Protecting SmartNICs with Physical Unclonable Functions (PUFs)

Reed Hinkel

VP Strategy & Business Development

INTRINSIC ID™

Authenticate Everything

Setting the Scene

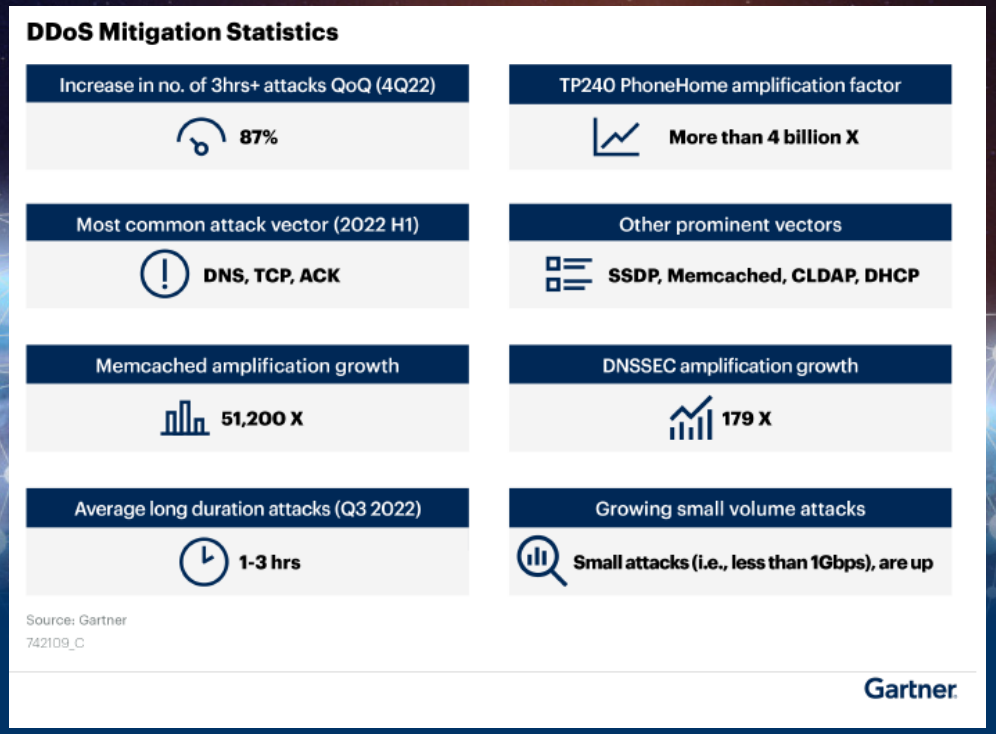
SmartNICs are programmable accelerators for data centers

Allow servers CPUs to offload processing of the following functions:

- Networking
- Storage
- Security

All high value applications that require a higher level of trust

Data Center Hacks are on the Rise



SC MEDIA
A CyberRisk Alliance Resource

Cloud security, Third-party risk

Two data centers used by major tech firms hacked

Tom Spring February 21, 2023

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

MALWARE & THREATS

Atlassian Confluence Servers Hacked via Zero-Day Vulnerability

Bloomberg

Businessweek | Feature

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

BLEEPINGCOMPUTER

Over 20,000 data center management systems exposed to hackers

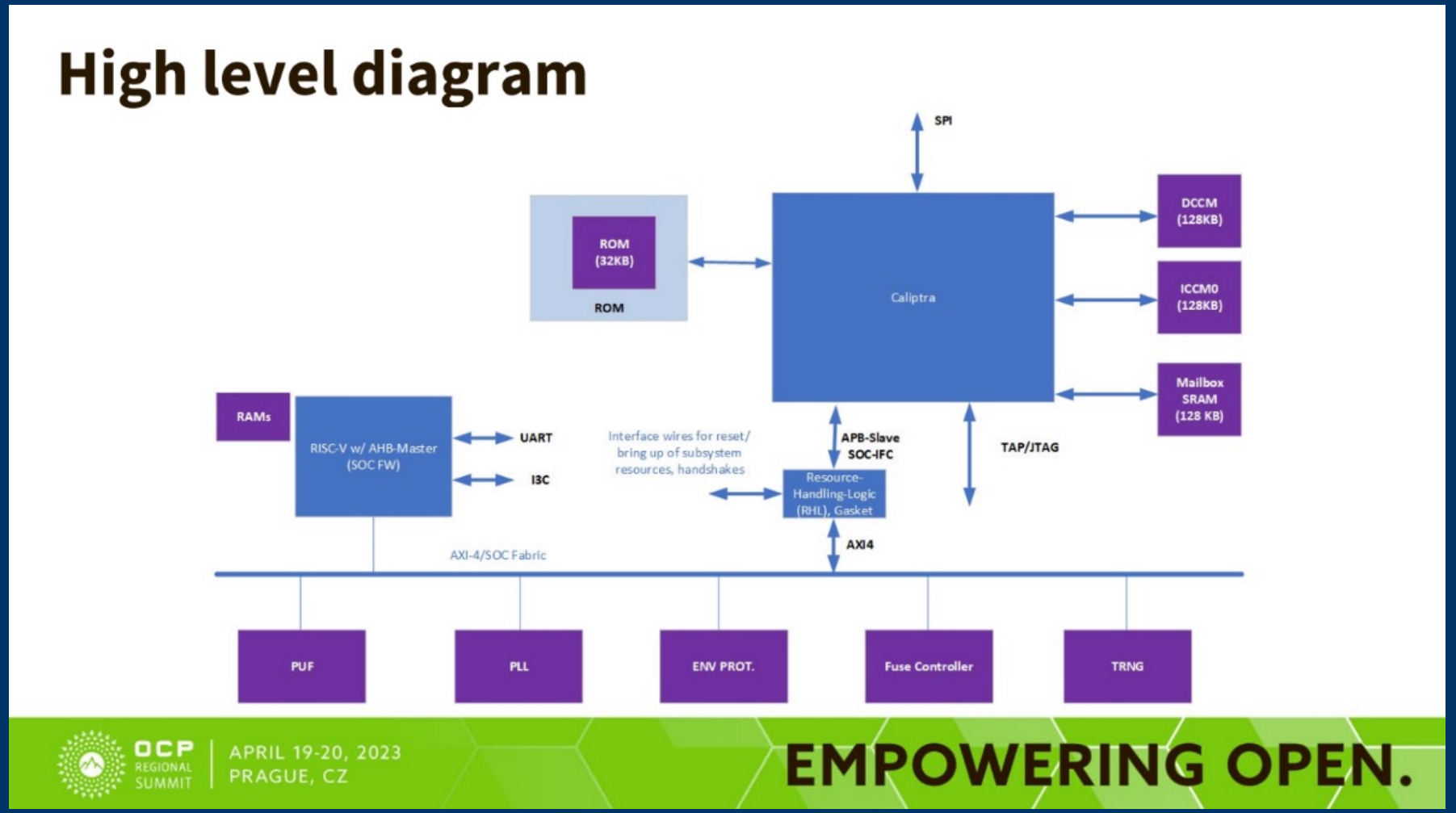
Root of Trust

- Fundamental building block for security of a device or system
- Part of the security one can trust and operates as expected
- Guarantees correct execution of fundamental security primitives

OCP Caliptra

Open-Source Root of Trust solution driven by OCP and CHIPS Alliance

The purple boxes are called out in the Caliptra specification, but are not part of the open-source IP



