Cross-platform **O**pen **S**ecurity **S**tack for **Con**nected Device

D4.4 CROSSCON Extension Primitives to Domain Specific Hardware Architectures - Final

Document Identification			
Status	Final	**Due Date**	31/08/2025
Version	1.0	**Submission Date**	27/08/2025

Related WP	WP4	**Document Reference**	D4.4
Related Deliverable(s)	D4.3	**Dissemination Level (*)**	PU
Lead Participant	BEYOND	**Lead Author**	Žiga Putrle (BEYOND)
Contributors	TUD, UWU	**Reviewers**	Piotr Król (3MDEB) Luís Cunha (UMINHO)

Keywords:
CROSSCON SoC, BA51-H, FPGA, FPGA TEE, Perimeter guard, PUF, Environmental fingerprinting, AES-GCM,

Document Information

List of Contributors	
Name	Partner
Žiga Putrle	BEYOND
Nikhilesh Kumar Singh	TUD
Tymoteusz Burak	UWU
Fabian Schmitt	UWU
Hamid Dashtbani	UWU

Document History			
Version	Date	Change editors	Changes
0.1	14/07/2025	Žiga Purtle	Initial contributions. Copying content from previous deliverable.
0.2	01/08/2025	Žiga Purtle, Nikhilesh Kumar Singh, Tymoteusz Burak	Updating the content.
0.3	04/08/2025	Žiga Purtle	Updating introduction and conclusion. Providing comments and suggestion to other sections.
0.3	04/08/2025	Nikhilesh Kumar Singh	Addressing comments in the previous version, adding references.
0.3	04/08/2025	Fabian Schmitt	Update section 2.2
0.4	13/08/2025	Žiga Putrle	Making minor adjustments before the review.
0.4	18/08/2025	Žiga Putrle	Fixing citations.
0.5	18/08/2025	Žiga Putrle	Updating the version of the document.
0.6	19/08/2025	Nikhilesh Kumar Singh	Addressing the reviewers' comments for TUD-related sections.
0.7	20/08/2025	Žiga Putrle	Addressing the reviewers' comments for BEYOND-related sections and other common sections.
0.8	21/08/2025	Hamid Dashtbani	Addressing the reviewers' comments for UWU-related sections.
0.12	26/08/2025	Juan Alonso	Quality Assessment.
1.0	27/08/2025	Hristo Koshutanski	Final version submitted.

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Žiga Purtle (BEYOND)	21/08/2025
Quality manager	Juan Alonso (ATOS)	26/08/2025
Project Coordinator	Hristo Koshutanski (ATOS)	27/08/2025

Table of Contents

List of Acronyms

Abbreviation / acronym	Description
CSI	Channel State Information
D4.3	Deliverable number 3 belonging to WP4
D4.4	Deliverable number 4 belonging to WP4
EC	European Commission
FPGA	Field-Programmable Gate Arrays
GP	Global Platform
HW	Hardware
IoT	Internet of Things
MS8	8th Milestone
PG	Perimeter Guard
PMP	Physical Memory Protection
PoC	Proof of Concept
PSA	Platform Security Architecture
PUF	Physically Unclonable Function
SoC	System-on-Chip
SPMP	S-mode PMP
TRL3	Technology Readiness Level 3
vFPGA	Virtual FPGA
Wi-Fi	Wireless Fidelity
WP	Work Package

Executive Summary

The deliverable D4.4 contains the implementation results of WP4 described in D4.3 “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Final“ [1] . It includes (1) a prototype implementation of interrogability layer between GlobalPlatform Crypto API and PSA Crypto API that simplifies the use of one API if the other is available, (2) an implementation of physically unclonable function (PUF) hardware primitive interface, (3) a prototype implementation of environmental fingerprinting hardware primitive interface, (4) a CROSSCON SoC bitstreams with BA51-H core, unified SPMP, Perimeter guard and AES-GCM that supports context switching, (5) a Spike (RISC-V) simulator extended with unified SPMP extension, (6) a prototype implementation of trusted anchor for FPGA that can be used to establish virtual FPGA environments. The provided artifacts serve as proof of concept (PoC) of the solutions developed in WP4 in collaboration with other work packages. This deliverable D4.4 contributes to the accomplishment of milestone MS8 “Final version of the CROSSCON stack components and extension primitives, and extended testbed” and MS9 “Final version of integrated CROSSCON stack and extension primitives”.

