2022 July 28th

Ensuring Security of Application & Service with Chip Fingerprint

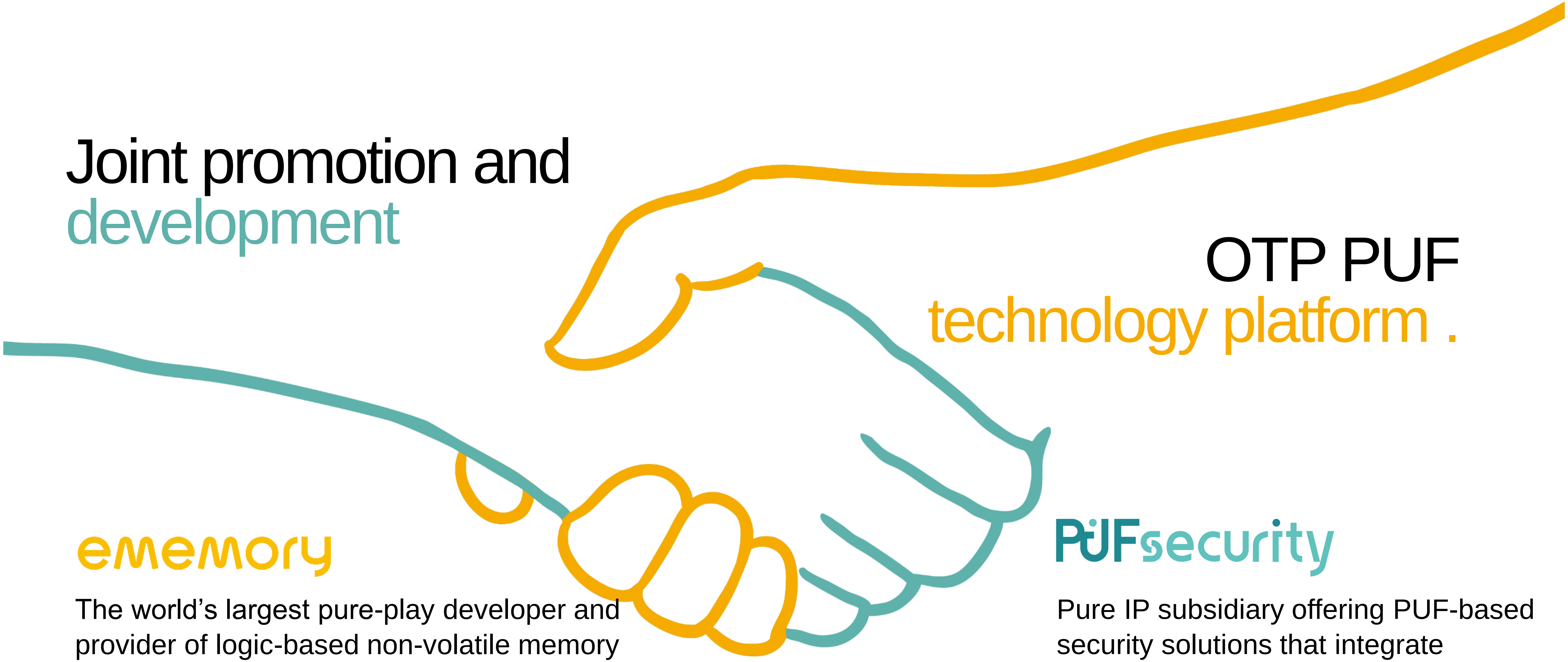
力旺電子 / 熵碼科技
楊青松

PUFsecurity

Agenda

1. Company Introduction
2. What is Security? What do You Need for Security?
3. Why is Hardware Root of Trust a Must?
4. Benefits of Using PUF (Chip Fingerprint)
5. Chip Design with PUF-based Solutions

Hardware Security by eMemory & PUFsecurity .



Joint promotion and development

OTP PUF technology platform .

eMemory

The world’s largest pure-play developer and provider of logic-based non-volatile memory (Logic NVM) technology and security IP.

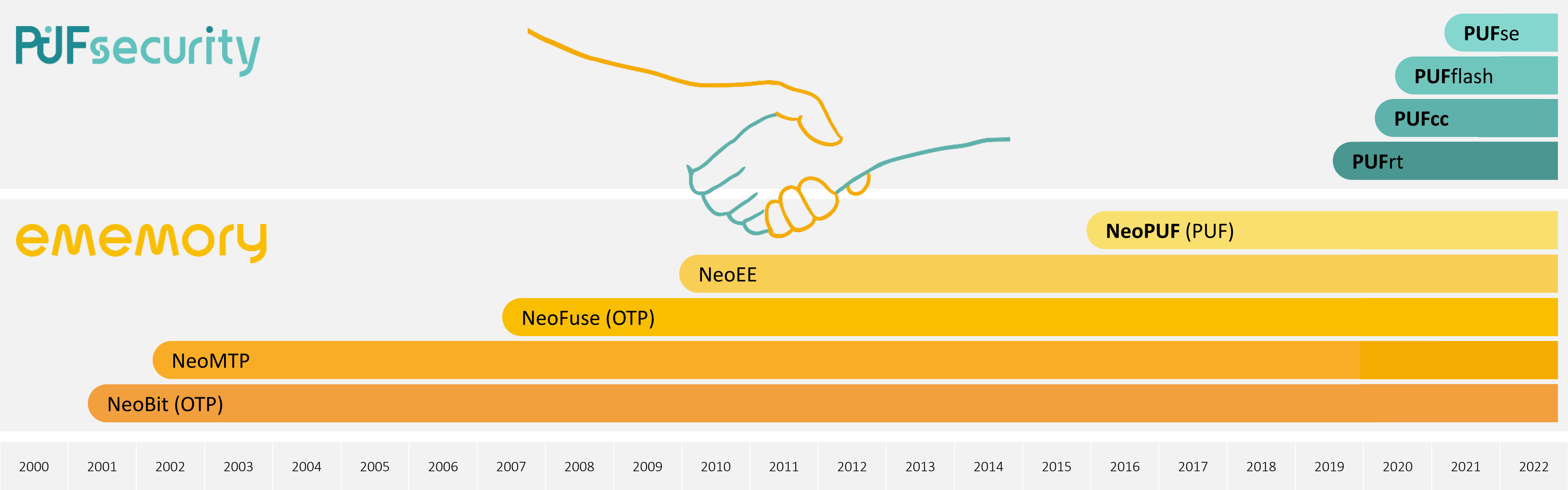
PUFsecurity

Pure IP subsidiary offering PUF-based security solutions that integrate eMemory’s OTP and security technology.

20+ Years of Process Development

- With access to eMemory's widely verified IP process platform, PUFsecurity is uniquely positioned to provide IP Security solutions with **extensive availability** across various foundries and process nodes.

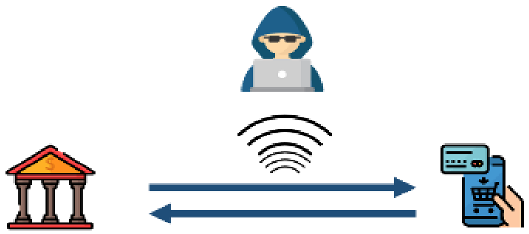
- **PUF** stands for Physically Unclonable Function which is **Fingerprint in Silicon**



