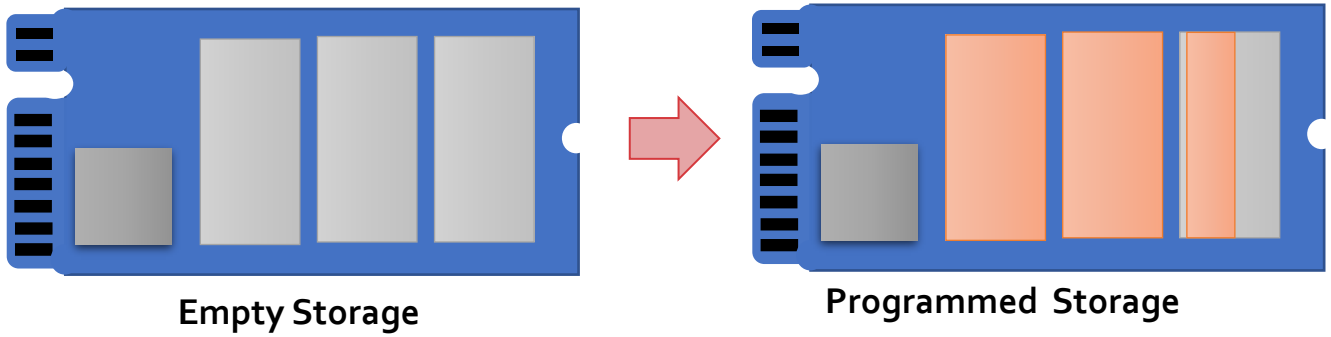
Secure Flash: Lattice of Trust

Vijay Anand

Flashing



Software flashing is the process of:

1. Programming an empty nonvolatile storage with firmware (software)

2. Updating or replacing the firmware (software)

that runs on an electronic device, such as a smartphone, tablet, or computer.

This process involves:

1. erasing the existing firmware if any and
2. installing new firmware

Chain of Trust

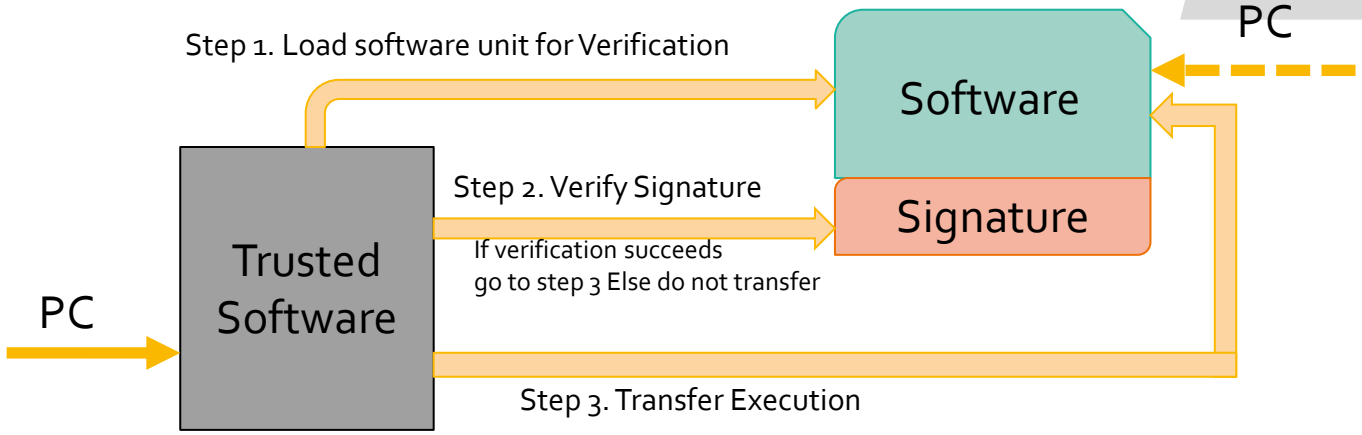
Chain of trust is the identification of transfer of execution paths among independent and contained computing processes whose trust is rooted in immutable trustworthy elements and processes.