From: Caliptra – Open-Source RoT Project Update at OCP Regional Summit 2023

UDS – Unique Device Secret

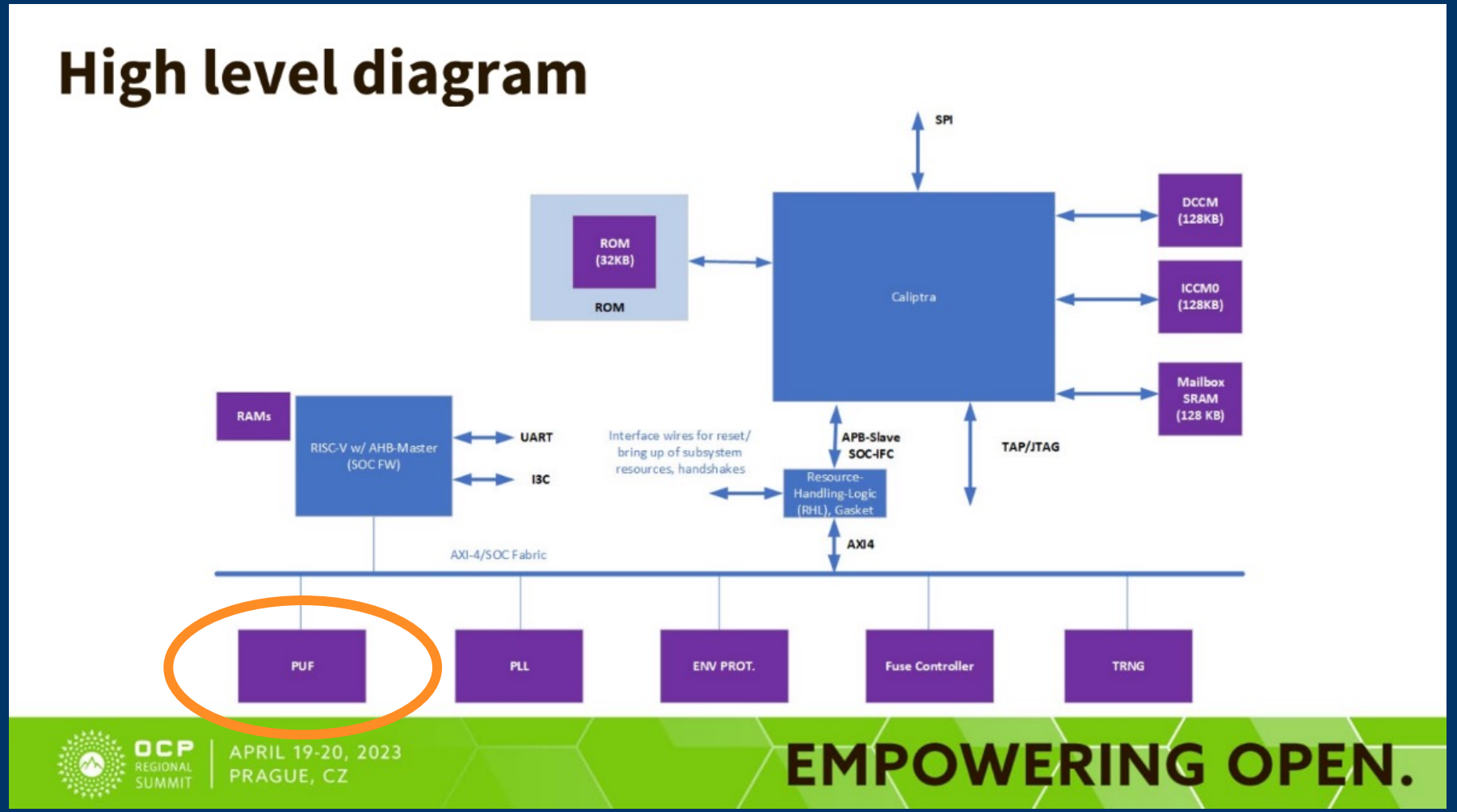
Caliptra's root secret is called UDS

- Within Caliptra framework every device has unique identity called **UDS** or Unique Device Secret
- The **UDS** is:
  - A block of entropy stored in fuses
  - Root secret for the Caliptra root of trust
  - Unique identity for every individual device
- From: Caliptra - A Datacenter System on a Chip (SOC) Root of Trust (RoT), Revision 1.0
  - "The Caliptra **UDS** is stored in fuses, and is encrypted at rest by an obfuscation secret"
  - "This obfuscation secret may be a chip-class secret, or a chip-unique PUF, **with the latter preferred**"

OCP Caliptra

Caliptra architecture recommends using PUF technology

The purple boxes are called out in the Caliptra specification, but are not part of the open-source IP



From: Caliptra – Open-Source RoT Project Update at OCP Regional Summit 2023

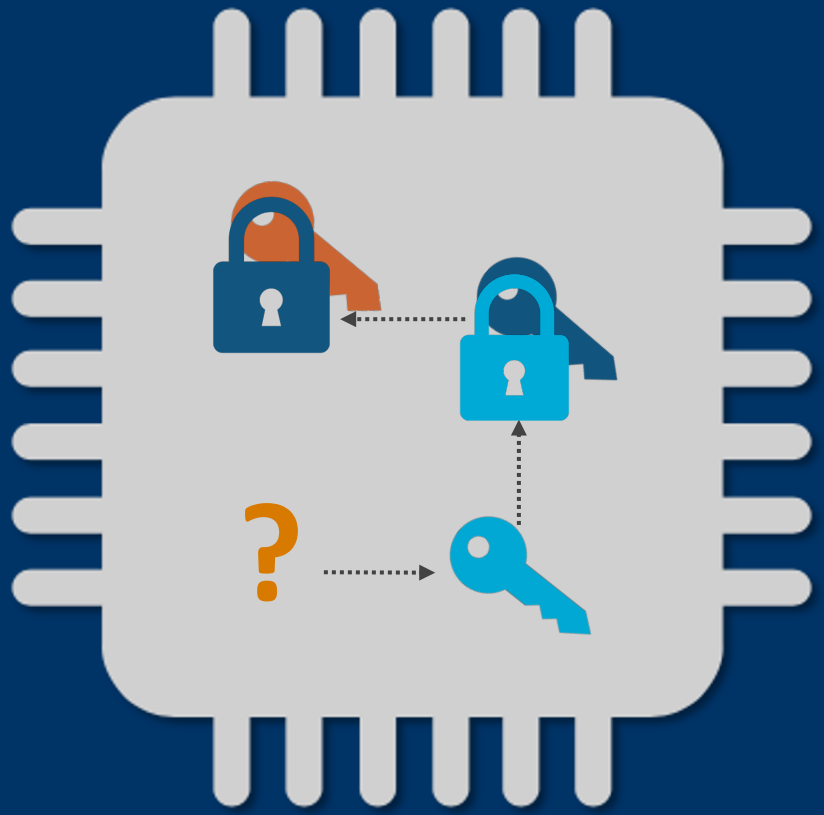
Kerckhoffs's Principle

"A Cryptosystem should be secure even if everything about the system, except the secret key, is public knowledge"