Why You Need Security

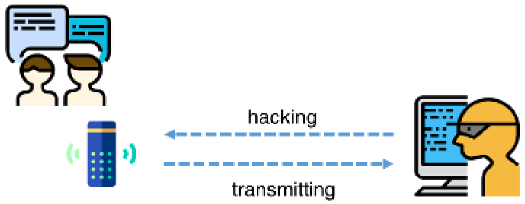
Mobile Payment

Unguarded devices with sound payment systems still lead to **property loss**



IOT Application

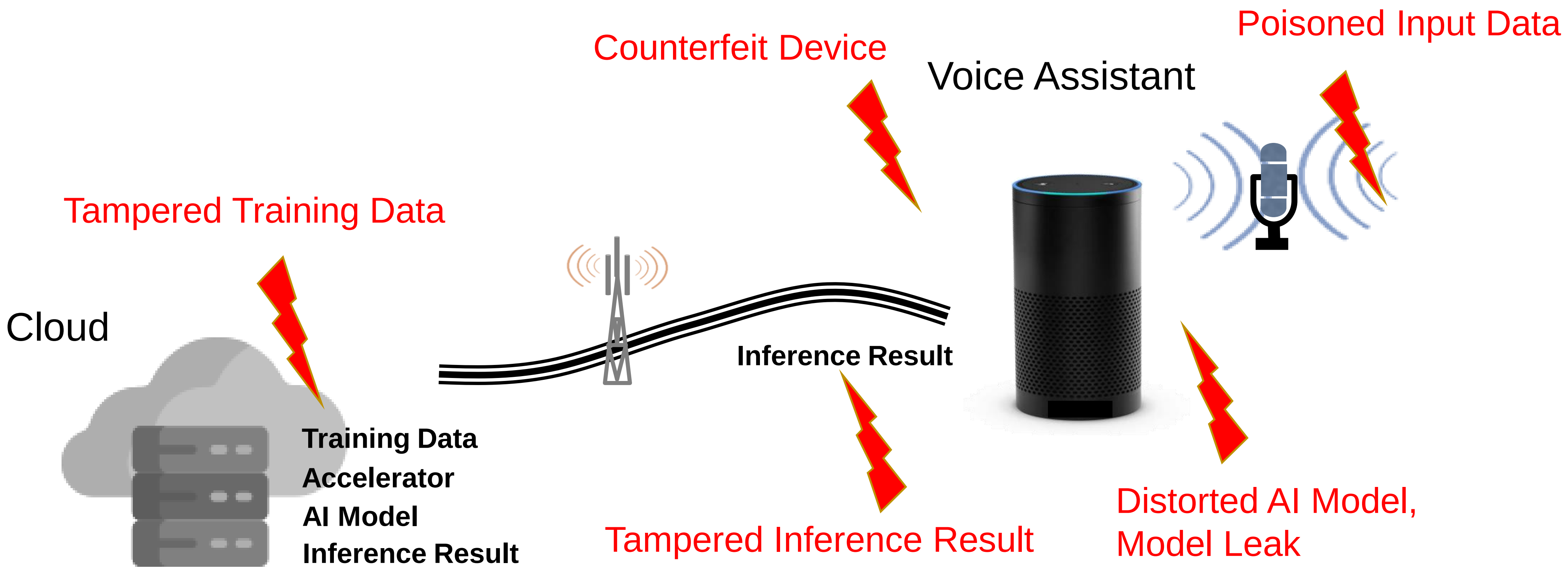
End devices incapable of "heavy" protection results in **privacy leak**



Automotive

Automobiles with tampered SW / FW may **endanger life**

Security Threats in AIoT Applications

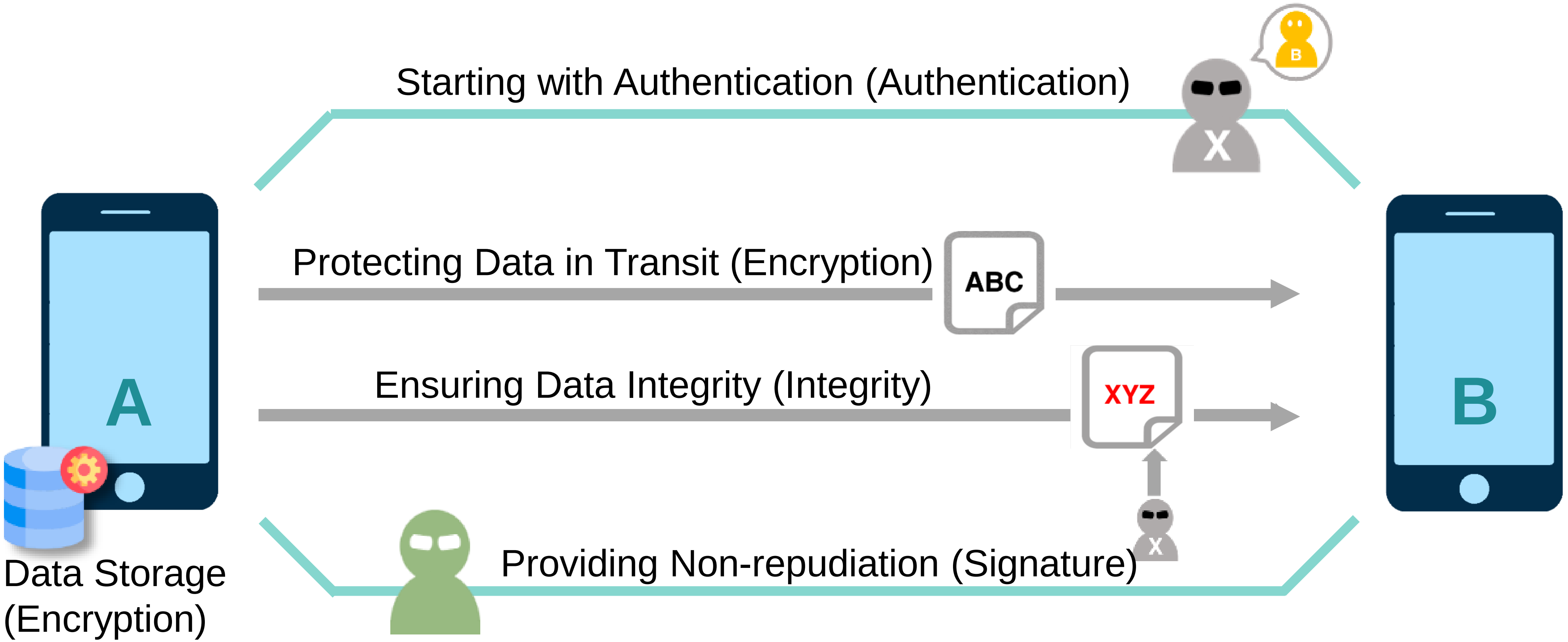


Privacy Leak, Malfunction, Property Loss

Agenda

1. Company Introduction
2. What is Security? What do You Need for Security?
3. Why is Hardware Root of Trust a Must ?
4. Benefits of Using PUF (Chip Fingerprint)
5. Chip Design with PUF-based Solutions

Required Security Function for Chip Security



Starting with Authentication (Authentication)

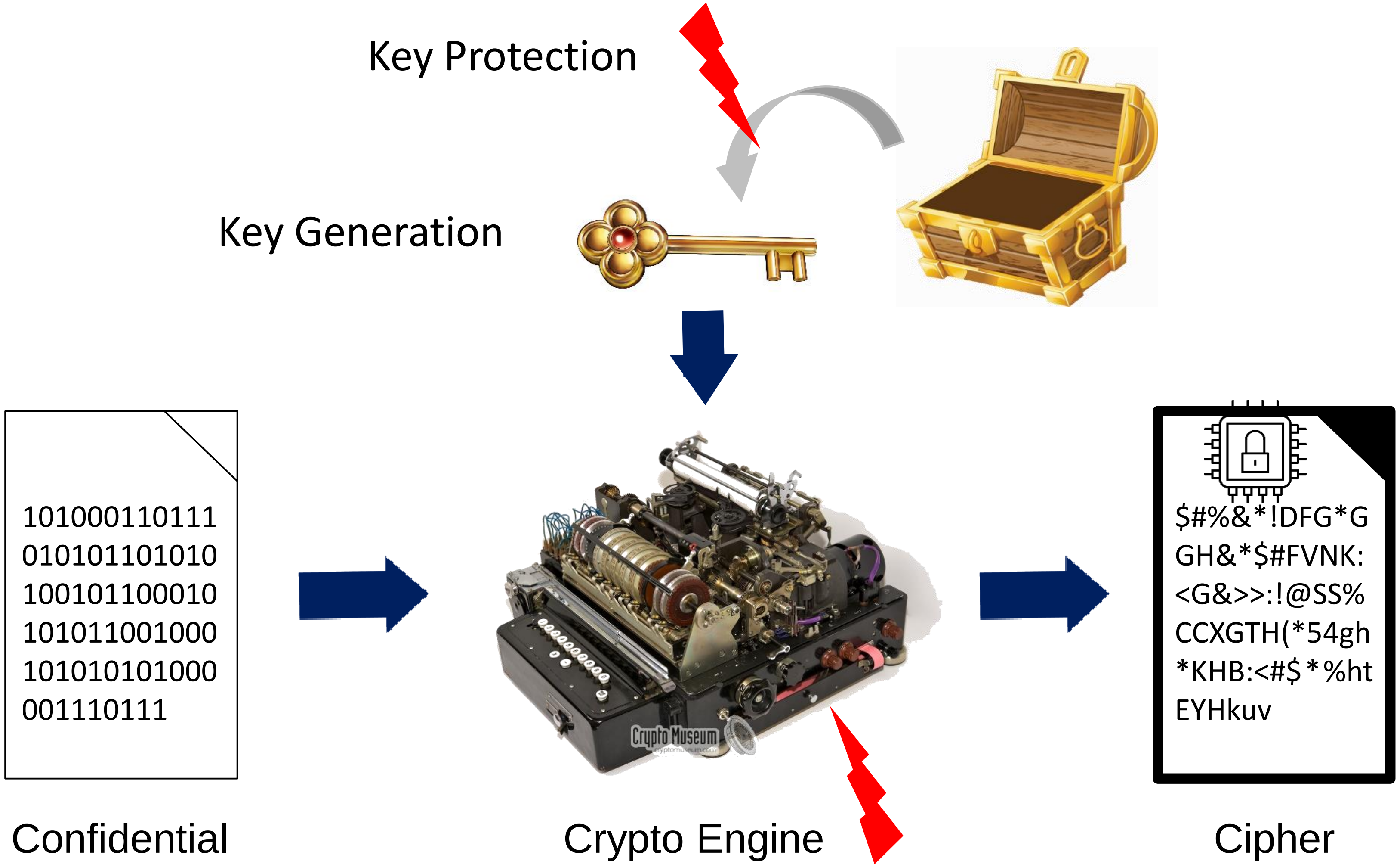
Protecting Data in Transit (Encryption)

Ensuring Data Integrity (Integrity)

Providing Non-repudiation (Signature)

Data Storage (Encryption)

