

Trusted Computing

Security from the ground up

Danny Fullerton – 2011/11/04




Why I used to hate TC

Palladium®

a chip soldered to our motherboard



A top-down view of several computer monitors arranged in a circle. The monitors are of various colors (grey, white, black) and have different screen displays (circular patterns, solid colors). A central text overlay is present.

all of your actions had to be approved by Microsoft®

I was some kind of frustrated liberal punk...



... there's no way I've could accept this

I've decided to fight this however I've could:

tell everyone how this would affect us

swore to never buy a motherboard with this chip



...and learn about it

How I came to love TC

Trusted Computing != Palladium

it has very interesting security properties

6059 101

Stereo

LONELY
NIGHT

BREAK THE RULES

STATUS
QUO

breaks the status quo
Hackfest 2010 – Broken by Design



No comments on the background



well, I'm still a liberal punk but *paranoiac* too

What went wrong?


My guess:

Trusted Computing is a disruptive innovation

I just didn't understand the technology

What is it?

se·cu·ri·ty

[si-kyoo-r-i-tee]  [Show IPA](#)
noun, plural -ties, **adjective**

-noun

1. freedom from danger, risk, etc.; safety.
2. freedom from care, anxiety, or doubt; well-founded confidence.
3. something that secures or makes safe; protection; defense.
4. freedom from financial cares or from want: *The insurance policy gave the family security.*
5. precautions taken to guard against crime, attack, sabotage, espionage, etc.: *The senator claimed security was lax and potential enemies know our plans.*



Ads

trust [truht] [Show IPA](#)

noun

1. reliance on the integrity, strength, ability, surety, etc., of a person or thing; confidence.
2. confident expectation of something; hope.
3. confidence in the certainty of future payment for property or goods received; credit: *to sell merchandise on trust.*
4. a person on whom or thing on which one relies: *God is my trust.*
5. the condition of one to whom something has been entrusted.



Protection objectives

High : software based attack

Medium : open case

Low : sophisticated local attack

The basic idea

We cannot trust the entire platform...

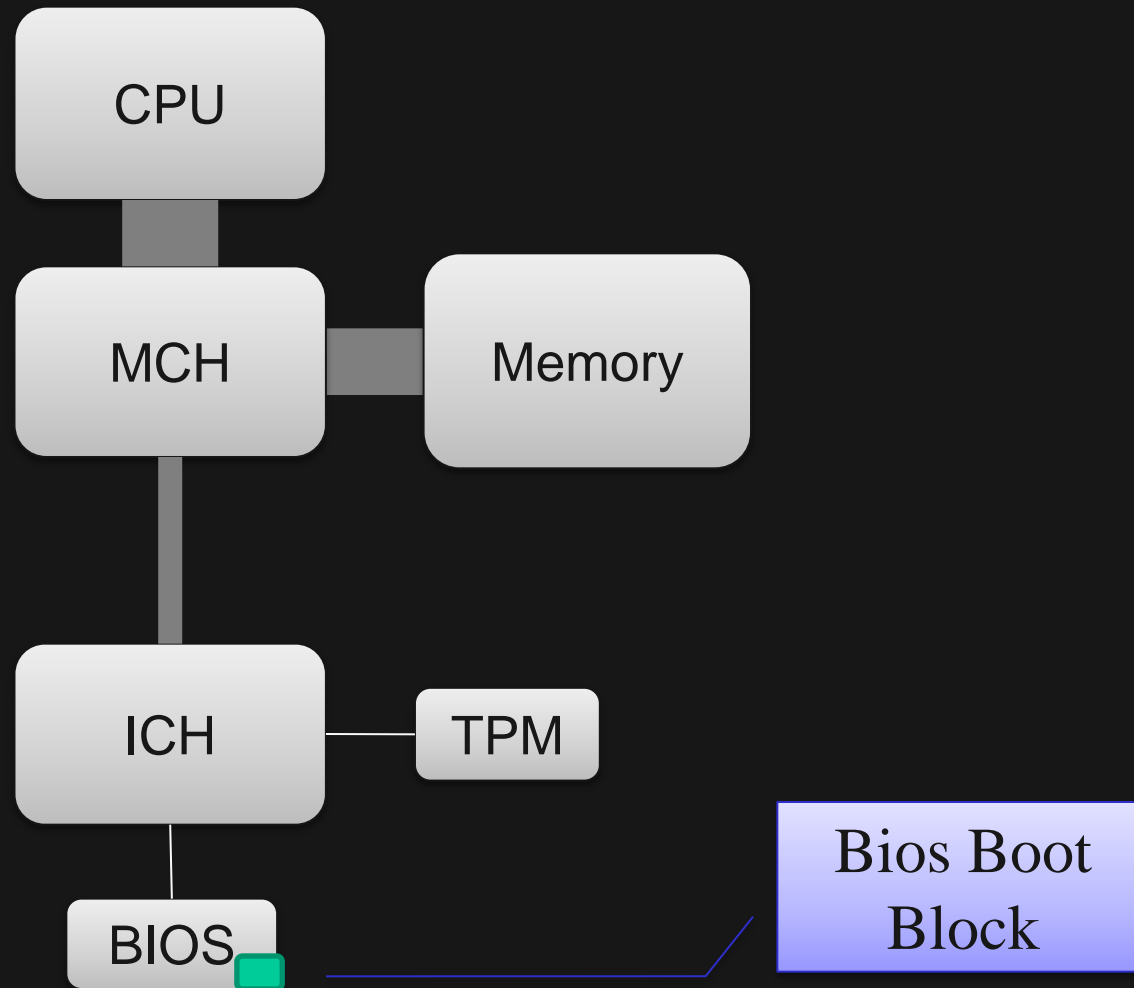
...but only a very small part of it

...and build a chain of **trust**

Root of Trust for Measurements + Trusted Platform Module

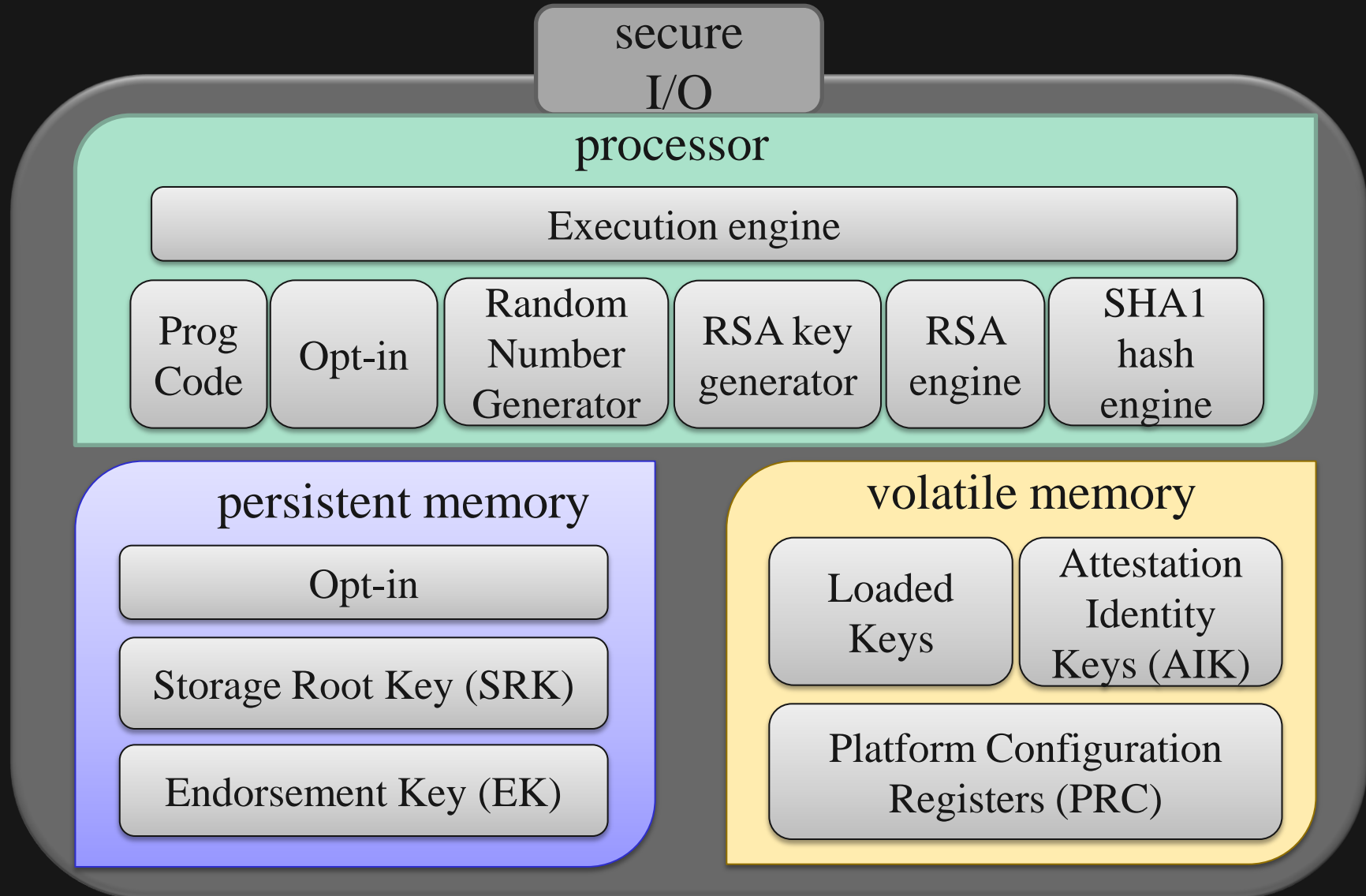
Not entirely true since we have to trust the MLE, and the hardware.