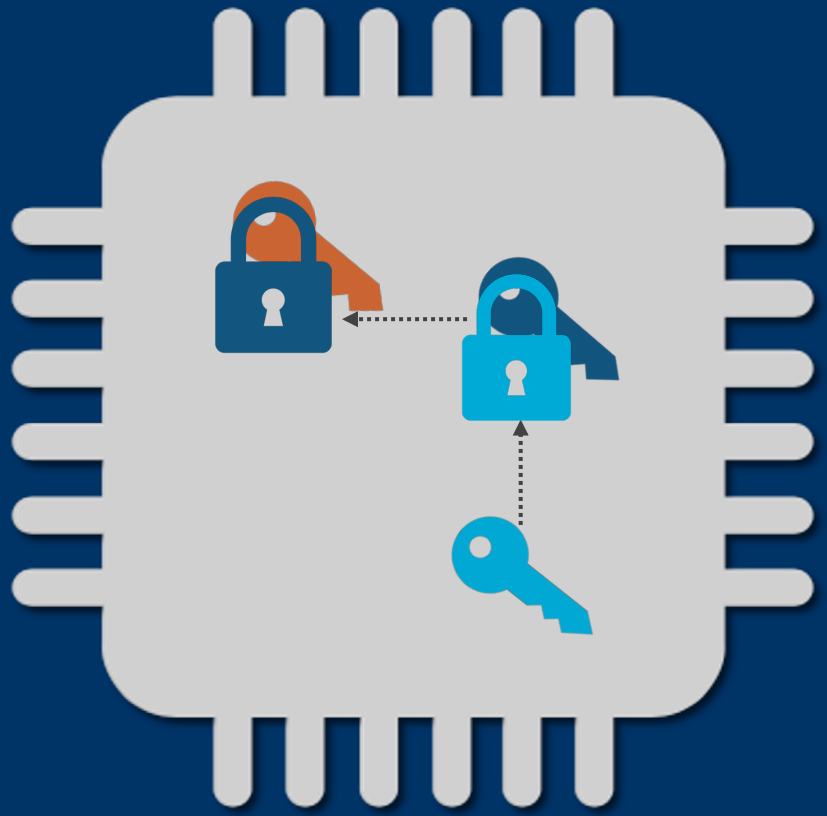
Auguste Kerckhoffs

Security depends on the **secrecy** of the **key**

An Unexpected Security Challenge: Secret Keys



The Solution: Never Store the Root Key



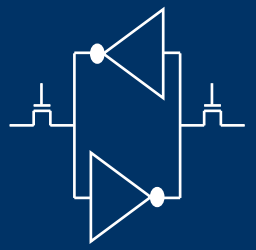
Protecting Strong Root Keys with SRAM PUFs

1

Process Variation

Deep sub-micron variations in the production process give every transistor slightly random electric properties

2



SRAM Start-up Values

When the SRAM is powered on this randomness is expressed in the start-up values (0 or 1) of SRAM cells

3

Silicon Fingerprint

The start-up values create a highly random and repeatable pattern that is unique to each chip

4

SRAM PUF Key

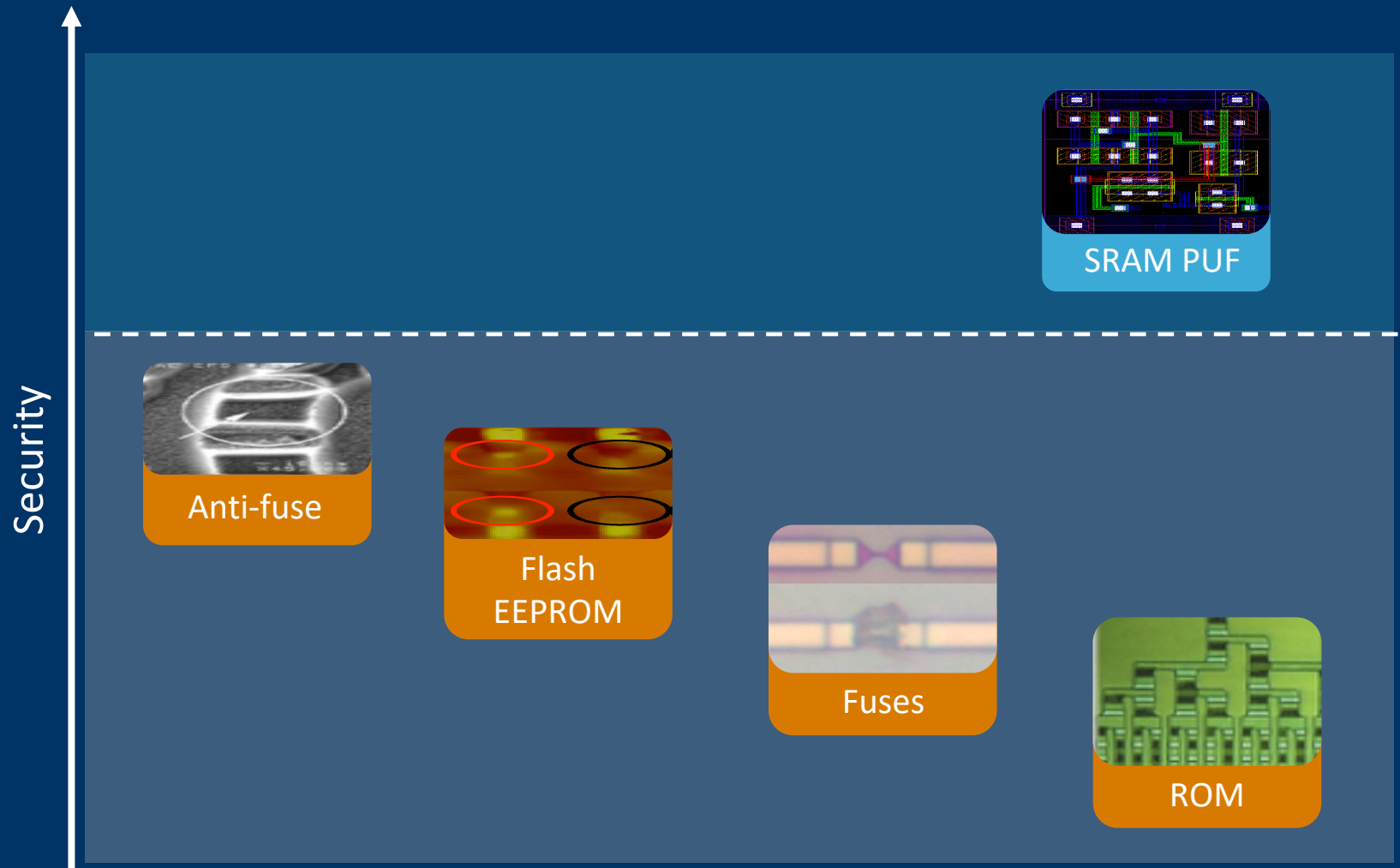
The silicon fingerprint is turned into a secret key that builds the foundation of a security subsystem