Chain of trust plays a role in :

- Authentication of the Application during installation and execution
- Revocation of the Application if an installed application poses a security threat
- Creation of Privileges, Authorization

Chain of Trust forms the basis for Secure Boot and Secure Flash.

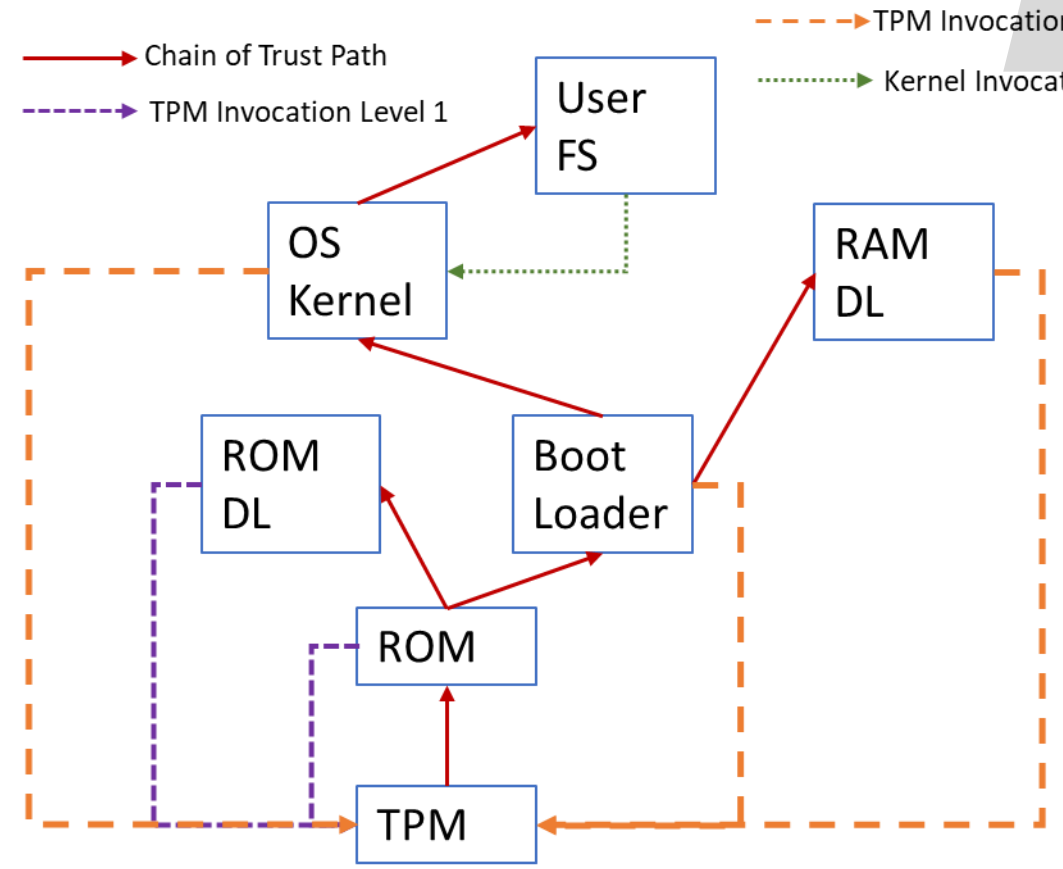
Trust Transfer Process



Steps at every trusted execution transfer interaction:

1. Load the software unit into RAM from Non Volatile Memory
2. Verify the signature of the software unit
3. If signature validation is successful transfer the execution else stay at current software execution

Chain of Trust Paths



ROM DL – ROM Downloader to Program Device
RAM DL – RAM based Application Programmer
OS Kernel – Operating System Kernel