Core Root Of Trust for Measurements

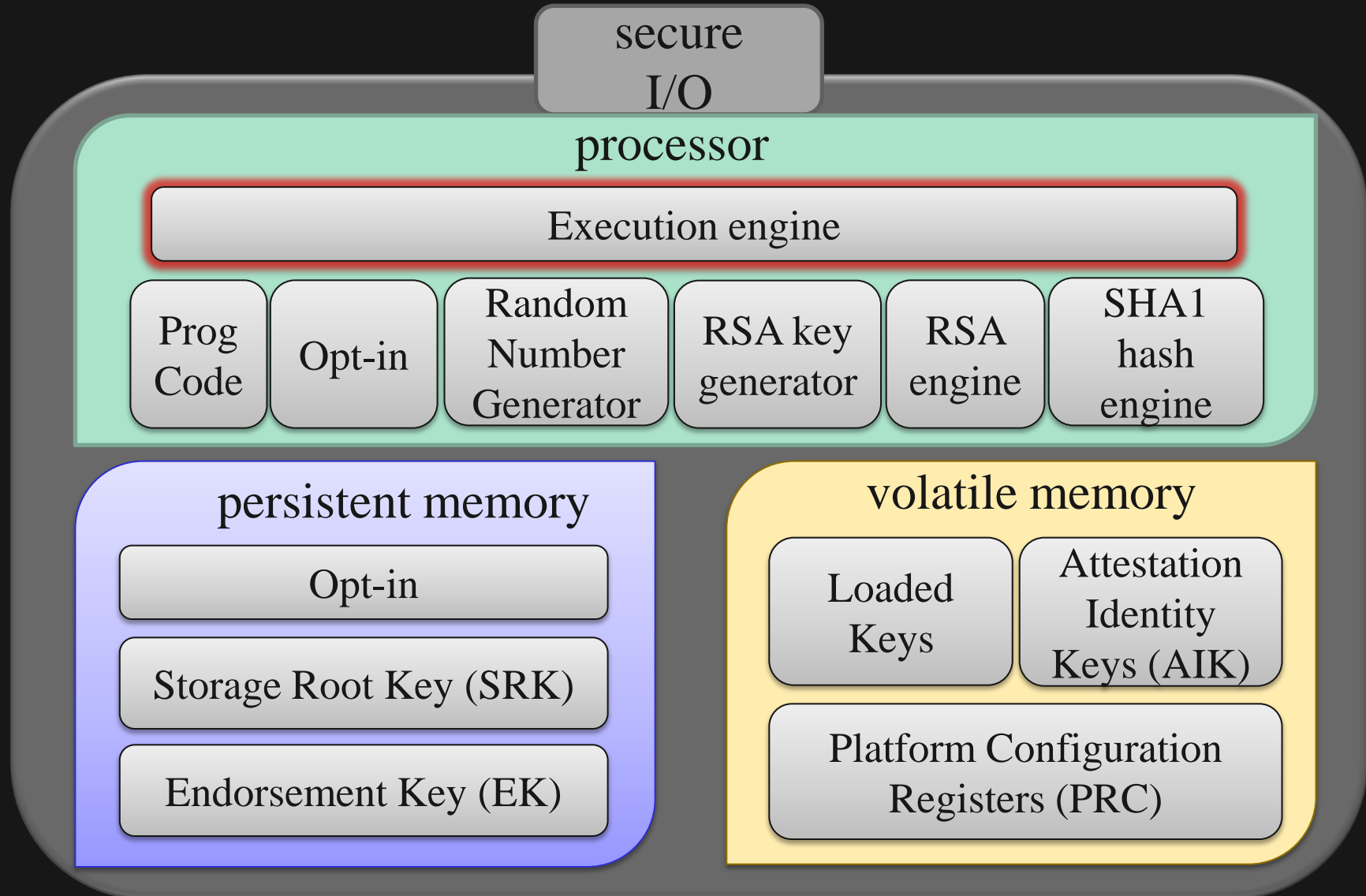


Trusted Platform Module

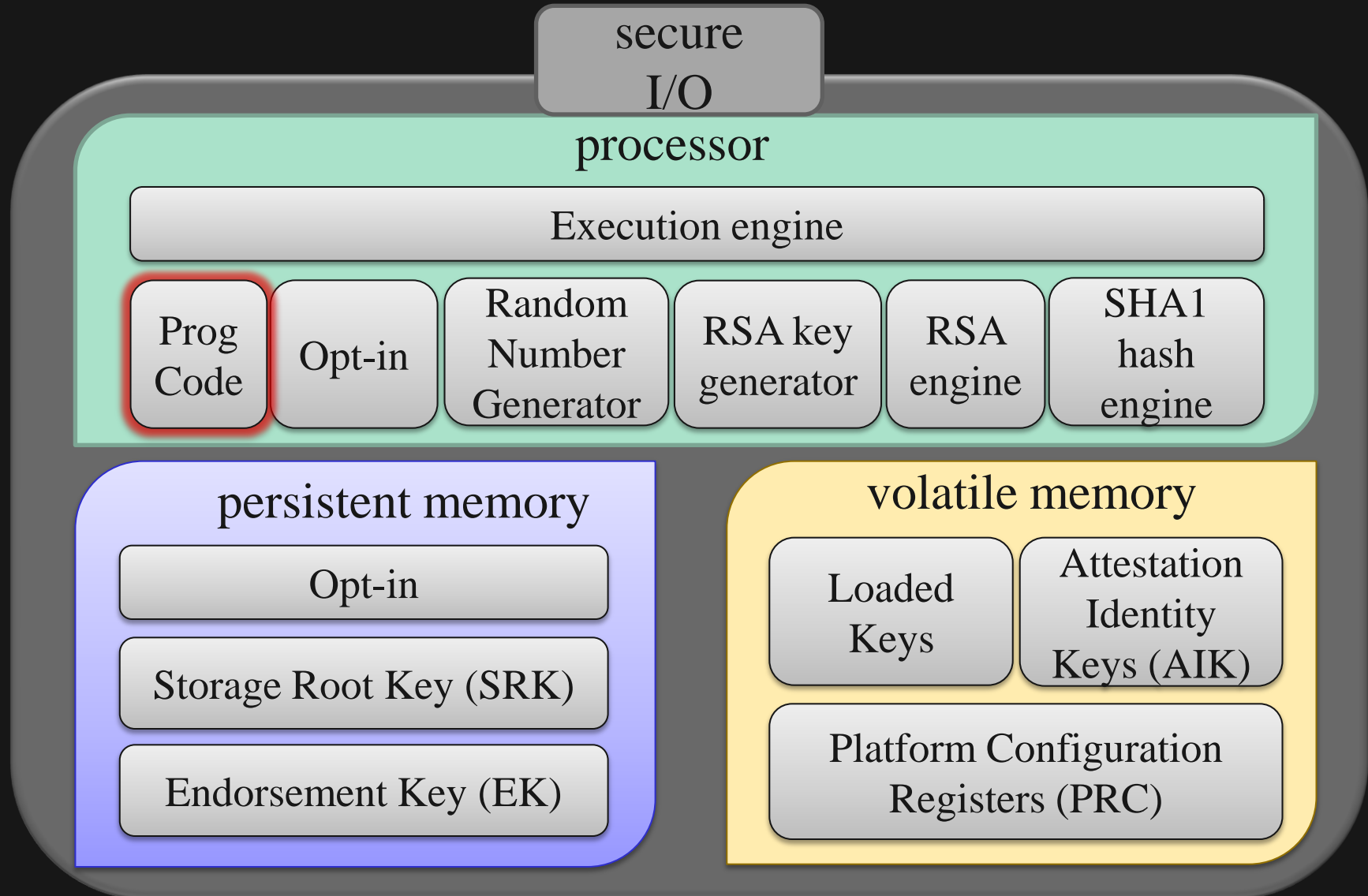
Typical TPM



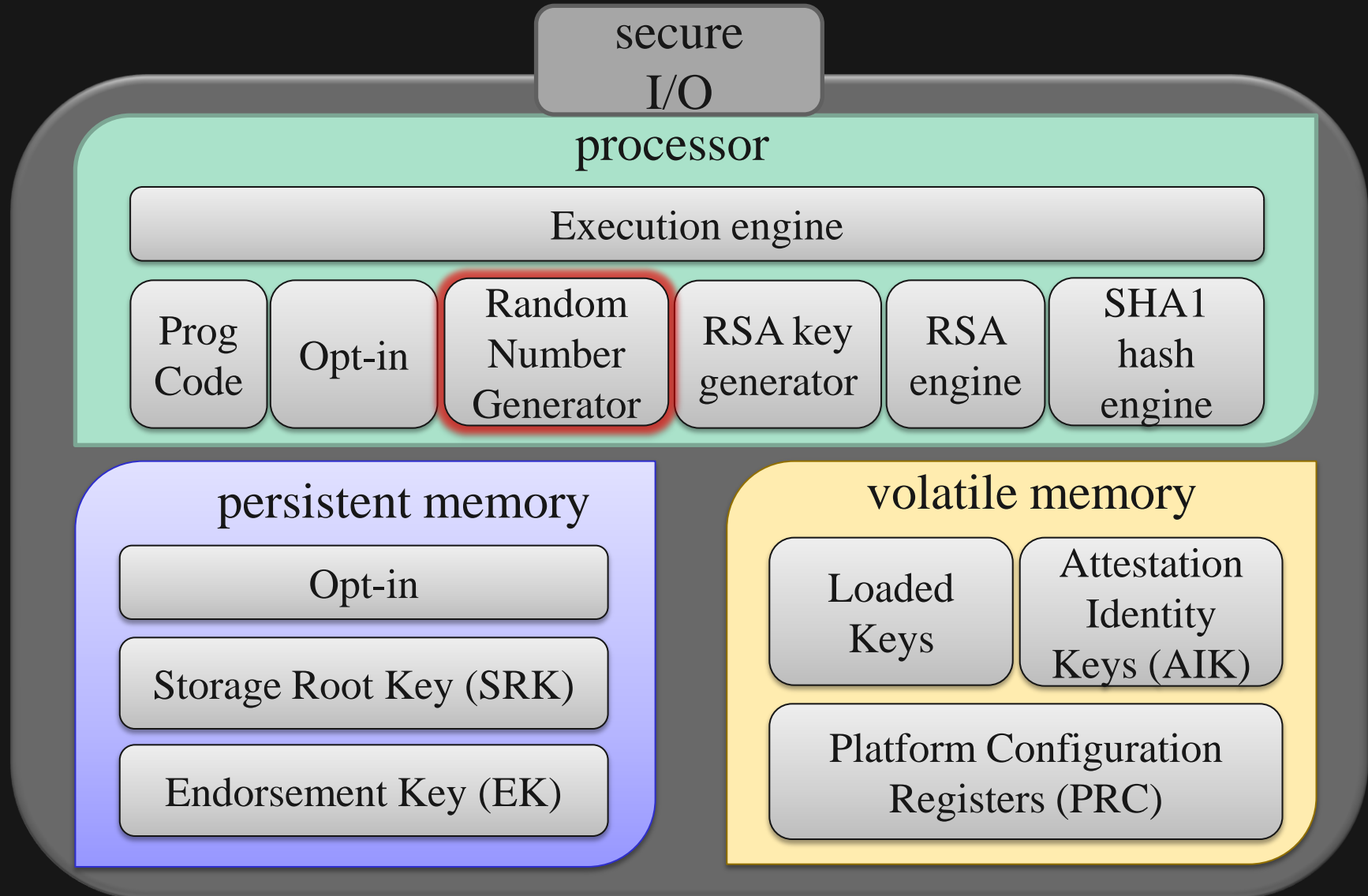
Orchestrator: receive request and dispatch



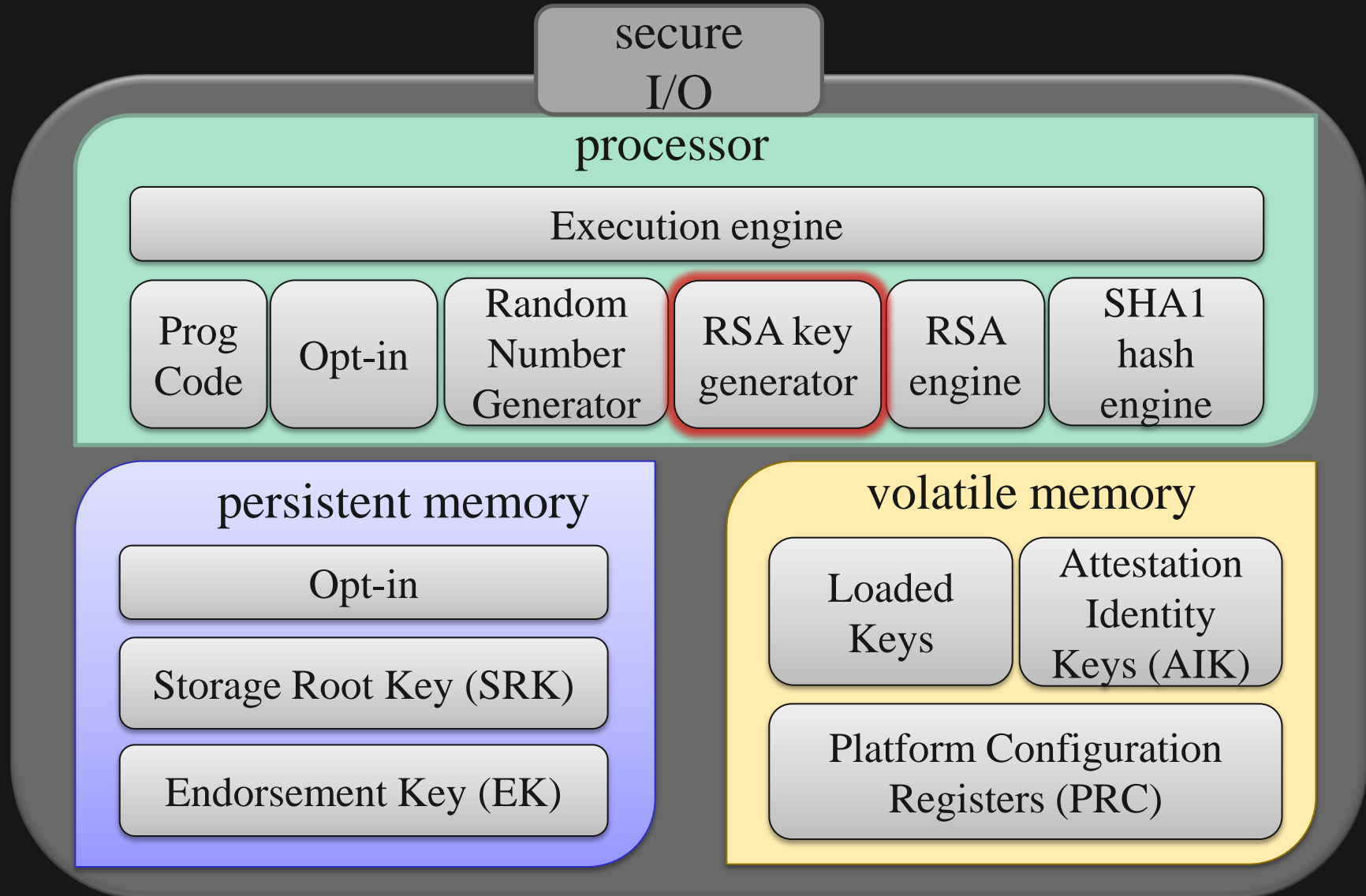
Implement the specs: validation, execute request, respond



