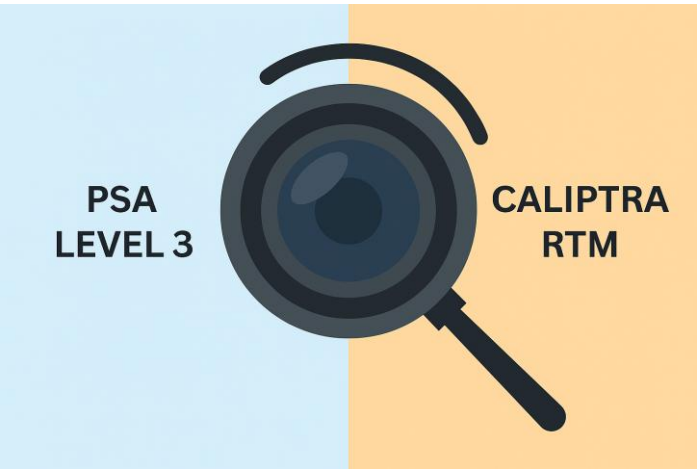


CONVERGING PATHS TO SILICON TRUST

ABSTRACT

This paper compares PSA Certified Level 3 and Caliptra RTM—two frameworks for silicon Root of Trust that address similar threats across software, hardware, and physical domains. Despite differing terminology, both support secure boot, attestation, and scalable trust. By mapping threat models, aligning APIs, and referencing NISTIR 8259A compliance, the paper offers actionable guidance for bridging fragmented trust architectures across embedded and cloud platforms

Author: Suresh Marisetty
Technical Leader Advancing Platform Technologies

Silicon Security in the Cloud Era: The Role of PSA Level 3, Caliptra, and OCP S.A.F.E. Frameworks

Author: Suresh Marisetty
Technology Leader advancing Platform Hardware Technologies across Cloud-AI & Embedded Systems Focused on Resilience (RAS), Security, Manageability, Firmware and System Software

Executive Summary

This paper addresses a growing challenge in secure silicon design: the fragmentation of trust models across domains. Whether you're working in embedded systems, datacenter firmware, or cloud infrastructure, chances are you're operating within a silo—optimizing for your own standards, APIs, and threat models.

Frameworks like Arm's Platform Security Architecture (PSA) Certified Level 3 and Caliptra Root of Trust for Measurement (RTM) of Open Compute Project (OCP) are converging in purpose. Despite their different origins of addressing the needs of IoT and Cloud domains respectively, they share the foundational goals: secure boot, scalable attestation, threat model and developer enablement.

This paper offers a cross-technology lens to help engineers, architects, and ecosystem leaders connect the dots. It highlights architectural commonalities, developer-friendly APIs, and integration paths via Security Protocol and Data Model (SPDM) and NISTIR 8259A. The goal is not to prescribe a single roadmap—*but to foster shared understanding and interoperability across silos.*

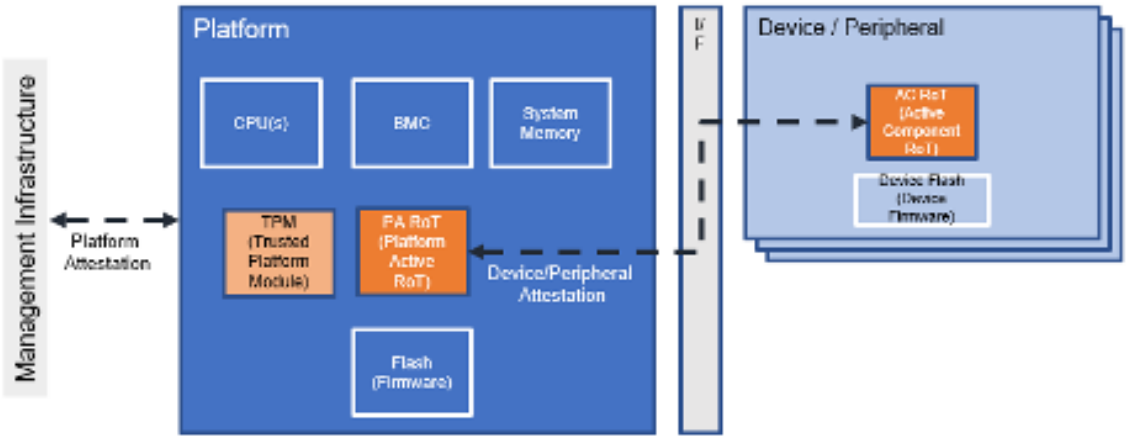
The intended audience of this paper is the security professionals who are already familiar with Root of Trust (RoT) concepts, industry standards that rely on security implementations (TCG, OCP, Global Platform, IETF, DMTF, NIST, UEFI, PCIe, etc.) and threat modelling.