The important “**Key**” to Security



Key Protection

Key Generation

101000110111
010101101010
100101100010
101011001000
101010101000
001110111

Confidential

Crypto Engine

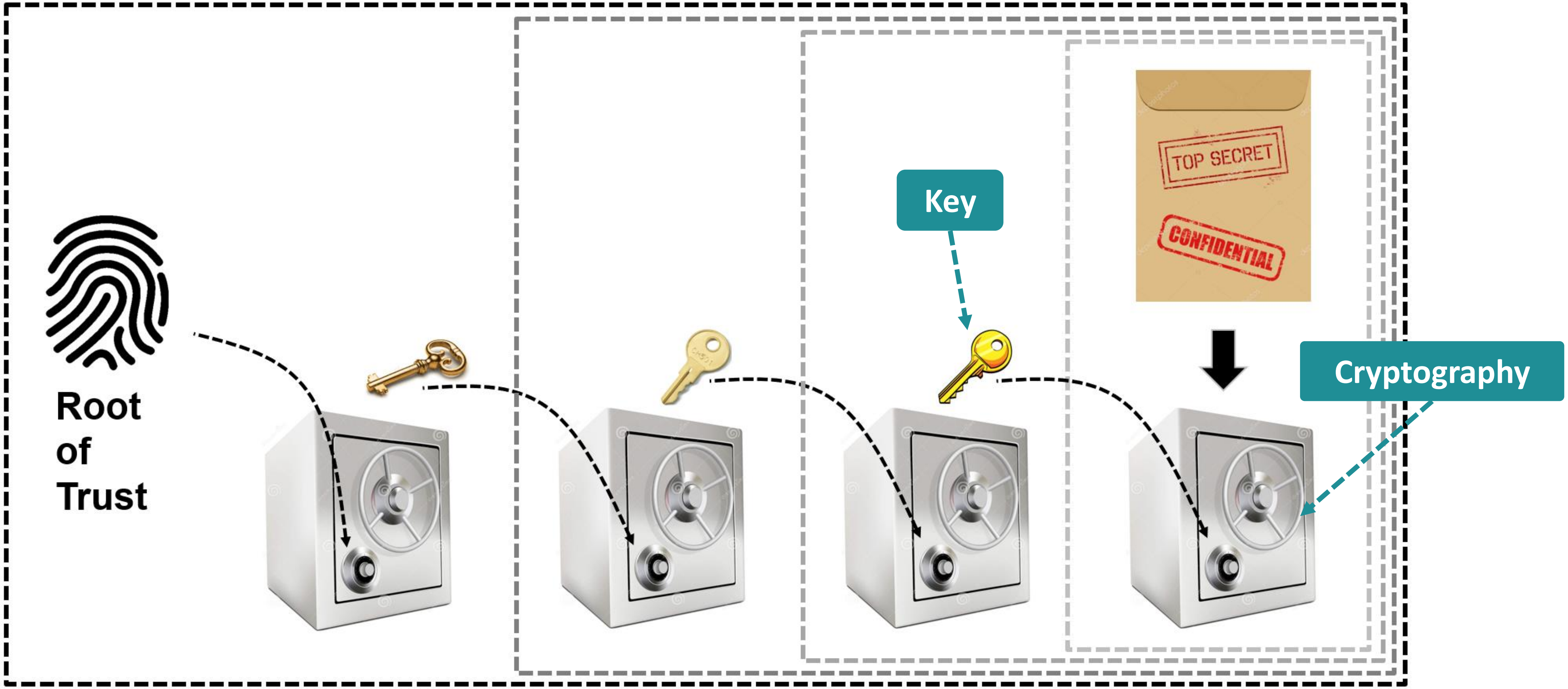
$#%&*!DFG*G
GH&*$#FVNK:
<G&>>:!@SS%
CCXGTH(*54gh
KHB:<#$%ht
EYHkuv

Cipher

Crypto Strength

Security and **Chain of Trust** Concept

Root of Trust (Root Key) is necessary and has highest level security authority.

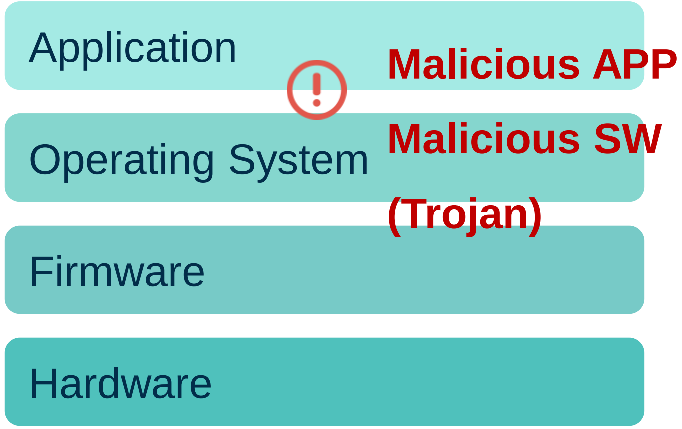


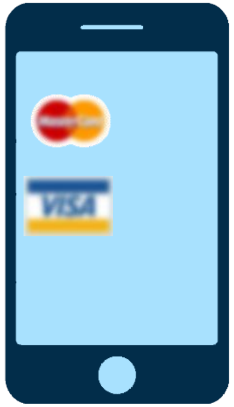
Agenda

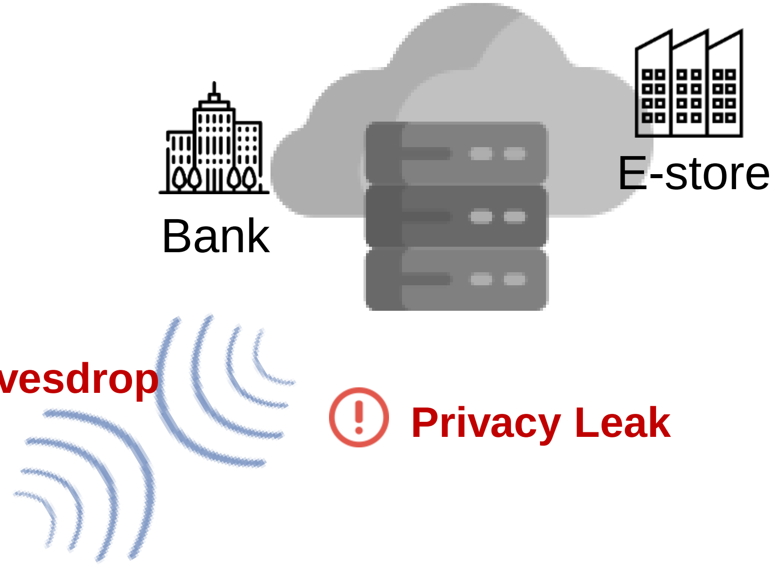
1. Company Introduction
2. What is Security? What do You Need for Security?
3. Why is Hardware Root of Trust a Must?
4. Benefits of Using PUF (Chip Fingerprint)
5. Chip Design with PUF-based Solutions

Threats When You Enjoy Applications

Be careful of free APP







Software defines application through re-configuration for a variety of applications

But, how do we make sure that **"software is secure?**

Hardware RoT is indispensable

Binding software/APP & hardware root of trust (FP).
Device registration with hardware root of trust (FP).

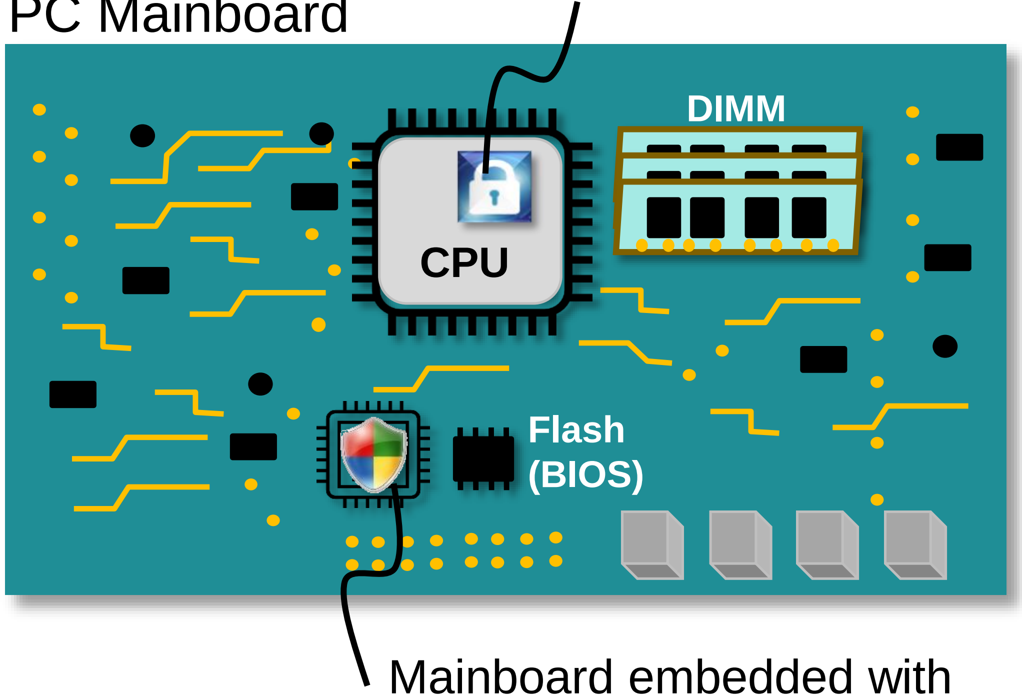
Hardware root of trust as secure anchor for