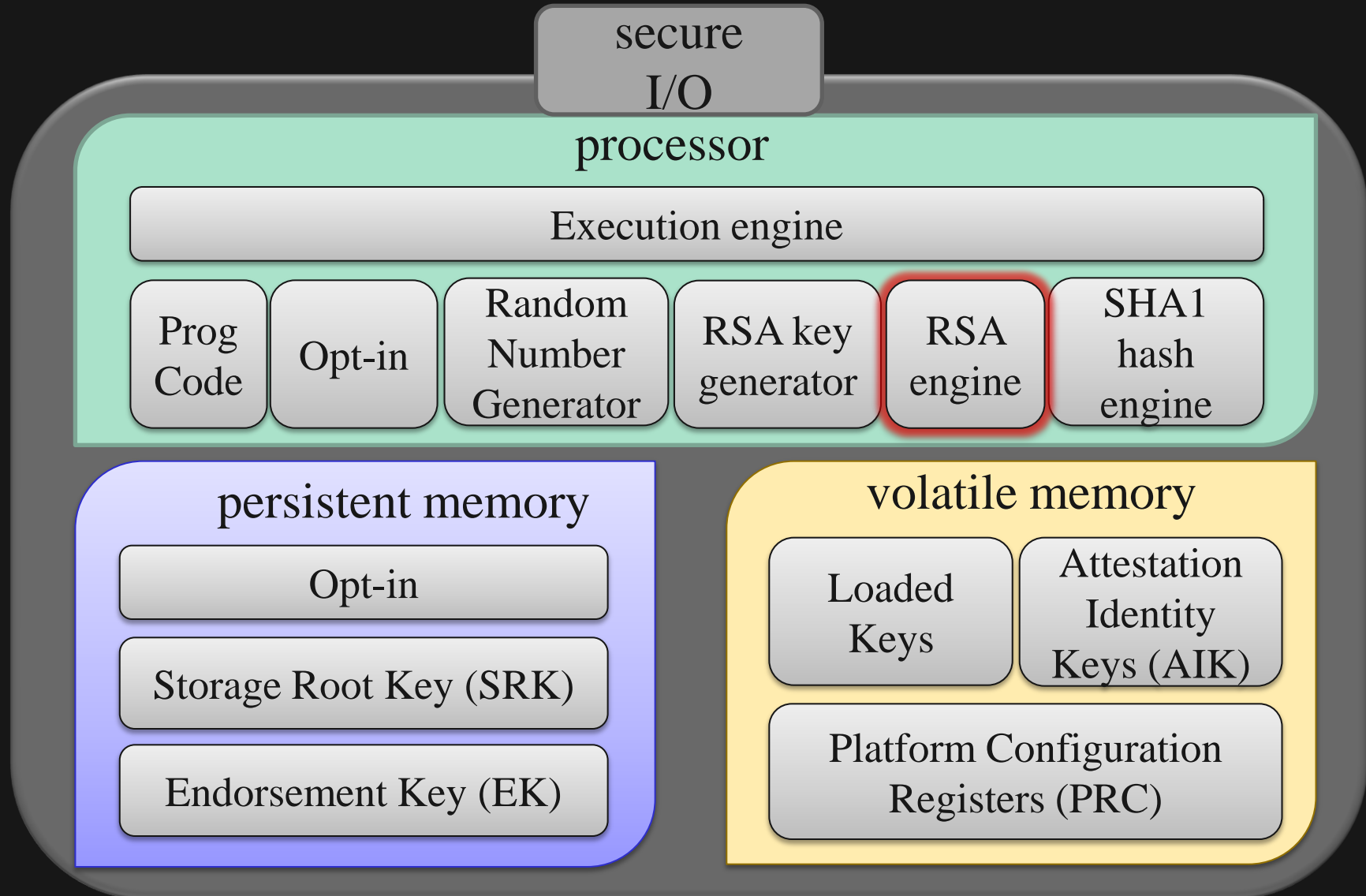
Create good random data for symmetric, asymmetric, nonce



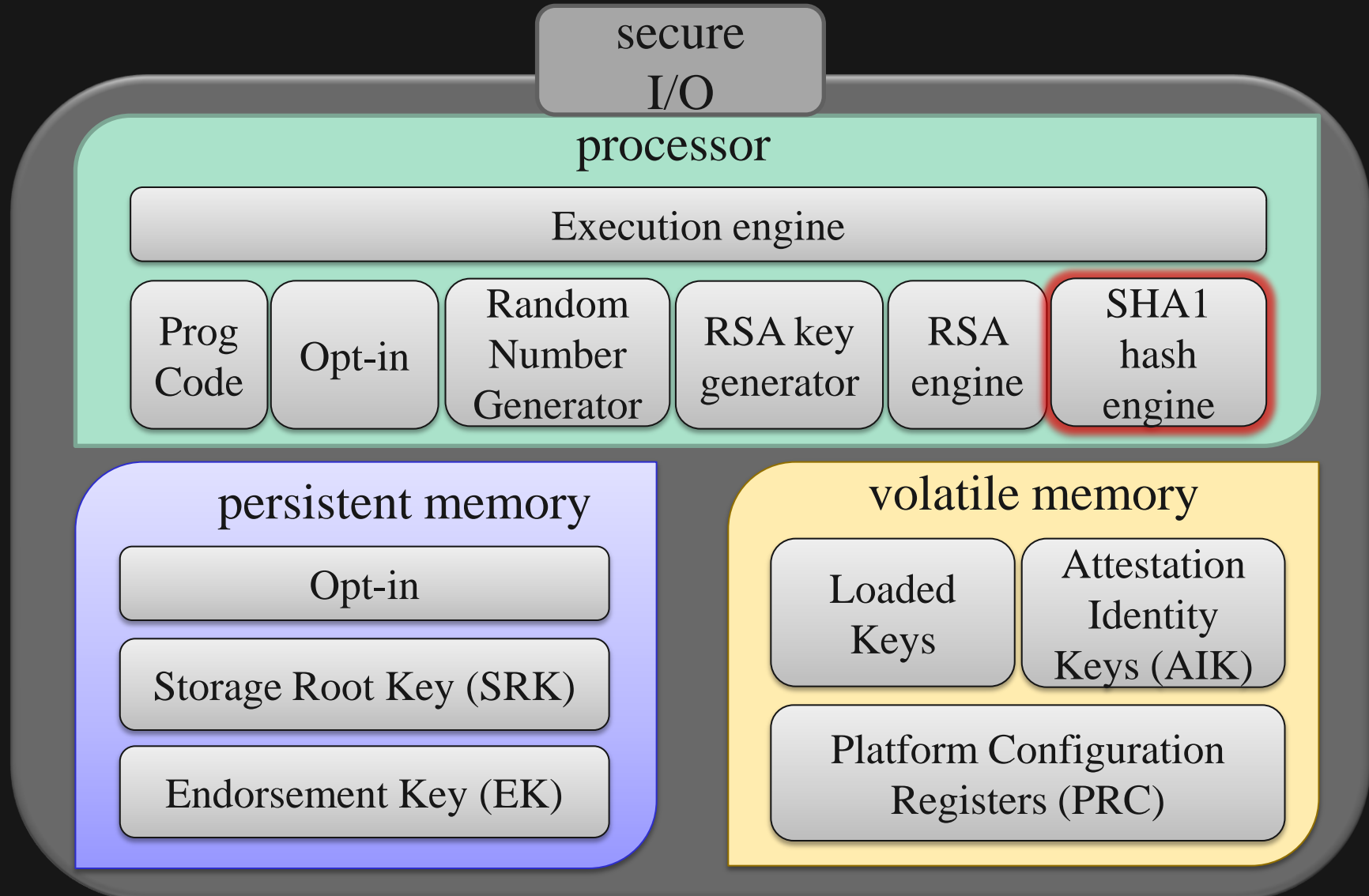
Securely create RSA key pairs: public, private



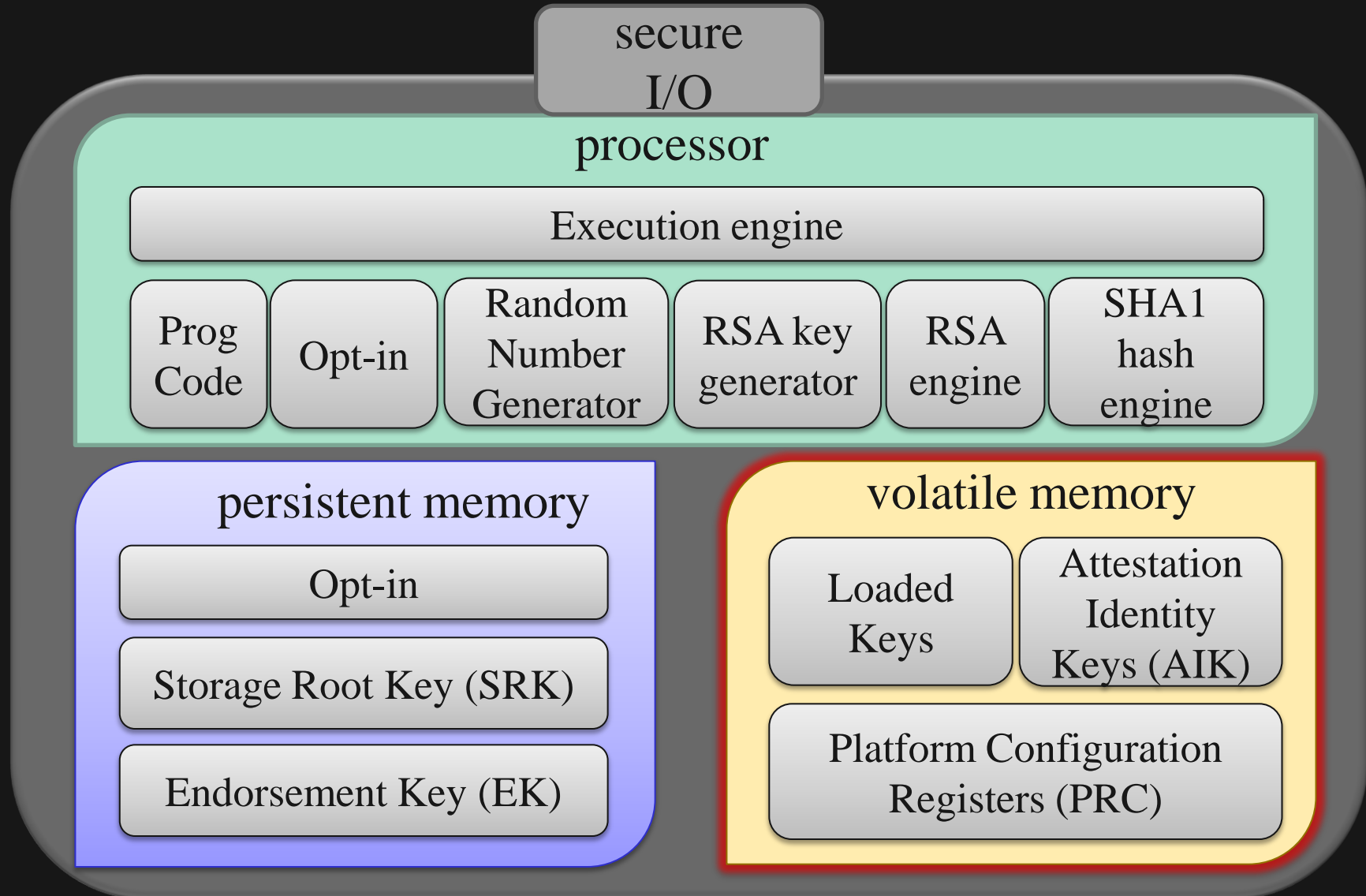
RSA encryption, decryption, signature, verification