SRAM PUF Benefits

- Device-unique, unclonable fingerprint
- Leverages entropy of mfg. process
- No key material programmed

No Keys at Rest

SRAM PUF Advantages in Secure Key Storage



SRAM PUF Technology

- Key generated by device entropy
- No traces of sensitive data
- No secrets stored on chip

Other Solutions

- Key programmed externally
- Permanent physical alteration
- Key visible in structure

Benefits of Using Intrinsic ID PUF Technology

Low Cost

- No secure storage on chip required

Certifications

- IID PUF-enabled products have been certified by EMVCo, CC EAL6+, Platform Security Architecture, ioXt, GlobalPlatform

Flexibility

- Generation of root keys anytime, anywhere
- Any party can store their own keys securely on chip

Highest Reliability

- From -55°C to 150°C
- Lifetime > 25 years

Highest Security

- Root key never stored
- HW source of randomness
- Many attack countermeasures

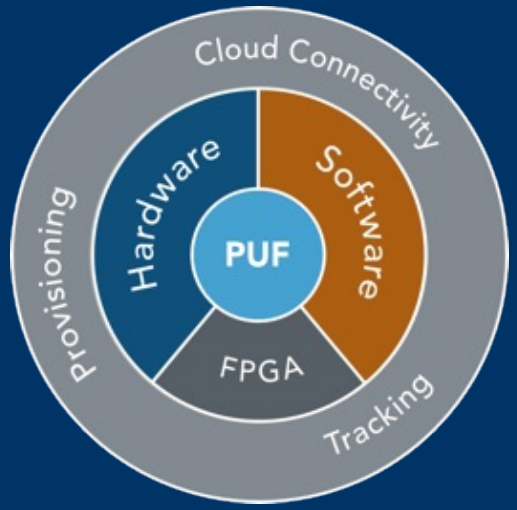
Proven

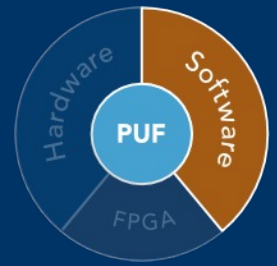
- 500M+ ICs with IID PUF implementations shipped
- G&D, banking, IoT
- From 350nm to 5nm

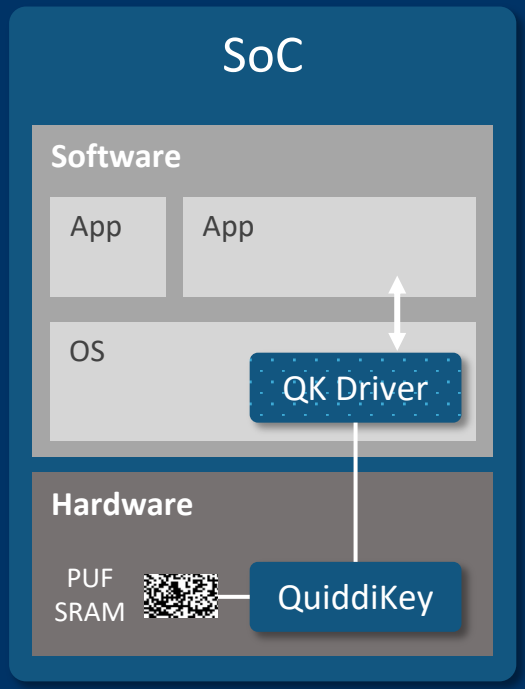
Intrinsic ID Addresses the Security Needs of Top Tech Companies