User FS – User File System
TPM – Trusted Platform Module
ROM – Read Only Memory

Trust Evaluation

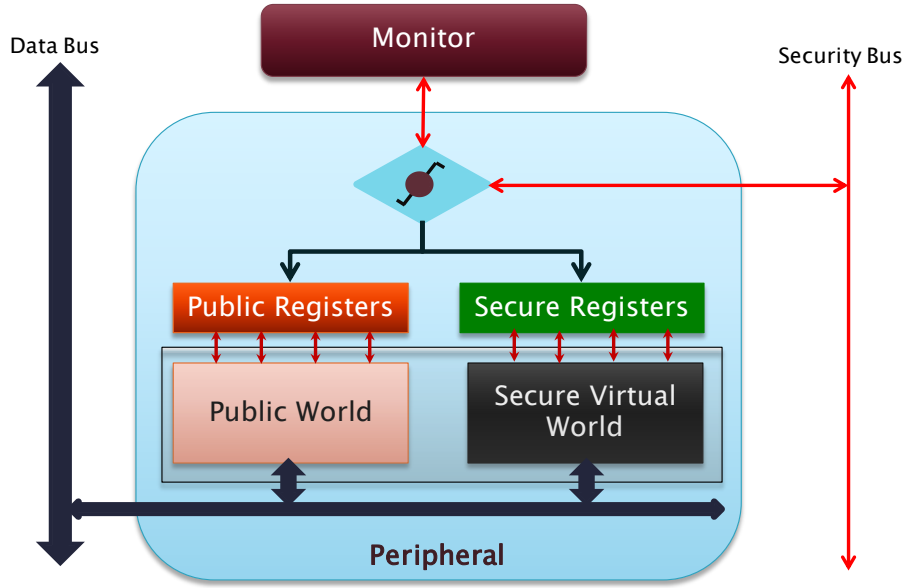
Trust in a computing system is rooted on confidentiality and integrity which are evaluated on the basis of encryption quality, protected key generation and storage, tamper resistant execution, and hashing.

Thus, in this chain of trust architecture for secure systems, the quality of trust can be isolated to :

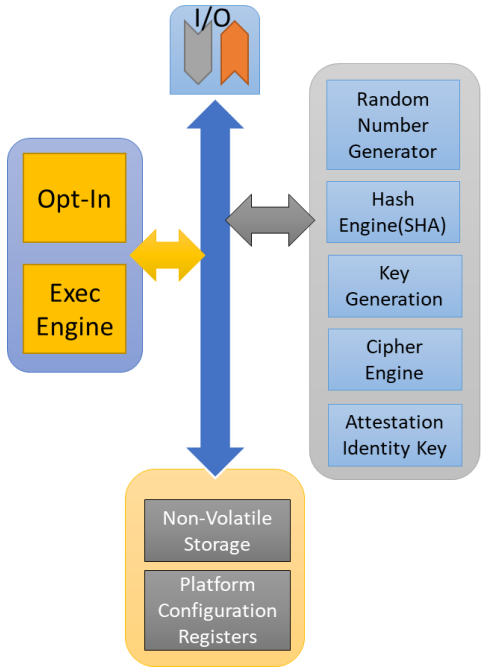
- The roots of trust (Keys)
- The quality of encryption,
- The quality of the hashing function,
- The software code quality and
- Hardware quality with respect to protecting the key assets in a system.

Trusted Platform Modules are hardware that provide such capabilities of establishing and evaluating trust

Trusted Platform Modules



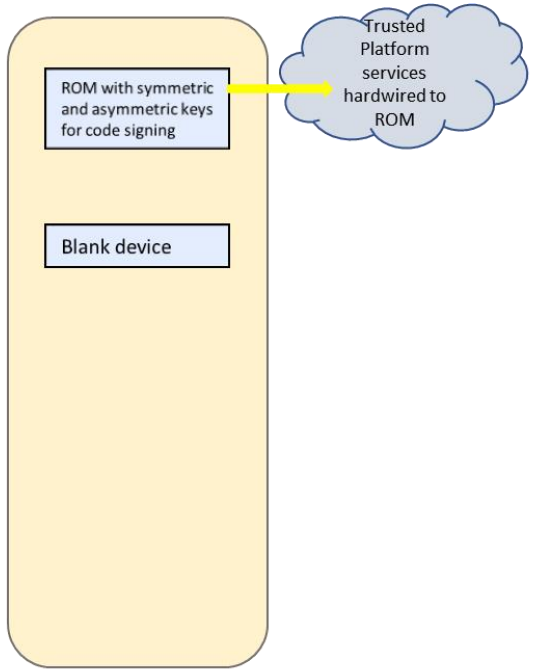
TrustZone



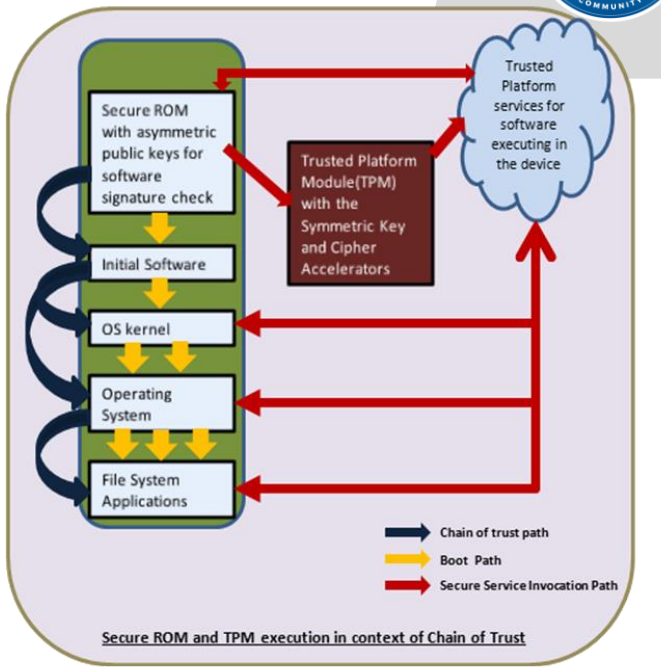
Trusted Computing Group

Trusted Platform Modules(TPM) are hardware implementation of security operations that provide hardware solutions to integrity and confidentiality aspects security. The two common TPM types are TrustZone® for ARM processors and Trusted Computing Group(TCG) TPM 1.2 specification

