Apple’s Secure Enclave

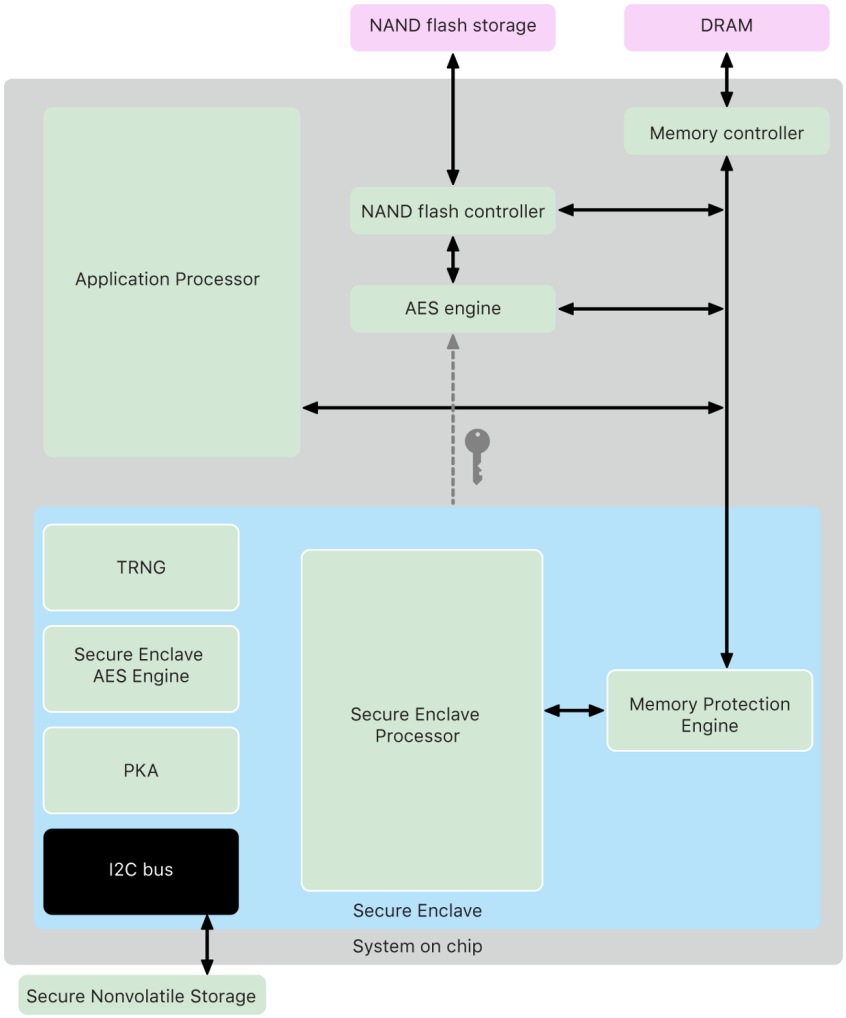
Vishal Srinivasan, Tim Shannon

What is The Secure Enclave Subsystem?

A system on Apple Systems with one purpose:
To protect your sensitive data

It manages:

- Passcodes
- Apple Pay Data
- Biometric data
  - Face ID
  - Touch ID
- Any additional password protected data

