Attestation in Client SSDs for Ensuring Data Security

David Yeh

Product Marketing Manager of Client SSD

Silicon Motion Technology Corp.

Agenda

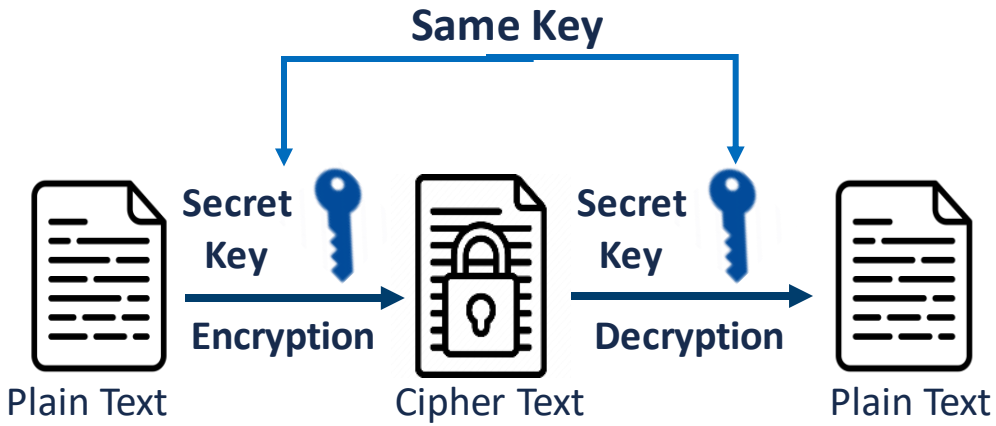
- Background
- HMAC (Hash-based Message Authentication Code) Algorithm
- RSA (Rivest-Shamir-Adleman) Algorithm
- Concept of Attestation
- DICE Attestation
- Summary

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 attestation as one of the security features, proving their identity to the system and ensuring the integrity of firmware and hardware.

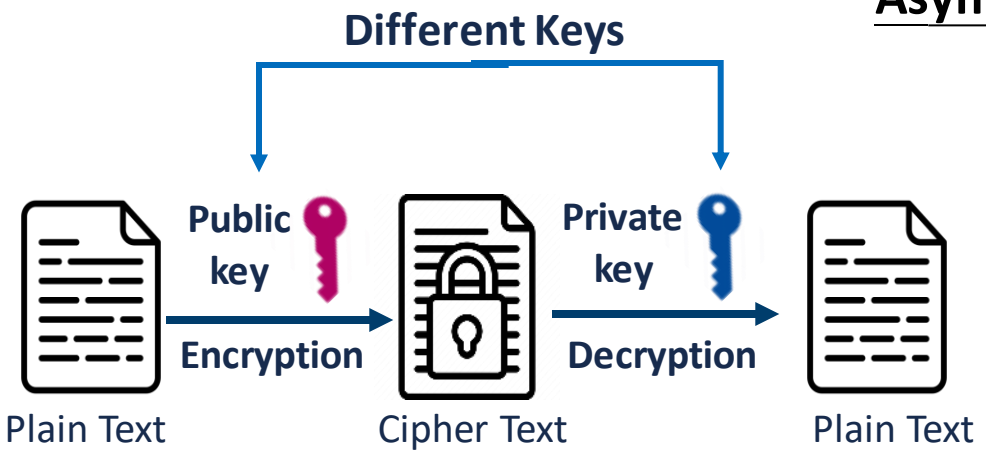
Symmetric and Asymmetric Cryptography

Symmetric Encryption



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

Asymmetric Encryption



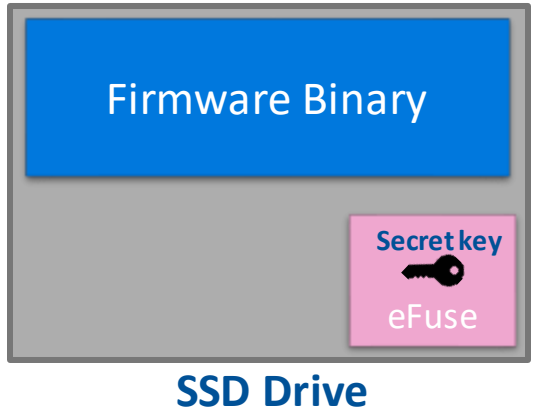
- Using a key pair for separated encryption and decryption.
- Ex. RSA (Rivest-Shamir-Adleman)

Introduction of HMAC

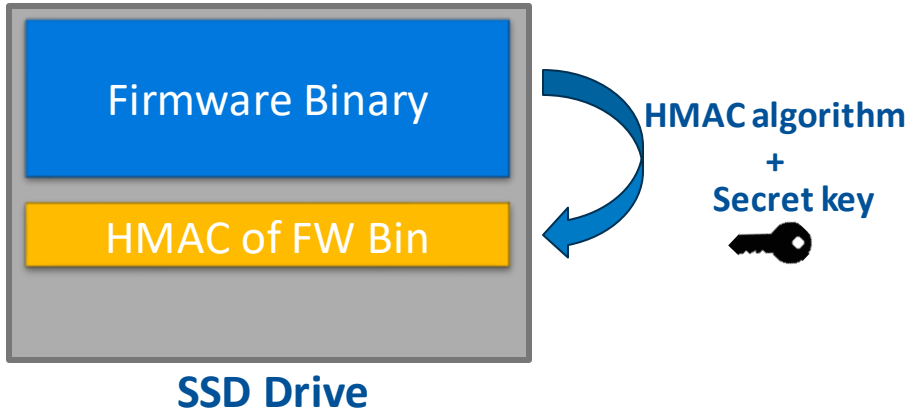
- HMAC (Hash-based Message Authentication Code) combines a hash function and a secret key(root key) to generate an authentication code.
- The receiver can verify the integrity of the message by recalculating the HMAC with the shared secret key.
- HMAC provides tampering resistance and detects even minor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

Firmware Protection - HMAC

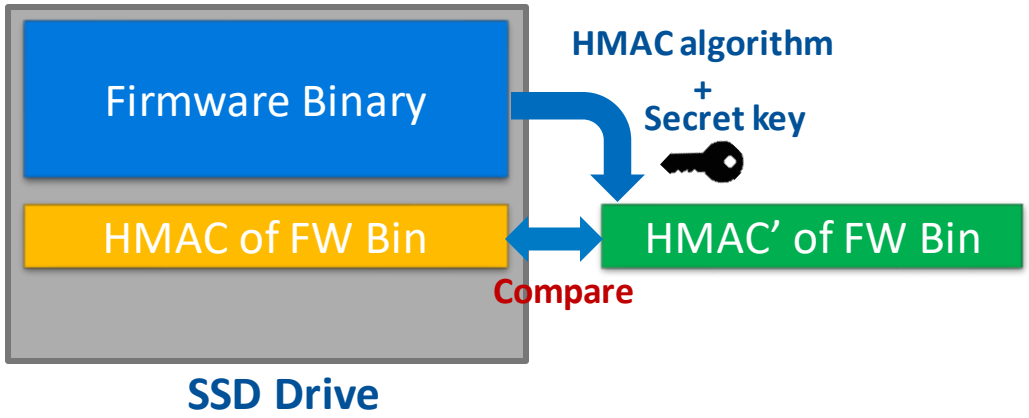
1. Generate a random key and store it in the eFuse.



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.



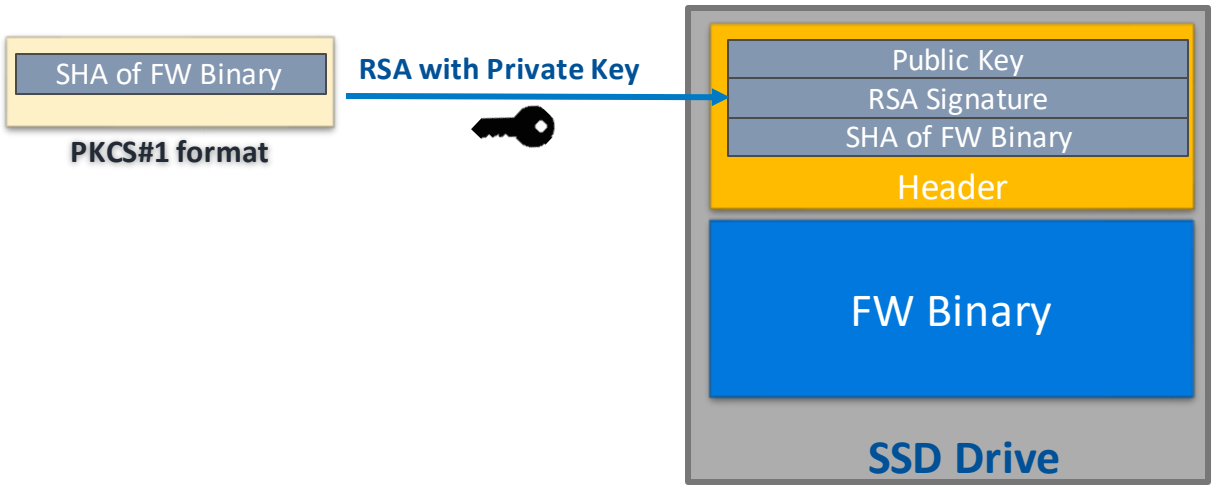
Pros and Cons of HMAC

- Pros:
  - Efficiency: HMAC use hash functions which the output length is fixed, so the computation and verification will be efficient and fast.
  - 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

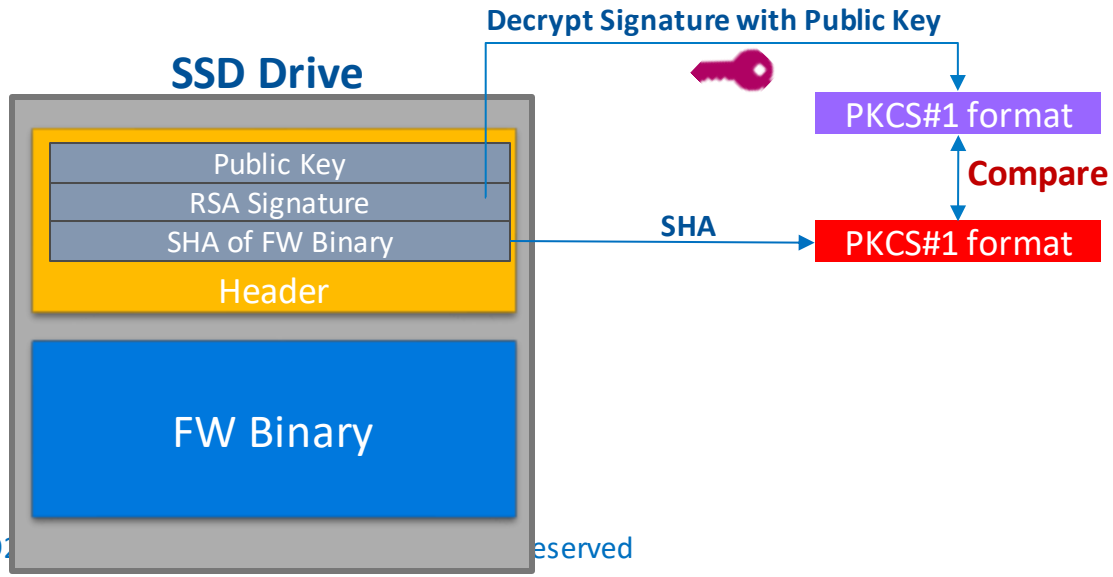
- RSA (Rivest-Shamir-Adleman) is an asymmetric encryption algorithm.
- It involves a pair of related keys: public key and private key for encryption/ decryption.
- The applications in digital signatures and key exchange.

Firmware Protection - RSA



Encryption

- The client (partner) will generate a key pair consisting of a private key and a public key.
- Using the private key to calculate RSA for SHA of FW Binary to generate an RSA signature.
- 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 drive.

Pros and Cons of RSA

- Pros:
  - Digital signatures: RSA is able to generate a digital signature by using the private key to verify the integrity of firmware.
  - Public-private key combination: RSA employs public key and private key, offering the advantages of asymmetric encryption.
- Cons:
  - Computational complexity: RSA encryption and verification operations are relatively complicated 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

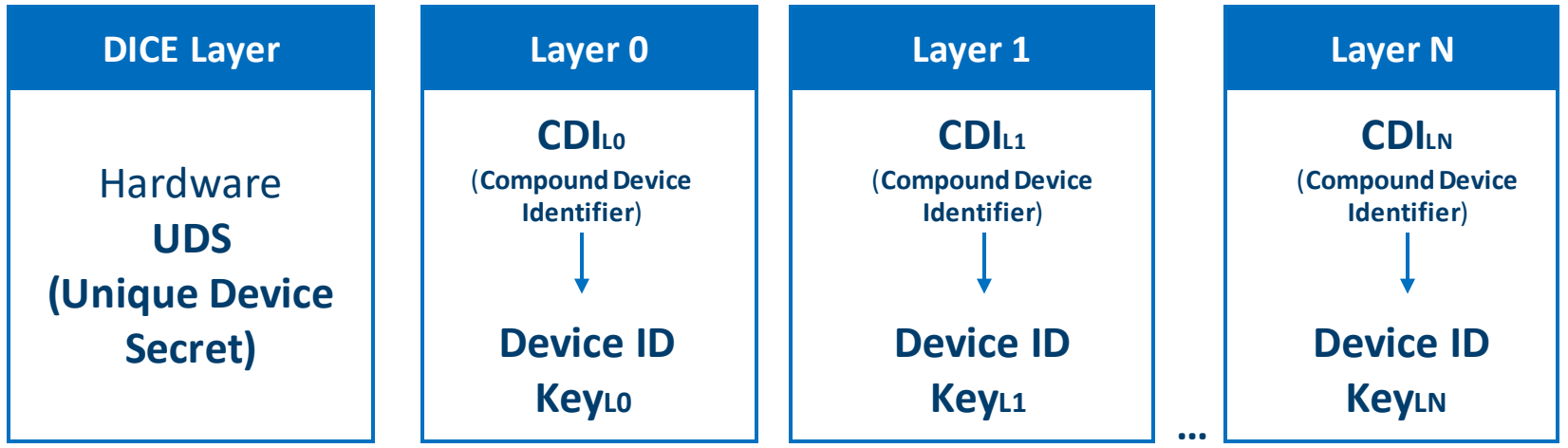
- HMAC and RSA primarily focus on verifying the integrity of firmware, while attestation is more concerned with verifying the security state of the system.

Implementation on 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 (Unified Extensible Firmware Interface) Secure Boot: It's a firmware interface used in modern computer systems. Mainly applied in BIOS protection.
  - Intel SGX (Software Guard Extensions): It's a security technology that provides a hardware-based trusted execution environment (TEE) for applications running on Intel processors.

DICE Attestation

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



Firmware Protection – DICE Attestation

Layer 1 (ISP)

- Alias Certificate and Alias Public Key
- Device ID Certificate and Device ID Public Key

Layer 0 (Boot Code)

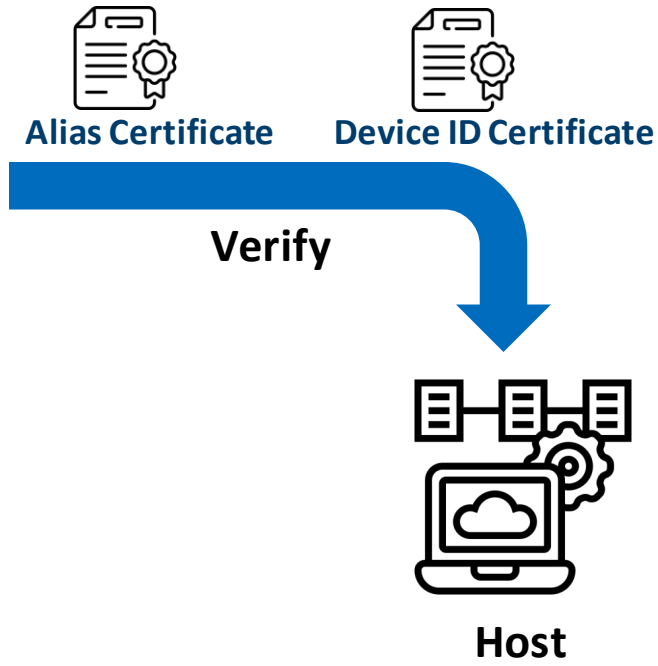
- Uses CDI to create Device ID key pair
- Generates Device ID Certificate by Device ID key
- Measures Layer1 and combines with CDI to create Alias key pair
- Creates Alias certificate by Alias key
- Reset the CDI and passes all certificates to Layer1

DICE Layer (ROM)

- To measures Layer0 and combines with UDS (Unique Device Secret) to create CDI (Compound Device Identifier)
- Passes the CDI to Layer 0

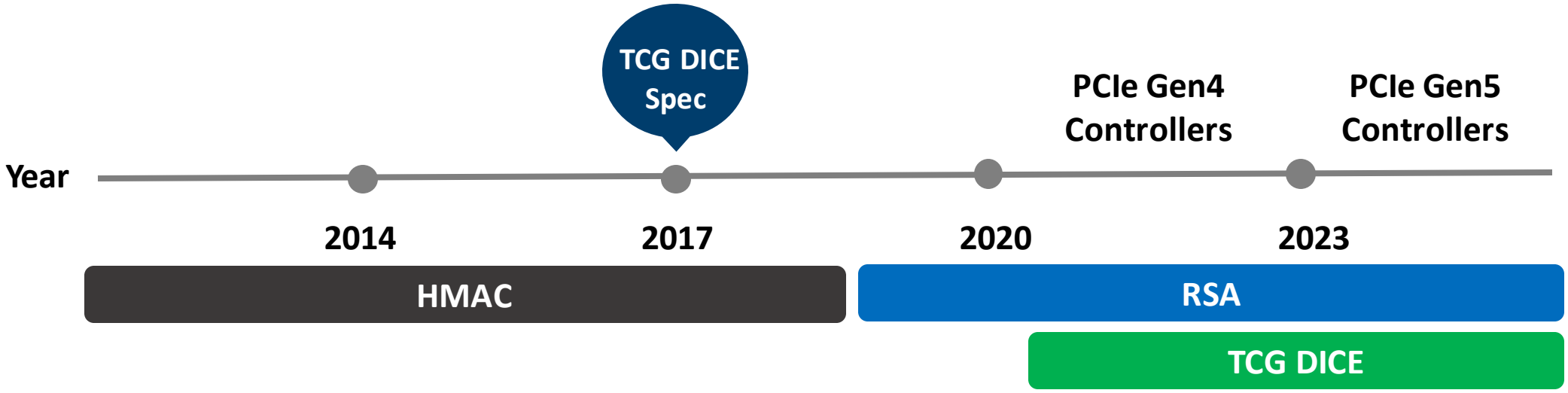
- Alias Certificate
- Device ID Certificate
- Alias Public Key
- Device Public Key

CDI



Security Capability of SMI SSD Controllers

- An increasing number of storage devices are adopting TCG DICE, and SMI PCIe Gen4 and Gen5 controllers come with support for TCG DICE.
- In addition to RSA, we also support TCG DICE to ensure firmware integrity and overall system protection.



Summary

- DICE attestation provides multiple layers of protection for ensuring the integrity of SSD firmware.
- DICE attestation on client SSD can provide a foundation of trust for the system and protect the firmware binary.
- Currently, SMI client SSD products continue to support DICE attestation to ensure a higher level of protection for the integrity of the SSD system.

SiliconMotion

Flash Memory Summit

Innovating Storage in Action!

Meet us at booth #315