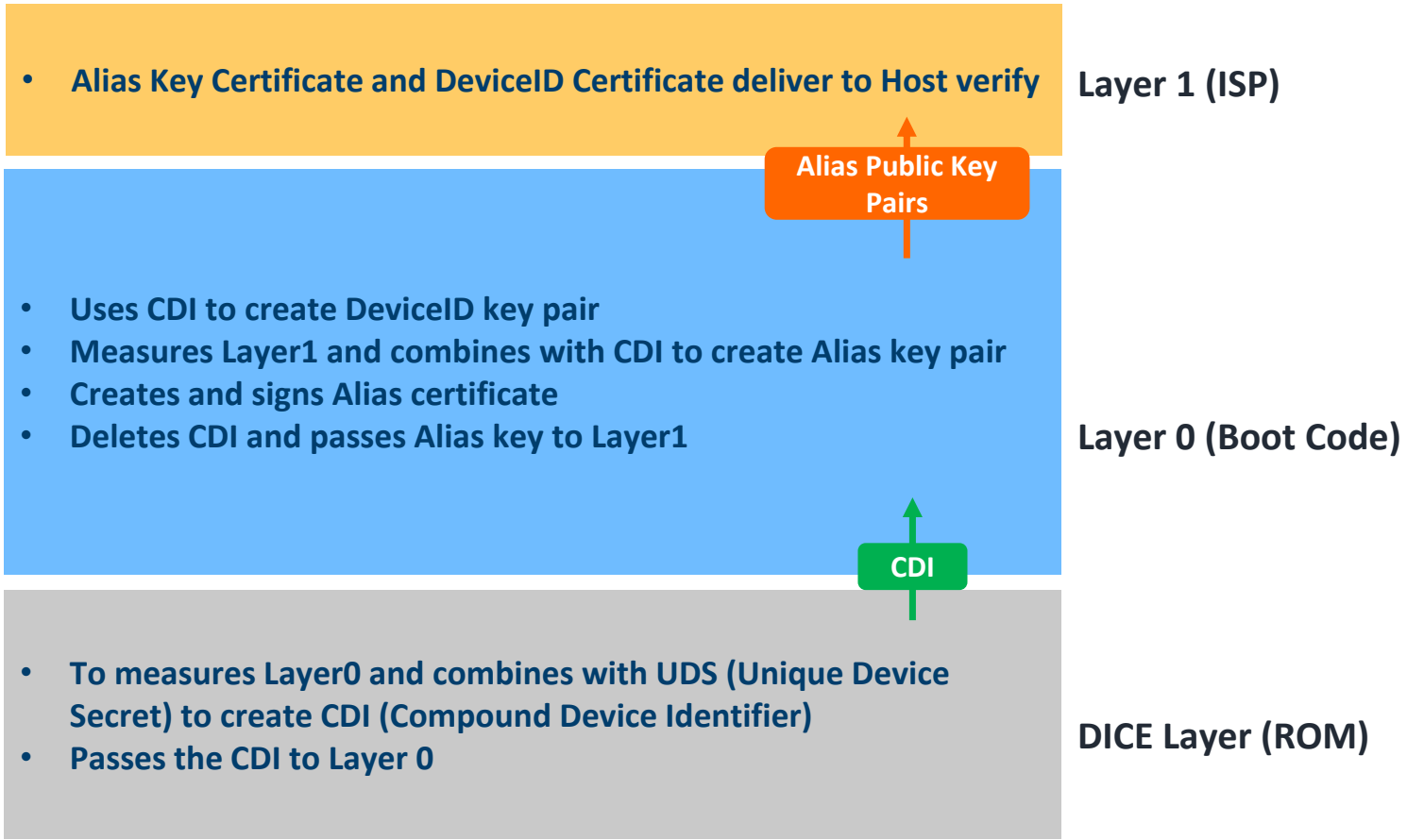
- Attestation is a technology used to verify and ensure the integrity and security of systems. Here are some techniques for implementing attestation:
  - TCG DICE (Trusted Computing Group Device Identifier Composition Engine): It's a technology used to verify the integrity of firmware and hardware.
  - UEFI Secure Boot: UEFI (Unified Extensible Firmware Interface) is a firmware interface used in modern computer systems.
  - Intel SGX (Software Guard Extensions): Intel SGX is a security technology that provides a hardware-based trusted execution environment (TEE) for applications running on Intel processors.

DICE Attestation

- DICE Attestation involves generating an attestation certificate that provides evidence of the device's integrity and authenticity.
- DICE relies on a chain of trust, starting from a trusted root of trust and extending to subsequent levels of trust within the device.



Firmware Protection – DICE Attestation



Summary

- RSA as a more robust encryption and digital signature algorithm compare to HMAC.
- Attestation ensures the verification of system, and maintain the overall integrity and trustworthiness of the system.
- DICE attestation provides a layer of protection by ensuring the integrity of data stored in SSD.
- Utilize DICE attestation on client SSD which provides a foundation of trust for the system, protecting firmware binary and preventing unauthorized access.

SiliconMotion

Flash Memory Summit

Meet us at booth #315

Scan to learn more!