- validating software integrity from initiation
- providing secure execution environment
- protecting data in-use & in-transit

PC Security Architecture Driven by Window 11

CPU embedded with
Security Element IP (PUFcc)

PC Mainboard



Mainboard embedded with
Security Controller (MCU + PUFrt or PUFcc)

CPU embedded with Security Element IP:
-As root of trust of CPU
-Perform crypto security functions & validate software for applications

Mainboard embedded with Security Controller:
-As root of trust of mainboard
-Validate boot code and ensure secure boot when power-on (BIOS)

Agenda

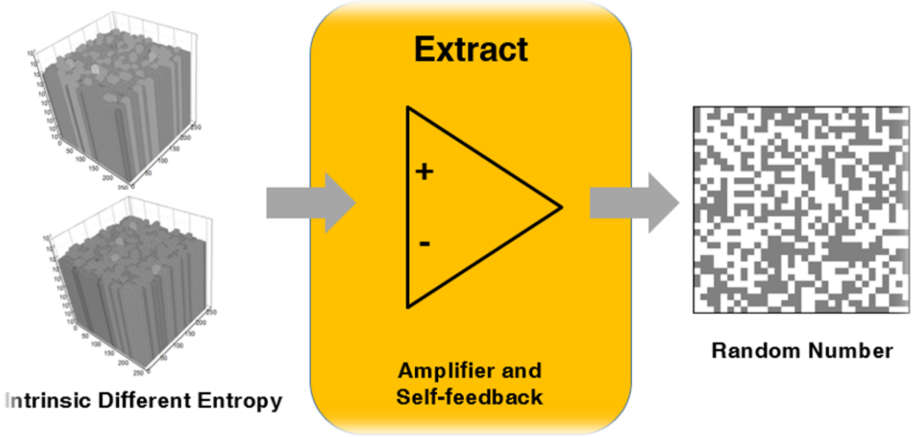
1. Company Introduction
2. What is Security? What do You Need for Security?
3. Why is Hardware Root of Trust a Must?
4. Benefits of Using PUF (Chip Fingerprint)
5. Chip Design with PUF-based Solutions

PUF: Physical Unclonable Function

Human Fingerprint

Collision probability $1/10^{20}$ (12points)

PUF (Chip Fingerprint)



$2^{64}= 1.8\text{x}10^{19}$; $2^{256}=1.5\text{X}10^{77}$

$2^{128}= 3.4\text{x}10^{38}$; $2^{512}=1.3\text{x}10^{154}$

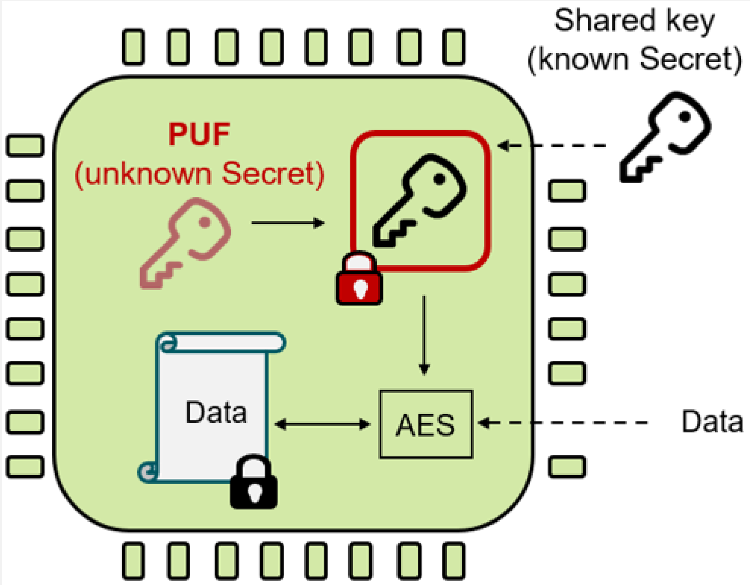
→ 256 bits ID can provide each IC unique identity

What **Chip Fingerprint (PUF)** can do .