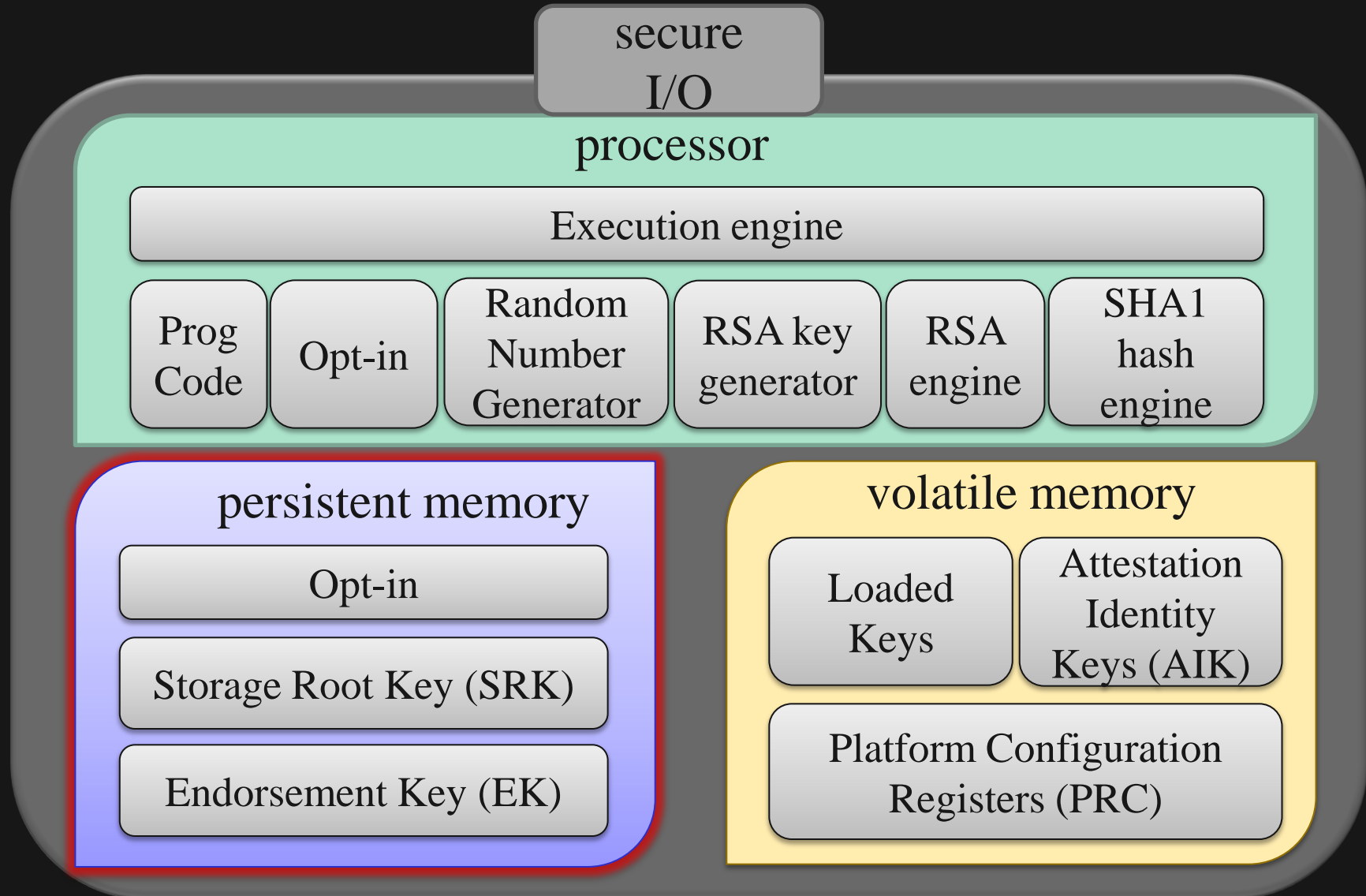
Authorization values, HMAC, etc



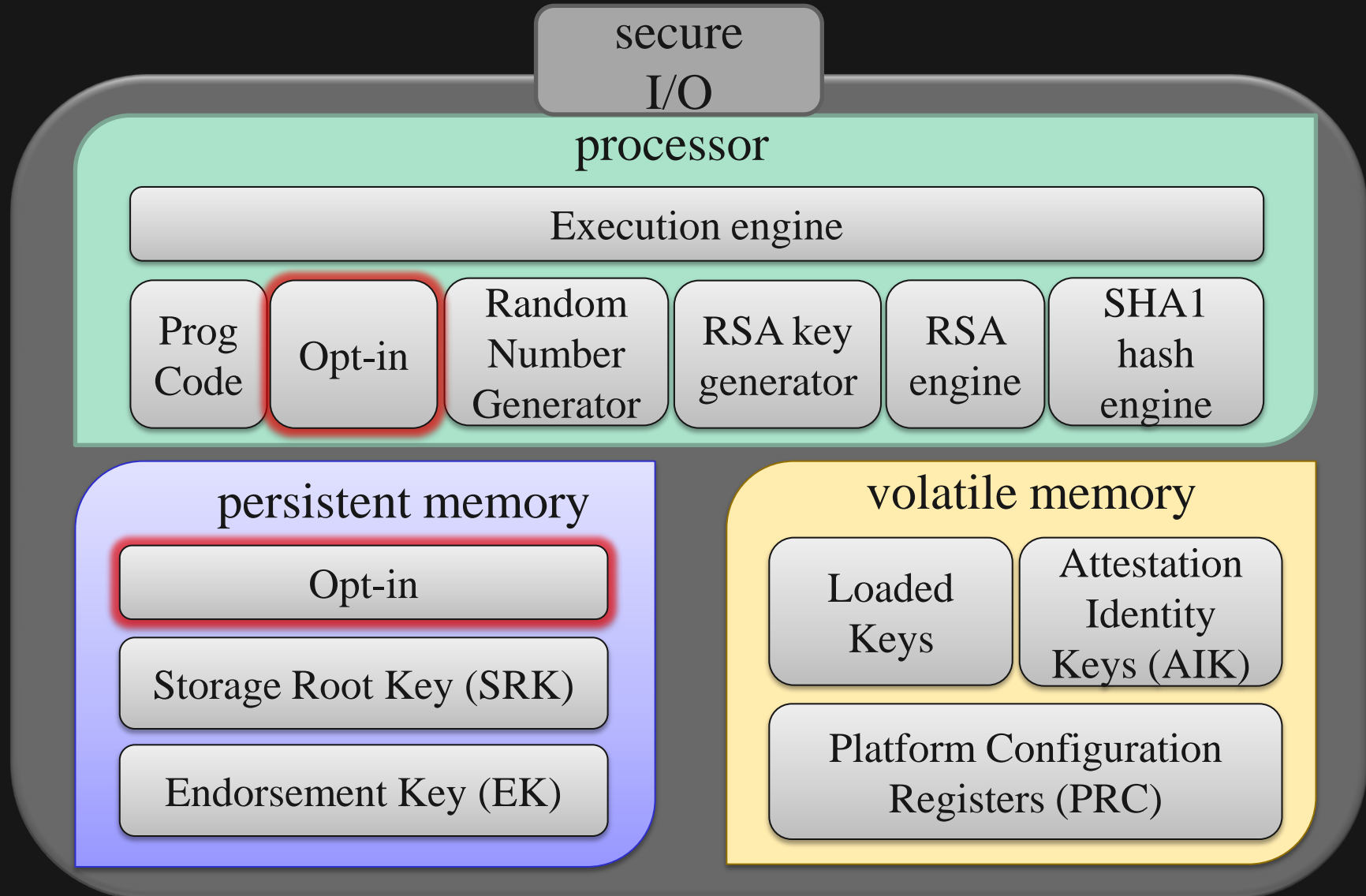
Keep track of internal state: sessions, etc



