14:40 - 15:10

實現零信任環境的起點：

PUF-based 硬體安全矽智財

Realize Comprehensive Zero Trust with PUF based Security Anchor in Silicon

田浩倫 (Howard Tien)

熵碼科技, 市場行銷 副處長

Marketing Deputy Director , PUFsecurity Corporation


PUFsecurity
AN eMemory COMPANY

Realize Comprehensive Zero Trust with PUF-based Security Anchor in Silicon

2023 Arm Tech Symposia

PUFsecurity
AN eMemory COMPANY

IPR Notice

Our Value Proposition to Semiconductor Industry

Our Value Proposition

- ✓ We are committed to provide Best-in-class ***Hardware Root of Trust (HRoT)*** to ***Security Subsystem IP*** which supports SoC vendor to establish Security Anchor for Zero Trust.
- ✓ Our IP is silicon proven among Worldwide ***Semiconductor Manufactories*** and SoC vendor would be very convenient to silicon production.

Our Achievement

- ✓ The IP portfolio of ***eMemory*** and ***PUFsecurity*** Group have been verified over ***550*** technology platform in worldwide semiconductor manufactories.
- ✓ The new HRoT and Security subsystem IP has successfully support over 60 SoC projects for SoC vendor in 3 years especially from 55nm to 5nm technology.

Who We Are .

eMemory

World's Largest
Pure-Play eNVM Provider

PUFsecurity

Subsidiary Dedicated to
PUF-based Security IP

23 Years
In the IP business
Based in Taiwan

300 +
Employees
(70% IP Developers)

6,700 +
Customer
Tape-Outs

1,100 +
International
Patents Issued

Neo Fuse

Neo PUF

eMemory
Hard Macro IPs

PUFsecurity
+ Digital RTL IPs

PUFrt

PUFcc

25 +
Foundry Partners
around the world

52M +
8" Wafer shipped

550 +
Process Platforms
from 0.35um down to 5nm

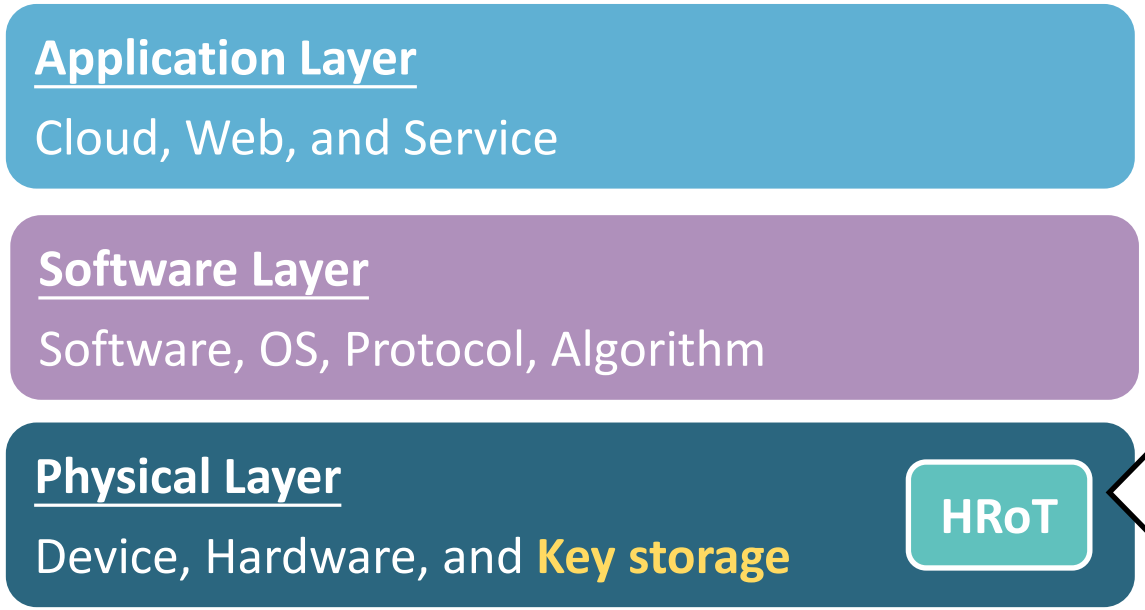
14 Years
Consecutive TSMC
IP Partner Award