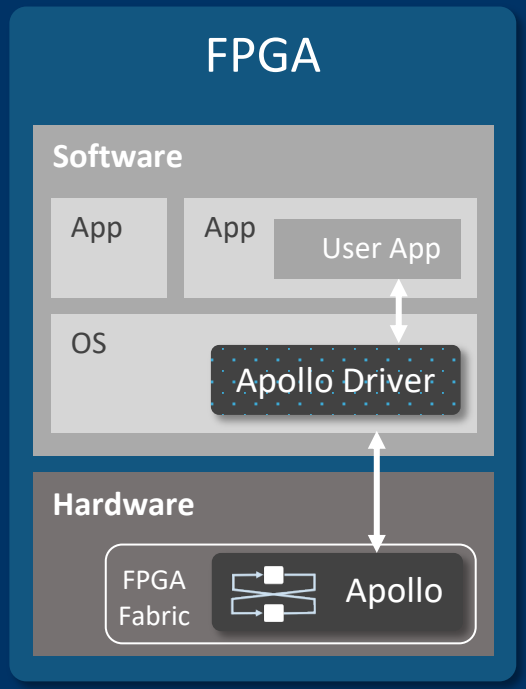
Top Tech Company NEEDS	Without Intrinsic ID	With Intrinsic ID
Higher Security	Multiple vulnerabilities	Highest security in the Industry
	✗ Keys visible in memories	✓ No keys at rest
	✗ Trust in other parties needed	✓ Supports a Zero Trust supply chain
Flexible	✗ Limited choice of foundry/process	✓ Works for all foundries/processes
	✗ Limited choice of programming	✓ Choice where to program the keys
	✗ Many touch points	✓ Zero Touch approach
	✗ De/re-commissioning issues	✓ Device lifecycle flexibility
Economics	✗ Additional silicon costs	✓ Standard silicon
	✗ High implementation cost	✓ No special steps needed
	✗ Liability cost	✓ No liability cost
Reliability	✗ Reliability issues in advanced nodes	✓ High reliability in all nodes

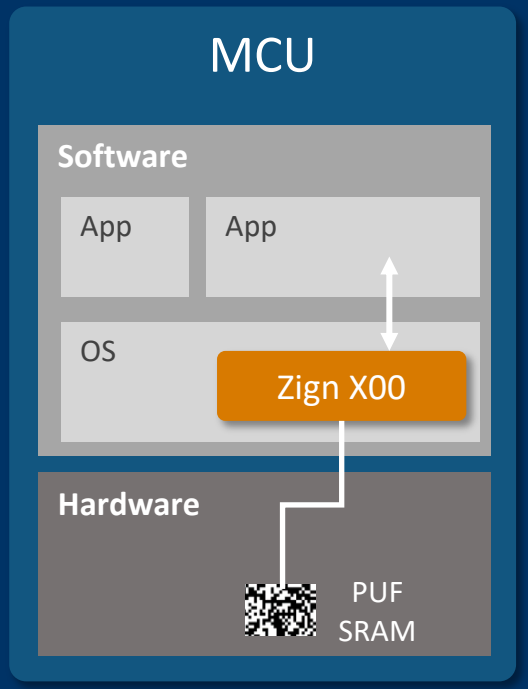
PUF-based Products











Industry Leaders Rely on Intrinsic ID

intel
NXP
FUNGIBLE
SILICON LABS
MICROCHIP
IDT
GOWIN
TDK InvenSense
GREENWAVES TECHNOLOGIES
qorvo