Power cycle resistant memory

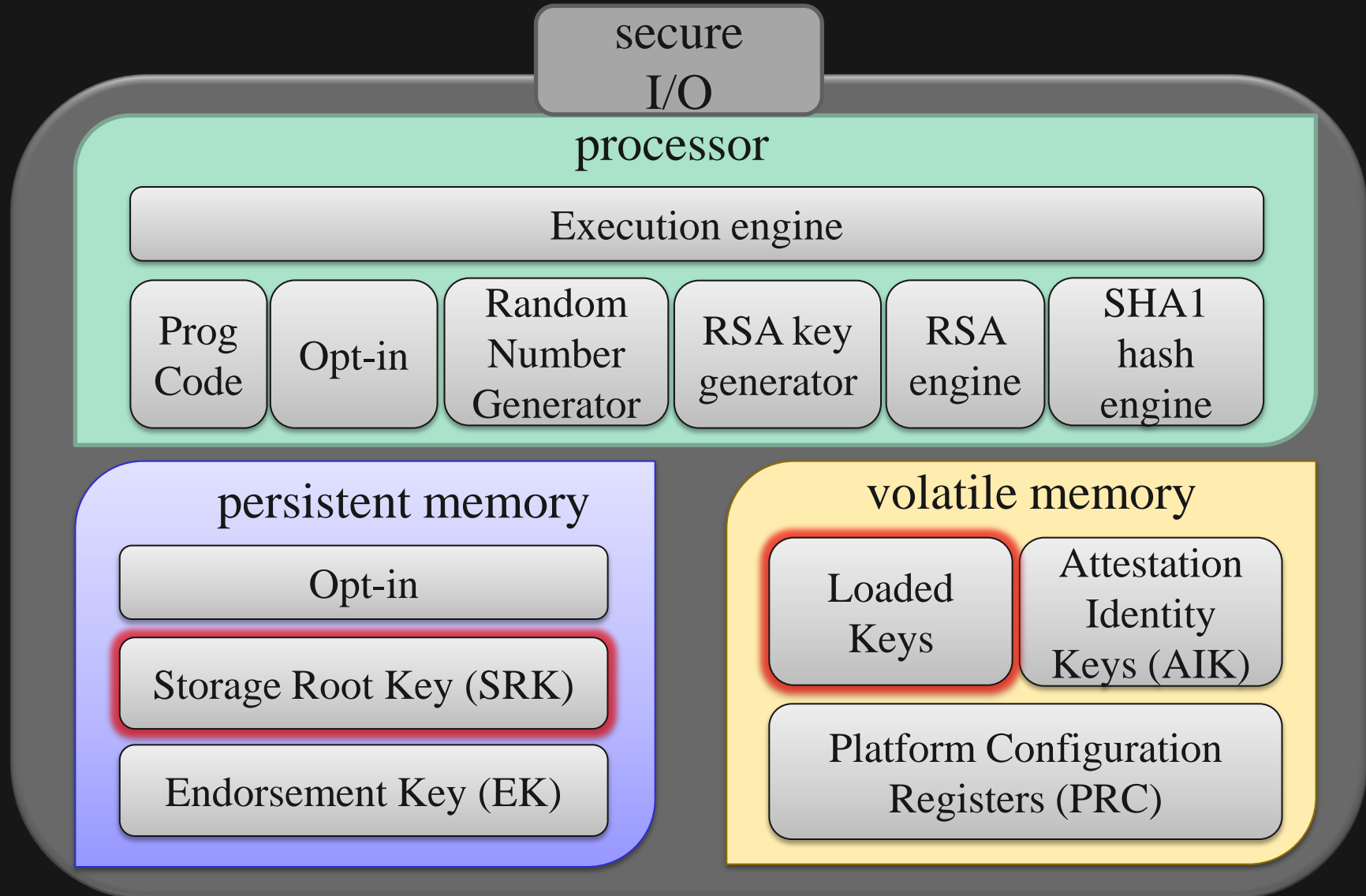


Enforce user's choice



at purchase time, TPMs are **not** operational

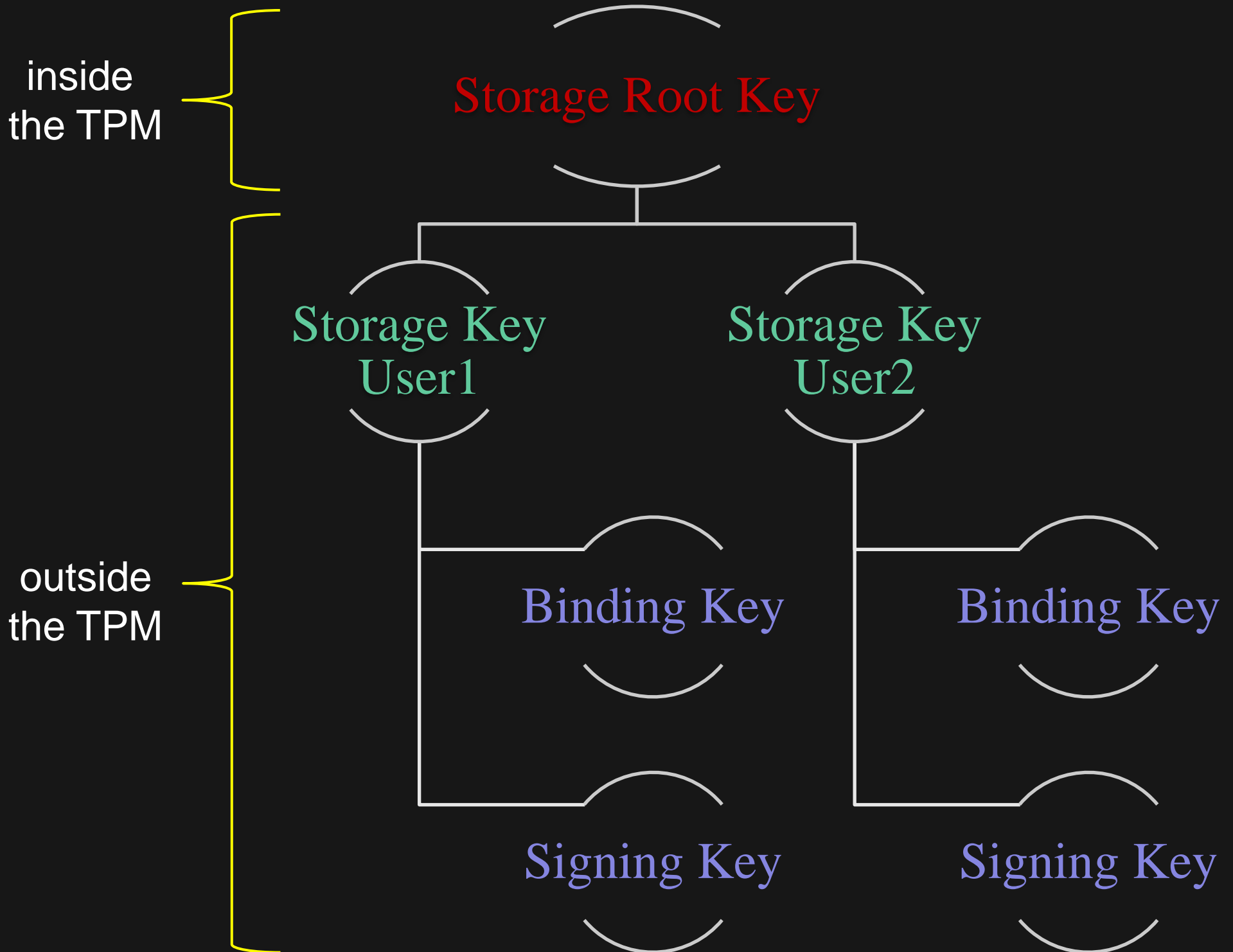
Root of all storage keys



created when **owner** activate the TPM

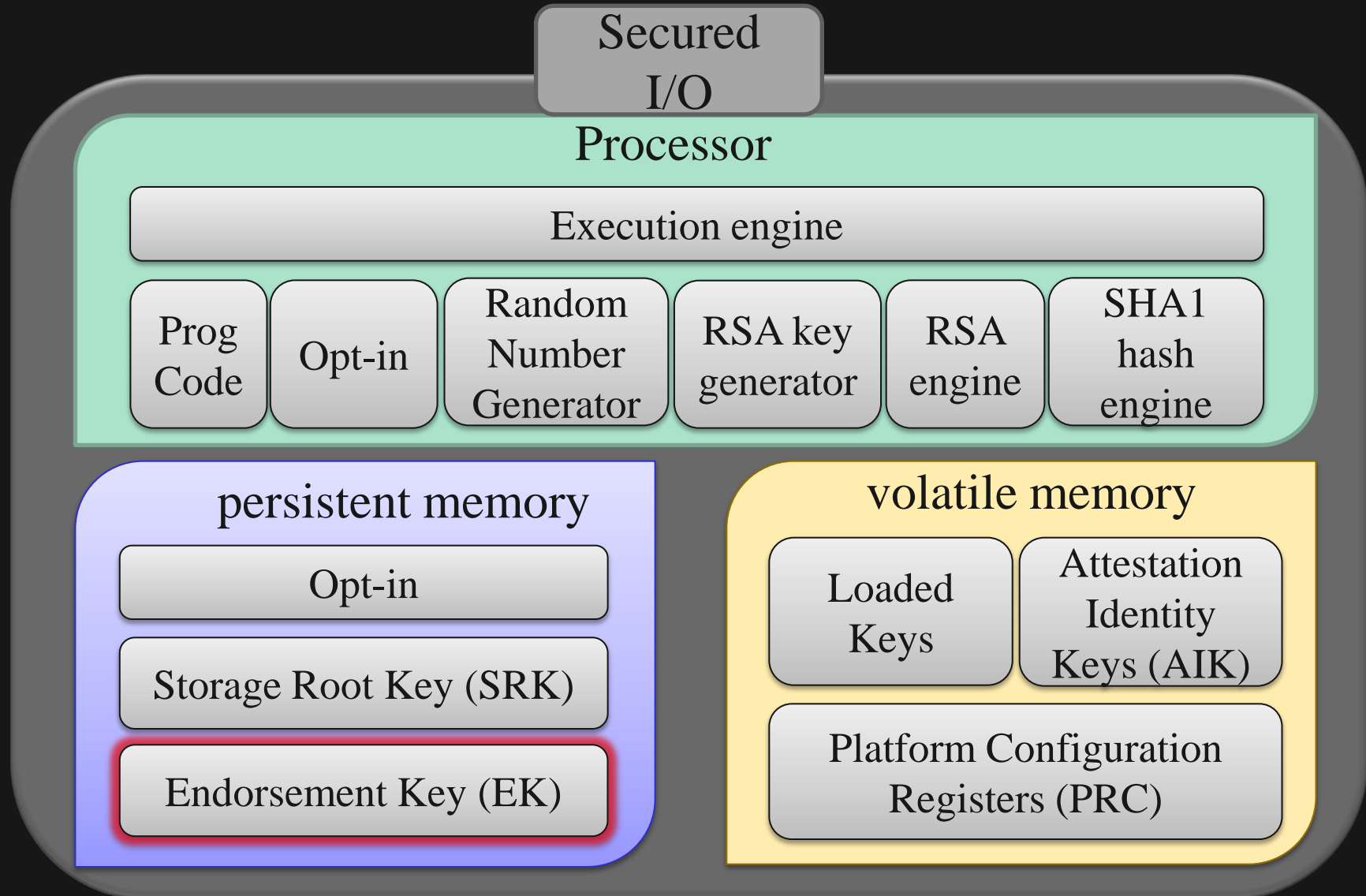
used to create secure key trees

provide, virtually, unlimited secure storage



The actual structure is malleable and can be very different.

TCG specifications assertion



endorsement certificate sign by the TPM manufacturer

uniquely identify the platform

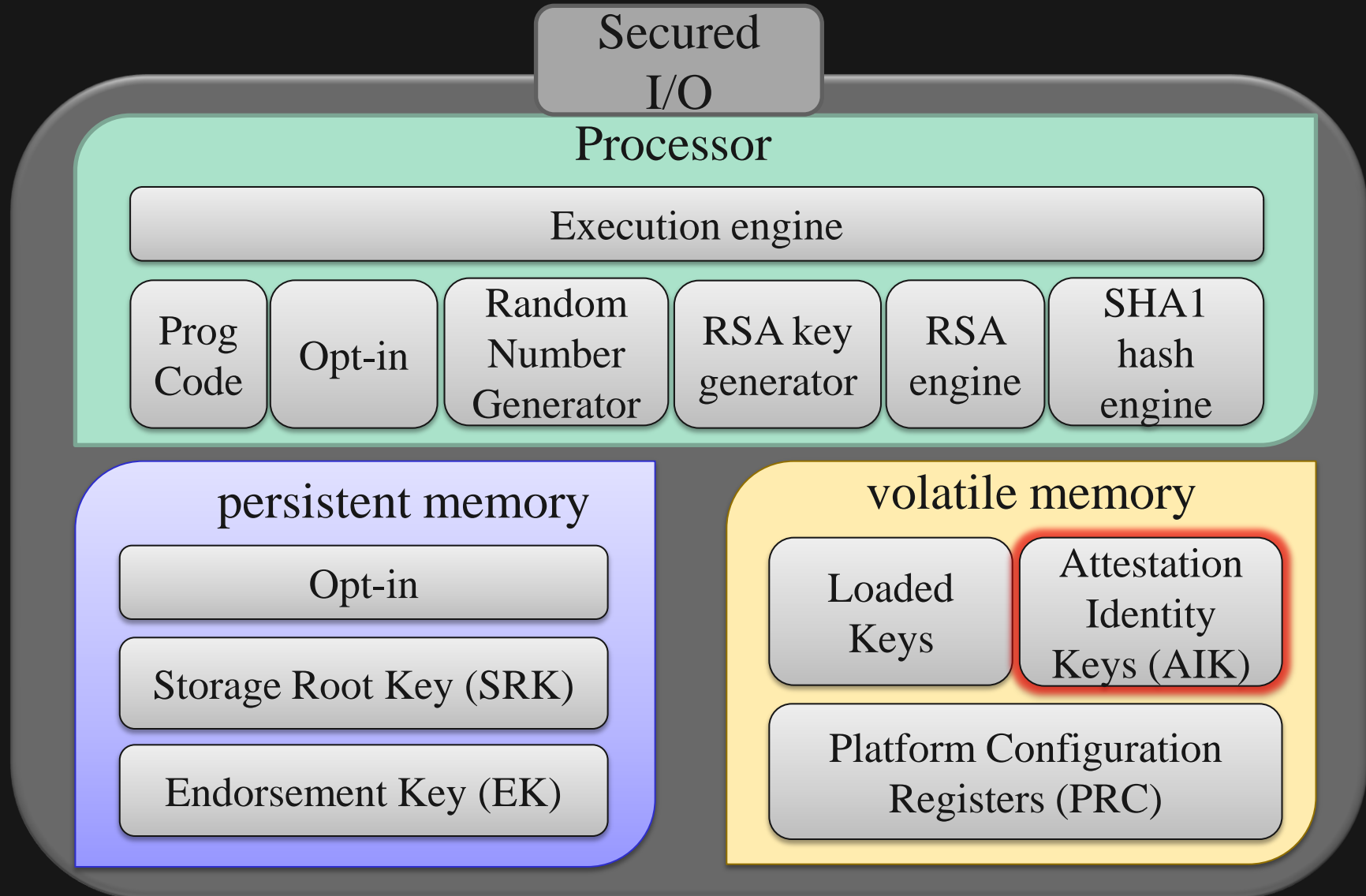
A man with short brown hair is peeking through a white shower curtain in a bathroom. He has a surprised or concerned expression on his face. The bathroom has bright blue walls and white tiled walls inside the shower area. A white bathtub is visible in the background. In the bottom left corner, there are several rolls of white toilet paper on a stand. A black text box with white text is overlaid on the image.