1 Introduction

1.1 Purpose of the document

The document outlines the implementation results of work done as part of WP4, described in D4.3 “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Final” [1], and provides references to the project repositories that are included in this deliverable. Each of the repositories contains an extended description of the implemented solution, instructions on how to use it, and related code/bitstreams.

1.2 Relation to other project work

This document is closely related to the deliverable D4.3 “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Final” [1] as it contains the actual implementation results of the solutions described in D4.3. The implementation results serve as prototypes of the solutions developed in WP4 in collaboration with WP2 and WP3, and further contribute to MS8 “Final version of the CROSSCON stack components and extension primitives, and extended testbed” and MS9 “Final version of integrated CROSSCON stack and extension primitives”. The solutions developed in WP4 are tightly related to the work done in WP2 and WP3; WP2 provided the initial research results and requirements needed for the development, where the solutions of WP3 were codeveloped with the solutions of WP4 as they are tightly related. The work in WP4 was used to refine and inform the development of open specification and formal framework in WP2. Additionally, the development and runtime environments used are necessary inputs for the integration and validation of the solutions as part of WP5.

1.3 Structure of the document

The document is structured into several independent sections that are a part of chapter 2. Each section contains a short description of the provided artifact with a reference to the repository that contains the extended description, the artifact itself, and instructions on how to use it.

2 WP4: Extension Primitives Final Version

As part of WP4, we have defined and developed hardware-software solutions that can be used to improve security and portability of IoT devices, and complement the CROSSCON Stack. In D4.4 “CROSSCON Extension Primitives to Domain Specific Hardware Architectures — Final Version”, we provide proof of concept implementation of the solutions with their description and instructions on how to use them. The developed solutions and related documentation are accessible in the CROSSCON’s GitHub repository [1].

2.1 Platform Security Architecture (PSA) Crypto API Demonstrator

CROSSCON aims to develop a unified software stack for resource-constrained IoT devices. As part of this effort, we seek to provide a unified interface for trusted services within CROSSCON to perform essential cryptographic operations. As IoT devices increasingly integrate domain-specific hardware components such as cryptographic accelerators, it is crucial for software stacks to incorporate these hardware components. An important task is to evaluate existing APIs to understand their versatility and potential for integration into the CROSSCON stack.

Related repo https://github.com/crosscon/optee_psa_extension_manifest [3]. This repository acts as an entry point and contains a proof of concept of how the PSA Crypto API could be used within OP-TEE via a wrapper layer or OP-TEE syscall extension. Due to the nature of OP-TEE, the work is distributed among several repositories [3][4][5][6], and the entry points for both scenarios are `*wrapper_qemu.xml*` and `*psa_syscalls_qemu.xml*`.

Related repo https://github.com/crosscon/crypto_API_demonstrator [7]. This repo contains an example of how the PSA Crypto API can be used to perform encryption and decryption with AES-128, as well as data hashing using SHA-256, on two different platforms, LPC55S69-EVK with ARM Cortex-M33 and ESP32-C3 with RISC-V microprocessor. Both devices are outfitted with hardware accelerators for these operations. The purpose of the demonstrator is not only to showcase the PSA Crypto API but also to provide guidance on how to configure the platform (e.g., by setting the correct compiler flags) to use or not use the available hardware accelerators without making changes to the actual code of the application itself.

2.2 Physically Unclonable Function Hardware Primitive Demonstrator

As part of the CROSSCON Stack, we have developed an innovative authentication service [8][9] powered by a PUF. The proposed service is PUF-agnostic by leveraging an abstraction interface, as described in D4.3 [1], which allows the implementation of different PUF backends/drivers. Furthermore, the service can use either weak or strong PUFs, which ensures broader compatibility and flexibility. The authentication schemes are described in D3.3 [10].

Related repo https://github.com/crosscon/ZK-PUF-Zephyr-Demo [3]. In this repository, we encapsulate the PUF interaction within a Trusted Application, adhering to GP’s IPC and lifecycle management model, while remaining agnostic to the specific PUF architecture or post-processing logic. Authentication follows the ZK-PUF authentication scheme [2]. Due to the lack of readily available hardware with native PUF support, the prototype targets the NXP LPC55S69 board, which exposes an SRAM-based PUF interface. Additionally, the platform lacks support for any recognized TEE implementation. As a result, the Trusted Application is implemented as a Zephyr RTOS VM running on top of the CROSSCON Hypervisor.

2.3 Environmental Fingerprinting Hardware Primitive Demonstrator

Within the CROSSCON Stack, we have developed a Context-based Authentication scheme that utilizes a device’s Wi-Fi hardware to create a location-dependent fingerprint of its environment based on other

devices and the connected Wi-Fi network within a pre-defined location. This scheme uses CSI data extracted by Wi-Fi peripherals and is designed to be platform-independent by using the interface described in D4.3 [1].

Related repo https://github.com/crosscon/context-based-auth-crosscon-demo [11]. In this repo, we demonstrate the use of the environmental fingerprinting primitive from a Trusted Application. The prototype targets the Raspberry Pi 4 board, which features the Wi-Fi hardware necessary for the collection of the required environmental information. A modified OP-TEE OS is used as a TEE running in a VM on top of the CROSSCON Hypervisor, which provides GlobalPlatform API compliance for gathering the fingerprint from the separate VM. As such, the API used by the Trusted Application is independent of the actual platform used.

Related repo https://github.com/crosscon/context-based-auth-optee-os [12]. This repo hosts a modified version of OP-TEE OS, which contains a PoC implementation of the proposed interface as a Pseudo Trusted Application. It must run on the CROSSCON Hypervisor and requires a separate Linux VM to interact with the hardware. These are assembled in the demonstrator below. The Pseudo Trusted Application mediates communication between the Trusted Application and the hardware.

Related repo https://github.com/crosscon/context-based-auth-nexmon-vm [13]. This repository contains the code to build the separate Linux VM mentioned above, on which the extended OP-TEE OS relies. It includes a modified firmware, which is required to extract the CSI samples from the Wi-Fi card, as well as a script that mediates communication between OP-TEE and the peripheral. It is the platform-specific part of this implementation.

2.4 CROSSCON SoC

CROSSCON SoC is a system-on-chip (SoC) design, developed as part of the CROSSCON project, that provides a secure RISC-V execution environment for mixed-criticality IoT devices that require strong security guarantees, flexibility, small code size, and low power consumption. It allows for strong software isolation through virtualization-based trusted execution environments (TEEs), with the ability to share hardware (HW) modules connected to the SoC interconnect between TEEs without compromising isolation.

Related repo https://github.com/crosscon/crosscon_soc [14]. This repository contains a CROSSCON SoC bitstream with several setup examples that demonstrate the main features of the SoC: (1) BA51-H core - highly configurable, low-power, deeply embedded 32-bit RISC-V processor with efficient virtualization support without virtual memory, (2) the first HW implementation of unified (2-stage) S-mode Physical Memory Protection (uSPMP) RISC-V extension, (3) Perimeter guard (PG) in several operation modes (lock-release with reset and context switching), that can be used for secure communication over the SoC interconnect and to enable sharing of HW modules in a secure manner, and (4) AES-GCM accelerator that supports context switching so that it can be used by several domains at a time.

2.5 Spike (RISC-V) Simulator Extended with unified SPMP Extension

Spike is a RISC-V ISA simulator [15] that provides a functional model for RISC-V cores and is generally considered as a golden model of the RISC-V specification. It allows one to run RISC-V programs with a variety of different RISC-V extensions, including the RV32I, PMP, and Hypervisor extension.

Related repo https://github.com/crosscon/riscv-isa-sim [16]. This repository contains the Spike simulator extended with a reference implementation of the unified SPMP (uSPMP) extension, which demonstrates how vanilla SPMP specification [17] can be extended to support the hypervisor extension, using a dual-stage SPMP. The uSPMP extension was suggested to the RISC-V community as part of the CROSSCON project. The extended Spike is used as base of a reference execution environment for the BA51-H core.

2.6 Trusted Anchor for FPGA

Field Programmable Gate Arrays (FPGAs) have become integral components in modern computing environments due to their adaptability and computing capabilities. As part of WP4, we explore the advancements and challenges in sharing FPGA resources among applications or users. Particularly, we are interested in extending trusted execution environment to FPGAs while providing IP protection for hardware designs configured on the FPGA.

Related repo https://github.com/crosscon/UC5-IP_Protection_for_Secure_Multi-Tenancy_on_FPGA [18]. This repository is the final implementation for the technology demonstration of the Secure FPGA Provisioning system integrated with the CROSSCON Hypervisor that provides secure FPGA-based acceleration and enables IP protection on FPGA-enabled SoCs within the CROSSCON Stack. The implementation is in line with GlobalPlatform APIs for cryptographic operations and communication. We provide a demonstrator with two reconfigurable virtual FPGAs (vFPGAs) on the AMD ZCU 102 board. Two client applications (CAs) run on the Linux VM and interact with the Trusted Applicaiton (TA) in the OPTEE VM. The CROSSCON hypervisor manages both the VMS. The demonstrator includes examples for status check of vFPGA, configuration requests from CAs, and deallocation of vFPGAs from the CAs.

Related repo https://github.com/crosscon/FPGA_TEE [19]. This repository contains the initial, proof of concept, implementation of the Secure FPGA Provisioning system, which runs baremetal without the integration of the CROSSCON Hypervisor. The repository has an additional branch *fpga-tee-enc* that includes added cryptographic features for the protection of the partial bitstream.

3 Conclusion

This deliverable contains the implementation results of the work done as part of WP4 described in D4.3 “CROSSCON Extensions to Domain Specific Hardware Architectures Documentation — Final” [1].The provided artifacts are an important and a necessary step towards developing full-featured solutions as they serve as base for further development and provide an opportunity for evaluation. Furthermore, the solutions can already be used to address real world problems which is an important milestone for the project to achieve greater adoption. We aim to further refine and improved the developed solutions to achieve greater maturity so that they can be easily used in industrial setting.

References

[1] **CROSSCON**, "D4.3 CROSSCON Extensions to Domain Specific Hardware Architectures Documentation - Final," August 2025.

[2] "**CROSSCON project GitHub repository**," [Online]. Available: https://github.com/crosscon. [Accessed August 2025].

[3] "**OP-TEE PSA Extension Manifest**", July 2025. [Online]. Available: https://github.com/crosscon/optee_psa_extension_manifest.

[4] "**OP-TEE PSA Extension OS**", July 2025. [Online]. Available: https://github.com/crosscon/optee_psa_extension_os.

[5] "**OP-TEE PSA Extension Examples**", July 2025. [Online]. Available: https://github.com/crosscon/optee_psa_extension_examples.

[6] "**OP-TEE PSA Extension Test**", July 2025. [Online]. Available: https://github.com/crosscon/optee_psa_extension_test.

[7] "**Crypto API Demonstrator**", April 2024. [Online]. Available: https://github.com/crosscon/crypto_API_demonstrator.

[8] "**PUF-based Authentication Proof of Concept Implementation**", 2024 July. [Online]. Available: https://github.com/crosscon/crosscon_puf_authentication.

[9] "**Zero-Knowledge PUF CROSSCON HV Demo**", July 2025. [Online]. Available: https://github.com/crosscon/ZK-PUF-Zephyr-Demo.

[10] **CROSSCON**, "**D3.3** CROSSCON Open Security Stack - Final," 2025 August.

[11] "**Context-based Authentication Demo**", July 2025. [Online]. Available: https://github.com/crosscon/context-based-auth-crosscon-demo.

[12] "**OP-TEE OS CSI Extension**", July 2025. [Online]. Available: https://github.com/crosscon/context-based-auth-optee-os.

[13] "**NEXMON VM on CROSSCON Hypervisor**", July 2025. [Online]. Available: https://github.com/crosscon/context-based-auth-nexmon-vm.

[14] "**CROSSCON SoC**", August 2025. [Online]. Available: https://github.com/crosscon/crosscon_soc.

[15] "**Spike RISC-V ISA Simulator**", [Online]. Available: https://github.com/riscv-software-src/riscv-isa-sim. [Accessed April 2024].

[16] "**Extended Spike (RISC-V ISA) simulator**", August 2025. [Online]. Available: https://github.com/crosscon/riscv-isa-sim.

[17] "**RISC-V SPMP Extension**", [Online]. Available: https://github.com/riscv/riscv-spmp. [Accessed April 2024].

[18] "**CROSSCON UC5 IP Protection for Secure Multi-Tenancy on FPGA**", August 2025. [Online]. Available: https://github.com/crosscon/UC5-IP_Protection_for_Secure_Multi-Tenancy_on_FPGA.

[19] "**FPGA TEE**", April 2024. [Online]. Available: https://github.com/crosscon/FPGA_TEE.