Agenda

1. **From Zero Trust to Hardware Root-of-Trust(HRoT)**
2. Challenge of HRoT and Our Answer of One-Stop IP Solution
3. Application and Use case

From Zero Trust to **Hardware Root-of-Trust(HRoT)**

- *Kerckhoffs' Principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.*
- ***Zero Trust*** architecture has been implemented over applications, software, and physical layers, which must begin with a reliable ***HRoT***.



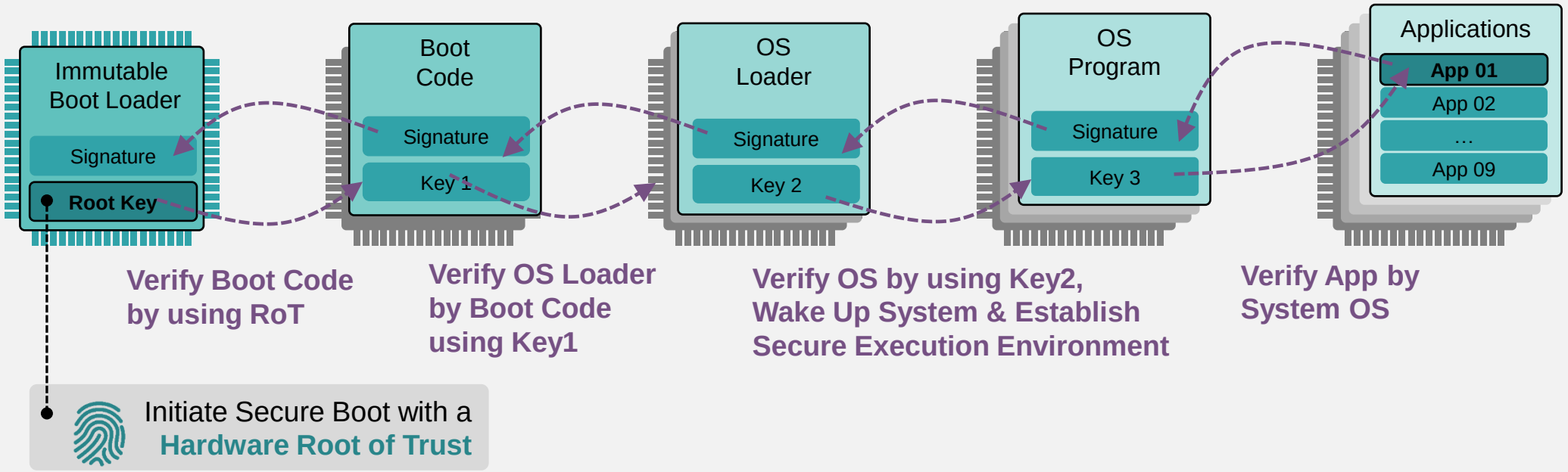
Hardware Root-of-Trust(HRoT):
RoT is ideally based on a hardware-validated boot process to ensure the system can only be started using code from an immutable source.

https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

The Chain of Trust Begins with HRoT

- **HRoT** works as Silicon **Secure Anchor** to protect**:** SW integrity, authentication, decryption, encryption, identification, and key exposure
- HRoT must includes key storage, entropy, and anti-tampering.