On-chip **Unique Identity (UID)**

Can’t be blank
Can’t be cloned
Can’t be assigned

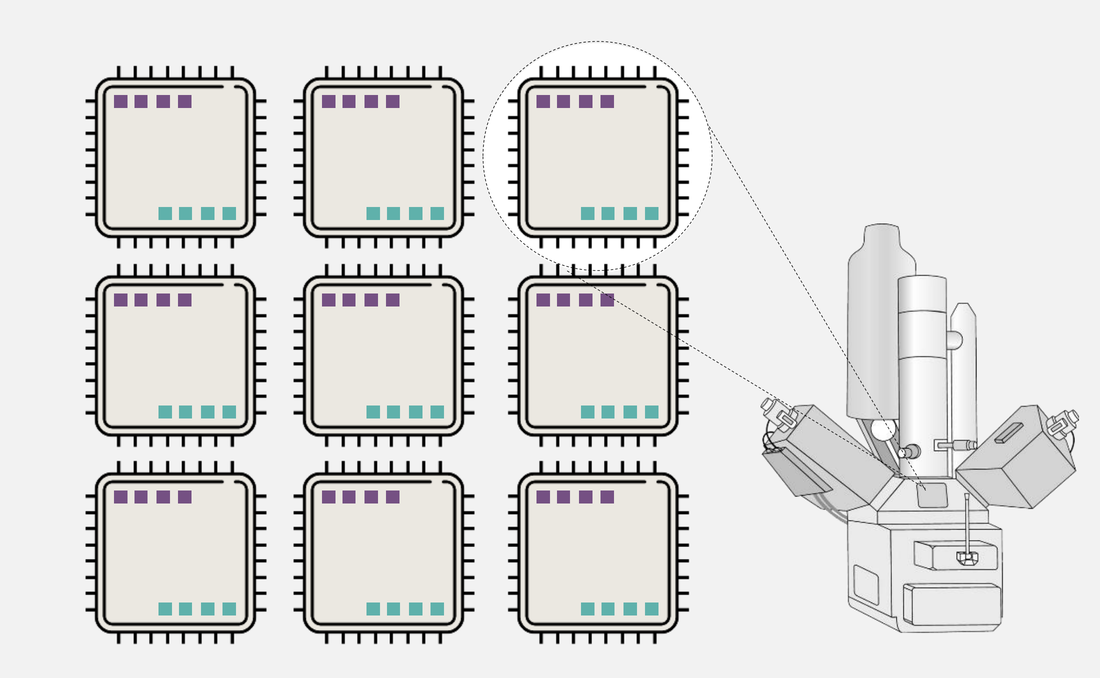
Inborn **Hardware Unique Key (HUK)**



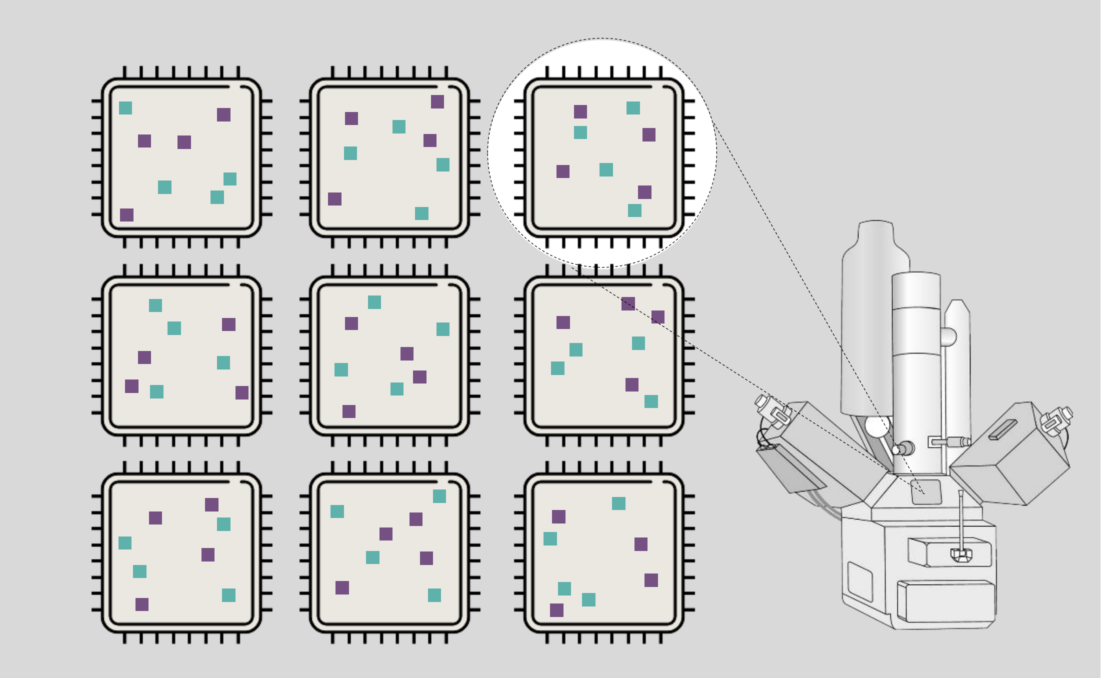
Secure OTP for Root Key Storage

Key Storage in OTP
Without PUF Protection

Key Storage in Secure OTP
With PUF Protection

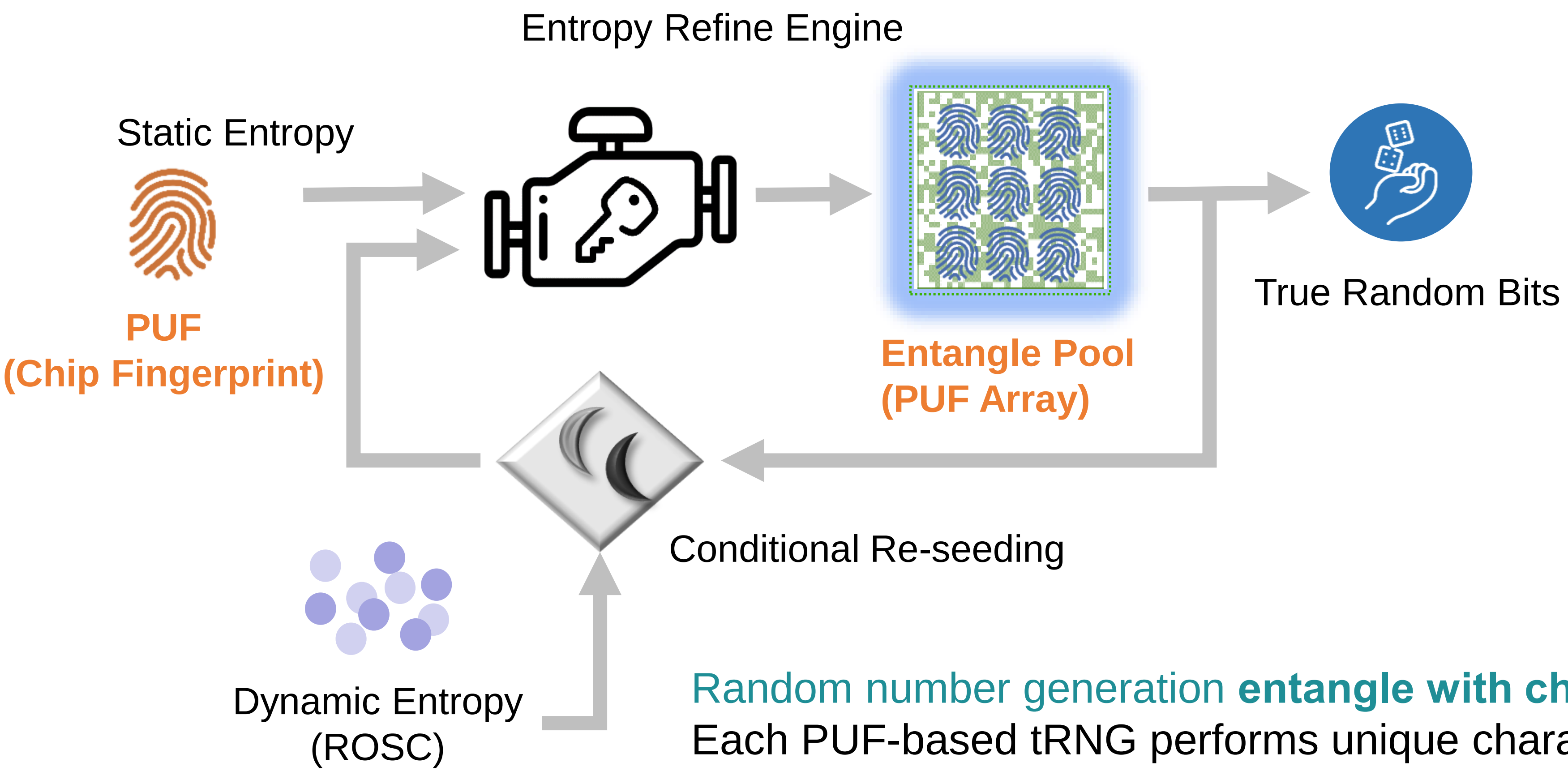


- Data at same physical location for each chip



- Data at **different** physical location which is **entangled with each chip PUF**

Each Chip has its **Own** PUF-based **tRNG**

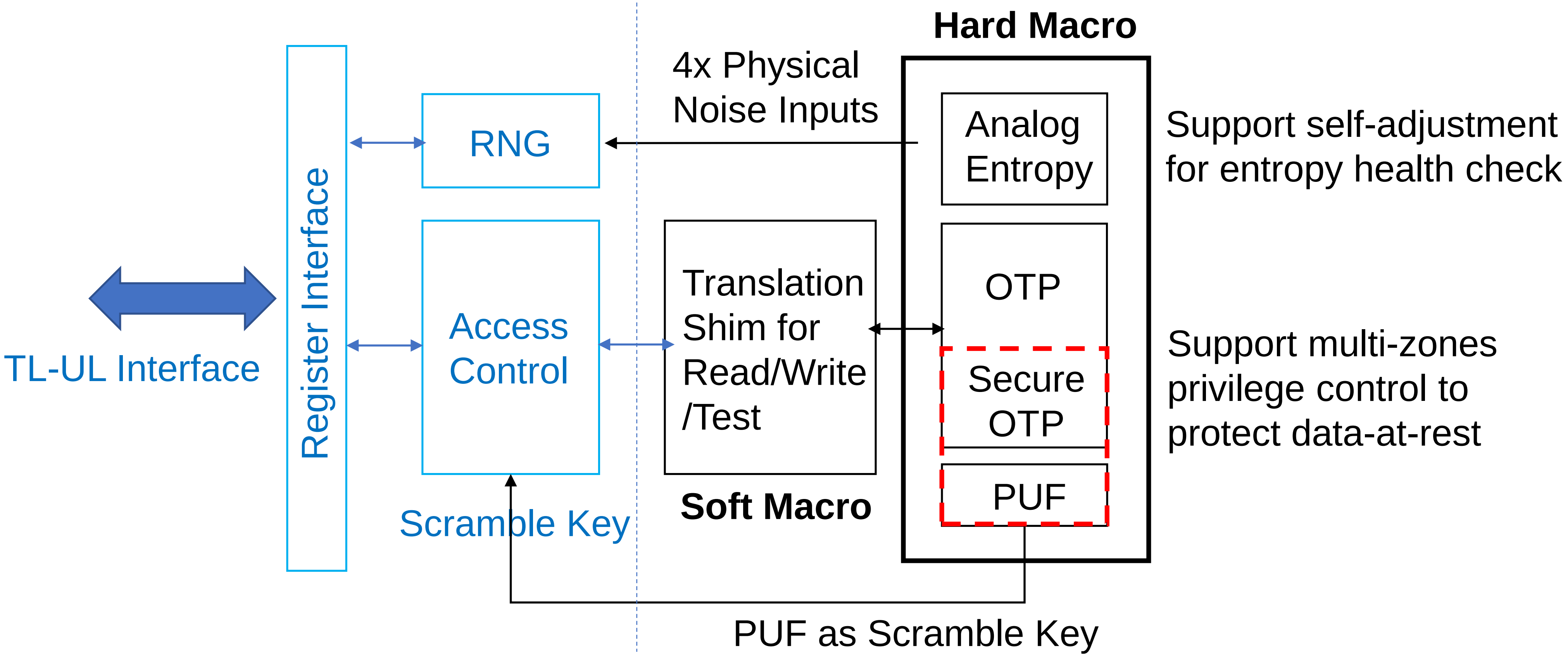


Random number generation **entangle with chip's own PUF array**. Each PUF-based tRNG performs unique characteristic which is different from chip to chip.

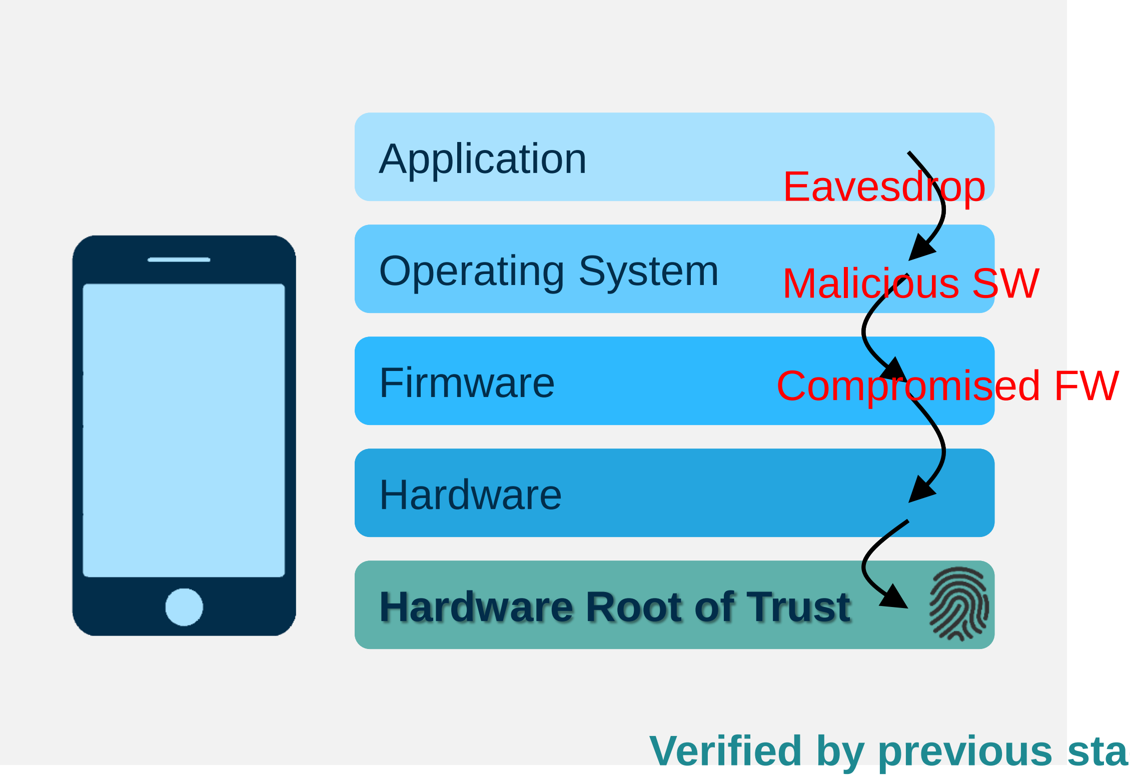
Easy Root of Trust Implementation for **OpenTitan**