privacy concerns

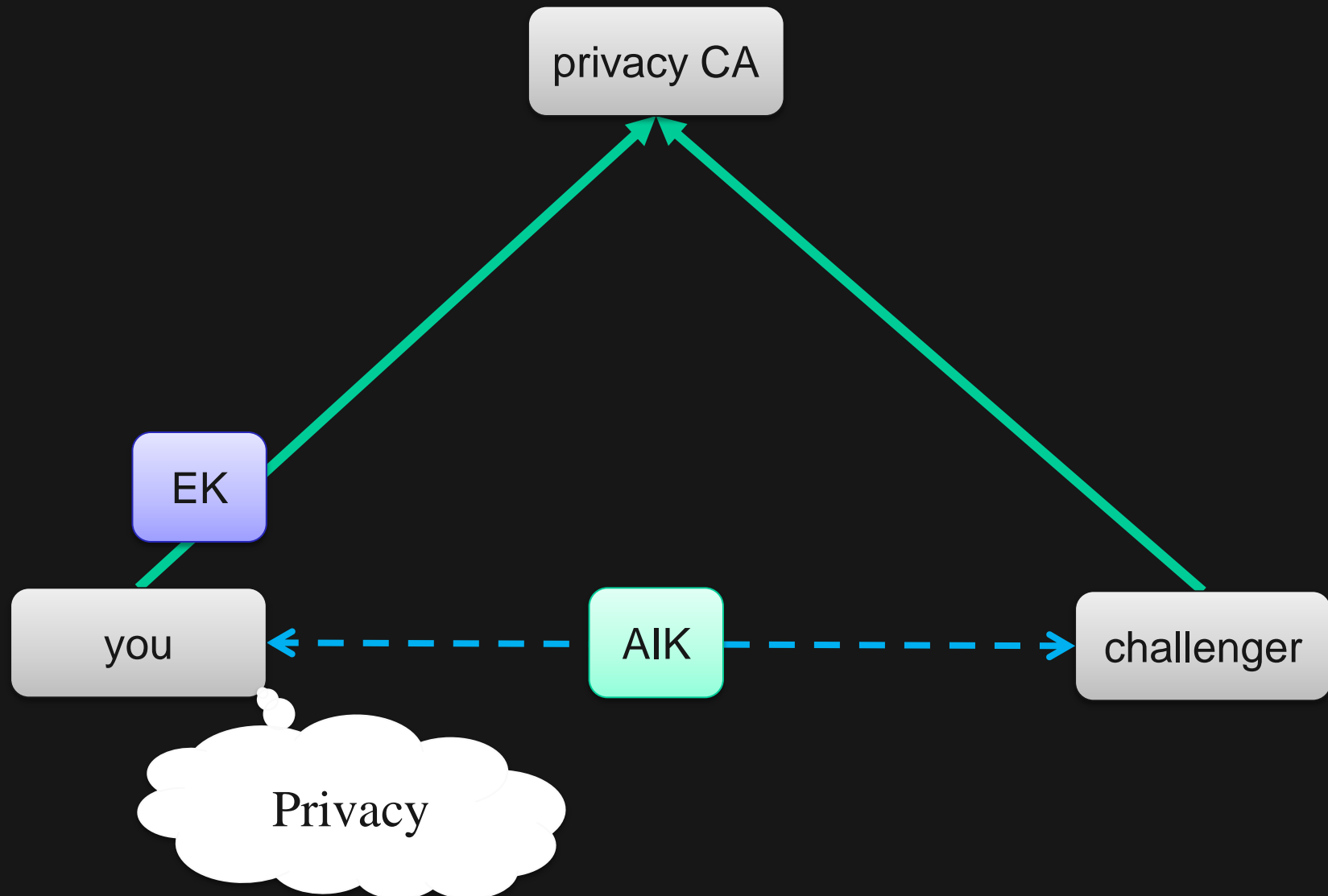
well yes... but no

EK is only used in conjunction with something else

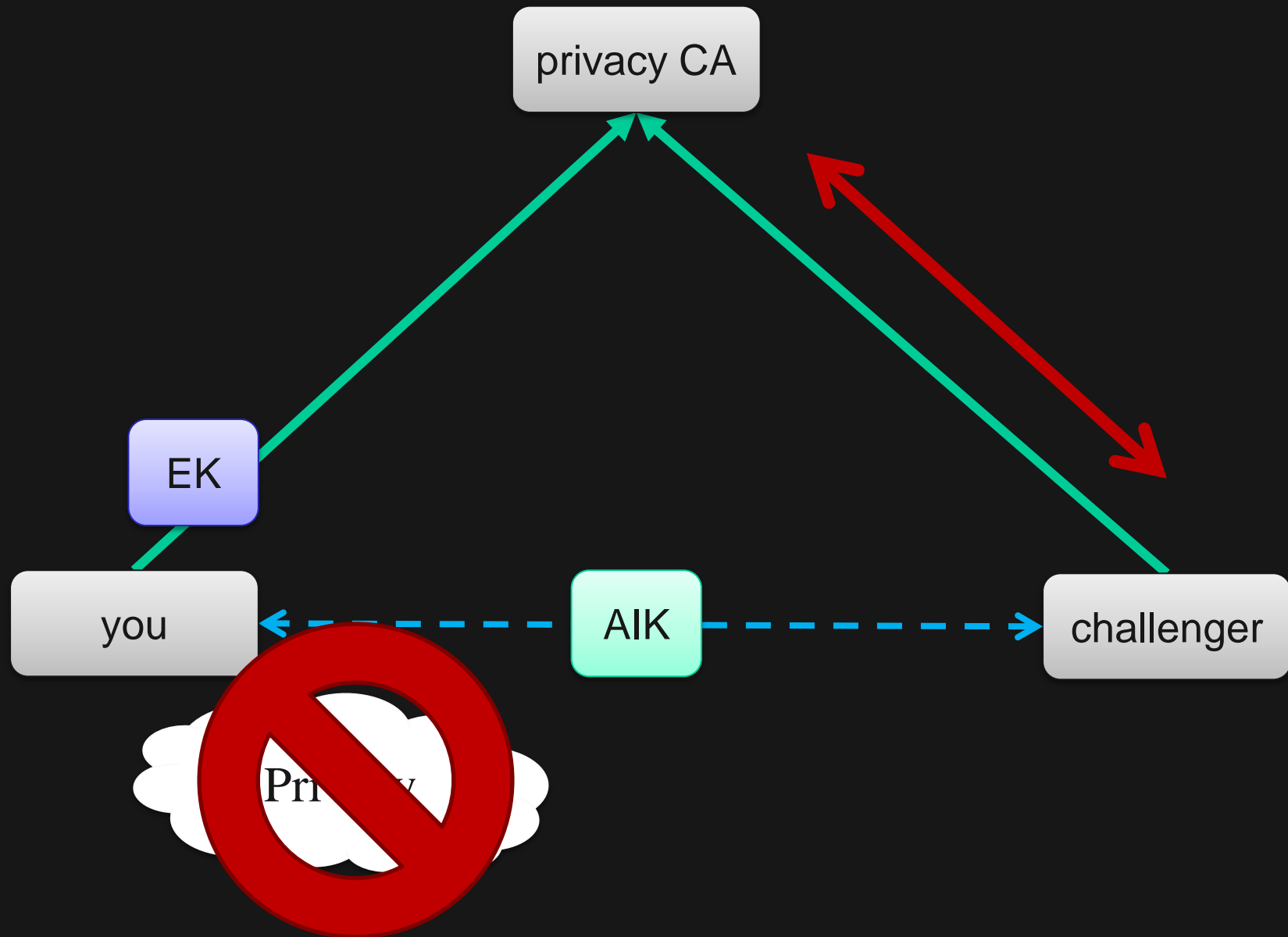
Some kind of privacy protector



mutual trust of the CA – signed AIK satisfy challenger



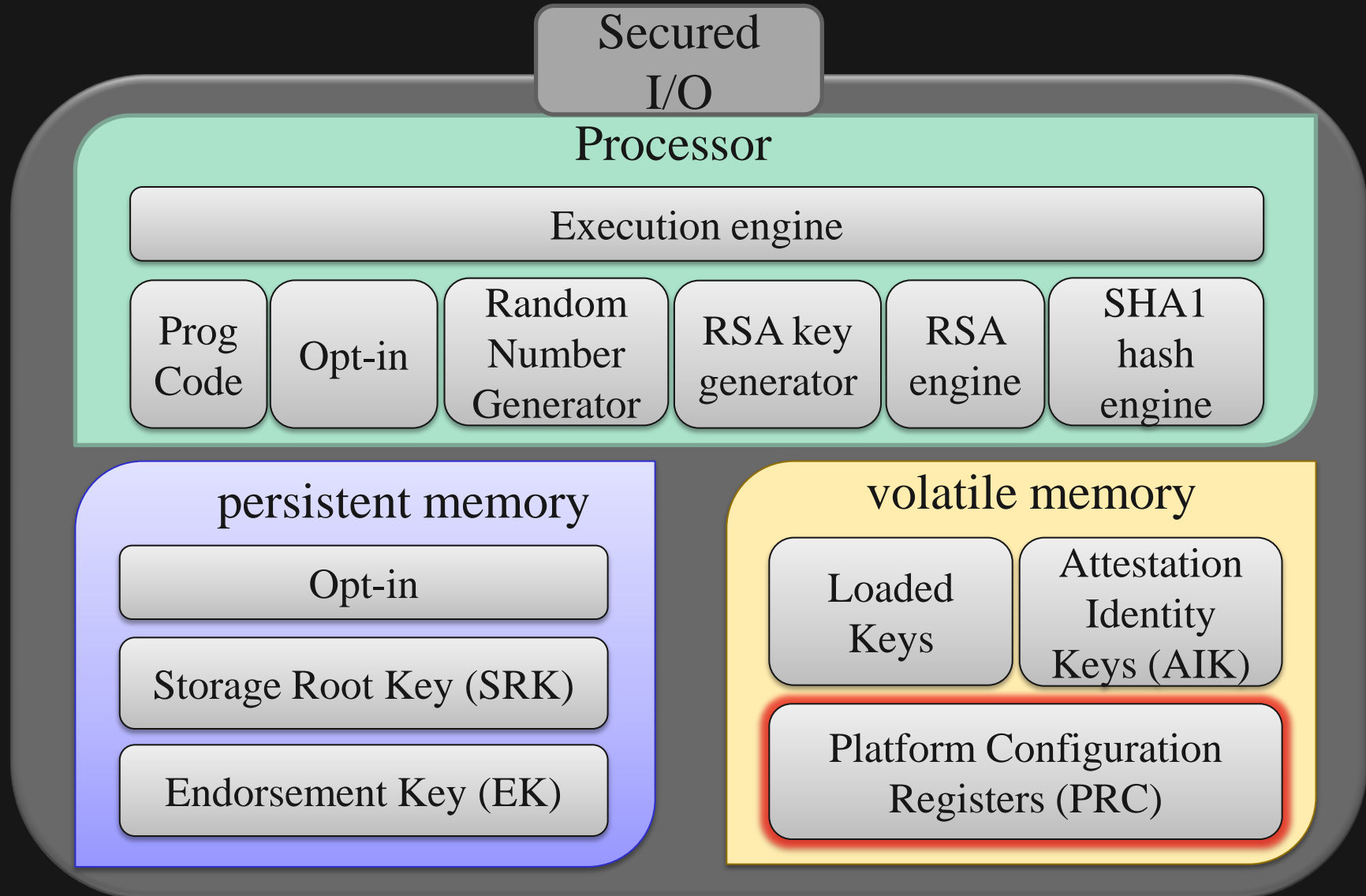
What if collusion arise?



Direct Anonymous Attestation (DAA)

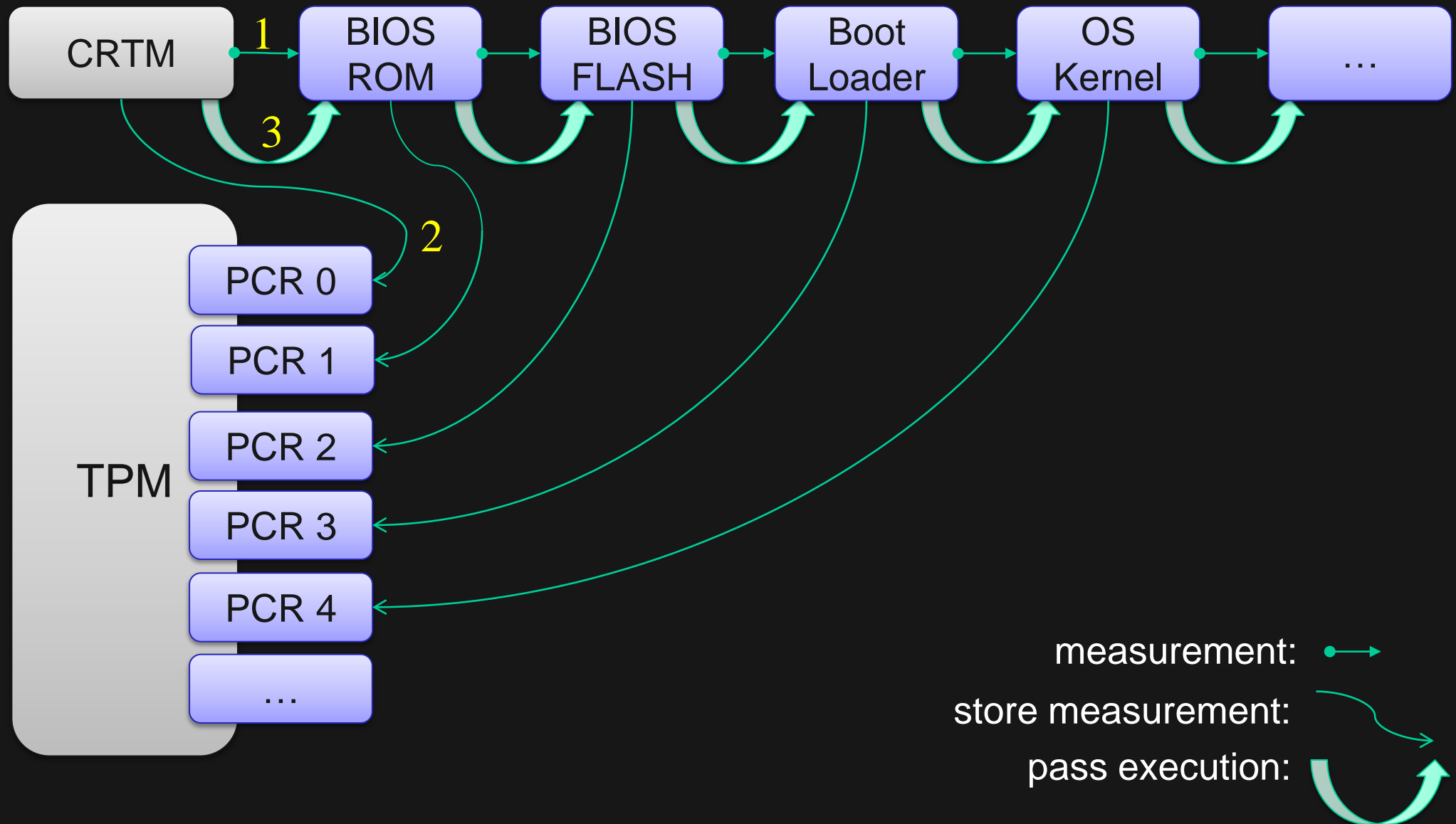
Zero Knowledge Proof

Store system measurements: SHA-1 hash



Static Root of Trust for Measurements (SRTM)

Launch time measurements



Boot process and PCRs attribution not accurate (highly simplified).

one PCR can be used to measure **multiple** elements

TPM_Extend()

PCR = hash(old value, new value)

0x0000 = boot()

0xAAAA = hash(0x0000, 0x1111)

0xB BBBB = hash(0xAAAA, 0x2222)

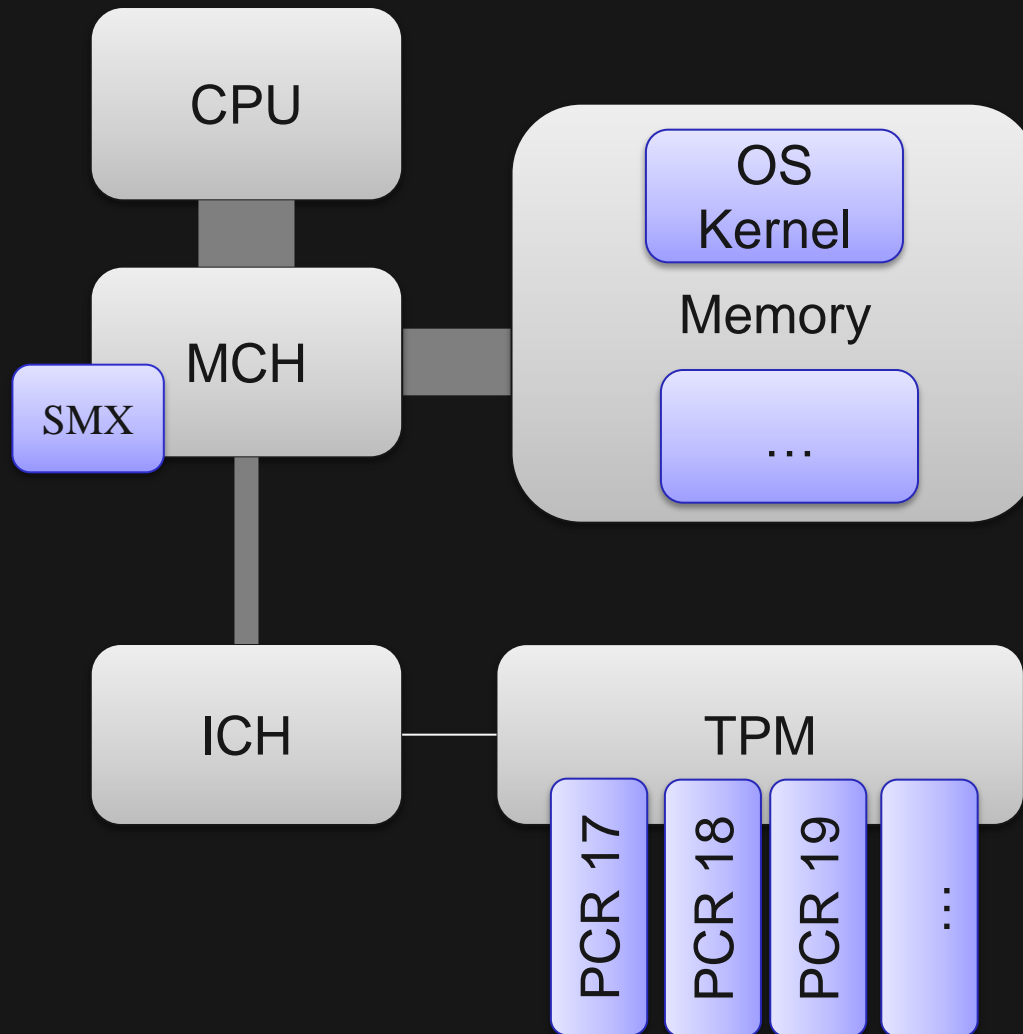
0xC CCC C = hash(0xB BBBB, 0x3333)

TPM doesn't act upon PCRs

PCRs are stored whether they're bad or good

Dynamic Root of Trust for Measurements (DRTM)

Late launch measurements

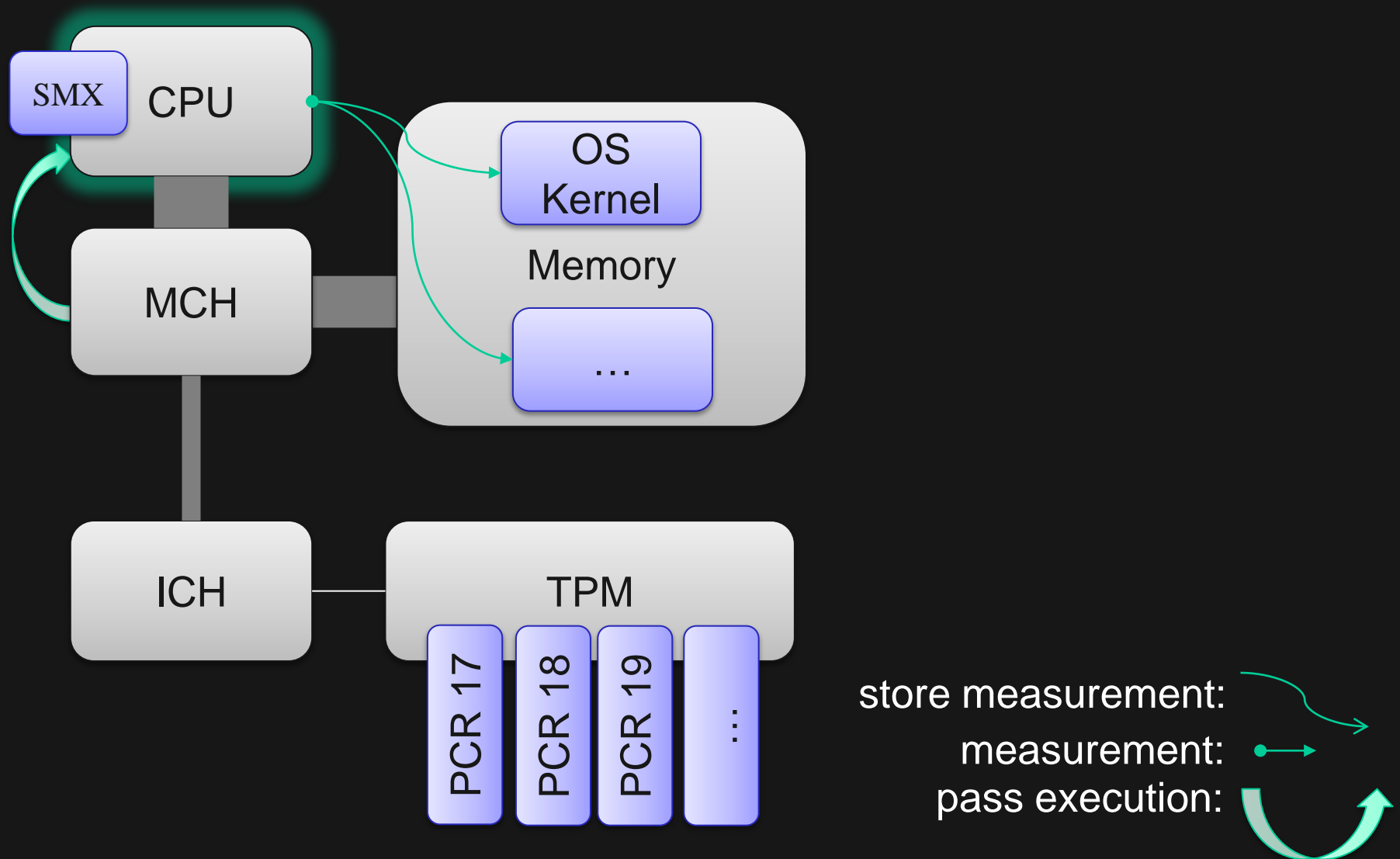


store measurement:
measurement:
pass execution:



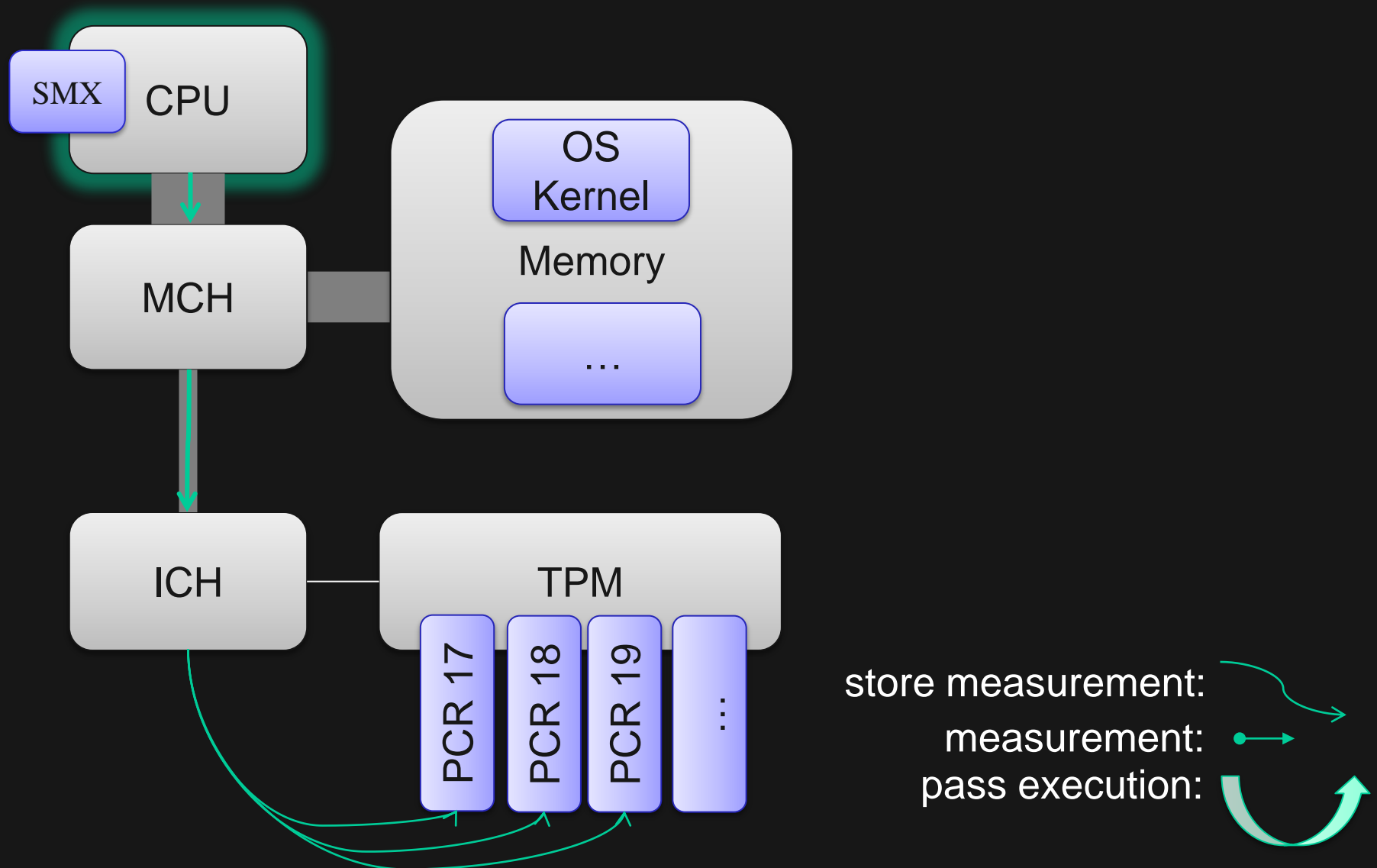
Process not accurate (highly simplified).

Late launch measurements



Process not accurate (highly simplified).

Late launch measurements



Process not accurate (highly simplified).

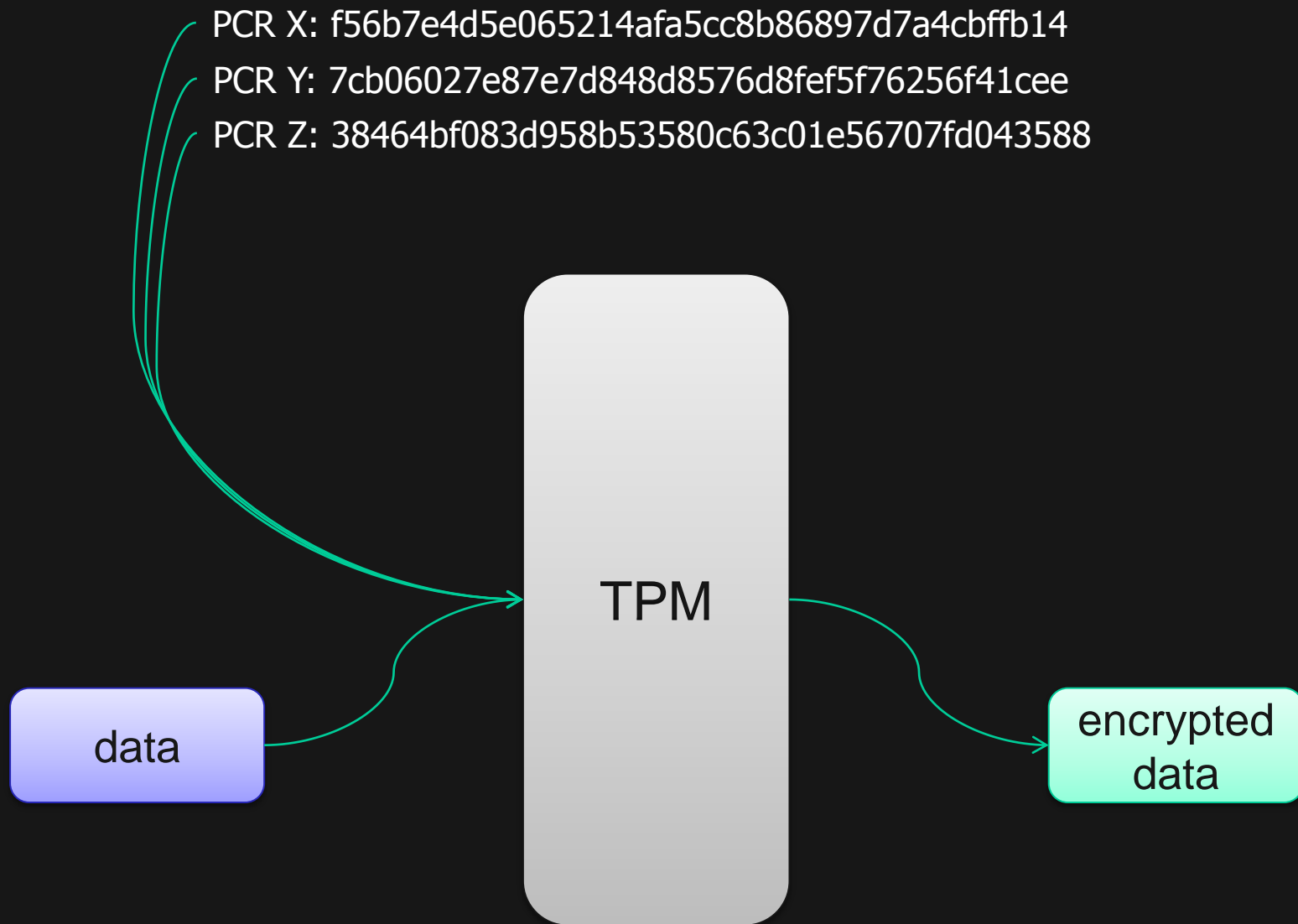
Security Enhancements



Measurements

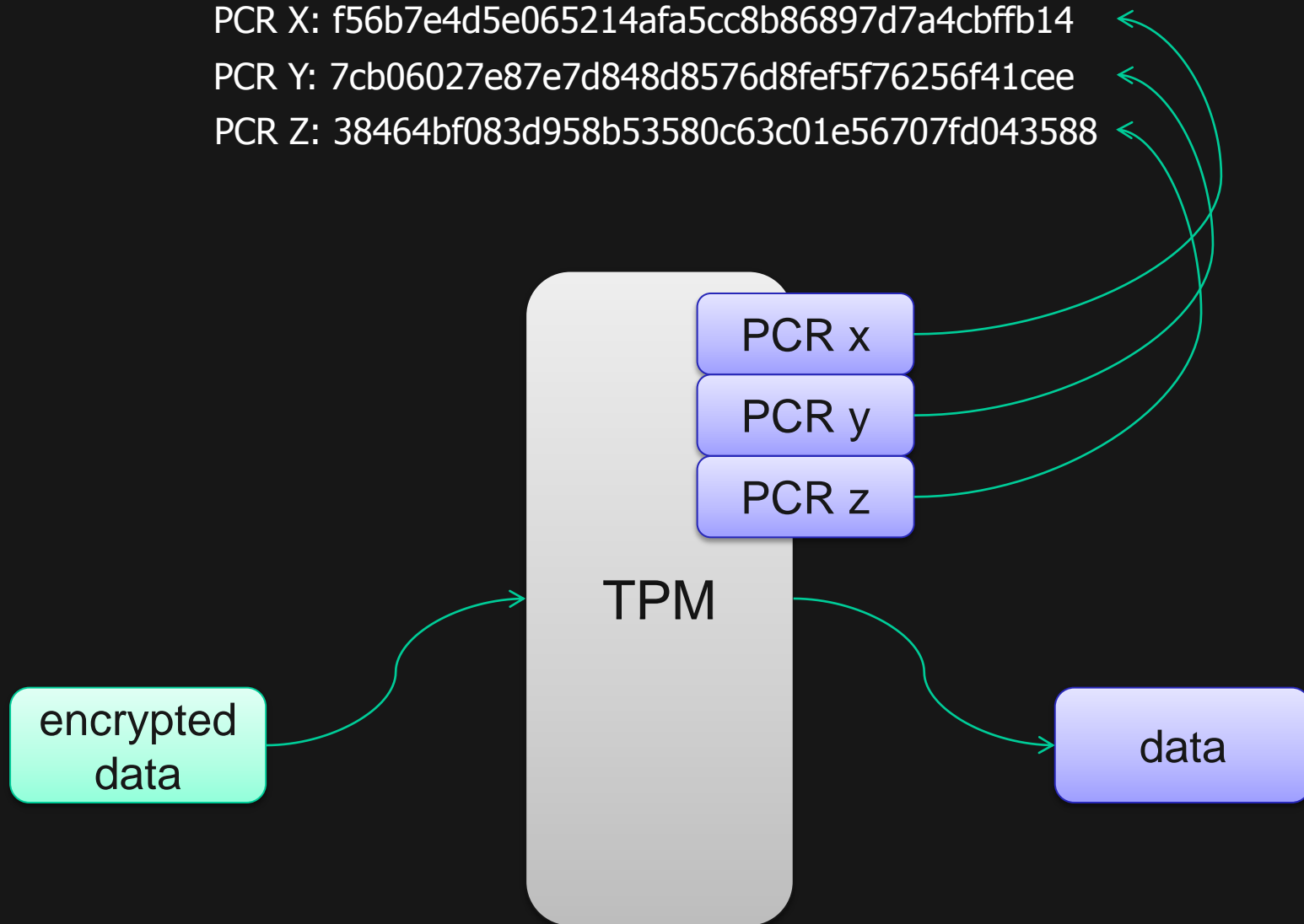
Sealed storage

TPM_Seal(): Encrypt data to a specific environment



TPM_Unseal(): Decrypt if a specific environment is active

PCR X: f56b7e4d5e065214afa5cc8b86897d7a4cbffb14
PCR Y: 7cb06027e87e7d848d8576d8fef5f76256f41cee
PCR Z: 38464bf083d958b53580c63c01e56707fd043588