1. Introduction

Fragmented trust models across embedded and cloud platforms have historically slowed innovation. Having worked extensively across IoT, hyperscale infrastructure, and silicon platforms, I've seen the need for unified, scalable trust mechanisms.

At the heart of this challenge lies the RoT, the foundational component that anchors all secure operations. Whether it's PSA Certified Level 3 or Caliptra RTM, both frameworks are designed to define, implement, and validate the RoT in silicon.

PSA and Caliptra represent two ends of the trust spectrum—one rooted in assurance and certification, the other in openness and transparency. Their convergence offers a path toward programmable, renewable, and interoperable trust.



2. Architecture Overview (with Threat Model Emphasis)
Both PSA Level 3 and Caliptra RTM are designed to establish and secure the Root of Trust (RoT) in silicon platforms. This includes immutable boot logic, identity derivation, attestation, and lifecycle control. Critically, both frameworks conform to well-defined threat models that span software, hardware, and physical attack vectors—making them suitable for high-assurance environments.

Both frameworks implement RoT components such as secure boot, identity derivation, attestation, and lifecycle control. They also define threat models that span software, hardware, and physical vectors.

PSA Level 3

- **RoT Components**: Secure boot, secure storage, cryptographic services, attestation
- **Threat Coverage**:
  - Software: Rogue code injection, firmware abuse, update manipulation, storage tampering
  - Hardware: Debug interface exploitation, weak crypto, impersonation
  - Physical: SPA/DPA, EM leakage, timing, glitching, voltage/clock faults
- **Evaluation**: SESIP or CSPN white-box lab testing

Caliptra RTM

- **RoT Components**: Measured boot (FMC and runtime), DICE-based identity, real-time attestation
- **Threat Coverage**:
  - Software: Mailbox fuzzing, firmware tampering
  - Hardware: DPA, DFA, glitching, ROM reverse engineering
- **Design Philosophy**: Open-source RTL and firmware, extensible threat modeling via CHIPS Alliance and OCP

OCP S.A.F.E
OCP S.A.F.E. is a **security assurance framework** developed by the Open Compute Project (OCP). The S.A.F.E. program specifically focuses on:

- **Security evaluations of devices** like CPUs, GPUs, FPGAs, SSDs, and network controllers
- **Firmware and microcode integrity**, update mechanisms, and cryptographic protections
- **Supply chain transparency** and code quality assurance

It enables vendors to demonstrate that their products meet rigorous security standards through independent reviews conducted by approved **Security Review Providers (SRPs)**

OCP S.A.F.E. and PSA Certified are both security assurance frameworks, but they differ in scope, methodology, and target ecosystems. OCP S.A.F.E. focuses on hardware and firmware security in hyperscale data centers, while PSA Certified targets IoT devices with structured certification levels.

Comparison: OCP S.A.F.E. vs. PSA Certified

Feature / Focus Area	OCP S.A.F.E.	PSA Certified
Full Name	Security Appraisal Framework and Enablement	Platform Security Architecture Certified
Governance	Open Compute Project (OCP)	GlobalPlatform (formerly Arm-led)
Target Ecosystem	Hyperscale data centers, cloud infrastructure, server components	IoT devices, embedded systems, edge platforms
Scope of Review	Firmware, microcode, boot integrity, update flows, physical resilience	Threat modeling, RoT architecture, firmware APIs, secure storage, attestation
Review Methodology	Manual code inspection by approved Security Review Providers (SRPs)	Structured multi-level certification by accredited labs
Certification Levels	No pass/fail — assurance via published review reports	Level 1 (questionnaire), Level 2 (source code review), Level 3 (penetration test)
Threat Model Requirement	Mandatory — informs scope of review and testing	Mandatory — forms basis for security requirements
Firmware Update Evaluation	Yes — secure update flows and rollback protection	Yes — PSA Firmware Update API and lifecycle controls
Physical Security Testing	Yes — fault injection, side-channel analysis (Scope 3)	Yes — at Level 3, includes physical attack resistance
Open Source Alignment	Encourages open firmware and shared review artifacts	Provides open-source APIs and test suites via TrustedFirmware.org