OpenTitan
open-source controller

PUFrt solution combines **Soft Macro** (security control interface) & **Hard Macro** (integrated with OTP/PUF/Entropy Source)



Establishing **Root of Trust** with Chip Fingerprint



Application

Eavesdrop

Operating System

Malicious SW

Firmware

Compromised FW

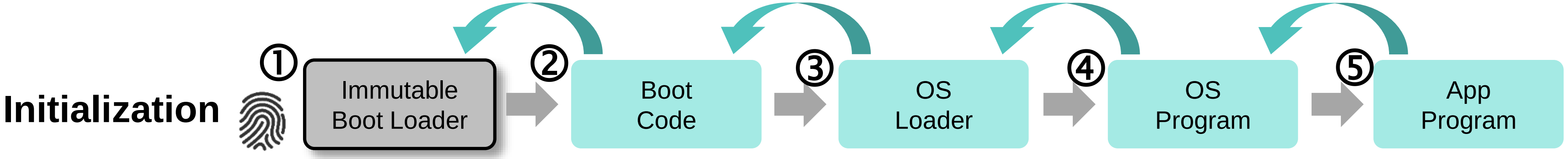
Hardware

Hardware Root of Trust

Hardware root of trust as secure anchor

- Application Authentication
- Data encryption
- Secure execution environment
- SW/FW integrity
- Certification, identity, key exposure

Verified by previous stage



Initialization

① Immutable Boot Loader

② Boot Code

③ OS Loader

④ OS Program

⑤ App Program

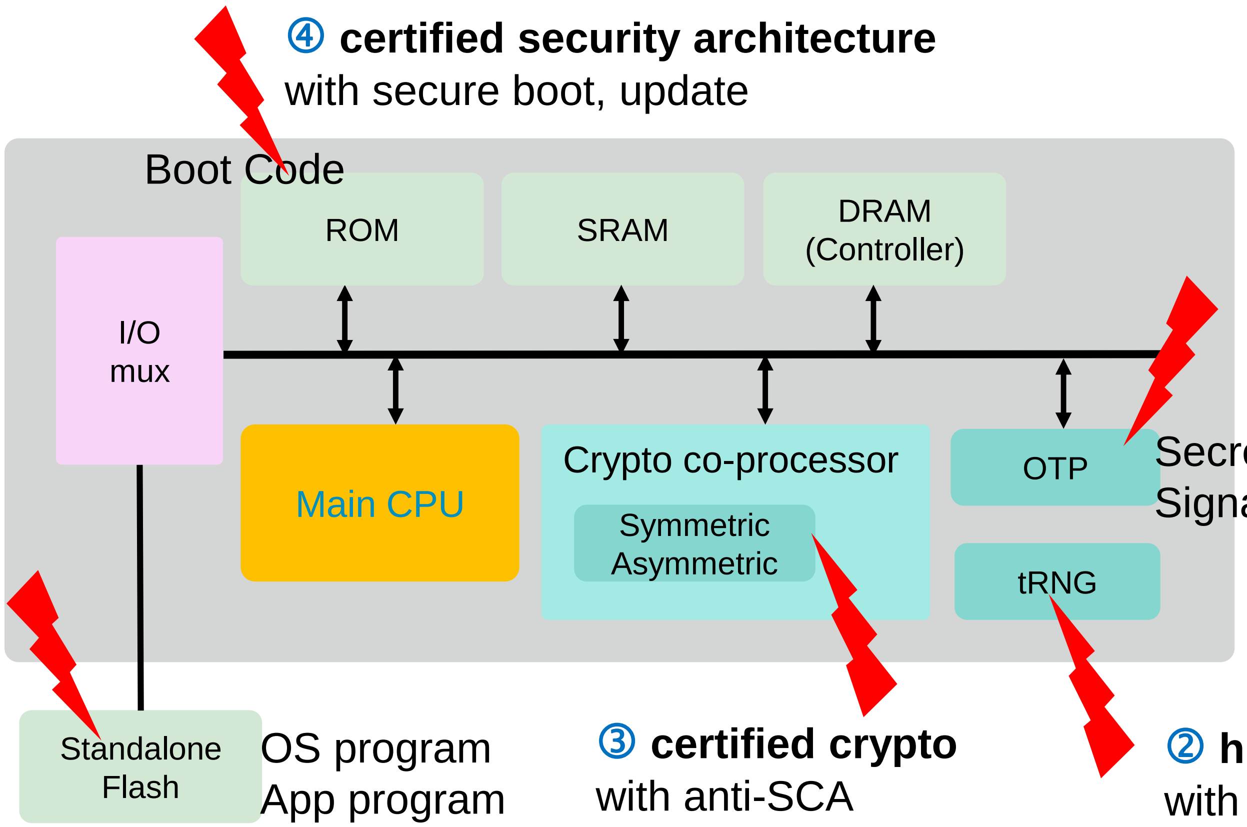
Secure Boot with Hardware Root of Trust

Agenda

1. Company Introduction
2. What is Security? What do You Need for Security?
3. Why is Hardware Root of Trust a Must?
4. Benefits of Using PUF (Chip Fingerprint)
5. Chip Design with PUF-based Solutions