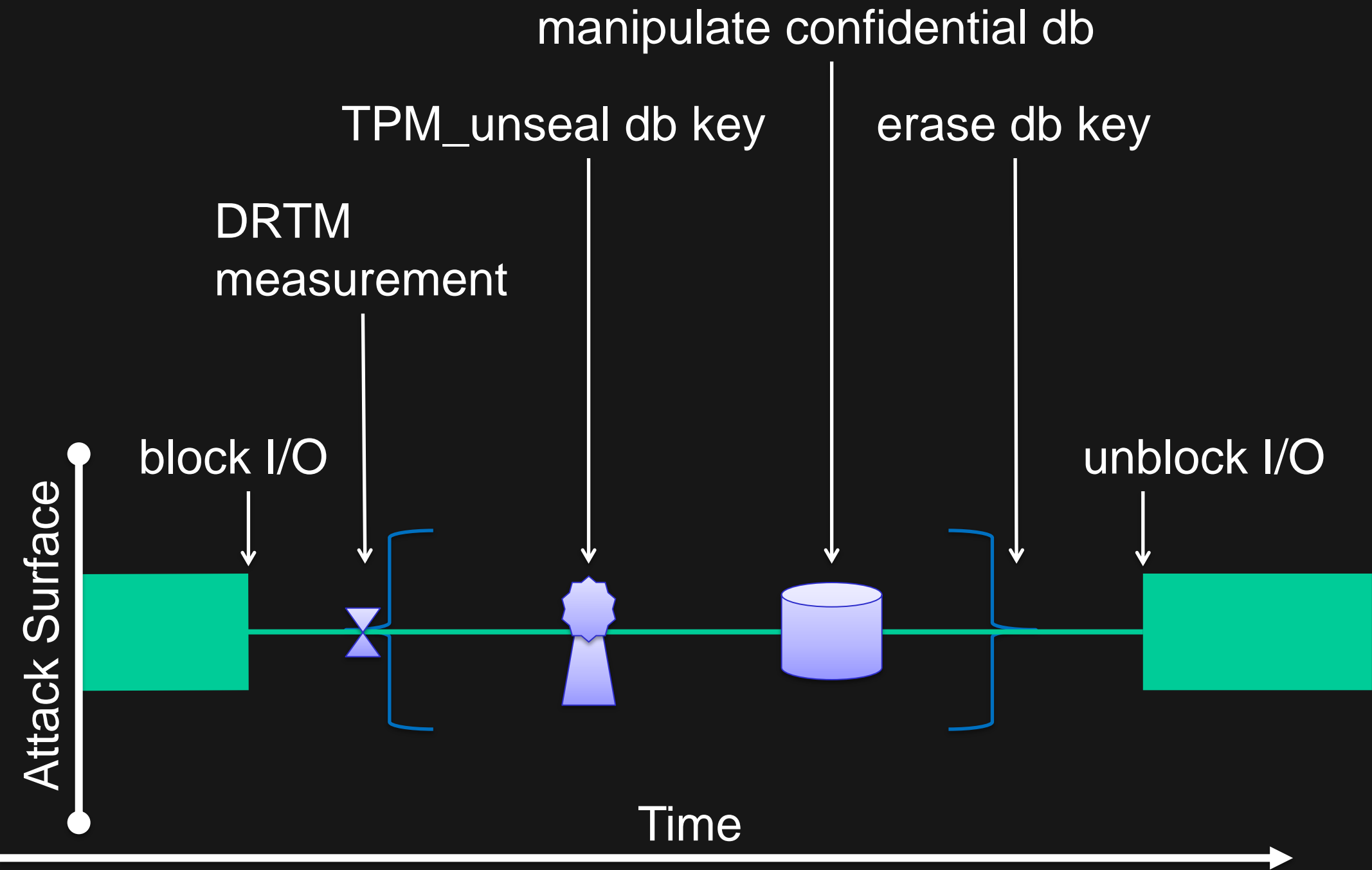


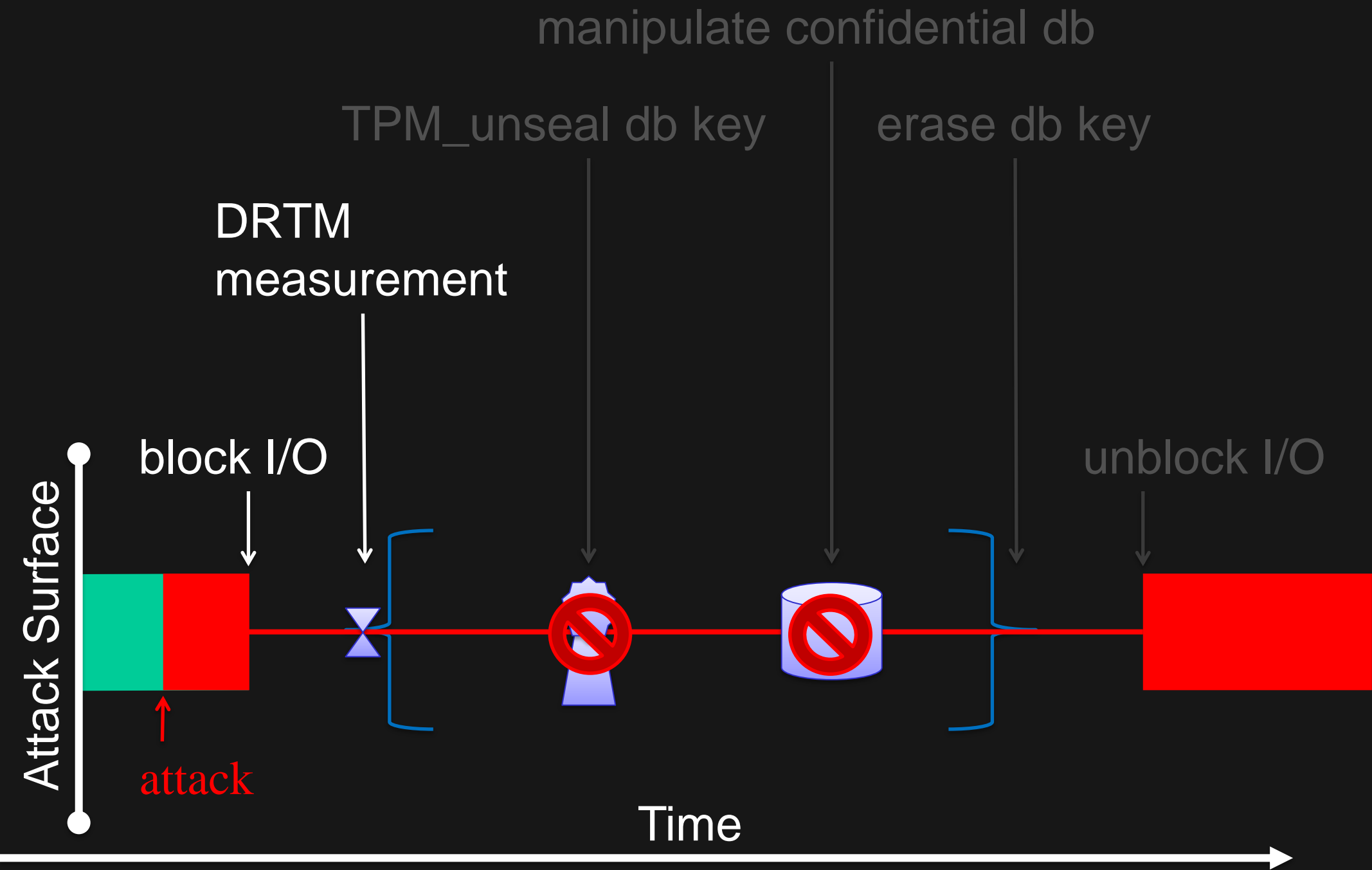
Detect malware

Keylogger / Meterpreter / KonBoot
Rootkits (user/kernel, MBR, BIOS)

Protect data

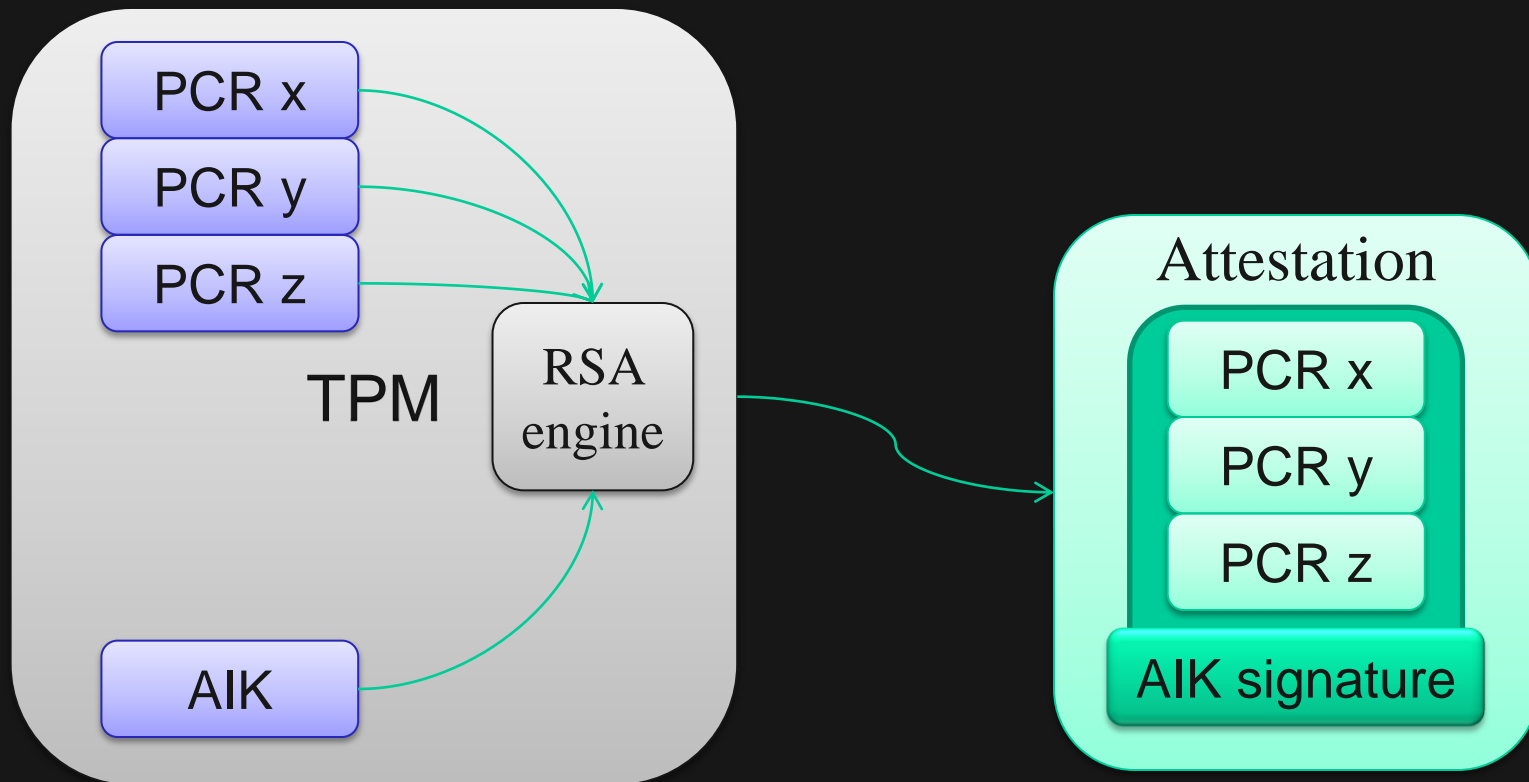
Keys, BitLocker, etc





Remote Attestation

TPM_Quote(): Sign PCRs with AIK



Strong Network Access Control (NAC)

Trusted Network Connect

assess the security of a kiosk with your mobile device

Conclusion

a TPM is a **passive** device

it cannot take over your platform by itself

at this point, there's no battle about
keeping our **freedom** / **rights**

Trusted Computing is a tool...

...nothing else



...and it's about time we start using it

Thanks!

MANTOR
ORGANIZATION