Feature / Focus Area	OCP S.A.F.E.	PSA Certified
Industry Adoption	Used by hyperscalers like Meta, Microsoft, Google for SSDs, NICs, accelerators	Adopted by Arm ecosystem, chip vendors, and IoT platform providers
Output Format	Short Form Report (SFR), GitHub publication, OCP Marketplace listing	Certificate with PSA-RoT level, public listing on PSA Certified site

3. Unified Threat Model Mapping

Despite differing terminology, PSA and Caliptra address similar threat categories. This mapping clarifies their alignment:

Unified Category	PSA Level 3 Terminology	Caliptra RTM Terminology
Software Integrity	Rogue code injection, firmware abuse, update manipulation	Firmware tampering, mailbox fuzzing
Storage Protection	Storage tampering	Runtime integrity (implicit)
Interface Exploits	Debug interface exploitation	Mailbox fuzzing
Cryptographic Weakness	Weak cryptography, impersonation	DPA, DFA
Side-Channel Attacks	SPA/DPA, EM leakage, timing	DPA
Fault Injection	Glitching, voltage/clock faults	Glitching, DFA
Reverse Engineering	Not explicitly listed	ROM reverse engineering

Shared Objective: Protect high-value assets and enable scalable trust—even in environments with physical access or sophisticated adversaries with the following attributes and goals:

- **PSA** emphasizes certification and structured threat profiles (SESIP/CSPN).
- **Caliptra** uses open-source transparency and community-defined threat modeling.
- Mapping these terms helps unify documentation, developer guidance, and ecosystem outreach.

4. Comparative Analysis

Capability	PSA Level 3	Caliptra RTM (OCP)	Compatibility / Notes
Secure Boot	Mandatory	Mandatory	✅ Both enforce secure boot
Measured Boot	Optional (via TF-M extensions)	Core Feature	✅ Caliptra leads here; PSA supports via DICE
Attestation	PSA IAT Token	DICE Certificate Chain	✅ Different formats, similar goals

Capability	PSA Level 3	Caliptra RTM (OCP)	Compatibility / Notes
Lifecycle States	Provisioned, Secure, Decommissioned	Renewable Identity	✅ Conceptually aligned
Physical Attack Resistance	Required (SESIP Level 3 criteria)	Vendor-defined	✅ With enhancements
Certification Path	SESIP/CSPN	Not yet formalized	🟡 Caliptra may evolve toward formal paths
Firmware Openness	✅ TF-M open source	✅ Caliptra firmware open	✅ Both support open firmware stacks
Hardware / RTL Openness	❌ Vendor-specific	✅ Fully open RTL	🟡 PSA could benefit from RTL transparency
NISTIR 8259A Alignment	Strong alignment—supports multiple core capabilities	Partial alignment—identity and attestation supported	🟡 Caliptra could be profiled in future NISTIR
Side-Channel & FI Attack Types	SPA/DPA, EM leakage, timing, glitching, voltage/clock faults	DPA, DFA, glitching, mailbox fuzzing, ROM reverse engineering	🟡 PSA has formal lab evaluation; Caliptra evolving

5. PSA Functional APIs

PSA's Functional APIs abstract secure operations into standardized interfaces, enabling developers to build secure applications without deep hardware knowledge. These are implemented in Trusted Firmware-M (TF-M) and widely adopted across PSA-certified platforms.

- Crypto API
- Secure Storage API
- Attestation API
- Firmware Update & Status Code API

6. Bridging PSA APIs and Caliptra RTL

Caliptra's open-source RTL and firmware offer transparency and extensibility. By layering PSA-compatible APIs on top of Caliptra's firmware, vendors can:

- Enable secure provisioning workflows
- Generate PSA IAT tokens for cloud attestation
- Integrate with PSA-certified software stacks
- Align with NISTIR 8259A cybersecurity capabilities

7. PSA + SPDM Integration

SPDM (Security Protocol and Data Model), standardized by DMTF, enables secure device authentication and measurement exchange. PSA and Caliptra can evolve toward SPDM integration to allow unified attestation across PCIe, MCTP, and cloud platforms through:

- PSA IAT Token Wrapping
- SPDM-AggSig Support
- CoRIM Integration

- Lifecycle Mapping

8. Standards Alignment: NISTIR 8259A

NISTIR 8259A defines a cybersecurity capability baseline for IoT devices, including identity, secure update, access control, and data protection. Originally developed as technical guidance, it has gained traction in federal policy.