Trusted Execution Path: Secure Boot



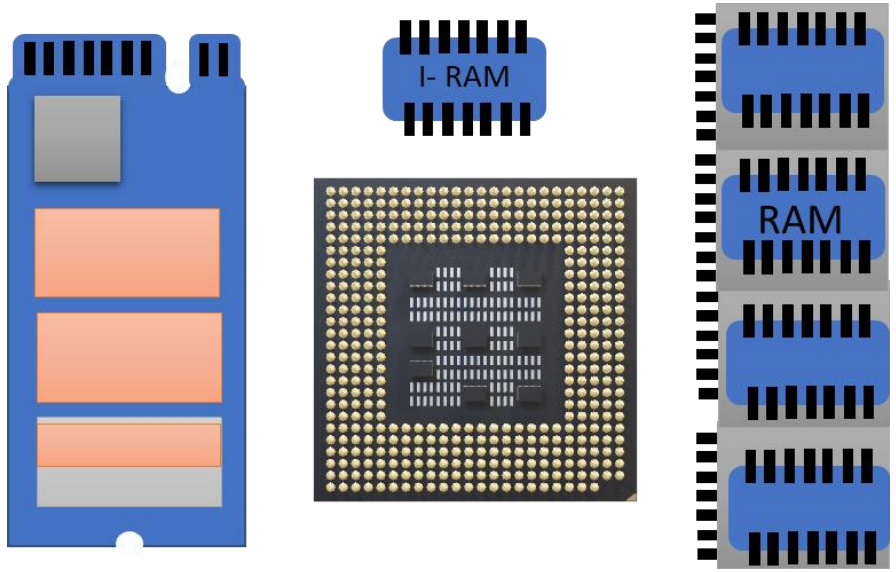
Device without any Software



Device with Operating System

Secure Boot

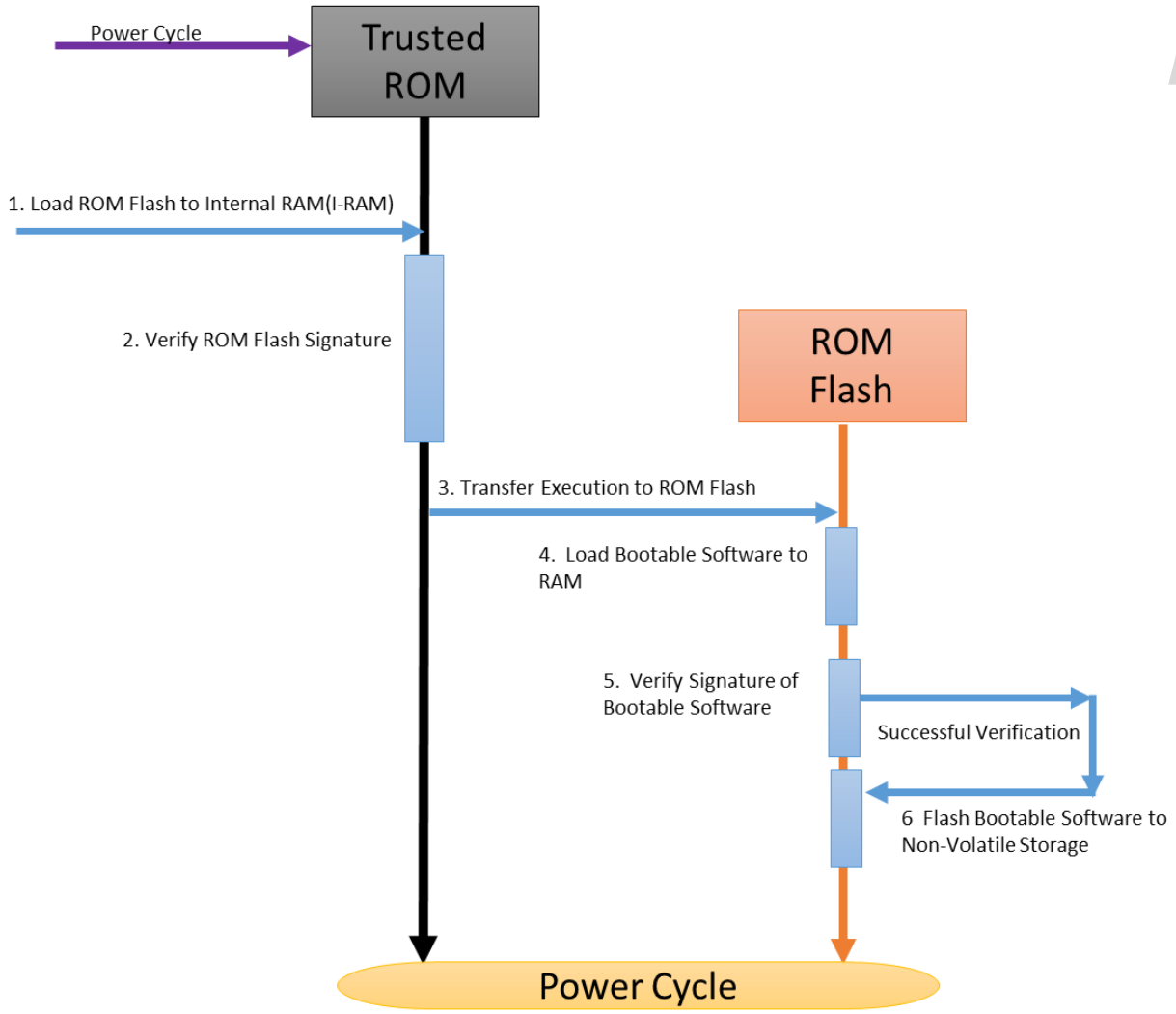
Hardware Setup for Flashing



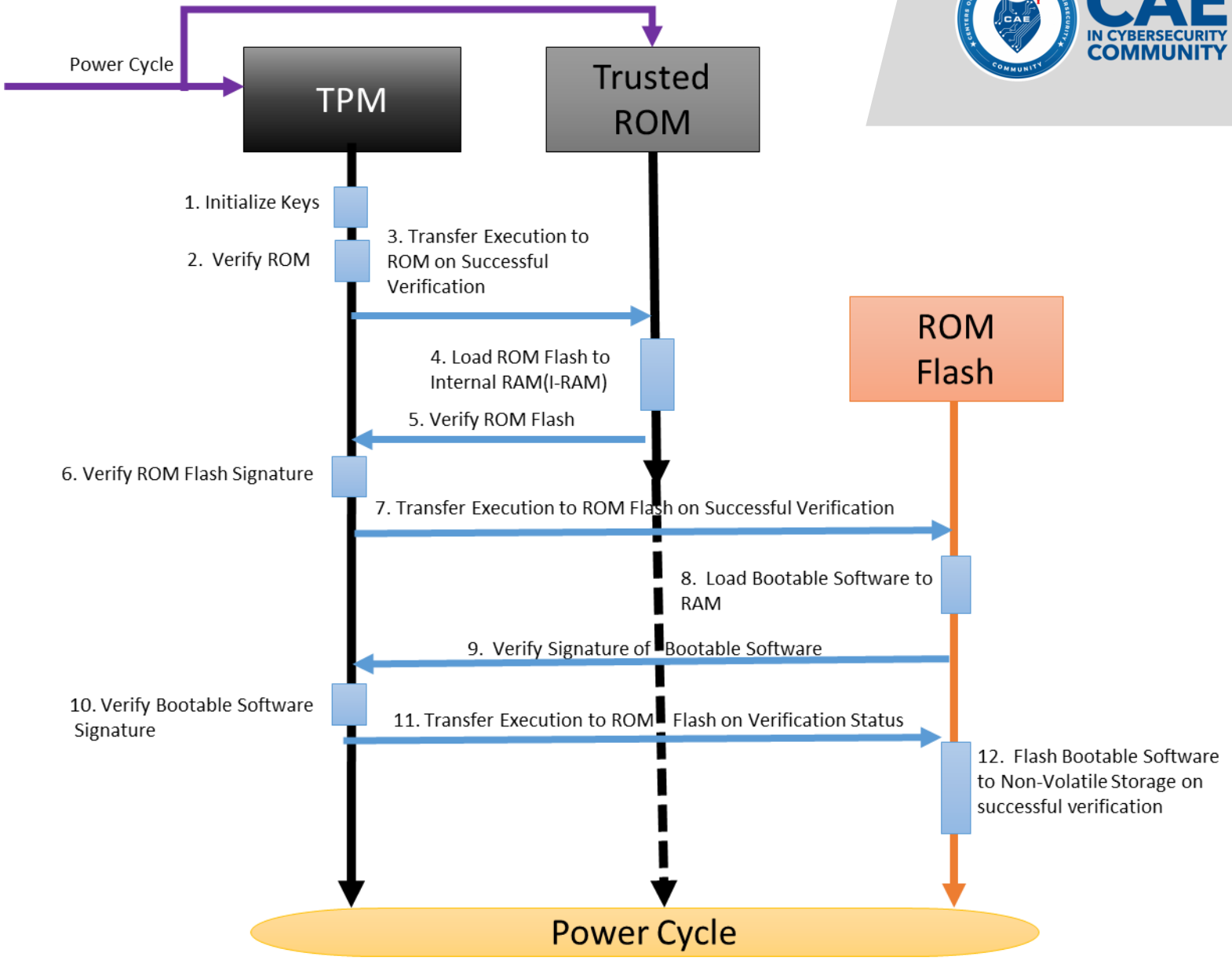
Computing Elements:

1. Processor
2. Internal Ram (I-RAM)
3. Random Access Memory(RAM)
4. Non-Volatile Storage

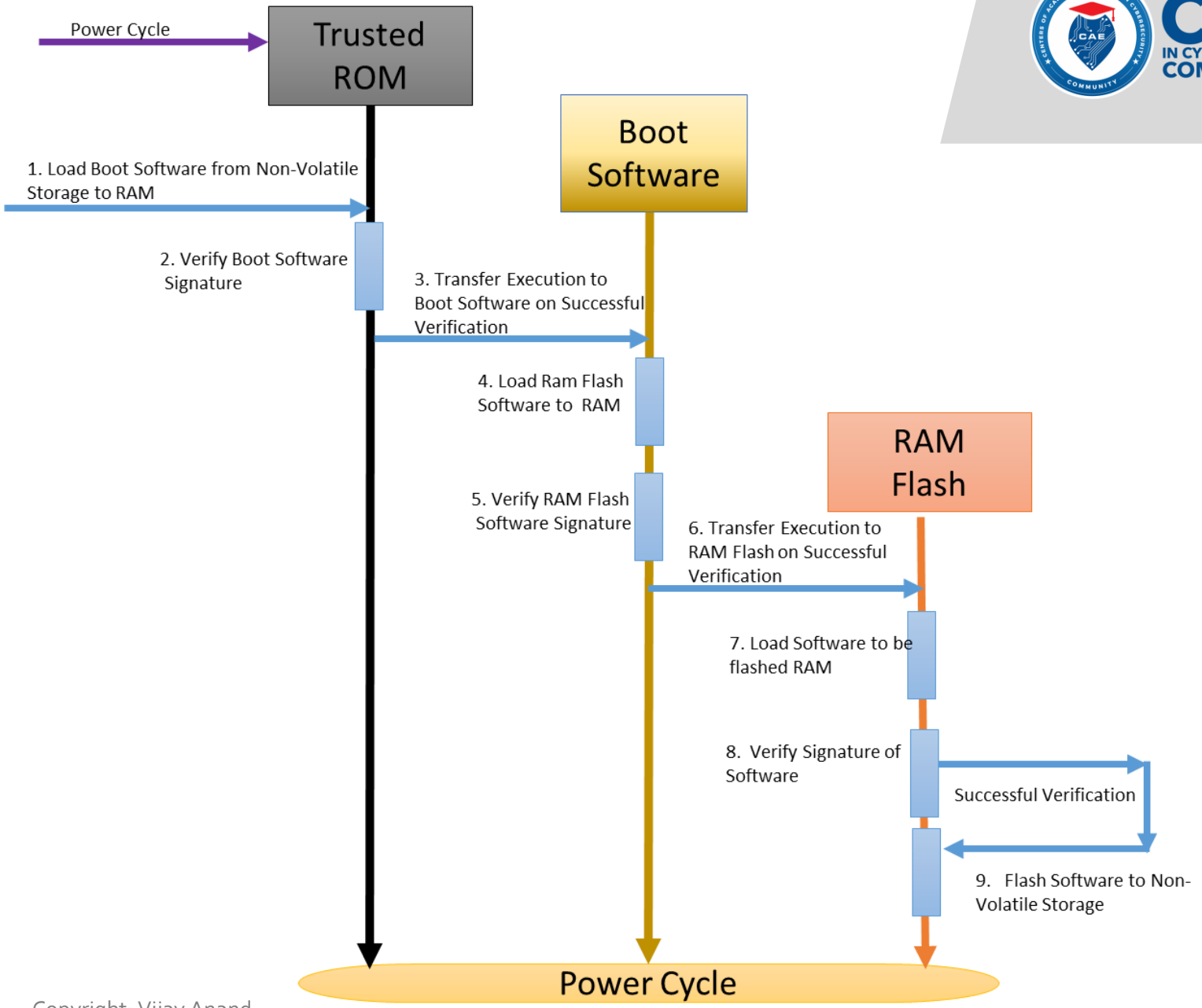
Secure ROM Flash