Defense Contractors

500M+
Deployments in the Field

4 of Top 5
MCU Vendors as a Customer

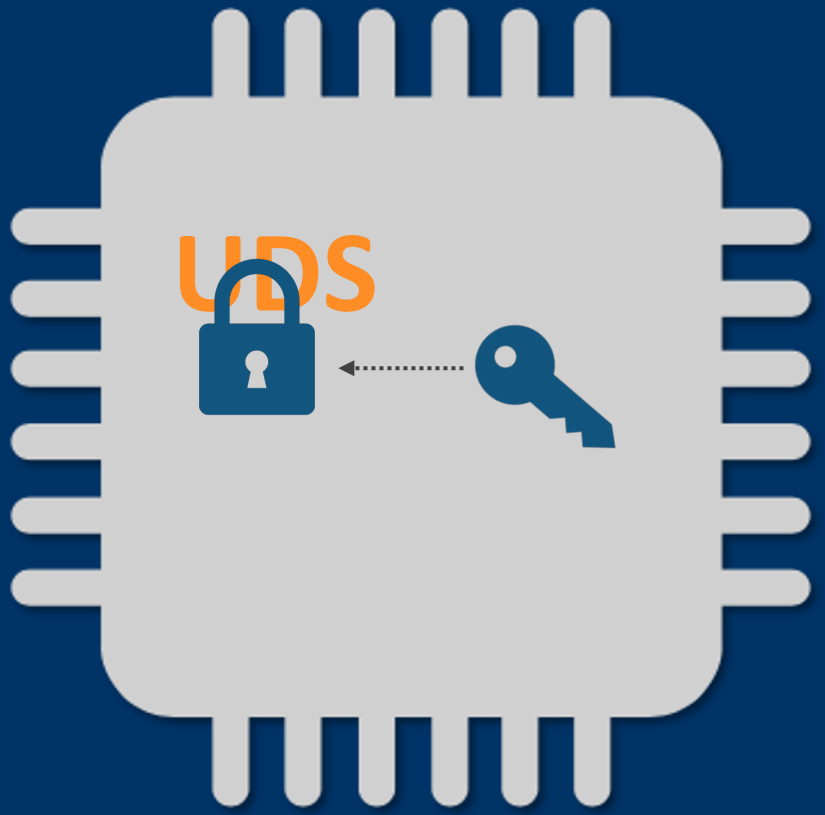
125+
Design Wins

Top 4
FPGA Platforms

10+
Global certifications and Government programs

Use Case: Obfuscating UDS

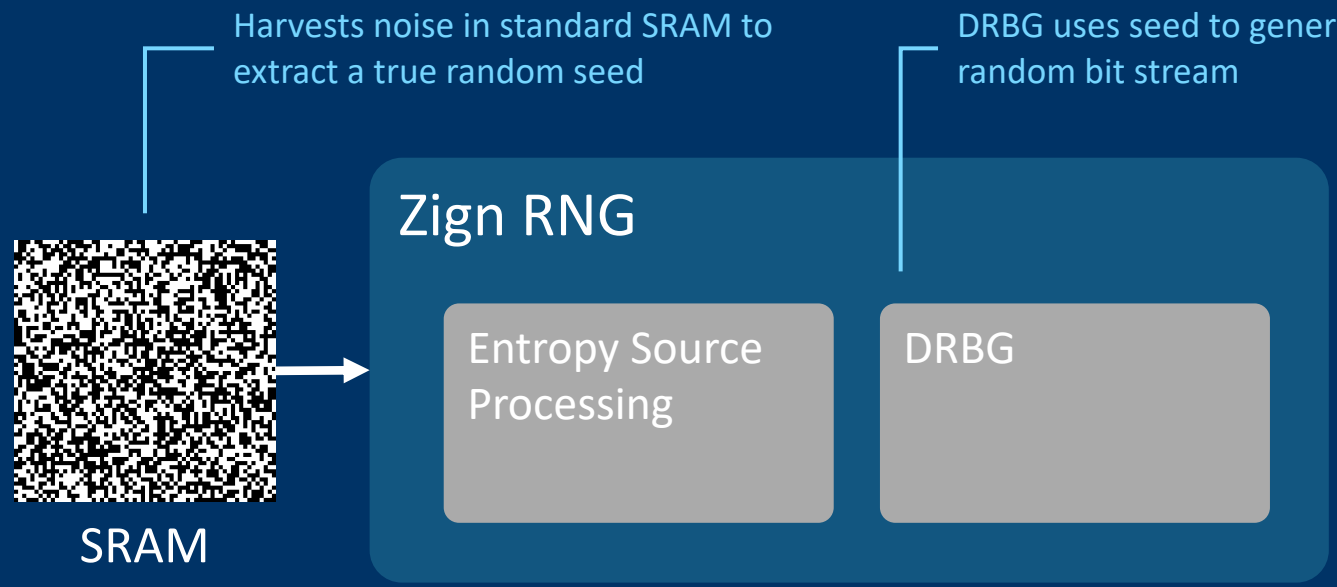
The UDS is the root secret for the Caliptra Root of Trust



- With PUF a Secure Vault is created by encrypting **UDS**
- No key stored = no way to decrypt **UDS**
- Encrypted **UDS** can be stored anywhere and remain secure

Use Case: Random Number Generation

Intrinsic ID SRAM PUF technology comes with NIST-compliant RNG



Features

- ✓ Uses standard SRAM start-up values as a true random source
- ✓ NIST CAVP certified for DRBG and AES
- ✓ Compliant with NIST SP 800-90
- ✓ Compliant with BSI AIS 20/31
- ✓ Supports FIPS 140-3 certification

