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

D3.4 CROSSCON Open Security Stack – Final Version

Document Identification			
Status	Final	**Due Date**	31/08/2025
Version	1.0	**Submission Date**	29/08/2025

Related WP	WP3	**Document Reference**	D3.4
Related Deliverable(s)	D2.3, D3.3, D5.5	**Dissemination Level (*)**	PU
Lead Participant	UNITN	**Lead Author**	Alberto Tacchella (UNITN)
Contributors	UMINHO, UNITN, UWU, TUD	**Reviewers**	Piotr Król (3MDEB)
			Yannick Roelvink (CYSEC)

Keywords:
CROSSCON Hypervisor, TEE Isolation, CROSSCON Trusted Services, CROSSCON Toolchain, Bare-Metal TEE

This document is issued within the frame and for the purpose of the CROSSCON project. This project has received funding from the European Union's Horizon Europe Programme under Grant Agreement No.101070537. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

(*) Dissemination level: **(PU)** Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page). **(SEN)** Sensitive, limited under the conditions of the Grant Agreement. **(Classified EU-R)** EU RESTRICTED under the Commission Decision No2015/444. **(Classified EU-C)** EU CONFIDENTIAL under the Commission Decision No2015/444. **(Classified EU-S)** EU SECRET under the Commission Decision No2015/444.

Document Information

List of Contributors	
Name	Partner
Alberto Tacchella	UNITN
João Sousa, David Cerdeira	UMINHO
Nikhilesh Singh	TUD
Tymoteusz Burak, Fabian Schmitt	UWU

Document History			
Version	Date	Change editors	Changes
0.1	05/11/2024	Alberto Tacchella (UNITN)	Initial version
0.2	30/07/2025	João Sousa (UMINHO), David Cerdeira (UMINHO)	Updated repositories in Sections 2.1 and 2.2
0.3	31/07/2025	Alberto Tacchella (UNITN)	Draft version for internal review
0,4	5/08/2025	Nikhilesh Singh (TUD)	Added repositories in Section 2.3.2
0.5	05/08/2025	Fabian Schmitt (UWU)	Added repositories in 2.3.3 & 2.3.4
0.6	13/08/2025	João Sousa (UMINHO)	Added Mulitple VMM repository in Section 2.2
0.7	26/08/2025	Alberto Tacchella (UNITN)	Final version for internal review
0.8	28/08/2025	Alberto Tacchella (UNITN)	Final version for QA
0.9	29/08/2025	Juan Alonso (ATOS)	Quality Assessment.
1.0	29/08/2025	Hristo Koshutanski (ATOS)	Final version submitted.

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Alberto Tacchella (UNITN)	28/08/2025
Quality manager	Juan Alonso (ATOS)	29/08/2025
Project Coordinator	Hristo Koshutanski (ATOS)	29/08/2025

Table of Contents

List of Acronyms

Abbreviation / acronym	Description
D3.4	Deliverable number 4 belonging to WP3
EC	European Commission
FPGA	Field-Programmable Gate Arrays
IoT	Internet of Things
PUF	Physical Unclonable Function
SoC	System-on-Chip
TA	Trusted Application
TEE	Trusted Execution Environment
TRL	Technology Readiness Level
VM	Virtual Machine
VMM	Virtual Machine Manager
WP	Work Package

Executive Summary

This deliverable contains the final implementation results of the work done as part of WP3 of the CROSSCON project and described in D3.3 “CROSSCON Open Security Stack Documentation - Final” [2]. It includes the final implementation of (1) the CROSSCON TEE Isolation Primitives, (2) the CROSSCON Hypervisor, (3) the CROSSCON Trusted Services, (4) the CROSSCON Toolchain, and (5) the CROSSCON Bare-Metal TEE.

The provided artifacts represent the final version of the CROSSCON Stack components and demonstrate the results of the project that will be used as a foundation for building future trustworthy platforms and applications.

This deliverable contributes to the accomplishment of milestone MS9 “Final version of the CROSSCON stack components and extension primitives, and extended testbed” with a targeted TRL 4 of artifacts’ release in agreement with the project workplan.

1 Introduction

1.1 Purpose of the document

This document contains a list of the final implementation results of the work done in WP3 of the CROSSCON project, as described in D3.3 “CROSSCON Open Security Stack Documentation - Final” [2], and provides references to the corresponding code repositories. Each repository contains an extended description of the implemented solution, instructions on how to use it, and related code and data. The open-source reference implementation of the CROSSCON stack and related documentation are accessible in the official GitHub repository of the CROSSCON project [1].

1.2 Relation to other project work

This document is closely related to the deliverable D3.3, “CROSSCON Open Security Stack Documentation - Final”, as it contains the actual implementation results described in D3.3 [2]. The implementation fulfils the milestone MS9 “Final version of the CROSSCON stack components and extension primitives, and extended testbed”.

The insights acquired through the implementation work were useful for further refinement of the CROSSCON Open Specification developed in the context of WP2, the final version of which has been described in D2.3 “CROSSCON Open Specification - Final” [3]. Additionally, the developed tools and runtime environment have been used for the integration and validation of the solutions as part of WP5, as described in D5.5 “Integrated CROSSCON Security Stack - Final Version” [4].

1.3 Structure of the document

This document consists of a single chapter containing multiple sections. Each section contains a short description of a WP3 task and a list of the relevant code repositories. Each repository encompasses an extended description of the tool, its implementation, and instructions on how to use it.

2 WP3: CROSSCON Stack Development

This chapter contains a list of all the components of the CROSSCON Stack that have been developed as part of WP3 of the CROSSCON project. The corresponding open-source reference implementations and related documentation are accessible in the GitHub repository [1].

2.1 Task 3.1 - CROSSCON TEE Isolation and Abstraction

The objective of this task is twofold. First, it aims to identify potential limitations in the GlobalPlatform internal Core API specification that hinder trusted application (TA) interoperability across heterogeneous trusted operating systems (OS). This includes assessing missing APIs to support new trusted services developed by CROSSCON. Additionally, the task addresses Trusted Execution Environments (TEE) interoperability by designing and implementing a TEE abstraction layer that supports multiple TEE models within a common execution platform. Second, this task focuses on improving isolation within the TEE architecture by enabling the decomposition of trusted services into multiple isolated execution domains. Both subtasks leverage the CROSSCON Hypervisor as a basis for TEE abstraction and isolation.

Related repositories:

- https://github.com/crosscon/CROSSCON-Hypervisor-and-TEE-Isolation-Demos [5]

  This repository contains the source code implementing TEE isolation features to isolate trusted services from trusted OSes on APU devices. It demonstrates the use of the CROSSCON hypervisor to: (i) execute the OP-TEE trusted OS in a Virtual Machine (VM) alongside a Linux VM, (ii) execute two independent OP-TEE VM instances each connected to a distinct Linux VM, and (iii) execute two OP-TEE VM instances both connected to a single Linux VM. All configurations were validated on both RISC-V and Arm architectures using their respective qemu-virt emulation platforms. To demonstrate the TEE coexistence and heterogeneity properties (see D3.3 [2]for definitions), this repository also includes a Linux VM that instantiates an SGX-like enclave on aarch64. TEE isolation for MCU devices is also implemented and validated using the CROSSCON Hypervisor MCU version, with one VM running the mTower trusted OS alongside a FreeRTOS VM, both executed on an Armv8-M platform (LPC series).

2.2 Task 3.2 - CROSSCON Hypervisor

The goal of this task is to develop novel hypervisor mechanisms to address static partitioning hypervisor limitations, enabling dynamic VM creation and management, as well as per-VM TEE services support. Another feature implemented in the context of the CROSSCON Hypervisor to address static partitioning limitations is the multiple Virtual Machine Manager (VMM) support.

Related repositories:

- https://github.com/crosscon/CROSSCON-Hypervisor [6]

  This repository includes the source code of CROSSCON hypervisor. The CROSSCON hypervisor is based on the Bao static partitioning hypervisor, enhanced to reach a broader range of devices and architectures. The CROSSCON Hypervisor provides the following additional features compared to Bao:(i) dynamic VM Creation and management and (ii) per-VM TEE.

- https://github.com/crosscon/multi-vmm [7]

  This repository includes the source code of Multiple-VMM support. Please refer to D3.3 [2]for multiple-VMM details.

2.3 Task 3.3 - CROSSCON New Trusted Services

The goal of this task is to design and implement new trusted services to enhance the security and functionality of the CROSSCON Stack. More specifically, the aim is to devise a set of novel trusted applications for deployment within the selected use cases to complement or enhance the security and privacy of IoT devices.

2.3.1 PUF Based Authentication

Related repositories:

- https://github.com/crosscon/ZK-PUF-Zephyr-Demo [8]
  This repository demonstrates how a novel trusted service can be built by encapsulating PUF interaction within a Trusted Application. The service integrates with GP's IPC and lifecycle management model, while remaining independent of the underlying PUF architecture or post-processing logic. Authentication is delivered through the ZK-PUF scheme. In this prototype the NXP LPC55S69 board, which exposes an SRAM-based PUF interface, despite the absence of native hardware and standardized TEE support. To overcome these limitations, the trusted service is hosted within a Zephyr RTOS VM on top of the CROSSCON Hypervisor, illustrating how novel trusted services can emerge even in constrained environments.
- https://github.com/crosscon/crosscon_puf_authentication [9]
  This repository contains the implementation of all three PUF-based authentication schemes provided as part of the CROSSCON stack (ZK-PUF, PAVOC, PAWOS). The schemes are provided as bare-metal applications for the NXP LPC55S69 board and are not considered Trusted Applications/Services.

2.3.2 Secure FPGA Provisioning

Related repositories:

- https://github.com/crosscon/UC5-IP_Protection_for_Secure_Multi-Tenancy_on_FPGA.git [10]

  This repository contains the final implementation of a Secure FPGA Provisioning system, integrated with the CROSSCON Hypervisor. It supports secure FPGA acceleration and protects intellectual property on FPGA-enabled SoCs within the CROSSCON software stack. The implementation follows GlobalPlatform specifications for both cryptographic functions and communication interfaces. A demonstrator is included, allowing client applications to configure and interact with virtual partitions in the FPGA fabric. The Trusted Application is isolated using the TEE provided by the CROSSCON Hypervisor.

- https://github.com/crosscon/FPGA_TEE [11]

  This repository contains the early proof-of-concept version of the Secure FPGA Provisioning system. It operates on bare metal, without CROSSCON Hypervisor integration. An additional branch is provided that incorporates enhanced cryptographic mechanisms to secure the partial bitstream.

2.3.3 Context Based Authentication

Related repositories:

- https://github.com/crosscon/context-based-auth-crosscon-demo [12]
  This repository contains a build system for the final version of the Context-based Authentication mechanism running on the CROSSCON Hypervisor. It includes an adapted version of OP-TEE OS to access the hardware primitives required by the service, and a Trusted Application which provides the authentication service.
- https://github.com/crosscon/context-based-auth-remote [13]
  This repository houses the remote authenticator counterpart for the TA. It contains the Machine Learning model which decides if two recorded fingerprints originate from the same environment and consequently decides if authentication succeeds or fails.

2.3.4 Remote Attestation

Related repositories:

- https://github.com/crosscon/remote-attestation-trusted-application [14]
  This repository contains the TA which client applications use to invoke the service, and a demo application for how to make calls to the trusted service. In addition, it links to the modified OP-TEE OS which is required for running the attestation itself.
- https://github.com/crosscon/remote-attestation-remote-verifier [15]
  This repository hosts the remote component of the remote attestation scheme. Given the evidence collected from within the TA, it decides if the target VM shows the intended behaviour.

2.3.5 Control Flow Integrity

Related repositories:

- https://github.com/crosscon/baremetal-tee [16]

  The control flow integrity service is integrated inside the Baremetal TEE for devices lacking MPU (BareTEE-noMPU), as detailed in the file [17].

2.4 Task 3.4 - CROSSCON TEE Toolchain

The goal of this task is to develop a toolchain that eases the design and implementation of Trusted Execution Environments (TEEs) and Trusted Applications (TAs).

Related repositories:

- https://github.com/crosscon/secure_update_consumer [18]

  This repository contains the code of the Firmware Consumer module for the CROSSCON Secure Update toolchain. It contains an extended version of the SUIT parser reference implementation supporting the update of multiple components, a Sofware Bill of Materials (SBOM) and the verification of a Behavioural Certification Manifest, alongside the CROSSCON API for the Secure Update.

- https://github.com/crosscon/secure_update_infrastructure [19]

  This repository contains some additional infrastructure for the CROSSCON secure update toolchain, including the extended manifest generator, the scripts for generating the proofs for some selected behavioural properties, a minimal implementation of Firmware and Verification Servers, a SBOM Verifier Server for on-demand vulnerability scanning, and a Status Server to collect update results from devices.

2.5 Task 3.5 - CROSSCON Bare-Metal TEE

The goal of this task is to design a software-based TEE for the bare-metal devices and implement it across multiple architectures.

Related repositories:

- https://github.com/crosscon/baremetal-tee [16]

  This repository contains two different versions of the CROSSCON Baremetal TEE, a Trusted Execution Environment for bare-metal devices. The first version (BareTEE-noMPU) is designed to work on hardware lacking any form of memory protection and is implemented for the MSP430 architecture. The second version (BareTEE-MPU) is designed to leverage the presence of an MPU (Memory Protection Unit) and is implemented for the ARMv7-M and the RISC-V architectures.

3 Conclusion

This report presents the final implementation of the work carried out in WP3 of the CROSSCON project and detailed in D3.3 “CROSSCON Open Security Stack Documentation – Final” [2]. In that document the CROSSCON Stack is covered in more detail, explaining the research results of the projects across the various WP3 tasks: TEE isolation and abstraction, hypervisor, new trusted services, toolchain and bare-metal TEE.

The listed software artifacts will continue to be refined and improved to support their usage and increase their maturity.

References

[1] **"CROSSCON Project Github Repository,"** [Online]. Available: https://github.com/crosscon. [Accessed August 2025].

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

[3] **CROSSCON**, "**D2.3** CROSSCON Open Specification - Final", N. Singh, 2025 March.

[4] **CROSSCON**, "**D5.5** Integrated CROSSCON Security Stack - Final Version", Y. Roelvink, 2025 August.

[5] **GitHub-CROSSCON** Hypervisor and TEE Isolation Demos, https://github.com/crosscon/CROSSCON-Hypervisor-and-TEE-Isolation-Demos

[6] **GitHub-CROSSCON** Hypervisor https://github.com/crosscon/CROSSCON-Hypervisor

[7] **GitHub-CROSSCON** Multi-vmm https://github.com/crosscon/multi-vmm

[8] **GitHub-CROSSCON** ZK-PUF Zephyr-Demo https://github.com/crosscon/ZK-PUF-Zephyr-Demo

[9] **GitHub-CROSSCON** PUF Authentication https://github.com/crosscon/crosscon_puf_authentication

[10] **GitHub-CROSSCON** UC5-IP_Protection_for_Secure_Multi-Tenancy_on_FPGA https://github.com/crosscon/UC5-IP_Protection_for_Secure_Multi-Tenancy_on_FPGA.git

[11] **GitHub-CROSSCON** FPGA TEE https://github.com/crosscon/FPGA_TEE

[12] **GitHub-CROSSCON** Context based auth CROSSCON demo https://github.com/crosscon/context-based-auth-crosscon-demo

[13] **GitHub-CROSSCON** Context based auth remote **https://github.com/crosscon/context-based-auth-remote**

[14] **GitHub-CROSSCON** Remote attestation Trusted application https://github.com/crosscon/remote-attestation-trusted-application

[15] **GitHub-CROSSCON** Remote attestation verifier https://github.com/crosscon/remote-attestation-remote-verifier

[16] **GitHub-CROSSCON** Baremetal TEE https://github.com/crosscon/baremetal-tee

[17] **Control Flow Integrity Service** (readme file) https://github.com/crosscon/baremetal-tee/blob/main/nonMPU-version/README.md.

[18] **GitHub-CROSSCON** Secure Update Consumer https://github.com/crosscon/secure_update_consumer

[19] **GitHub-CROSSCON** Secure Update Infrastructure https://github.com/crosscon/secure_update_infrastructure