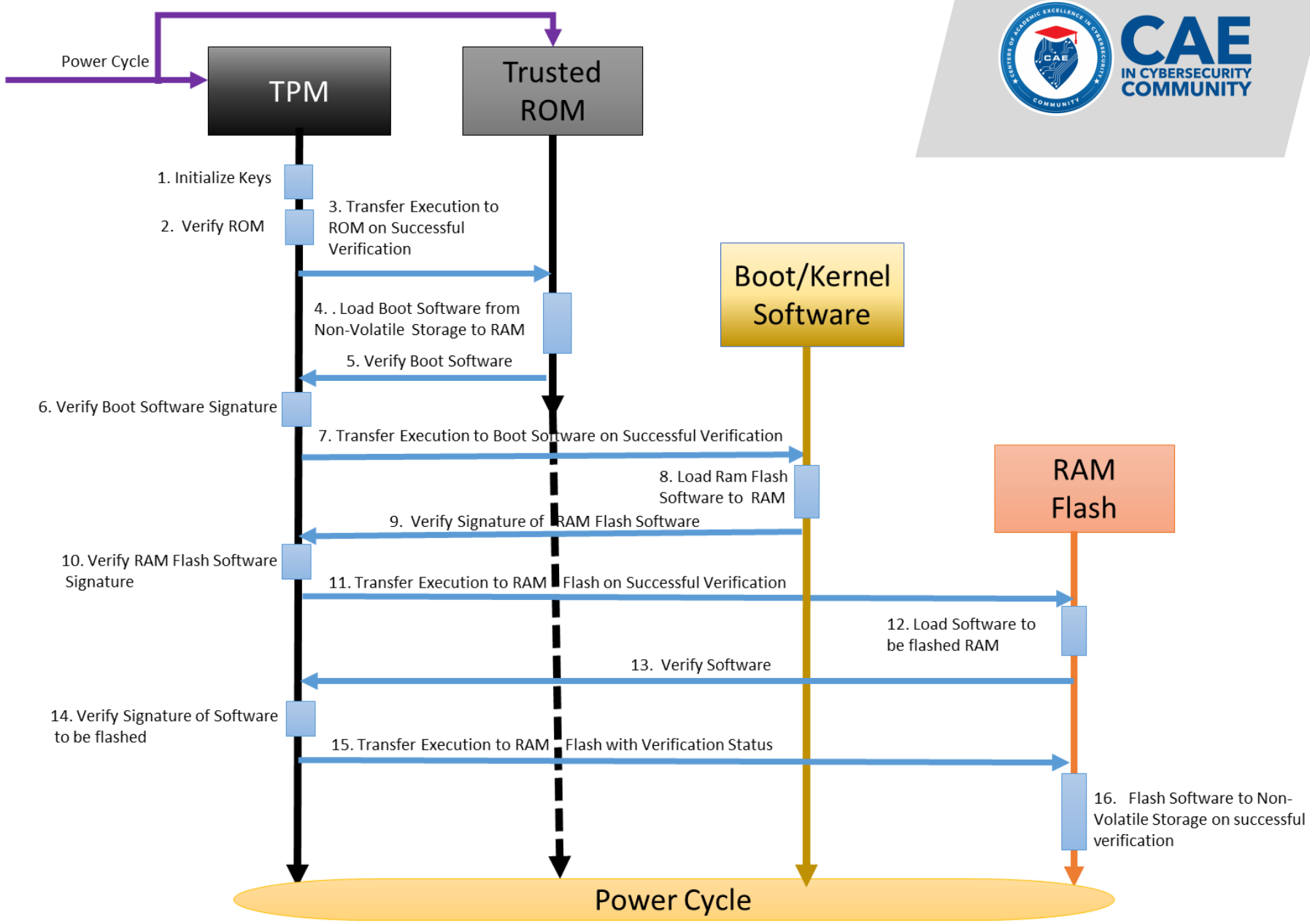
TPM Enabled Secure ROM Flash



Secure RAM Flash



TPM Enabled Secure RAM Flash



Thank You

Questions?