Security Consideration for Chip Design

④ **certified security architecture**
with secure boot, update



① **secure storage** with
certified anti-tampering

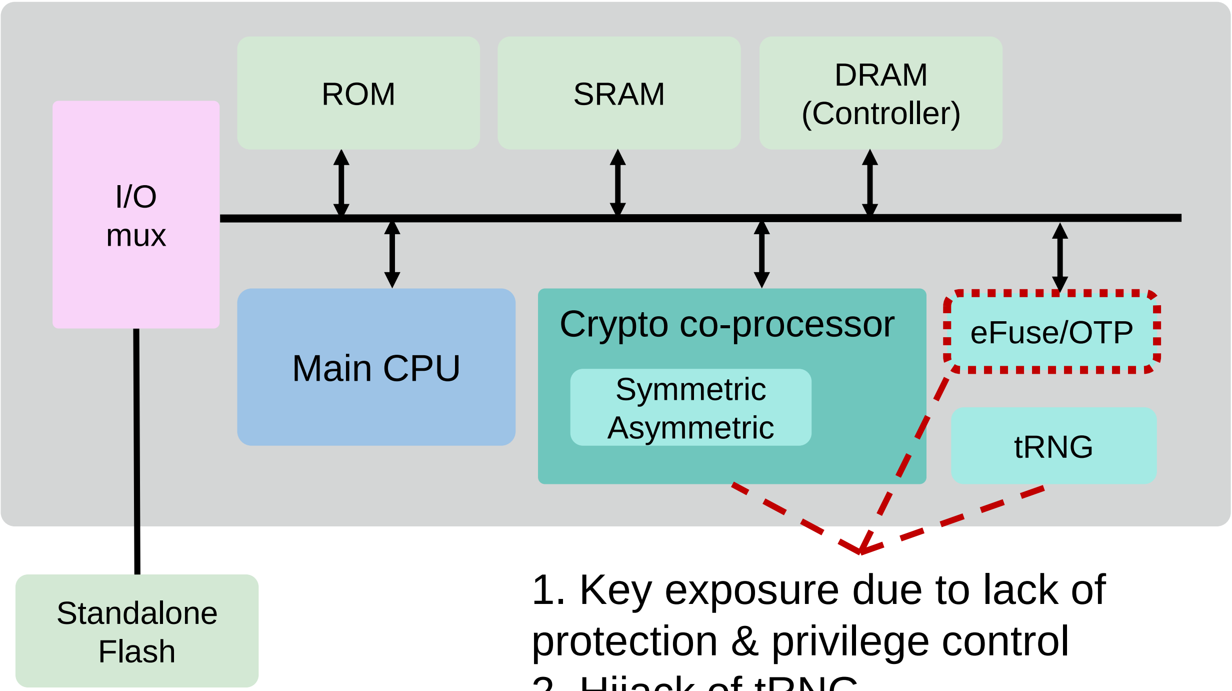
③ **certified crypto**
with anti-SCA

② **high quality tRNG**
with anti-tampering

① **secure storage**
with privilege control

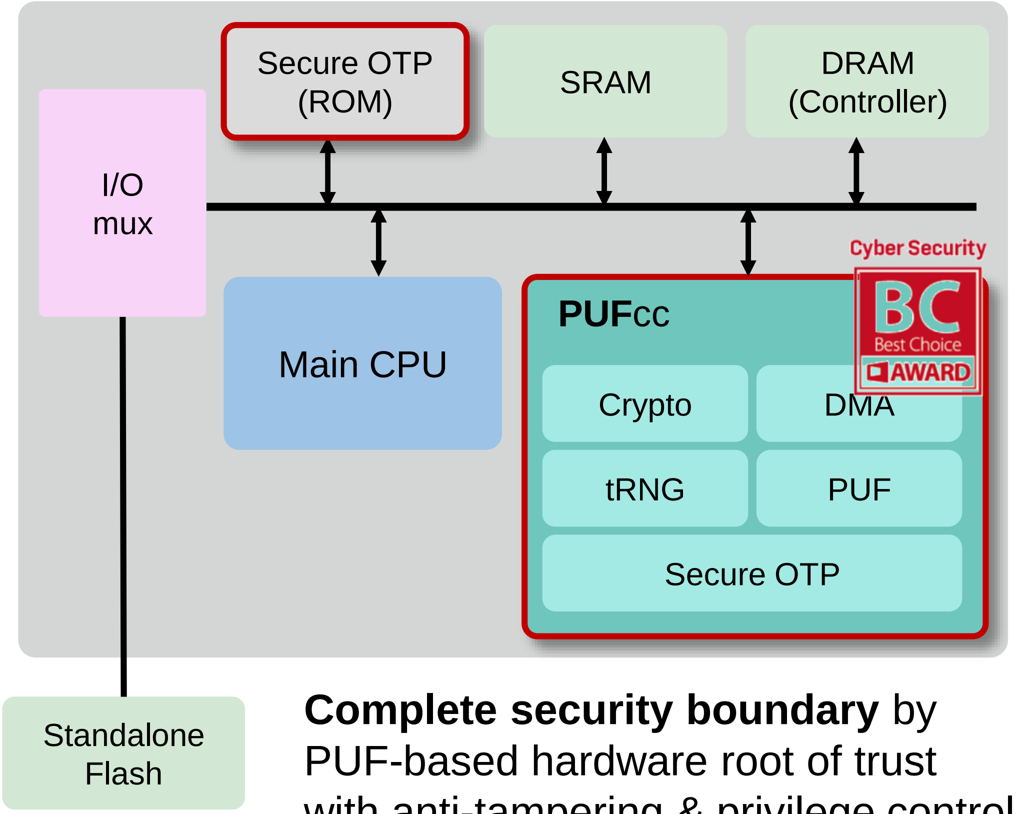
Complete **Security Boundary** by PUF-based HW RoT

Conventional Security Architecture



1. Key exposure due to lack of protection & privilege control
2. Hijack of tRNG
3. Side channel attack on crypto

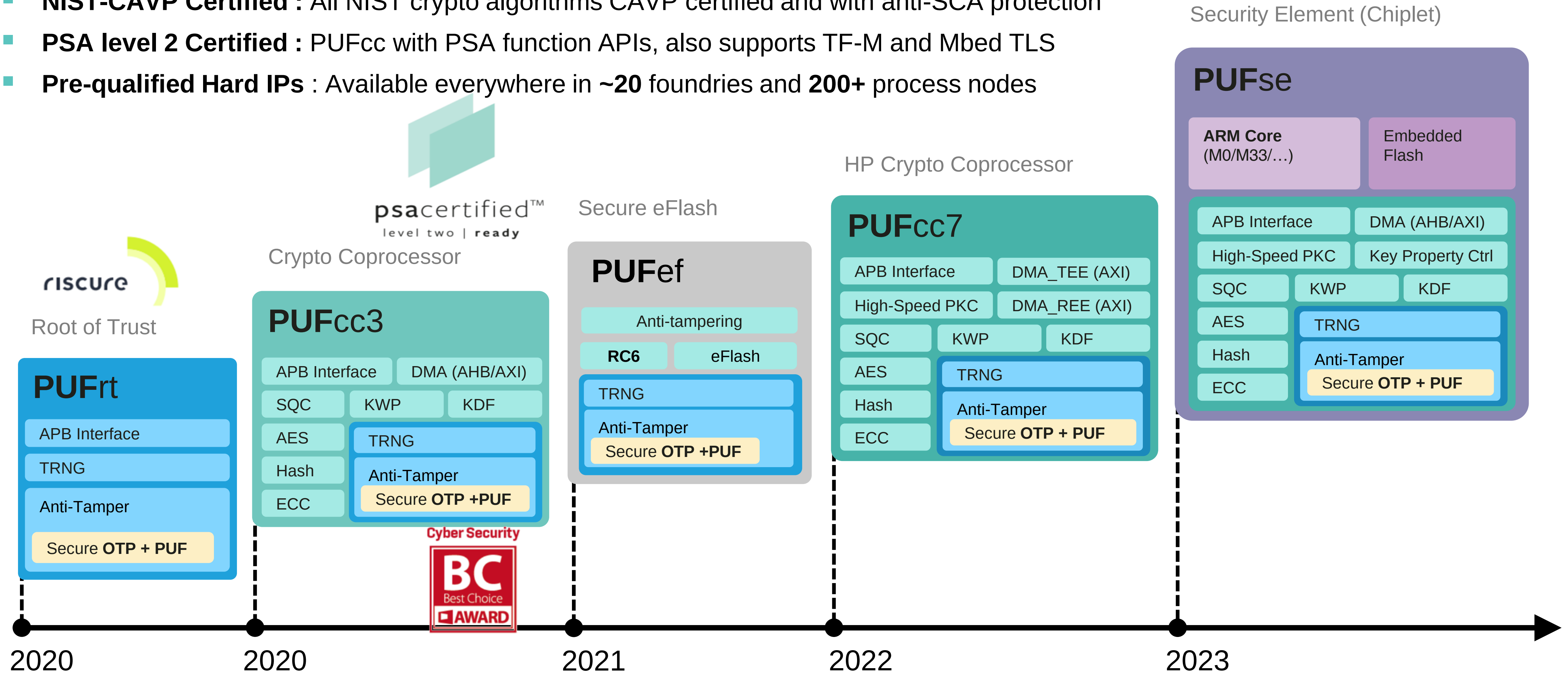
PUF-based Security Architecture



Complete security boundary by PUF-based hardware root of trust with anti-tampering & privilege control

PUFsecurity Product Portfolio

- **Riscure Certified :** PUFrt HRoT design
- **NIST-CAVP Certified :** All NIST crypto algorithms CAVP certified and with anti-SCA protection
- **PSA level 2 Certified :** PUFcc with PSA function APIs, also supports TF-M and Mbed TLS
- **Pre-qualified Hard IPs** : Available everywhere in **~20** foundries and **200+** process nodes



Root of Trust

PUFrt
APB Interface
TRNG
Anti-Tamper
Secure **OTP + PUF**

2020

Crypto Coprocessor

PUFcc3
APB Interface | DMA (AHB/AXI)
SQC | KWP | KDF
AES
Hash
ECC
TRNG
Anti-Tamper
Secure **OTP +PUF**

2020

Secure eFlash

PUFef
Anti-tampering
RC6 | eFlash
TRNG
Anti-Tamper
Secure **OTP +PUF**

2021

HP Crypto Coprocessor

PUFcc7
APB Interface | DMA_TEE (AXI)
High-Speed PKC | DMA_REE (AXI)
SQC | KWP | KDF
AES
Hash
ECC
TRNG
Anti-Tamper
Secure **OTP + PUF**

2022

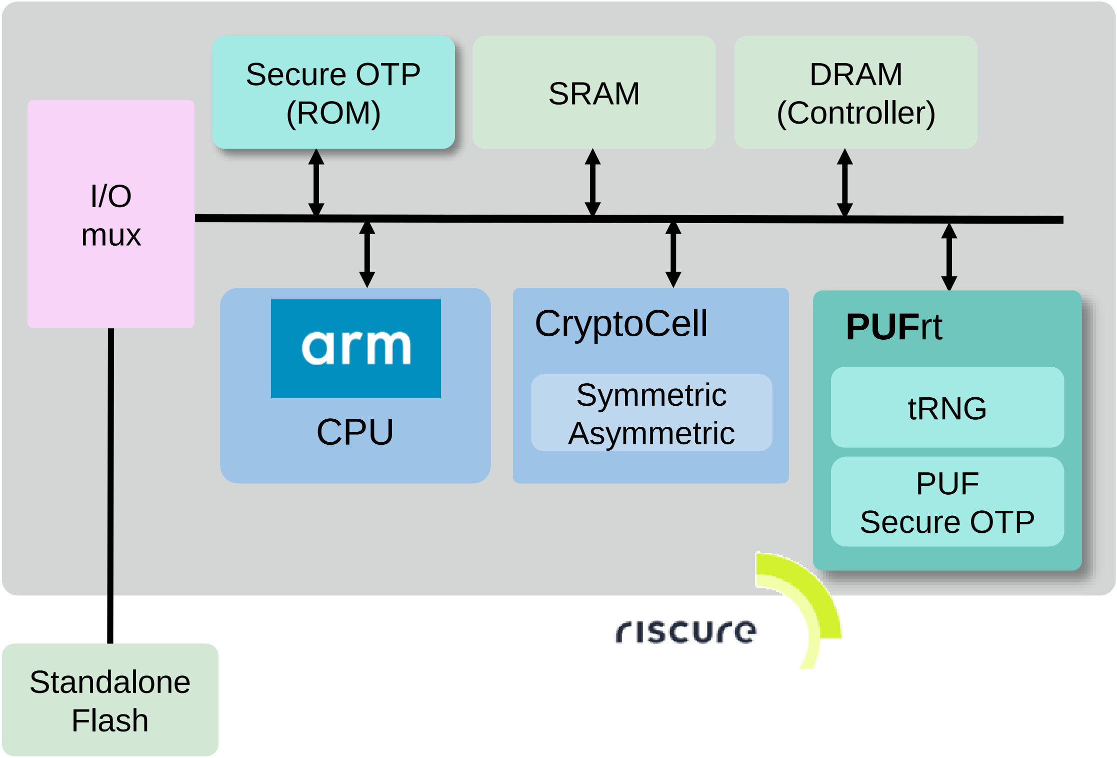
Security Element (Chiplet)

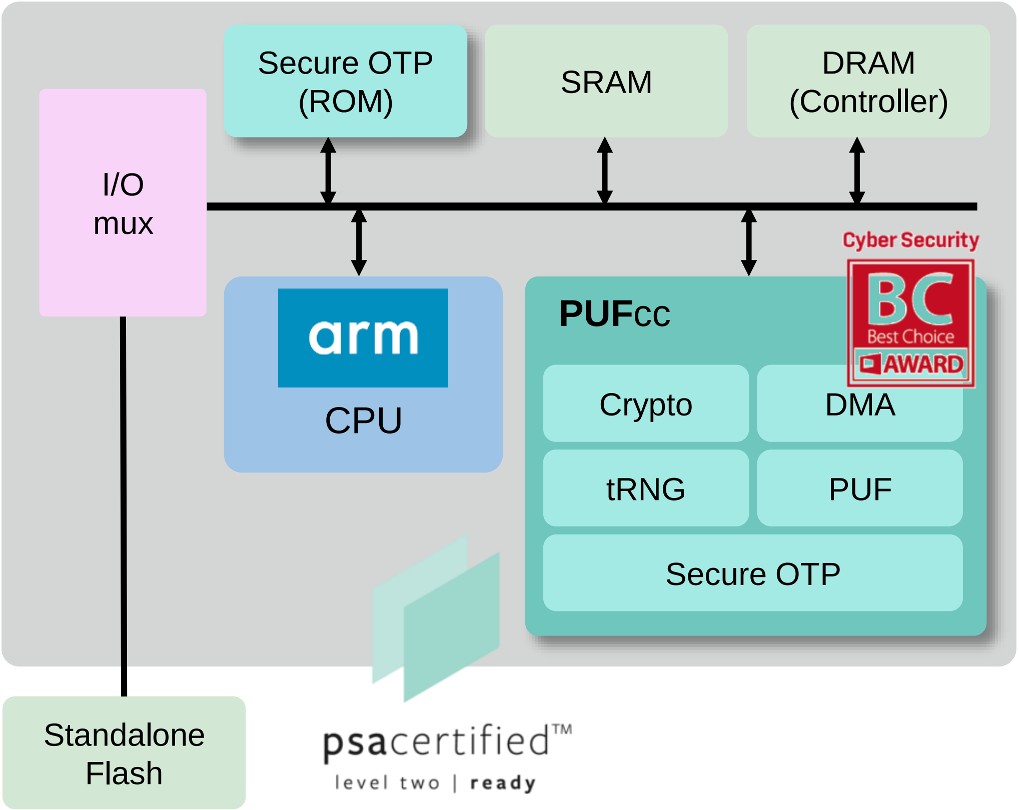
PUFse
ARM Core (M0/M33/…) | Embedded Flash
APB Interface | DMA (AHB/AXI)
High-Speed PKC | Key Property Ctrl
SQC | KWP | KDF
AES
Hash
ECC
TRNG
Anti-Tamper
Secure **OTP + PUF**

2023

Riscure & PSA L2 Certificated for Ecosystem Security

Pass Security Functional Requirements: **Initialization, Secure Storage, Firmware Update, Secure State, Crypto**. Support TF-M & Mbed TLS for AIoT & Automotive ecosystem security.





Free Evaluation for **PUF**-based IPs

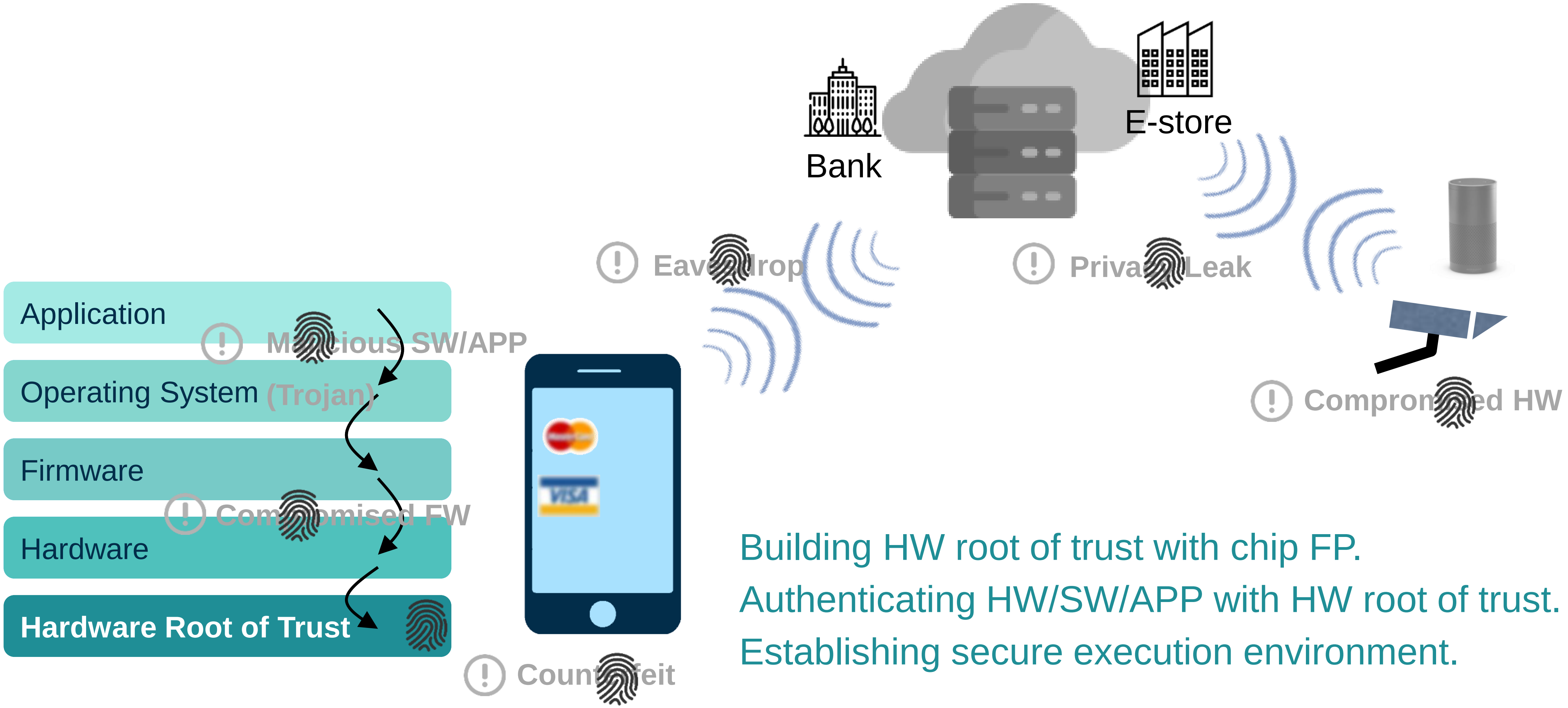
Evaluation Kit Program

ip GO 2.0

In IP GO 2.0, the application no longer requires an NDA and replaces it with an online user agreement, allowing developers easier access to the IP library.

https://www.pufsecurity.com/ip-go

Enjoy Applications with **Secure Device**



Building HW root of trust with chip FP.

Authenticating HW/SW/APP with HW root of trust.

Establishing secure execution environment.

Key Takeaway

- Flexibility & re-configuration of software could be vulnerable and be used for cyber attack if unable to ensure software integrity & genuineness.

- An immutable root of trust is the indispensable foundation for ensuring chip and application security.

- PUF (inborn chip fingerprint) is an important critical function in strengthening the chip root of trust.

- A true PUF-based hardware root of trust realizes genuine trust, secret protection, and a secure execution environment and protects applications throughout the product lifecycle.

Thank You

PUFsecurity