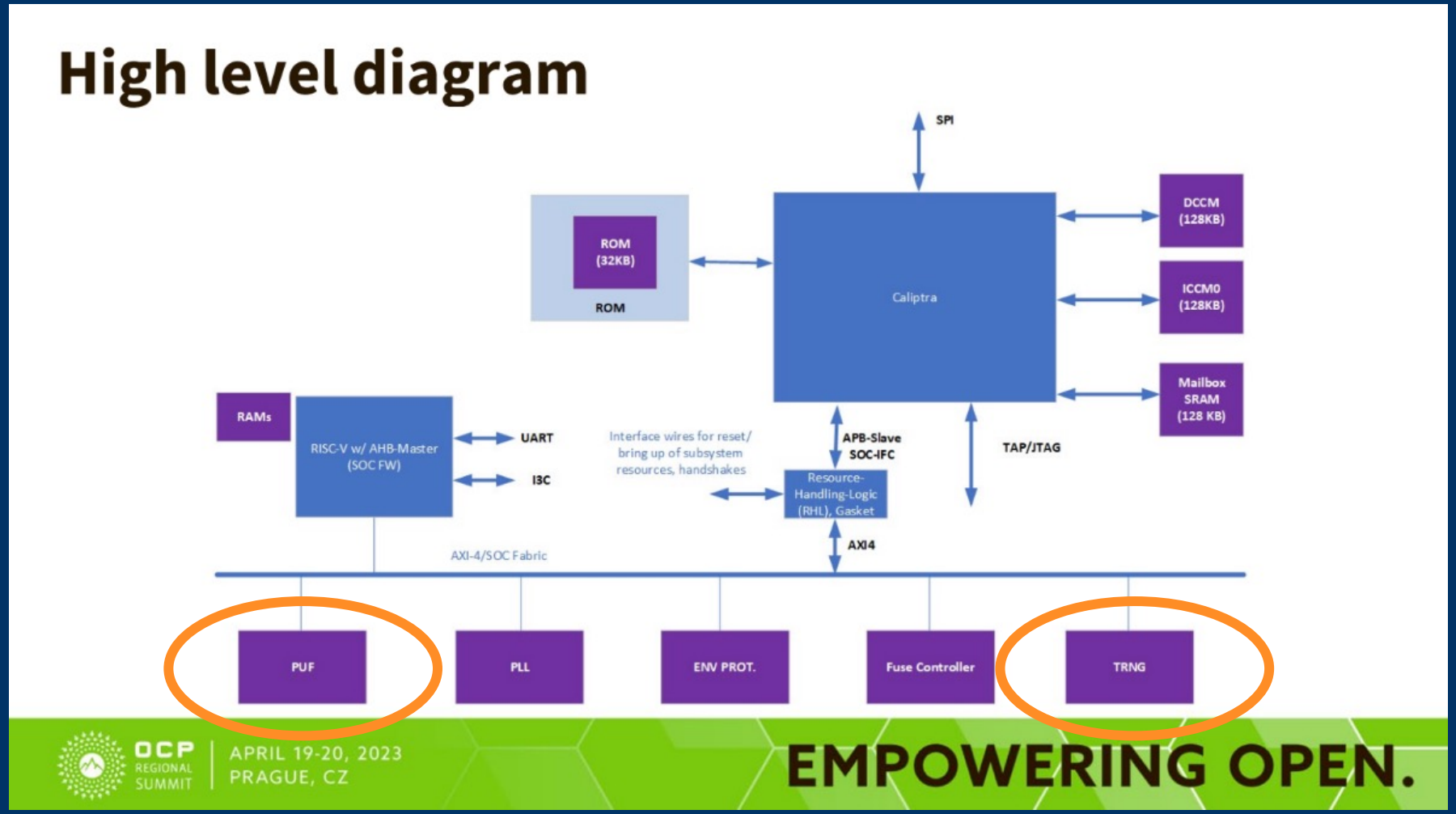
Benefits

- ✓ No need for additional or modified silicon
- ✓ Can be added at any point in the supply chain
- ✓ Fits in resource-constrained embedded devices
- ✓ Portable across different technologies

Intrinsic ID PUFs for OCP Caliptra

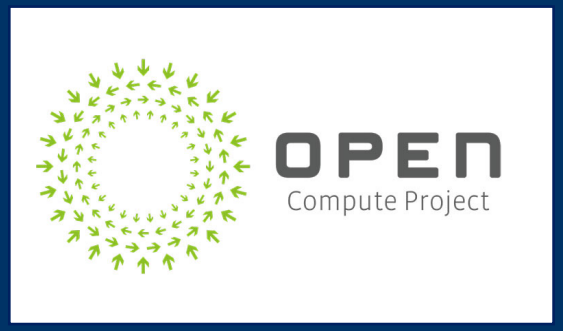
Intrinsic ID PUFs provide both the PUF and TRNG for OCP Caliptra

The purple boxes are called out in the Caliptra specification, but are not part of the open-source IP



From: Caliptra – Open-Source RoT Project Update at OCP Regional Summit 2023

Conclusions



- SmartNICs allow offloading of security functionality
- The new standard for datacenter secure authentication is Caliptra
- Critical components of Caliptra: PUF & TRNG
- Intrinsic ID PUF solutions provide both these functions and are integrated directly with OCP Caliptra

INTRINSIC ID™

Thank You!

www.Intrinsic-ID.com