

Accelerating Caliptra Adoption

with a Pre-integrated Subsystem + PUFrt ■

PUFsecurity
AN ememory COMPANY

Caliptra: An Open-Source Silicon RoT

- **Caliptra 2.x Subsystem: a core element for securing devices**
 - A trusted chain anchored through hardware
 - Comprehensive protection, detection, and recovery
- **Open-Source: Transparency and Consistency**
 - Transparent design brings high security assurance
 - Consistent security foundation for every silicon
- **OCP L.O.C.K. Framework**
 - Driving open-source key management for trusted storage



OPEN
Compute Project



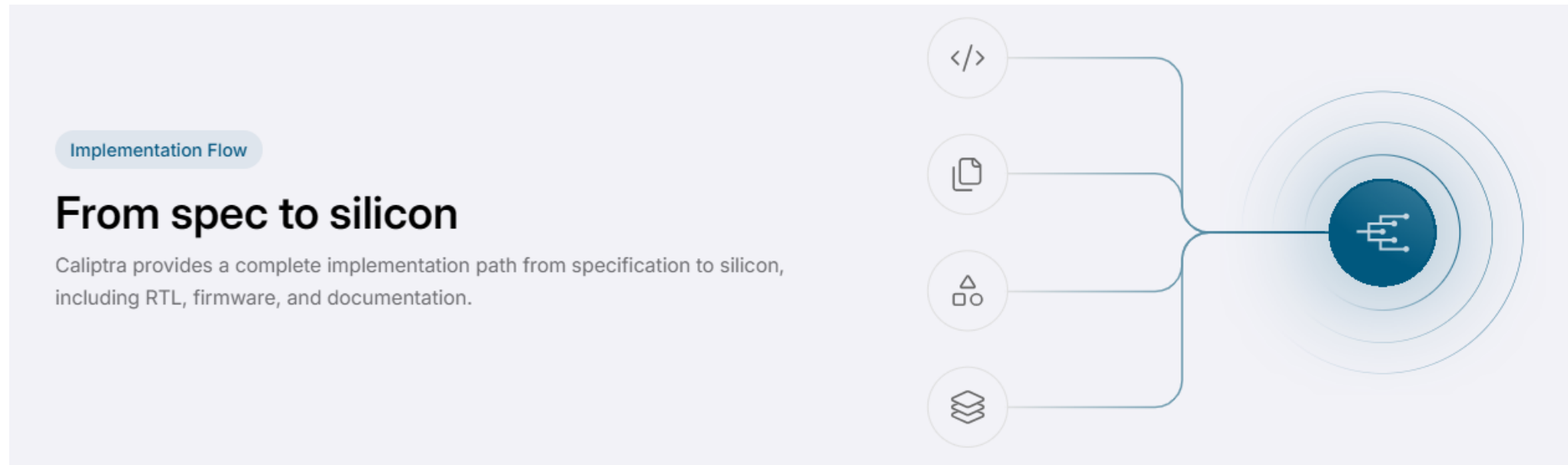
From Open Specification to **Real Silicon** ■

Open-source offering

- Caliptra RTL and software
- Standard verification flow
- Reusable OCP S.A.F.E. certification

More are needed in real silicon

- **Entropy** and **immutable storage**
- Vendor-specific verification flow
- Certification & **Caliptra Trademark**