8.1 Federal Adoption & Implications

The U.S. Senate Homeland Security and Governmental Affairs Committee has supported requiring NISTIR 8259A compliance for devices used in federal networks. This aligns with broader efforts under Executive Orders to strengthen cybersecurity across critical infrastructure. Implications to vendors include:

- Devices must demonstrate NISTIR 8259A capabilities to qualify for federal procurement.
- PSA Level 3 aligns strongly with these requirements.
- Caliptra RTM supports identity and attestation, with potential to expand into update and access control mechanisms.

9. Currently Listed PSA Level 3 Devices w/DICE

Vendor	Device / Platform	DICE Integration	Notes
Silicon Labs	Secure Vault EFR32MG21 SoC	DICE-based identity and attestation	First PSA Level 3 certified SoC; Secure Vault architecture
STMicroelectronics	STM32U5 Series (with TF-M)	DICE via TF-M and immutable RoT	PSA Level 3 capable with TrustZone-M and TF-M stack
Infineon	PSoC™ 64 Secure MCU	DICE-based provisioning and lifecycle	PSA Level 3 with SESIP profile; supports renewable identity
NXP	i.MX RT1170 with EdgeLock® Enclave	DICE-enabled attestation	PSA Level 3 ready; integrates TF-M and DICE

10. Caliptra Adoption Landscape

Vendor / Organization	Role in Caliptra Ecosystem	Notes
Microsoft	First-party adopter	Uses Caliptra in Azure datacenter silicon
Google	First-party adopter	Integrating Caliptra into custom cloud silicon
AMD	Committed adopter	Incorporating Caliptra into server-class CPUs
Marvell	Ecosystem contributor	Participating in Caliptra community for datacenter SoCs
ASPEED, Axiado, AMI	Contributors and implementers	Supporting Caliptra through firmware and verification tools

11. Evolution and Quantum Outlook

Both PSA and Caliptra are actively evolving. This paper does not prescribe a definitive roadmap but offers a cross-domain lens to highlight integration opportunities. As open standards mature and ecosystems converge, the potential for unified trust architecture becomes increasingly actionable.

To future-proof platform security for Post-Quantum Cryptography (PQC), both PSA Level 3 and Caliptra RTM must evolve & scale to support PQC primitives. RSA, ECC and ECDSA that are extensively used by RoT will be replaced with new NIST defined FIP203-205 alternatives.

Post-Quantum Cryptography Resilience & Framework Readiness

Category	Current Algorithm	PQC-Resilient Alternative	PSA Level 3 Readiness	Caliptra RTM Readiness
🔑 **Key Exchange**	RSA, ECDH	**ML-KEM (Kyber)**	Not yet integrated; depends on vendor crypto libraries	Architecturally extensible; PQC-ready mailbox and manifest paths
✍️ **Signatures**	RSA, ECDSA, EdDSA	**ML-DSA (Dilithium), SPHINCS+**	PSA Crypto API can abstract PQC; TF-M updates required	ML-DSA supported in manifest signing; SPHINCS+ under evaluation
🔐 **Encryption**	AES-128	**AES-256**	PSA Crypto supports AES-256; TF-M compliant	AES-256 used in secure boot and mailbox encryption
🧮 **Hashing**	SHA-256	**SHA-512, SHA3, SHAKE256**	SHA-512 supported in TF-M; SHA3 adoption in progress	SHA-512 used in DICE and attestation flows
📜 **Attestation**	ECC-based IDevID, IAK	**PQC-based IDevID (e.g., LMS, ML-DSA)**	PSA IAT tokens may wrap PQC; SPDM updates needed	DPE can emit PQC-based tokens; hybrid attestation feasible

15. Sidebar: PSA vs. Caliptra — Assurance or Implementation?
“RoT as we know is generic and is independent of where it goes into (MCU, CPU, NPU or GPU).” — Suresh Marisetty

This section invites cross-silo reflection on the evolving landscape of platform trust. While PSA Level 3 and Caliptra both aim to anchor security, they diverge in philosophy and implementation.

🧠 **Key Questions**

1. **Can OCP leverage PSA and its certification?** Yes. PSA Certified offers a flexible, SESIP-based framework that aligns with OCP’s goals for open, interoperable security. It can complement Caliptra’s lifecycle and telemetry model.

2. **Can Caliptra firmware be extended to support PSA APIs?** Technically feasible. Caliptra's open-source firmware could implement PSA APIs for attestation and crypto services, enabling PSA-compliant applications to run atop Caliptra platforms.
3. **Is TF-M missing anything relative to Caliptra firmware?** TF-M is optimized for V8-M MCUs and lacks Caliptra's mailbox telemetry, lifecycle anchors, and hardened PQC IPusage. However, TF-M excels in modularity and PSA API coverage.