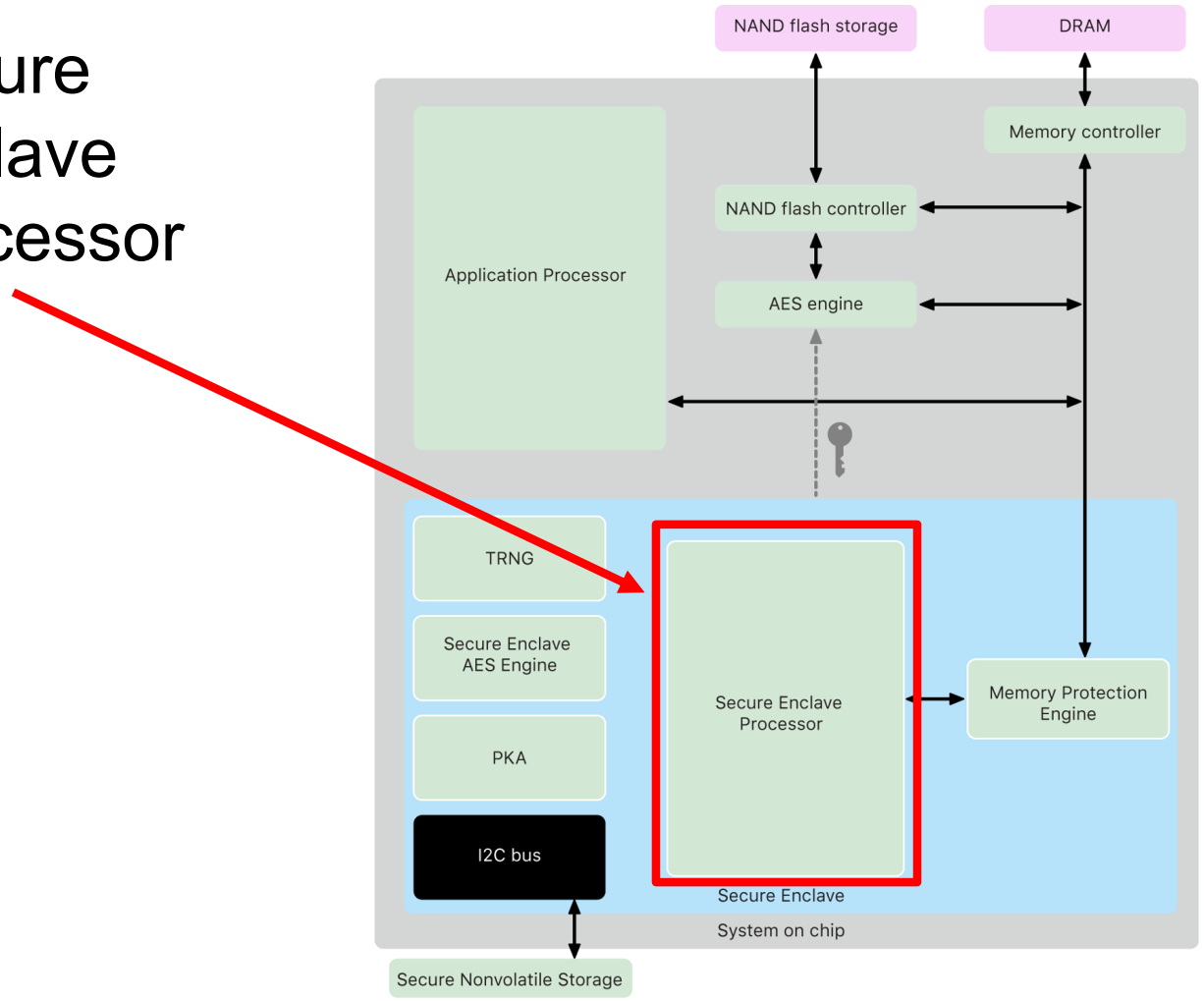


Secure Enclave:
System Design and Components

System Component List

- Secure Enclave Processor
- Memory Protection Engine
- Secure Enclave Boot ROM
- Secure Enclave Boot Monitor
- True Random Number Generator
- Root Cryptographic Keys
- Secure Enclave AES Engine
- Public Key Accelerator
- Secure nonvolatile storage
- Secure Neural Engine
- power and clock monitors

Secure Enclave Processor



Securely booting the secure operating system (sepOS)

1. Secure Enclave Boot ROM

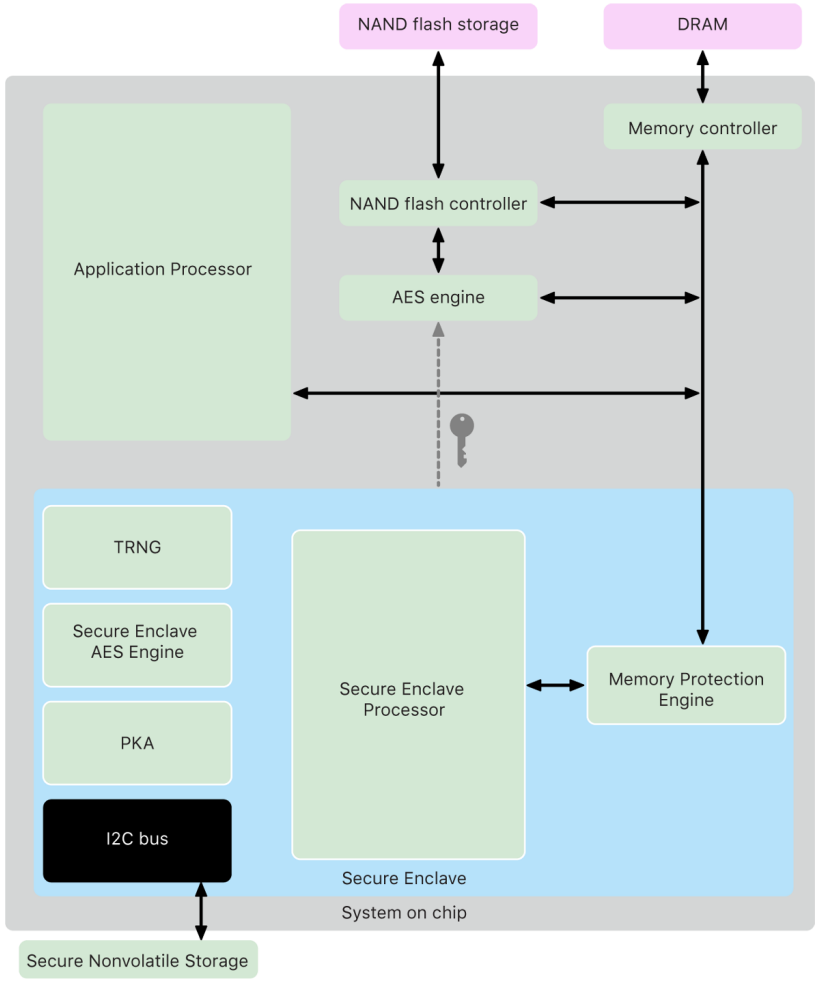
   Read only = immutable = trustable

   Responsible for executing the sepOS

1. Memory Protection Engine

   Isolates section of memory used for Secure Enclave

   Creates key to protect memory, Any data sent to DRAM is encrypted automatically



Securely booting the secure operating system (sepOS)

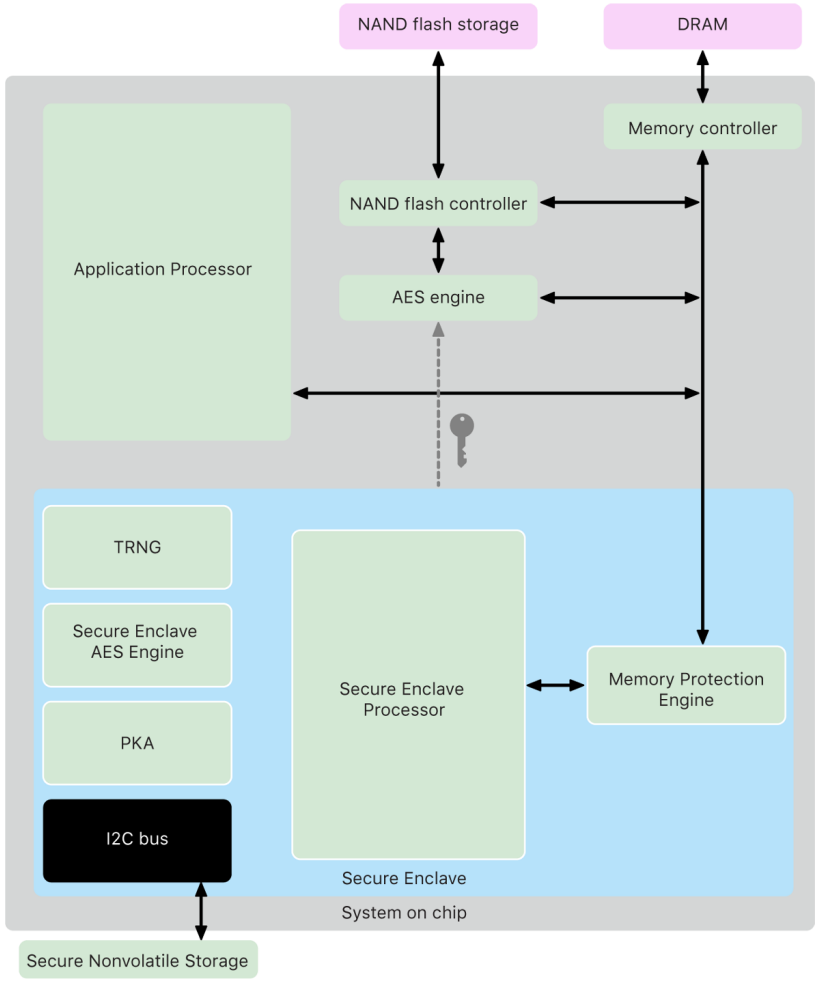
3. Boot Monitor

   Ensures integrity of booted sepOS through hash

   Ensures only trusted ROM code is ran until sepOS is authenticated

   Works with Boot ROM to release privileges to sepOS

3. Copy and Execute!



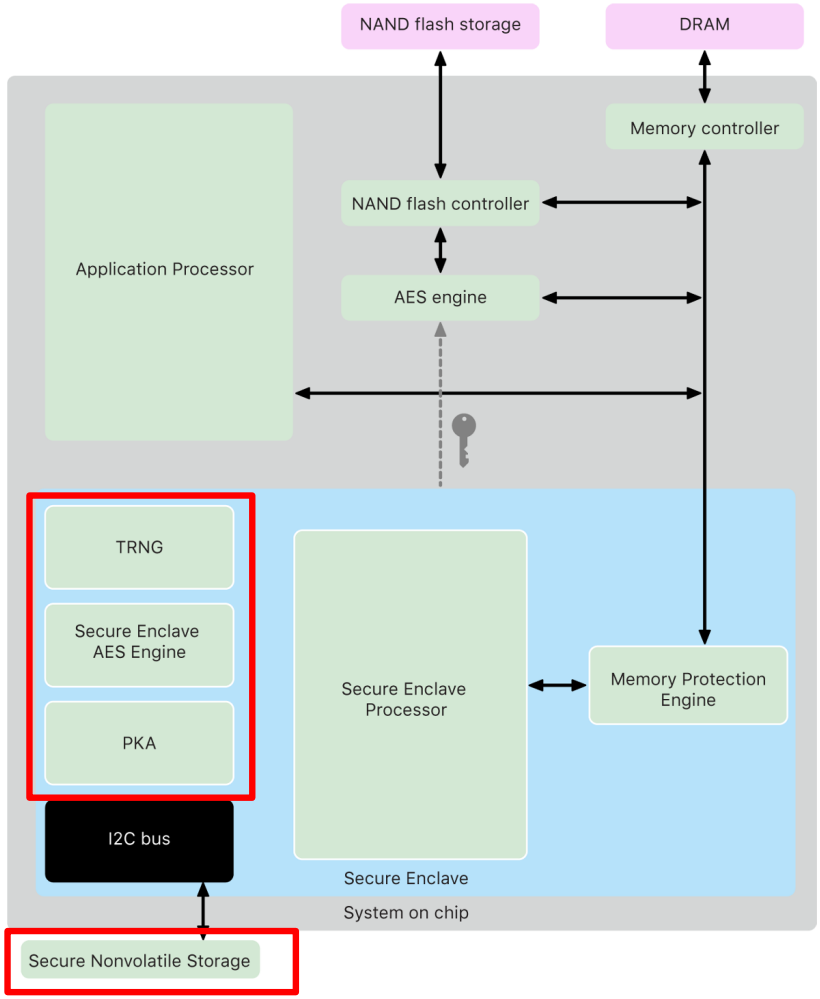
Root Cryptographic Keys

- Secure enclave has a unique ID (UID) root cryptographic key which is generated by TRNG and is written to fuses by the secure enclave during manufacturing
- UID is not accessible to Apple or its suppliers
- UID is used to protect device specific secrets including touch ID and face ID data
- Secure enclave also includes a group ID (GID) which is common for all devices running a specific processor
- GID is used to encrypt device firmware
- Both IDs are 256 bit AES keys

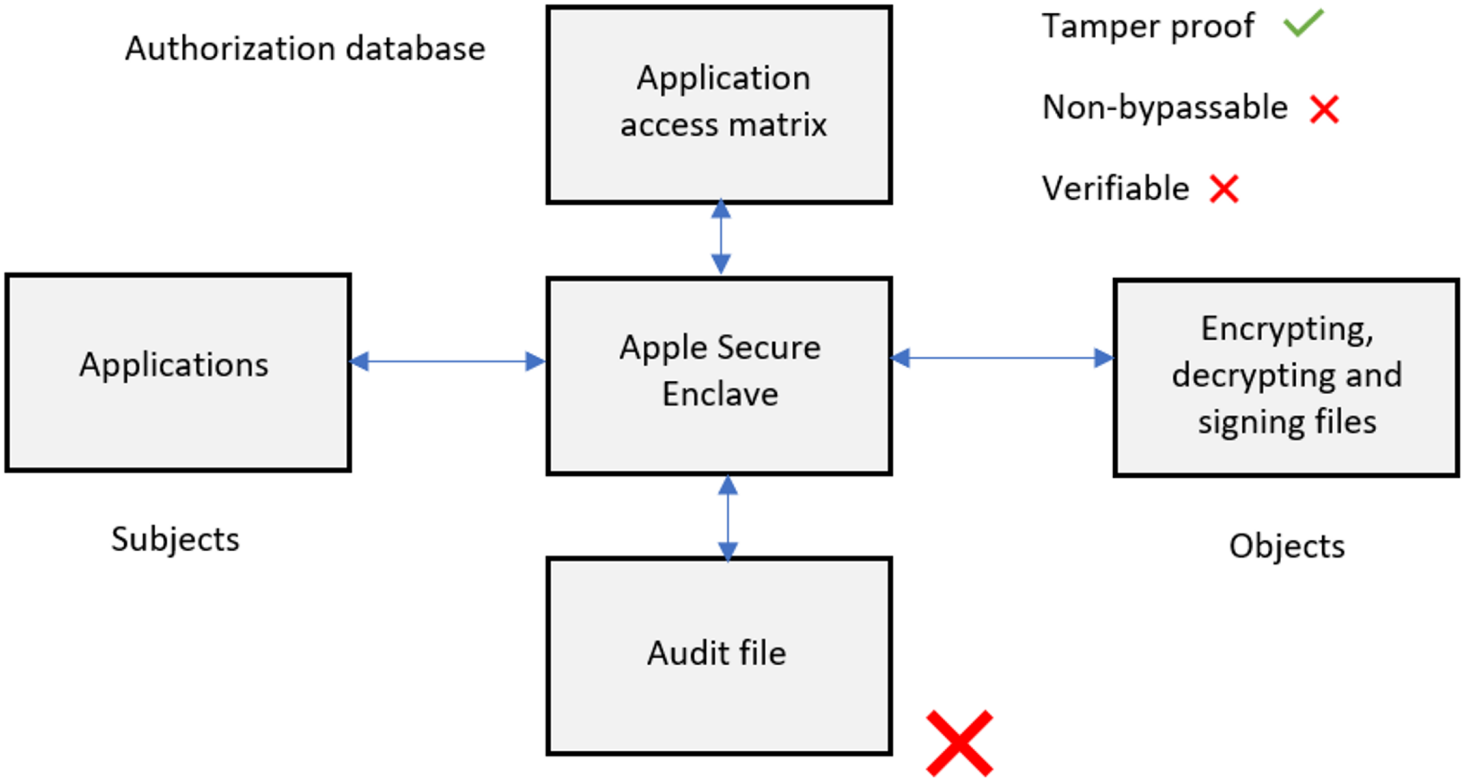
Helpful Hardware features

- True Random Number Generator
- AES Engine
- Public Key Accelerator
- Secure Nonvolatile storage
- Power and clock monitors

excluding neural engine, not necessary to cover. Not present in all apple devices anyways



Comparison to reference monitor



Advantages and Limitations

- Isolated from the main processor which keeps sensitive data secure even if application processor kernel becomes compromised
- It has separate memory and flash storage to protect against unauthorized access
- Holds all the encryption keys and keys are never shared to application processor
- UID is burned into the processor at the time of manufacturing and is generated by the inbuilt TRNG which means even Apple does not have access to this
- Data recovery becomes difficult if the device is damaged since the storage cannot be read without decryption from the secure enclave

Vulnerabilities

- In 2017 a hacker published the private key which allowed access to the secure enclave firmware
- But this information did not put any user data at risk

- In July 2020 a chinese group known as the Pangu Team disclosed a previously unknown vulnerability which affected the secure enclave at a hardware level which could grant access to private keys
- This meant that this vulnerability could not be patched by Apple
- All processors from A7 to A11 bionic are affected by this vulnerability
- Current research does not indicate possibility of remote exploit which means physical access to a device is needed. However this does make it feasible for governmental and law enforcement to break into these devices

References

1. https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web
2. https://www.apple.com/kr/business-docs/iOS_Security_Guide.pdf
3. https://appleinsider.com/articles/20/08/03/security-enclave-vulnerability-seems-scary-but-wont-affect-most-iphone-users
4. https://appleinsider.com/articles/17/08/17/encryption-key-for-iphone-5s-touch-id-exposed-opens-door-to-further-research