<https://chipsalliance.github.io/caliptra-web/#>

Considerations for Physical Implementation

Unique Device Secret

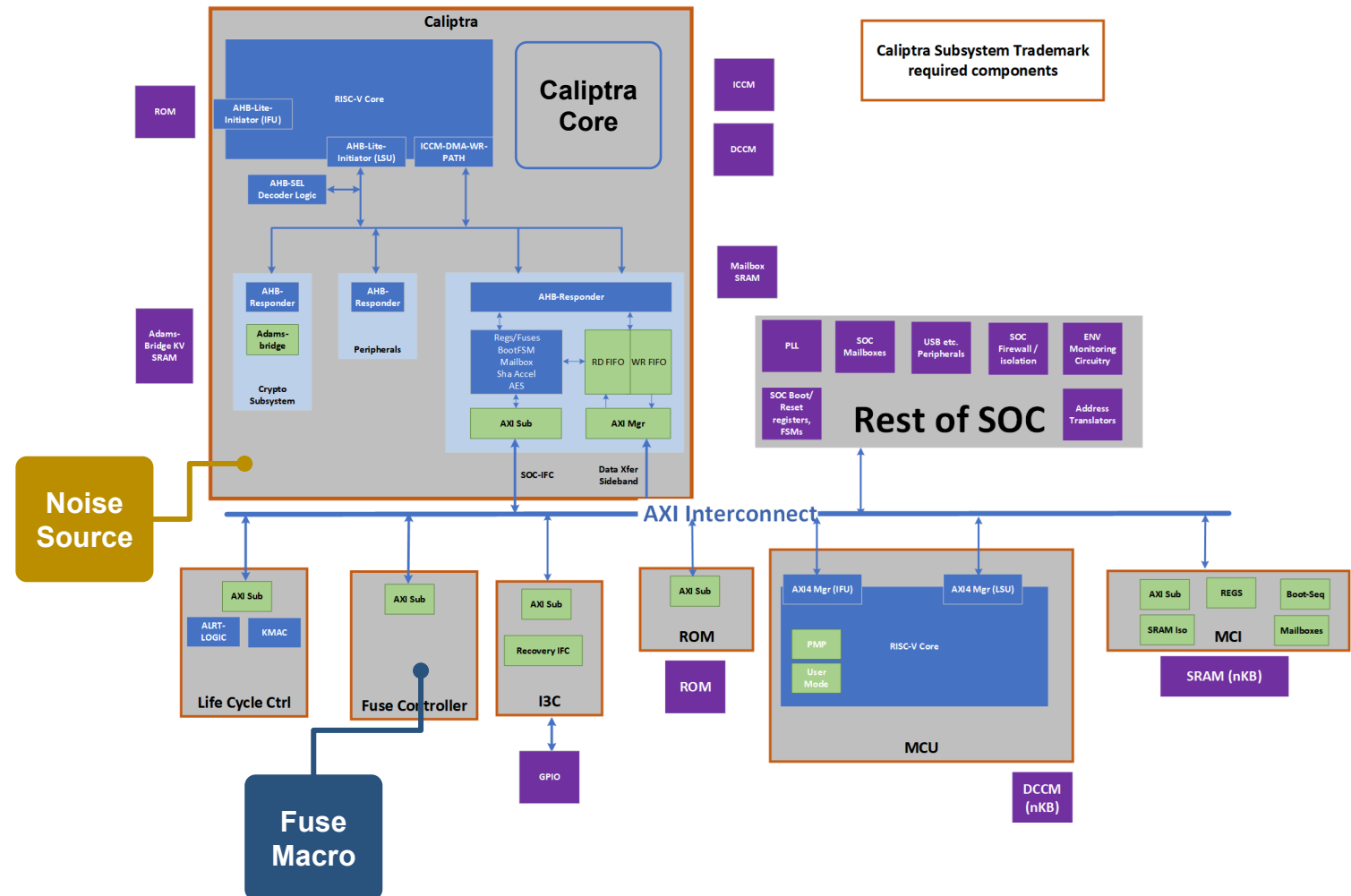
- Device secret
- Provisioned/generated
- Source of obf. Key

Fuse Macro

- Security Storage
- Interface with Fuse CTRL
- Yield & Reliability

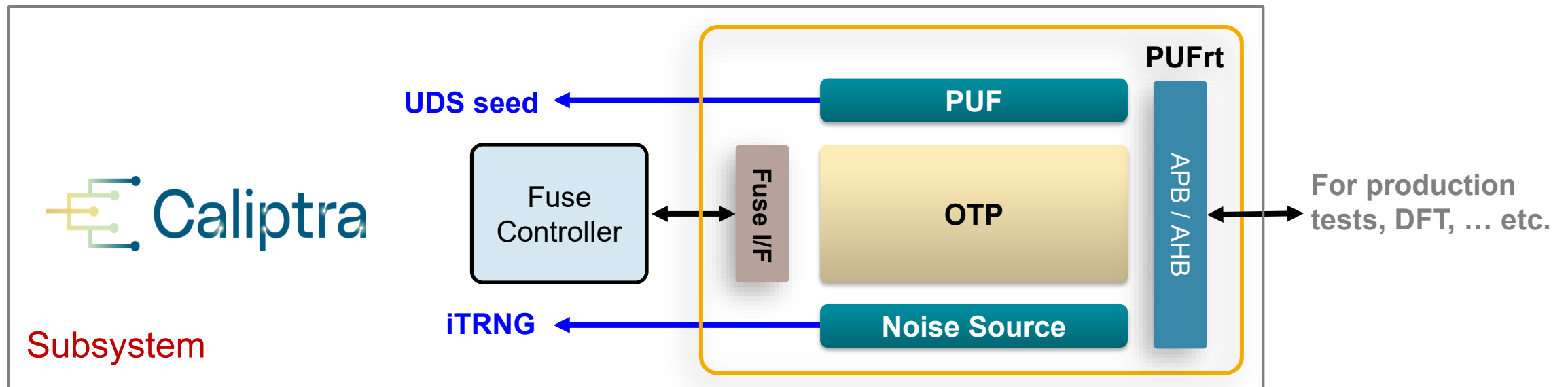
Noise Source

- For Caliptra iTRNG
- For UDS generation
- FIPS certification (ESV)



PUFrt: All-in-one Physical Anchor for Caliptra

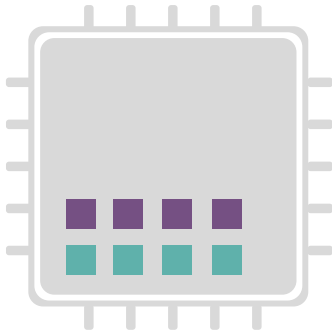
- **Pre-hardened PUF** → assured randomness for UDS seed
- **Qualified anti-fuse OTP** in most advanced processes → reliable storage for key and LCS
- **ESV certified Noise source** → met SP800-90B requirement for Caliptra iTRNG
- **Integrated design** with access control & anti-tampering → physical security
- **Advanced Technology** support down to 3nm silicon (2nm and below are coming)



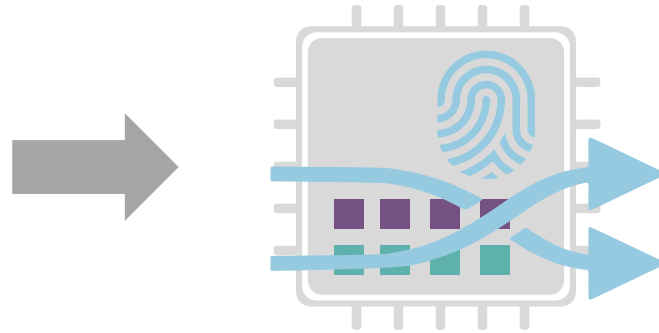
Enhanced Secure Storage Enabled by PUF

- High security and unique design for Root Key or any sensitive data storage

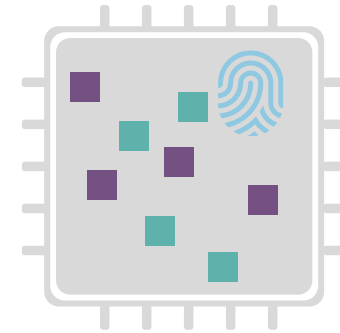
Original Data in OTP



Scrambled by PUF



Chip-Unique Secure Storage



Asset category	Asset	Security property	Attack profile	Attack path	Mitigation
Fuse/OTP high value secrets	UDS Seed	Confidentiality and integrity	Expert	Malicious manufacturing spoofing of UDS Seeds	UDS obfuscation with class RTL key
Fuse/OTP high value secrets	UDS Seed	Confidentiality and integrity	Expert	Invasive attack (fuse analysis)	Shield fuse IP

https://chipsalliance.github.io/caliptra-web/docs/2.1/caliptra_overview.html#caliptra-assets-and-threats

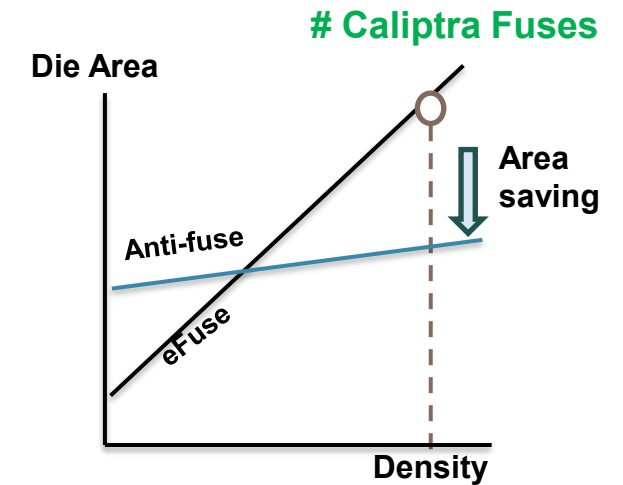
OTP is Foundational for Caliptra and SoC ■

Anti-fuse OTP is a better choice for Caliptra

- Better area efficiency in advanced node & large density
- More reliable especially supporting many read cycles
- Anti-fuse is field programmable

Emerging use cases for the entire SoC

- Support boot code patch (e.g., MCU-ROM patch)
- Support DFT and SRAM repair
- Trimming for PVT sensors



Emerging Use Cases



Boot Code

Enhanced flexibility for developers



DFT / SRAM Repair

More SRAM used in HPC / adv. node



Trimming for PVT sensors

Distributed sensors for performance tracking

One-Stop Shop Services

Pre-integrated IP Package

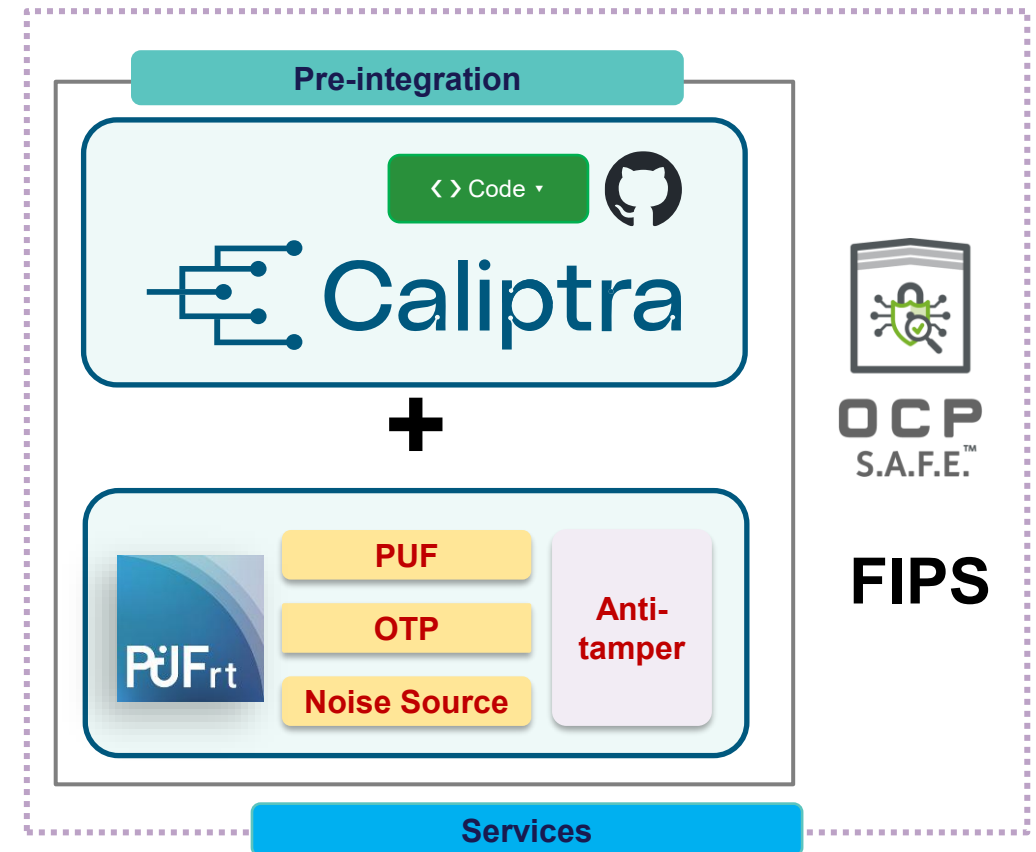
- Design Reference Kit (Physical & Digital IPs)
- Integration Guide
- Test Methodology Manual