🔍 **Assurance vs. Implementation**

Aspect	Caliptra Focus	PSA L3 Focus
RTL Implementation	Open-source, prescriptive	Agnostic, implementation-independent
Firmware Behavior	Mailbox, lifecycle, telemetry	PSA APIs, secure services
Certification Path	OCP-led, Caliptra-specific	SESIP-based, vendor-neutral
End-User Priority	Implementation transparency	Assurance level and threat coverage

💡 **Food for Thought & Key Takeaway's**

- Caliptra's gate count may be high for MCUs, but its robustness matches PSA L3.
- PSA L3-compliant MCUs have achieved similar threat coverage with lighter implementations.
- Open-source RTL and firmware are valuable, but end users prioritize assurance—what threats are covered, how trust is anchored, and whether the system can be certified.

12. Conclusion

Trust must scale—from embedded devices to hyperscale platforms. PSA, Caliptra, and S.A.F.E. offer complementary strengths. By integrating developer APIs, aligning with SPDM, referencing NISTIR 8259A, and adopting S.A.F.E. for continuous appraisal, one can build a future where silicon trust is measured, renewable, programmable, and interoperable.

This paper does not advocate replacing one model with another. Instead, it encourages dialogue between PSA and Caliptra communities to explore interoperability, reuse, and shared assurance goals. The goal is not convergence, but clarity and collaboration.

13. Bibliography and References

1. **Arm PSA Certified** PSA Certified Level 3 Protection Profile and Certification Scheme https://www.psacertified.org
2. **Trusted Firmware-M Project** Open-source reference implementation for PSA Functional APIs https://www.trustedfirmware.org/projects/tf-m
3. **Caliptra RTM Specification** Open Compute Project (OCP) Caliptra Root of Trust for Measurement https://www.opencompute.org/projects/caliptra
4. **CHIPS Alliance** Collaborative development of open-source RTL and verification frameworks https://chipsalliance.org
5. **NISTIR 8259A** Core Cybersecurity Capabilities for IoT Devices https://csrc.nist.gov/publications/detail/nistir/8259a/final

6. **DMTF SPDM Specification** Security Protocol and Data Model for device authentication and attestation https://www.dmtf.org/standards/spdm
7. **SESIP Certification Scheme** Security Evaluation Standard for IoT Platforms https://www.globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip
8. **Five Steps to Successful Threat Modelling** Arm Community Blog. Suresh Marisetty. https://community.arm.com/arm-community-blogs/b/internet-of-things-blog/posts/five-steps-to-successful-threat-modellin
9. Marisetty, Suresh. *PSA Functional APIs: Enabling Developer Portability Across Secure Silicon*. Technical Talk, 2025 IoT Security for Software Developers: The Platform Security Architecture APIs
10. Marisetty, Suresh. *Demystifying Security Root of Trust Approaches for IoT/Embedded*. Linaro Connect San Francisco 2017 (Session SFO17-304). Demystifying Security Root of Trust Approaches for IoT/Embedded - SFO17-304 | PPTX

14. Glossary

- DICE (Device Identifier Composition Engine): A method for deriving device identity and attestation based on hardware and firmware measurements.
- SPDM (Security Protocol and Data Model): A standard protocol for secure device authentication and measurement exchange.
- RTL (Register Transfer Level): A hardware design abstraction used to describe the operation of digital circuits.
- SESIP (Security Evaluation Standard for IoT Platforms): A certification scheme for evaluating the security of IoT platforms.
- IAT (Initial Attestation Token): A cryptographically signed token to prove device integrity.
- NISTIR 8259A (NIST Interagency Report 8259A): A cybersecurity capability baseline for IoT devices, published by NIST.
- CSPN (Certification de Sécurité de Premier Niveau): A French security certification scheme for IT products.
- SPA/DPA (Simple/Differential Power Analysis): Types of side-channel attacks that analyze power consumption to extract secrets.
- DFA (Differential Fault Analysis): A type of attack that induces faults in hardware to reveal cryptographic keys.
- CoRIM (Concise Reference Integrity Manifest): A standardized format for expressing device integrity measurements.

14. Acknowledgement

I sincerely acknowledge a set of my professional acquaintances for participating in limited discussions, peer review and feedback on the contents of this paper.

Disclaimer & Copyright Notice: