Safeguarding the Arm Ecosystem

With PSA Certified PUF-based Crypto Coprocessor

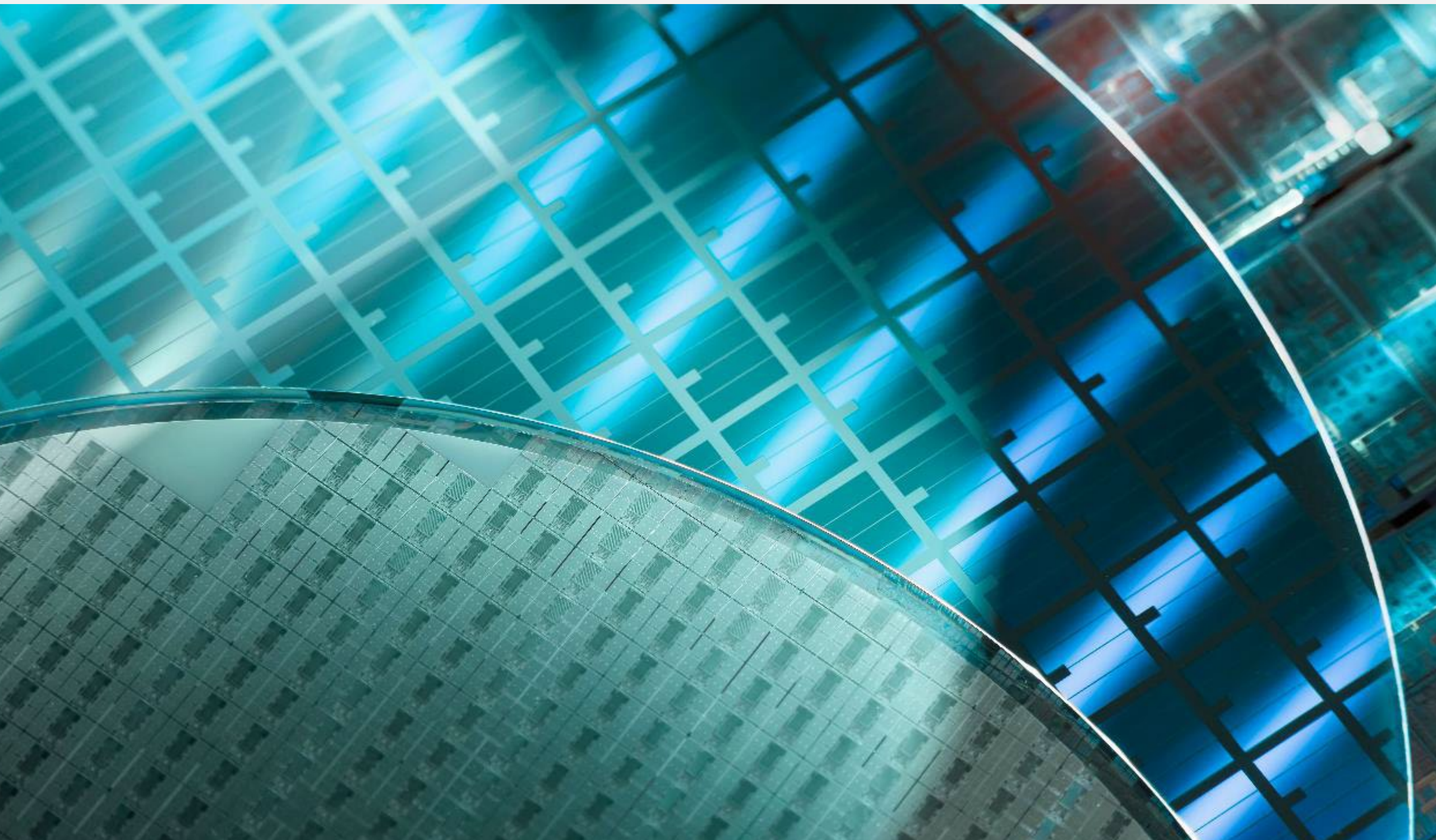
Whitepaper

Lawrence Liu (劉持志)

Dr. Evans Yang (楊青松)

Stephanie Smith

March 2023



Silicon-to-System Security

For the past five years, Arm has reaffirmed its commitment to safeguarding its architecture with their Security Manifesto. It outlines a clear "call to arms" for the semiconductor industry to address the rising threats facing computing today. Software alone can only mitigate vulnerabilities to a certain degree. However, hardware methods can establish a firm foundation for a device that can support the security ecosystem on which it operates.

The reality is that a comprehensive security ecosystem is required to provide a cooperative and layered solution. From the IoT and AI, to mobile devices, there is virtually no computing process that does not involve Arm Architecture. This makes them ideally placed to drive a holistic *"silicon-to-systems effort to strengthen security"* alongside their partners and bring comprehensive protection to the hardware level.

Standardizing IoT Security with PSA Certified

Due to the rapid expansion of the IoT market, security standardization has been left trailing to catch up, which led Arm to spearhead PSA Certified with its partners in 2019. They aimed to bring IoT security into proactive thinking and ultimately secure and protect IoT devices from malicious attacks. With a robust set of common standards in place, PSA Certified is helping reduce the fragmentation of security protocols amongst the myriad of IoT devices, applications, and solution providers.

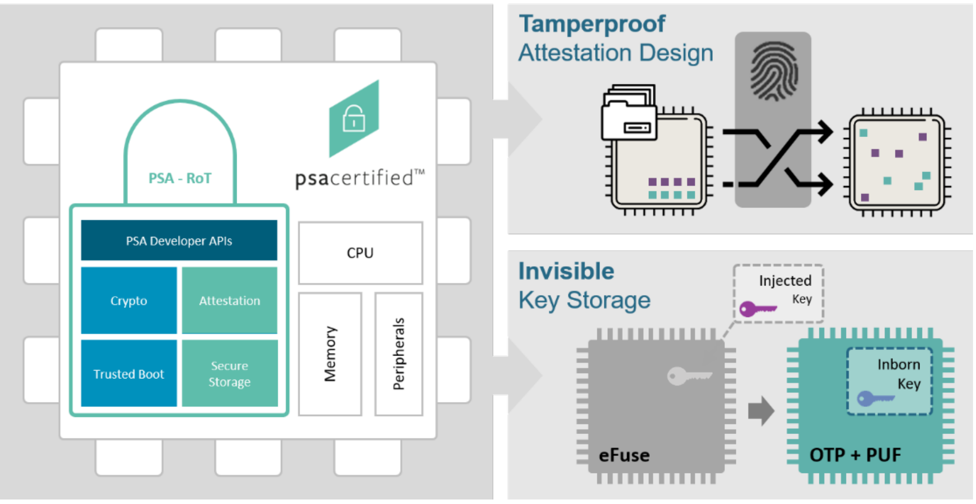


Figure 1: PSA Standard Requirements for IoT Root of Trust

Through promoting shared foundational security features verified by third-party laboratories, PSA Certified helps allay consumer fears about privacy invasion and gives solution vendors a leg-up towards meeting current and soon-to-come government IoT security requirements. As there is no "typical" IoT product, what is considered secure for one device might be insufficient for another, so the PSA Certified program offers different levels of certification. These include PSA Certified Level 1, PSA Certified Level 2, PSA Certified Level 2 ready, and PSA Certified Level 3. This gradation of security levels reflects the reality that there is no one-size-fits-all solution for IoT security.

PSA Certified Level 1 Certification means a third-party laboratory has examined the questionnaire for accreditation, but no in-lab testing has been performed. It should also demonstrate that an IoT chip/device/software follows the best security practices derived from IoT threat models, the PSA Certified 10 Security Goals, and worldwide government guidelines and requirements.

PSA Certified Level 2 and PSA Certified Level 3 Certifications are slightly different. These are a measurement of security robustness and, as such, require testing in the laboratory, with a selected battery of software-only attacks, adding physical penetration evaluation (including side-channel analysis) for PSA Certified Level 3. Focused on hardware solutions, PSA Certified Level 2 and PSA Certified Level 3 require that the evaluation target (TOE) must implement a Root of Trust (RoT) and satisfy nine security functional requirements to be certified. These functions include:

1. Initialization
2. Software Isolation
3. Secure Storage
4. Firmware Update
5. Secure State
6. Cryptography
7. Attestation
8. Audit / Debug
9. Physical

Note the overlap between these nine functions and the eight categories for level 1 certification, as a secure Hardware Root of Trust (HRoT) must naturally follow best security practices.

PSA Certified Level 2 Ready Certification could be considered a preparation step to help companies achieve PSA Certified Level 2 and PSA Certified Level 3. It is designed to help system architects speed up the final certification. As designs have become more complex over time, it is expected nowadays that a product may incorporate one or more IPs from third-party vendors that specialize in the missing pieces of the design puzzle. This leads to savings in the required human resources and budgets that seem to be squeezed tighter and tighter each year. Overall product development is shortened, and now with PSA Certified Level 2 Ready certification, the time required for a final product's post-design security certification can also be reduced.

A PSA Certified Level 2 Ready Crypto Coprocessor

PUFsecurity's PUFcc Crypto Coprocessor is an example of such a product that is a perfect candidate for which the PSA Certified Level 2 Ready certification was designed to meet the needs of.

PUFcc combines a Hardware Root of Trust with a full suite of cryptographic accelerators, Secure OTP storage, and a TRNG. This forms an adaptable security IP module suitable for integration into a wide array of system architectures. This 'off the shelf' solution allows designers to 'drop and play' a complete IP solution that enables a system's required security protocols hassle-free.

PUFcc can securely perform sensitive operations that are operationally separated from normal functions (that the main system is typically responsible for) through hardware isolation from within its security boundary and bolstered by anti-tampering designs. Thus, PUFcc is a general-purpose integrated security IP module capable of supporting the most common cryptographic algorithms, allowing users to build a variety of security protocols.

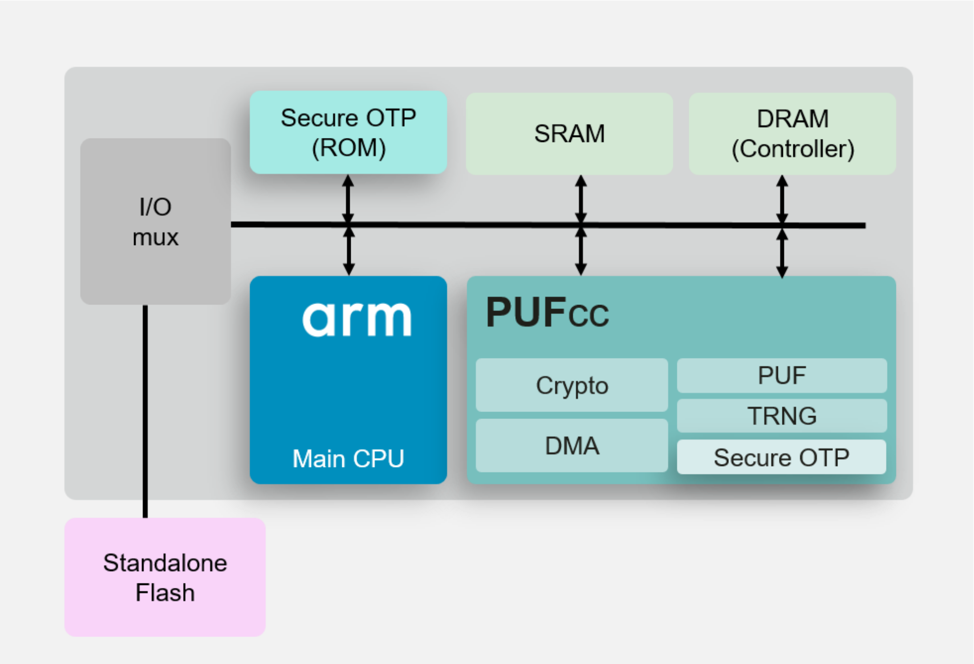


Figure 2: Typical integration diagram for PUFcc

As a security coprocessor, the operations that are executed within the boundaries of PUFcc need to be implicitly trusted by the system. These operations ensure the overall security of the entire system, especially when the components outside the security boundary of PUFcc cannot be guaranteed to be 100% secure. For example, the system memory, bus, and other devices sharing the system bus are prime targets for attacks by hackers to gain access or control of the system.

To guarantee that PUFcc can meet the security requirements demanded of a trusted, isolated subsystem, PUFsecurity has contracted with a third-party laboratory to certify PUFcc as PSA Certified Level 2 Ready for the functional security requirements of initialization, secure storage, firmware update, secure state, and crypto (five out of the nine security functions).

Crypto Coprocessor PSA-RoT Functionality

Secure *initialization* means that the TOE needs to ensure that only authorized software is executed on a device. PUFcc accomplishes this by validating the signed boot code during the secure boot flow, using the MCUboot boot loader that is part of the Trusted Firmware M (TF-M) package. PUFcc itself implements the hardware key used for this initialization through the process of internal key provisioning.

Secure storage prevents private data from being cloned or stolen from a device. PUFcc implements secure storage through an AES (GCM mode) based on authenticated encryption with associated data (AEAD) secure data policy to protect the integrity and authenticity of private system data. The key used for this secure data policy is derived from the Hardware Unique key (HUK), which only PUFcc can access, sourced from the built-in, die-unique physically unclonable function (PUF). This PUF contains entirely different random values from one PUFcc to the next, ensuring that the HUK for every PUFcc is unique and completely random.

A firmware update (or secure update), which is tangentially related to secure boot – is the only authorized update allowed to be made to the device. However, the execution of updated firmware is still done by the secure boot (initialization) flow. PUFcc accomplishes this by limiting write access to the firmware image slots, allowing only those correctly signed firmware images to be written during the secure-update process. Then, during secure boot, the most recently verified firmware image is chosen to boot from, while at the same time, the security counter is updated to match the latest version of the installed firmware.

A secure state isolates trusted, less trusted, and non-trusted services from each other. Through the Secure Partition Manager (SPM), any errors in isolation between partitions (as part of the PSA firmware framework) will result in the termination of the said process through a panic (interrupt) call. In addition, PUFcc forms a security border to execute secure/non-secure operations that are safely isolated from one another.

The security functional requirement of *crypto* is short for cryptographic / trusted services. These services support critical system security functions such as security lifecycle, isolation, secure storage, attestation, secure boot, and the secure loading and the binding of data. PUFcc supports a full suite of cryptographic primitive functions such as symmetric/asymmetric ciphers, hashes, message authentication codes (MACs), and AEAD to fulfill the crypto security functional requirement.

As PUFcc was not designed to be a stand-alone product, the other security functional requirements for complete PSA Certified Level 2 or PSA Certified Level 3 certification depend on the larger, incorporating system to implement: software isolation, attestation, audit, and debugging. Hence PUFcc is PSA Certified Level 2 *Ready* certified instead of fully PSA Certified Level 2 certified.

CoreLink SSE-200 Integration

The PSA Certified Level 2 Ready certification for PUFcc was performed using an Arm MPS3 evaluation board. An FPGA implementation of the Arm CoreLink SSE-200 subsystem (as described in application note AN524) was integrated with PUFcc, and a Trusted Firmware-M port on the MPS3 board. CoreLink SSE-200 is a collection of pre-assembled elements (including two Cortex-M33 cores) suitable for use as the basis of an IoT SoC, sourced from the Arm system SIE-200 library. The lower power drawn from the Cortex-M33 cores makes CoreLink SSE-200 based systems ideal for edge IoT applications.

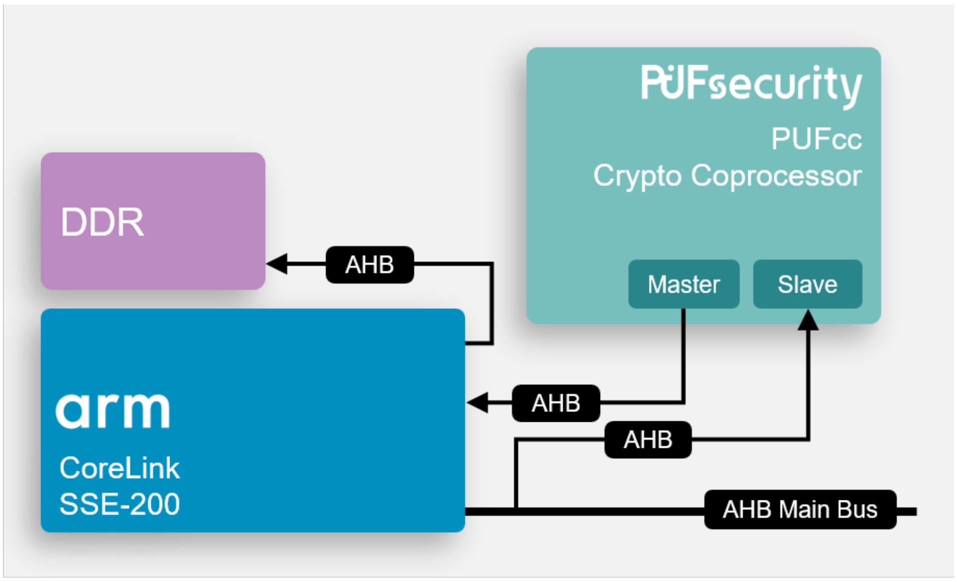


Figure 3: PUFcc Integration on an Arm SSE-200 Subsystem

Designed to provide the primitive elements to build a PSA-RoT, PUFcc combines a unique identifier (PUF), secure storage (OTP), TRNG, and cryptographic coprocessor into a secure IP supporting cryptographic operations. Thus PUFcc can be used as a peripheral inside the Secure Processing Environment (SPE). As the cryptographic keys can be internally generated by the root of trust (PUFcc) itself, key leakage is avoided so that

PUFcc can be considered as being within its own secure boundary. The hard macro (PUF, OTP) functionality of PUFcc is simulated using RTL behavioral models.

For integration with the CoreLink SSE-200 subsystem, PUFcc uses both AHB and APB buses for connections. PUFcc's AHB master is linked to the CoreLink SSE-200 Manager Security Controller (MSC) for sending requests to Implementation Defined Attribution Units (IDAU) as required for PUFcc operation, such as external memories that are accessed through PUFcc's Direct Memory Access (DMA) module. The APB slave bus module is connected to CoreLink's Peripheral Protection Controller (PPC) to receive both secure and non-secure requests from the CoreLink SSE-200, as part of the Expansion 1 Interface.

Corstone SSE-300 Integration

In addition to the CoreLink SSE-200, the same type of Arm MPS3 evaluation board with a port of Trusted Firmware-M was used to demonstrate PUFcc integration with the Corstone SSE-300 subsystem, as described in application note AN552 (Soft Macrocell Model – SMM). The AN552 features a single Cortex-M55 with Custom Datapath Extension and an Ethos-U55 machine learning processor. Like the CoreLink SSE-200, Corstone SSE-300 is a collection of pre-assembled elements selected from the SIE-200 library (with the addition of the SIE-300 library in this case). With the more powerful Cortex-M55 core, Corstone SSE-300 based systems are well suited for applications that demand higher performance over the CoreLink SSE-200.

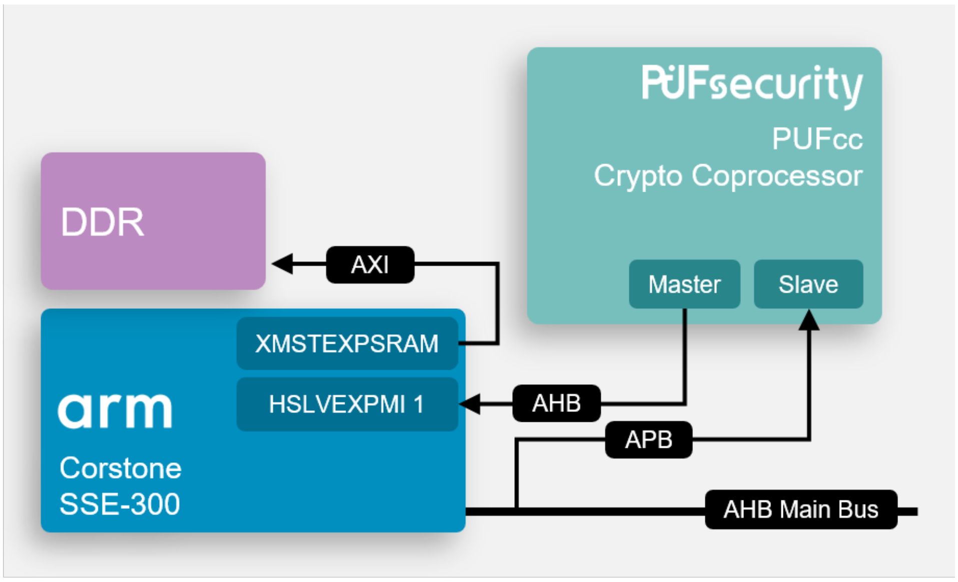


Figure 4: PUFcc Integration on an Arm Corstone SSE-300 Subsystem

Integration of PUFcc with the Corstone SSE-300 subsystem is very similar to the SSE-200 case, which also uses both AHB and APB buses. PUFcc's

AHB master is again connected to a Manager Security Controller (MSC) in the CoreLink SSE-300, using the one located in the Slave Main Expansion interface (HSLVEXPMI1). Finally, the APB slave bus module is once again connected to Corstone's APB Peripheral Protection Controller (PPC) in both the Non-Secure and Secure Peripheral Regions of the AN552 memory map.

Conclusion

Arm's Total Solutions for IoT is an ambitious program for fueling the next stage of the IoT industry's development. With Total Solutions aimed at unleashing the promised potential of IoT, the PSA Certified program stands ready to protect that bright future. And as PUFcc is the first of many PUFsecurity solutions to be certified under the PSA Certified program, PUFsecurity plans to join Arm hand-in-hand as partners, promoting a secured IoT universe and protecting our connected world.

PUFsecurity Corporation.

8F, No. 5, Tai-Yuan 1st St., Jhubei City,
Hsinchu County,
302082, Taiwan
Tel: +886-3-560-1168
www.pufsecurity.com