The **Secure Boot** Process

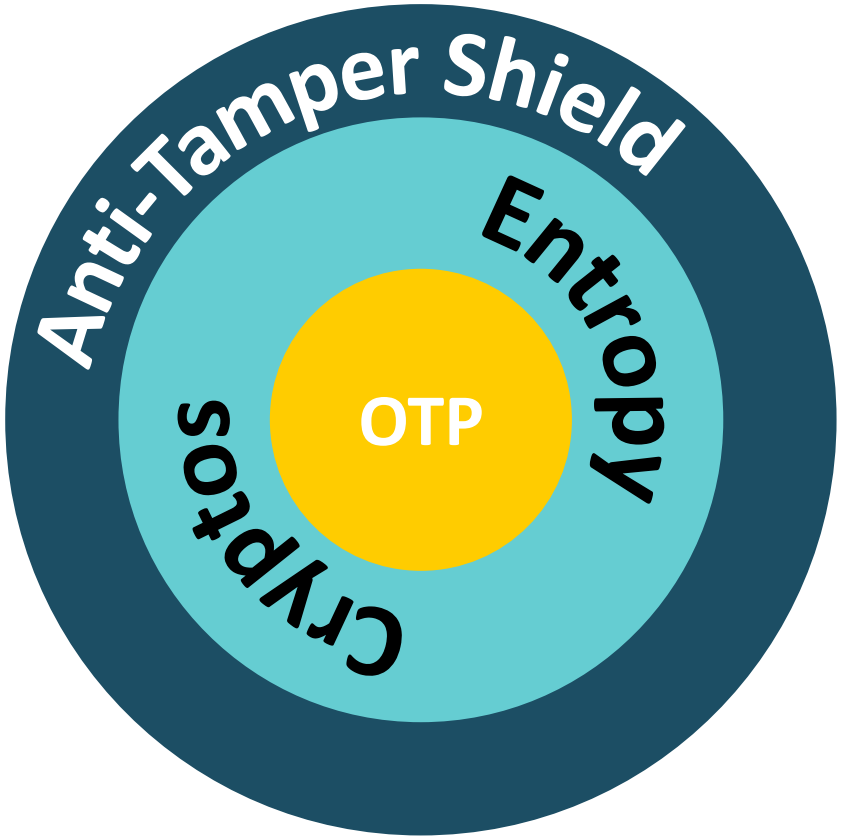


Necessary **Components** of HRoT

- HRoT requires OTP for key storage, entropy to protect key storage and security operation, and H/W cryptographic to support task of SE with design of Anti-tampering.

Components of HRoT
OTP
Static Entropy: PUF
Dynamic Entropy: TRNG
Hardware Cryptographic
Anti-tampering

Task of SoC Security Anchor
Secure Storage
Secure Operation
Secure Environment

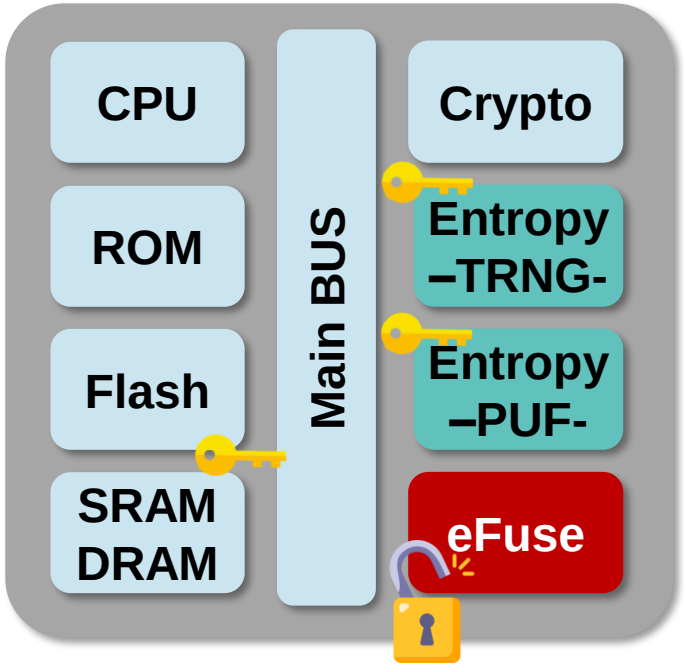


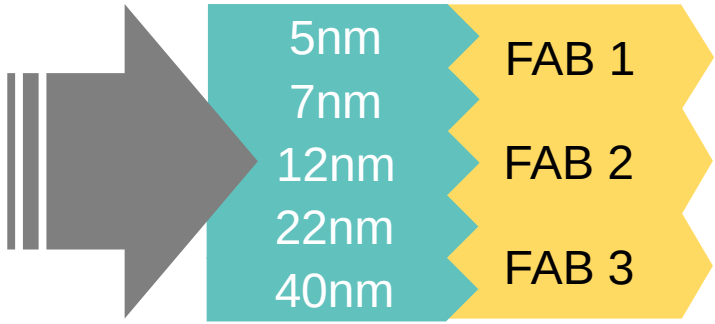
Agenda

1. From Zero Trust to Hardware Root-of-Trust(HRoT)
2. **Challenge of HRoT and Our Answer of One-Stop IP Solution**
3. Application and Use case

The Challenge Traditional Design Faces

- Designer needs HRoT and Entropy to build security anchor, **but**…
- SoC requires OTP to store secret data, **but**…

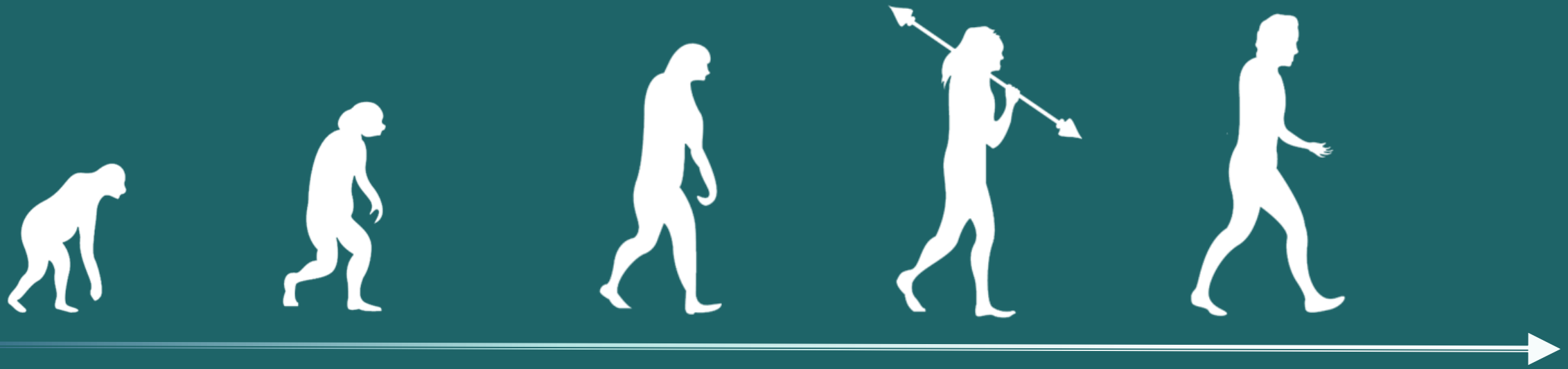




How to solve PVT issues?

How to solve eFuse untrusted issue?

Our Answer: Evolution of One-Stop IP Solution



eFuse

Insecure Storage

NeoFuse

Invisible Anti-fuse OTP

Evolution 1: Innovation of **Entropy**

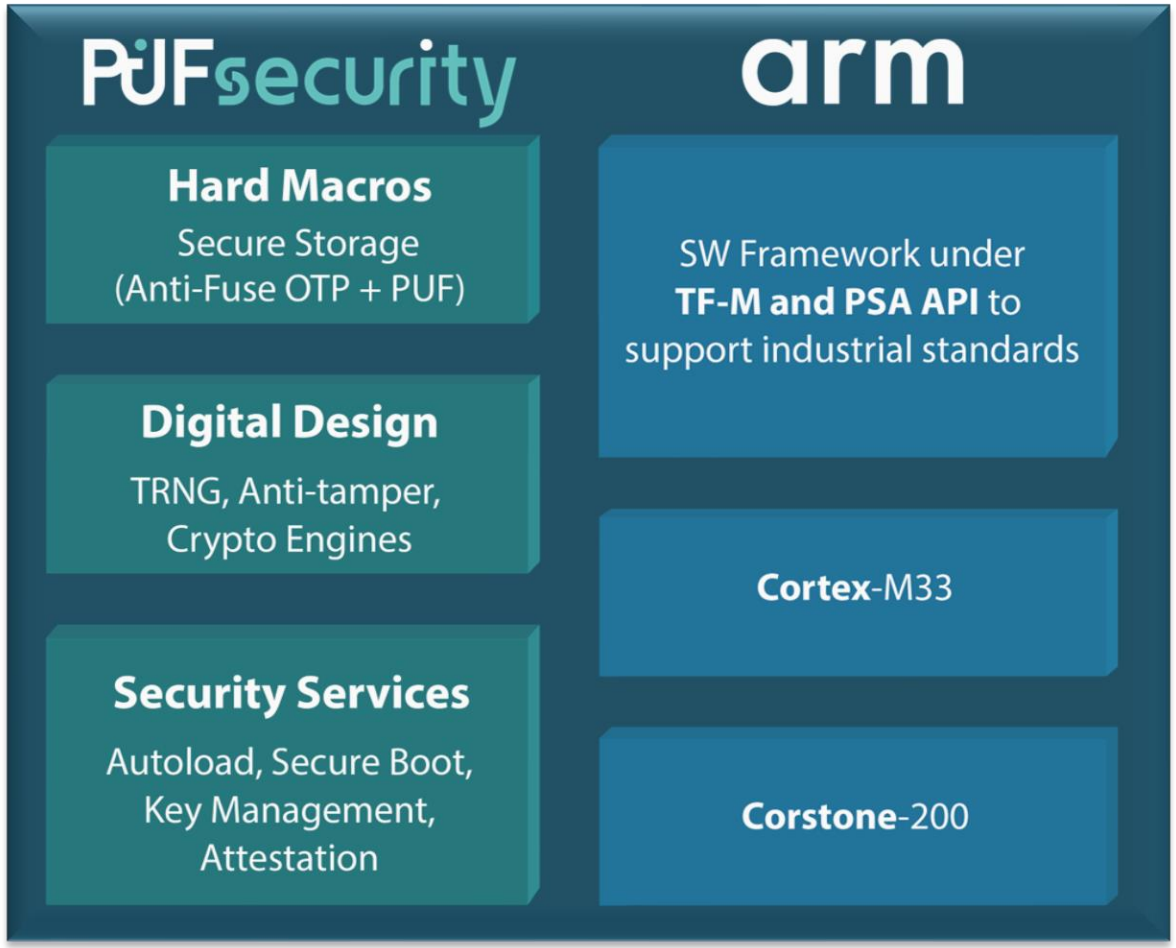
Evolution 2: Re-define **HRoT**

Evolution 3: **High Integration**

Agenda

1. From Zero Trust to Hardware Root-of-Trust(HRoT)
2. Challenge of HRoT and Our Answer of One-Stop IP Solution
3. **Application and Use case**

Latest Joint Solution for PSA Certified Level 2 Ready



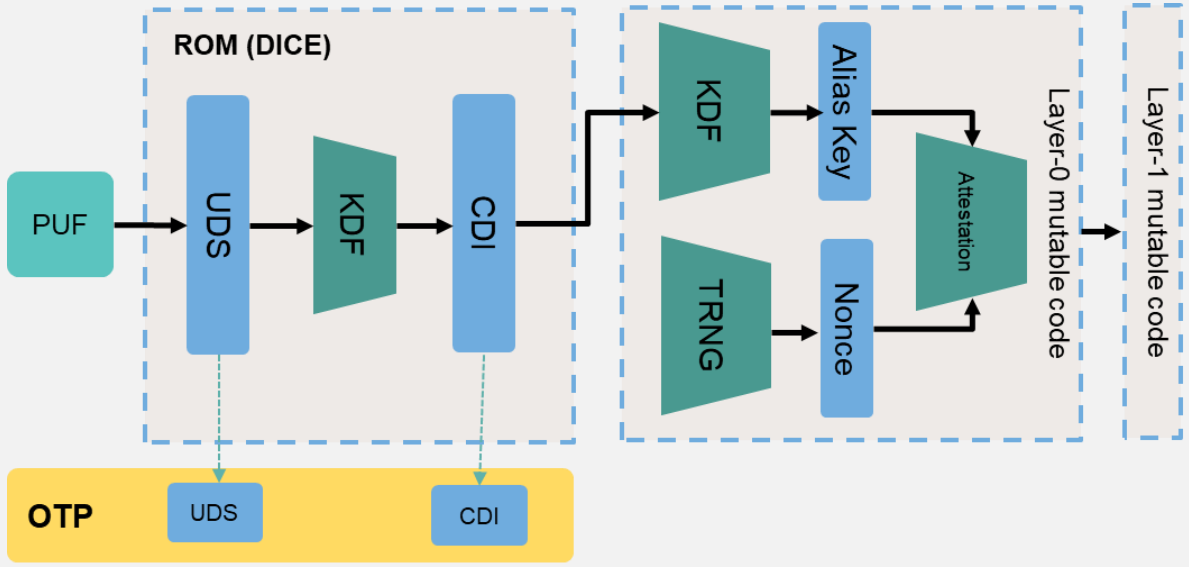
Certification and Availability

- **Pre-qualified Hard IPs:** Available everywhere in **~20** foundries and **200+** process nodes
- **Best Choice Award:** for PUFcc crypto coprocessor in the Cyber Security category
- **Riscure Certified:** PUFrt (HRoT) can support the anti-tampering requirements for CC EAL5+
- **NIST-CAVP Certified:** All NIST crypto algorithms are CAVP certified and with anti-SCA protection
- **PSA Certified Level 2 Ready:** PUFcc with PSA function APIs, also supports TF-M and Mbed TLS
- SESIP-LV3 to be ready (2023/Q4)

Use Cases in Other Key Applications

PUFrt: SoC Security Anchor | PUFcc: Security Subsystem

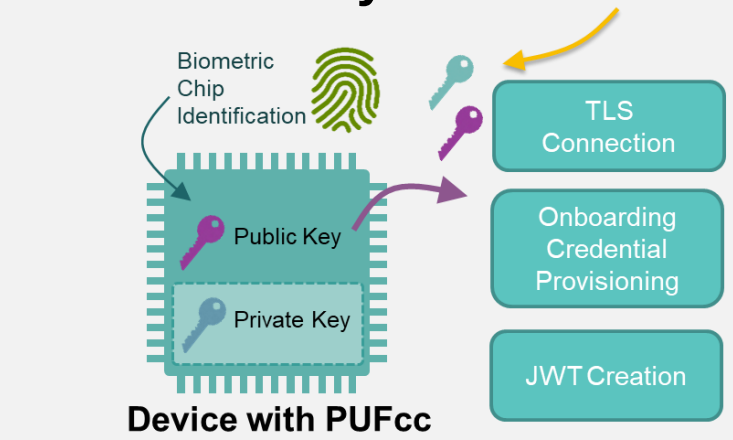
Calitpra Silicon RoT: TCG DICE Layer Measurement



Ref: Open Compute Project - Calitpra Silicon RoT
By Microsoft, Google, AMD, Meta, Intel, Cisco, Nvidia

matter

Cloud Security



Key Benefits for Customers and Partners

Save Cost

Minimize Risk

Standard Alignment

Time to Market

Thank you

howard@pufsecurity.com

PUFsecurity
AN eMemory COMPANY