Pre-Verified/Certified Design

- FPGA Verification Platform
- OCP S.A.F.E. Evaluated IP
- NIST ESV Certified Entropy Source

Technical Support Services

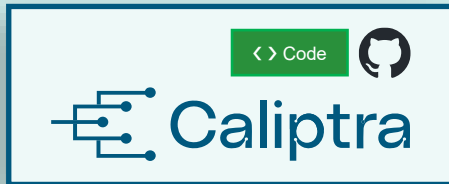
- Pre- and Post-Silicon Support
- Certification support (e.g., OCP S.A.F.E.)



Pre-Integrated Caliptra-SS for MCU Bring Up .

Customer's Design

Develop your own MCU software on FPGA platform.



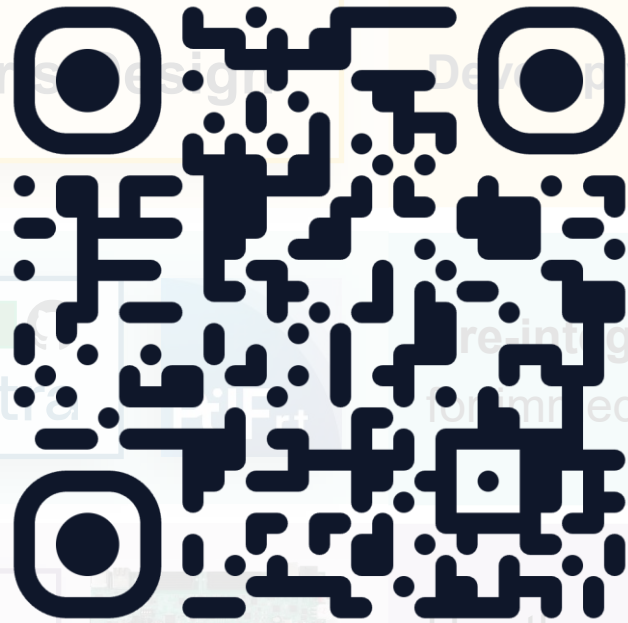
Pre-integrated and fully validated Caliptra-SS + PUFrt
for immediate development and seamless migration.

Versal™ AI Core
Series **VCK190** Ev-Kit
AMD



Use the official Caliptra reference FPGA platform
—no FPGA or platform migration required.

Pre-Integrated Caliptra-SS for MCU Bring Up .



Available on
GitHub!

Bring Up
Your Own Caliptra

Takeaways

From spec to silicon: an Implementation gap for Caliptra

Physical primitives are required to bring open-source Caliptra into silicon

PUFrt: all-in-one physical anchor for Caliptra

Provides PUF, OTP, noise source and tamper protection to enable Caliptra 2.1 Subsystem

One-stop service: accelerating Caliptra deployment

We deliver comprehensive subsystem pre-integration and security validation support



Thank You .



PiFsecurity