CROSS-CON

Cross-platform Open Security Stack for Connected Devices

Project Overview

[Presenter, Organization]
[Location, Date]

Atos
UNIVERSITÀ DI TRENTO
Universidade do Minho
SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY
barbara
Julius-Maximilians-
UNIVERSITÄT WÜRZBURG
TECHNISCHE UNIVERSITÄT DARMSTADT
BEYOND SEMICONDUCTOR
3MDEB
CYSEC

October 2023

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Agenda

- Project Details
- Terminology
- Motivations
- Objectives
- Use-Cases
- CROSSCON Stack
- CROSSCON Approach
- Project Roadmap

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Details

- **Project Name:** Cross-platform Open Security Stack for Connected Devices
- **Project Call:** HORIZON-CL3-2021-CS-01
- **GA Number:** 101070537

- **Budget:** 4.6M €

- **Duration:** 36 Months (Nov-2022 to Oct-2025)

- **Consortium:** 10 Members (8 countries)
- **Project Coordinator:** Hristo Koshutanski (ATOS)
- **Scientific Coordinator:** Bruno Crispo (UNITN)
- **Exploitation Coordinator:** Aljosa Pasic (ATOS)

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Terminology

- **Open-Source Hardware (OSH)** - Hardware designs and specifications that are made freely available to the public under an open-source license;
- **Heterogeneous devices** - Collection of devices or components within a system that differ from one another in terms of their hardware architecture, capabilities, or characteristics.
- **Trust** - Level of reliability and assurance that a device possesses to ensure different security primitives;
- **Root-of-Trust (RoT)** - The foundational and most trusted element in a computing system, serving as the starting point of the Chain-of-Trust;
- **Chain-of-Trust (CoT)** - A sequence of trusted relationships established between different components within a device;
- **Trusted Services** - A set of secure and reliable mechanisms designed to enhance the security, privacy, and trustworthiness of devices and applications, e.g., device authentication, secure firmware updates, remote attestation, etc;

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Terminology

- **Security Stack** - A set of software/hardware technologies designed and deployed to protect a device against cybersecurity threats;
- **Interoperability** - The ability of different systems, devices, or software to work together and exchange information seamlessly;
- **Formal Verification** - A method that uses mathematical approaches to prove the correctness of hardware or software systems;
- **Toolchain -** A set of software development tools that are used to perform a specific task or to build a particular type of software for a target device;
- **Trusted Execution Environment (TEE)** - A secure and isolated environment within a device where critical operations can be executed with a high-level of confidentiality and integrity;
- **Hypervisor** - A software layer that creates and manages multiple isolated execution environments (virtual machines) on a device;

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Motivations

Cross-platform Open Security Stack
CROSS-CON
for Connected Devices

Lack of Open-Source Hardware Solutions

- Most IoT solutions rely on proprietary hardware with closed-source licence, limiting innovation and collaboration;
- **Open-source hardware promotes transparency, fosters creativity, and drives advancements;**

Lack of Root- and Chain-of-trust

- Current IoT devices lack robust and complete Root-of-Trust and Chain-of-Trust, posing significant security risks;
- **Establish a robust security foundation for IoT ecosystems fosters trustworthiness among users and stakeholders;**

Lack of Interoperability Between IoT Devices

- Due to the wide spectrum of heterogeneous devices, current IoT devices often struggle to communicate effectively with each other;
- **Device interoperability ensures seamless connectivity across the network;**

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Motivations

Cross-platform Open Security Stack
CROSS-CON
for Connected Devices

High Costs of Developing Trusted Services

- Developing a secure IoT service might require significant investments (e.g., in specialized hardware), advanced security expertise, and extensive testing processes. High costs can become prohibitively expensive for small startups or organizations with limited resources, hindering their ability to enter the market.
- **Through open, modular, and cost-effective IoT security solutions, trusted service development becomes accessible to a broader audience, fostering innovation across various applications.**

Vulnerabilities in Core Trust Components

- Security flaws in crucial trusted components could undermine the reliability of IoT systems;
- **By strengthening the key trusted components, we are creating the path to a more secure and reliable IoT landscape;**

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Objectives

1. **CROSSCON** envisions a secure ecosystem where security starts at RoT and extends to all CoT components;

2. **CROSSCON** strengthen memory protection and isolation in both new and existing TEEs, mitigating the impact of cybersecurity threats;

3. **CROSSCON** enhances trusted services offered by TEEs;

4. **CROSSCON** deliver a toolchain with lightweight techniques for security assurance;

5. **CROSSCON** establish a security approach by tackling CoT issues and designing a new **open, modular, highly portable, and vendor independent** IoT security stack that can run on a wide range of devices;

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Use-Cases

UC1: Device Multi-Factor Authentication

Single-Factor Authentication (SFA) only uses one credential/method for the authentication process, e.g., username/password, pin code, etc.

Passwords alone can pose significant security risks, as they can be easily compromised through phishing or man-in-the-middle attacks (MITM). This underscores the importance of enhancing security, and introducing Multi-Factor Authentication (MFA) schemes.

Multi-Factor Authentication (MFA) traditionally authenticate access with two or more factors which could include:

- Something you have (e.g., Smart card, tokens);
- Something you are (e.g., Biometrics);
- Something you know (e.g., Passwords);

CROSSCON aims at introducing new authentication methods based on context and behavioral authentication.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Use-Cases

UC2: Firmware Updates of IoT Devices.

Keeping IoT devices secure is closely tied to the vital process of **updating their firmware,** which is usually performed via the Internet. Typically, these updates come in two main flavors:

- **Full Updates:** Which completely replace the device's firmware;
- **Partial Updates:** Which modify specific sections of the firmware instead of applying changes to the entire firmware version;

Such updates must be performed securely, otherwise malicious or patched software can intentionally create or open several vulnerabilities and risks.

CROSSCON aim to cover secure firmware updates Over-The-Air (OTA).

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Use-Cases

UC3: Commissioning and Decommissioning of IoT devices.

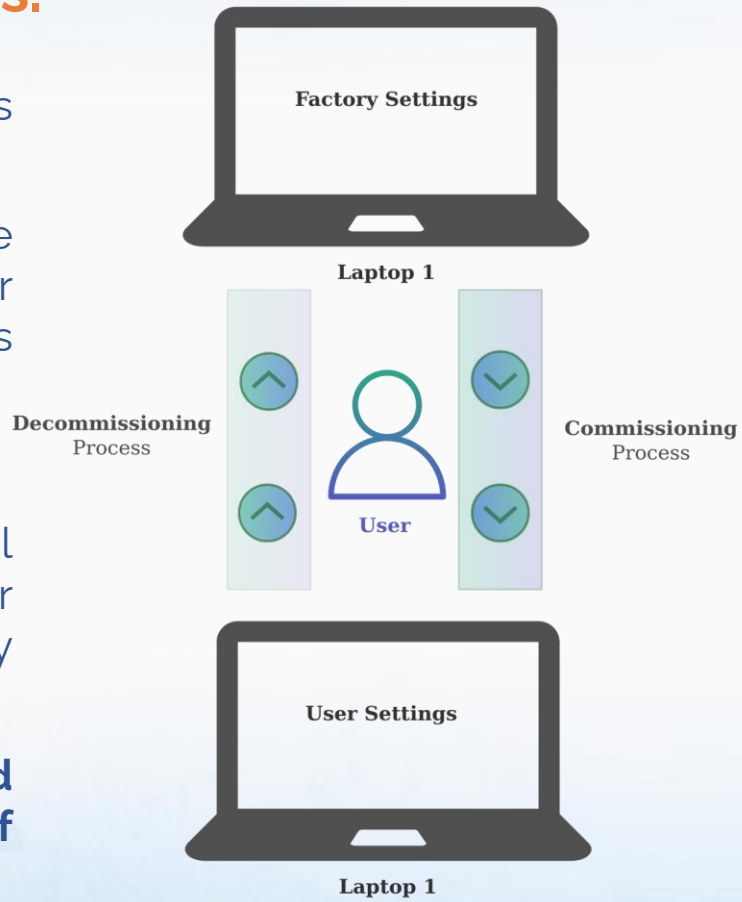
When setting up an IoT device, it's important to go through a commissioning process to ensure proper operation:

- **IoT Device Commissioning** is the process by which connected devices acquire the necessary information and configuration parameters for their intended use or application. Commissioning is a critical step in the IoT device lifecycle and needs to happen before the device starts.

By its turn, the decommissioning process restores the device to its original state:

- **IoT Device Decommissioning** is the process of returning the device to its original state when it is no longer in use or is repurposed for a different customer or purpose; Decommissioning is particularly crucial for industrial devices that may contain sensitive information.

CROSSCON is committed to implementing robust commissioning and decommissioning procedures for applications, ensuring the highest levels of security and reliability in IoT device operations.



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Use-Cases

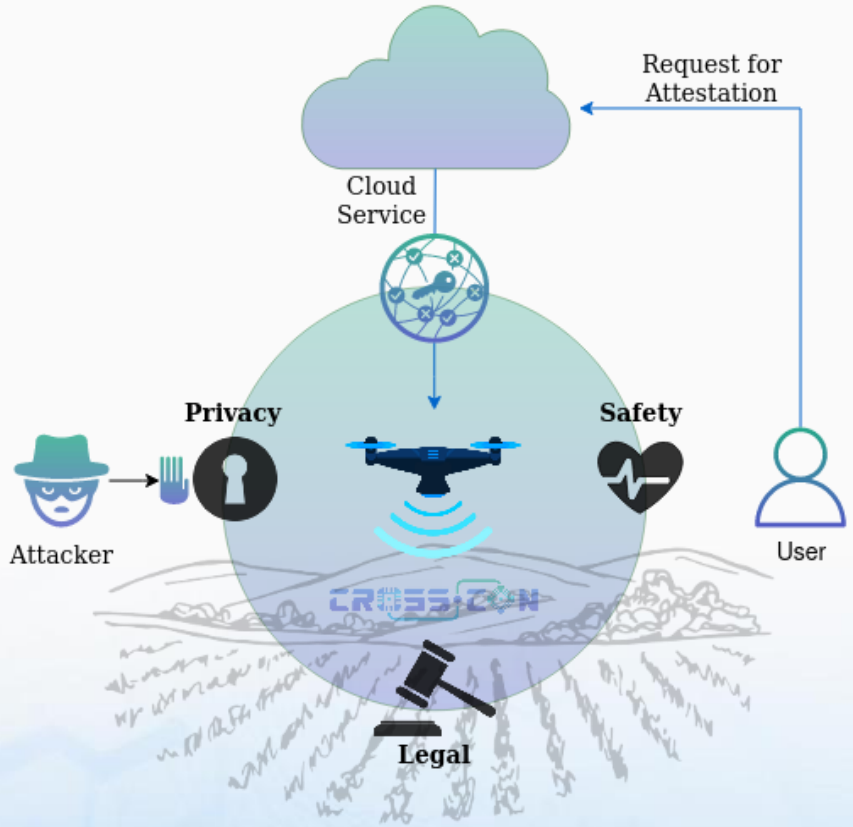
UC4: Remote Attestation for Identification and Integrity Validation of Agricultural Unmanned Aerial Vehicles (UAVs)

Agricultural UAVs are essential for helping farmers in several tasks, e.g., seeding, fertilizing, irrigating, and pest controlling. Nevertheless, they also bring several privacy- and safety-related challenges and concerns within the realm of agricultural UAVs.

Remote attestation: is a method by which a client authenticates it's hardware and software configuration to a remote host.

Using remote attestation, a user can ensure that a UAV is running a trusted software and hardware stack that meets the necessary **privacy**, **safety,** and **legal** requirements.

CROSSCON will provide secure remote attestation on agricultural UAVs.



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Use-Cases

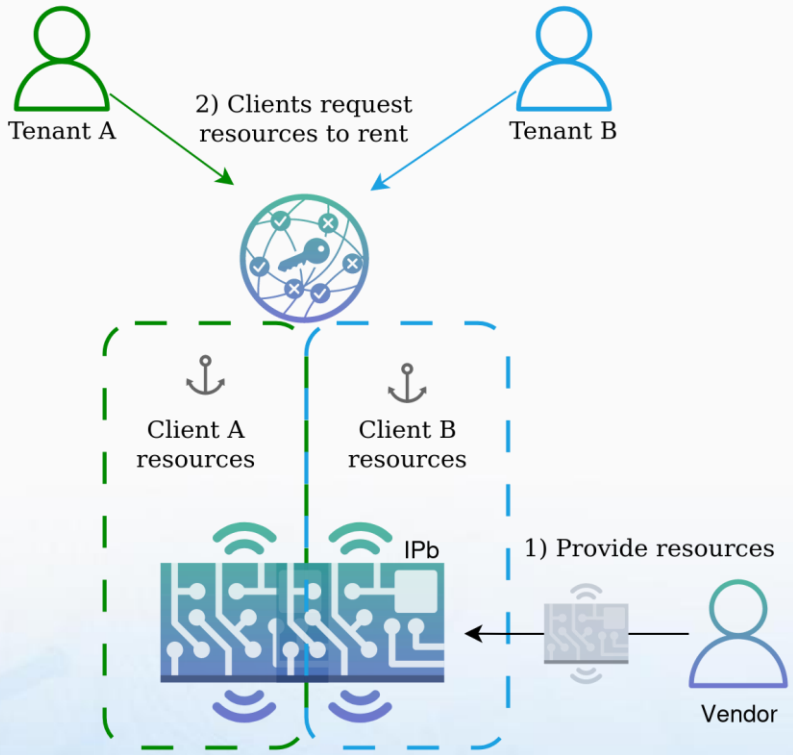
UC5: Intellectual Property Protection for Secure Multi-Tenancy on FPGA

Reconfigurable technology supports compute-intensive tasks. To optimize resource usage, multiple clients (i.e., tenants) can share the **reconfigurable platform**.

Thus, these resources must be temporal and/or spatial isolated:

- **Temporal**: Only one tenant has access resources at a time;
- **Spatial**: Tenants have access to resources simultaneously;

CROSSCON will provide secure multi-tenancy, assuring that the workload of one tenant cannot interact with others (or affect the hardware resources), also ensuring that no data can be leaked by any means.

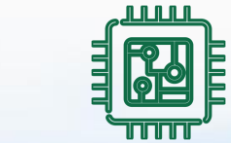


This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

CROSSCON Stack

CROSSCON Stack Overview:

- Extends **interoperability** across heterogeneous devices;
- Offers a unified level of **abstraction** across **multiple hardware platforms**;
- Enriches existing **security** features by adding **new trusted services**;



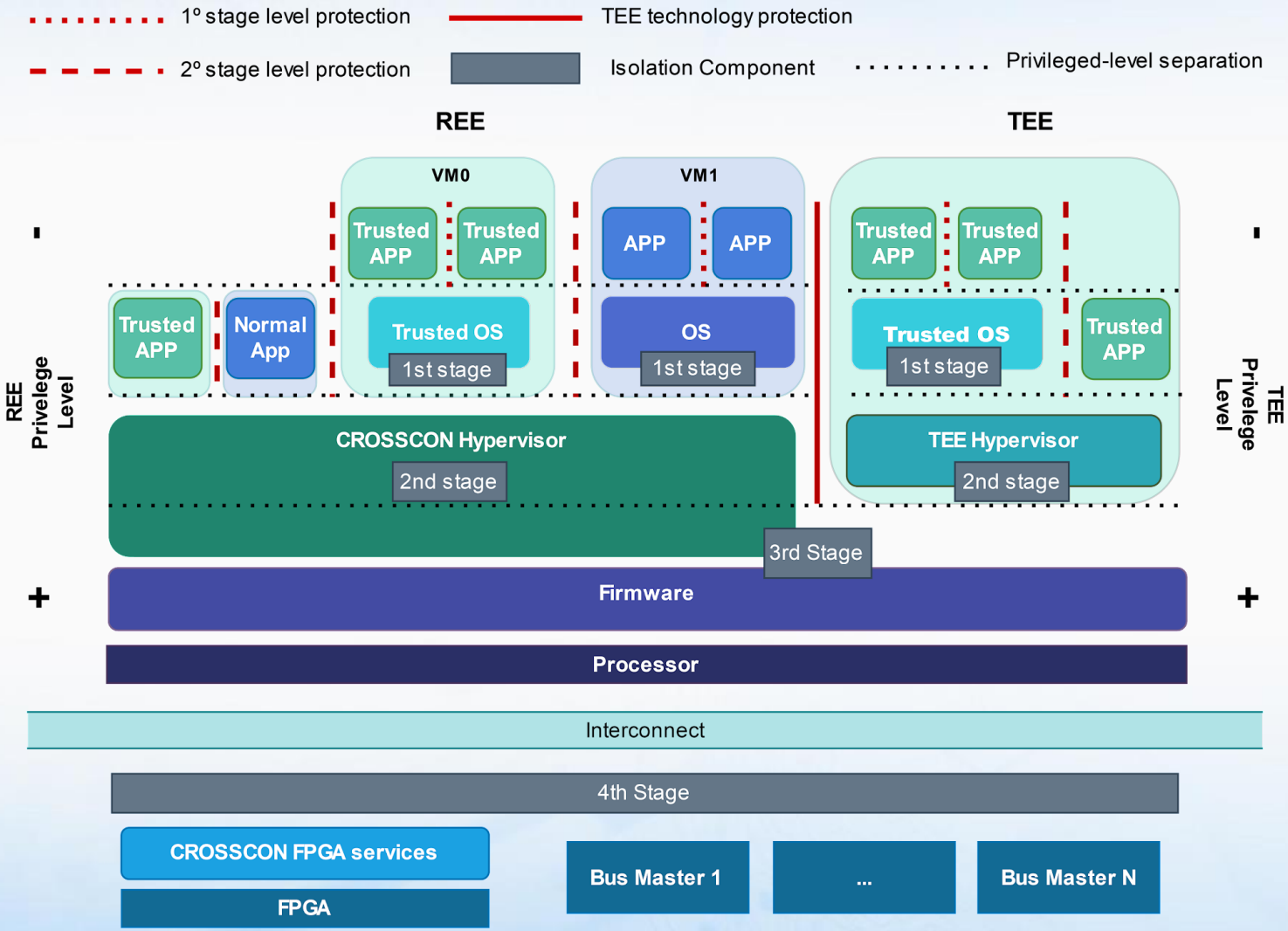
CROSSCON SOC

Trusted Services

CROSSCON Hypervisor

CROSSCON TEE

HW Security primitives

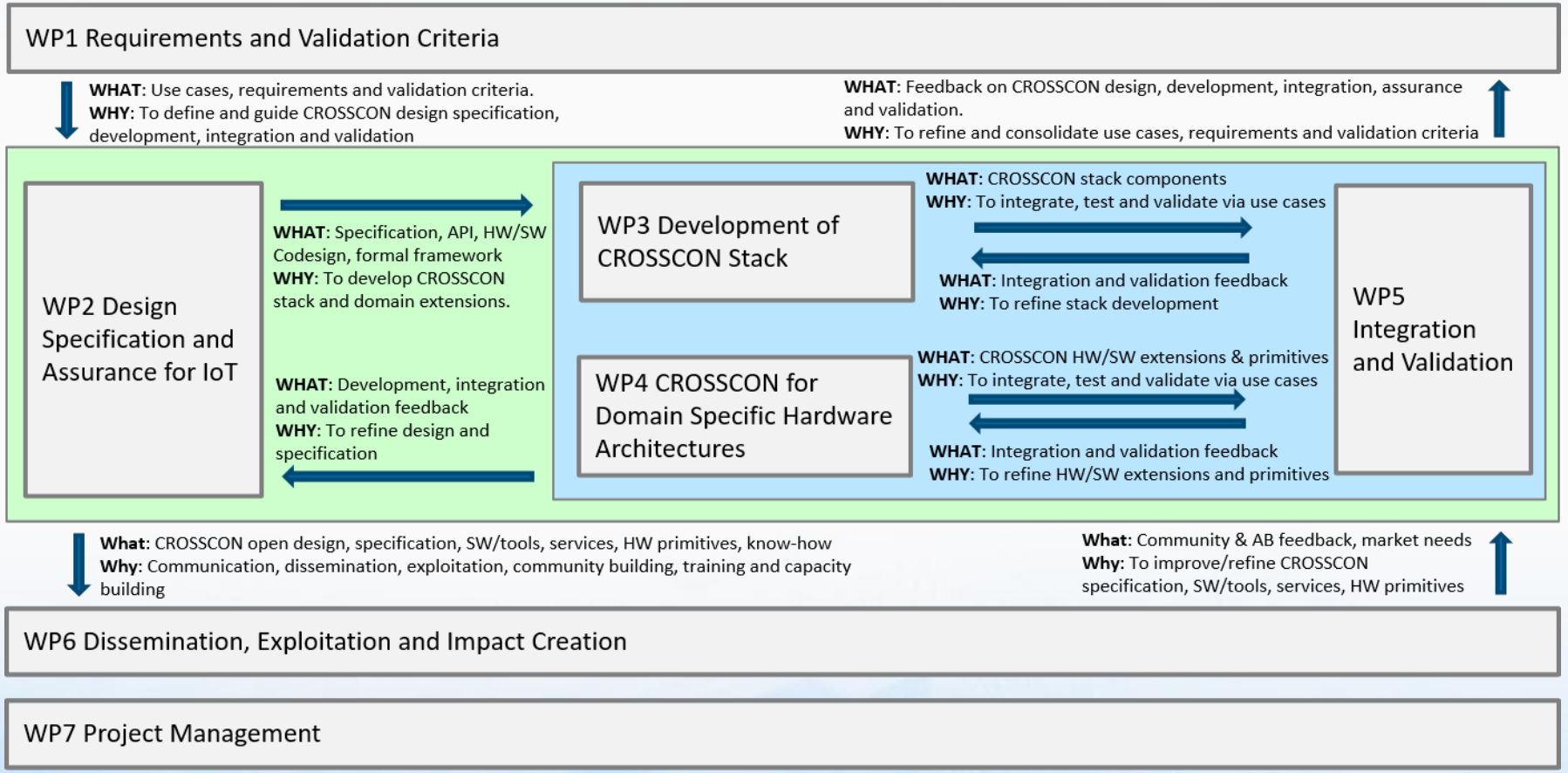


This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

CROSSCON Approach

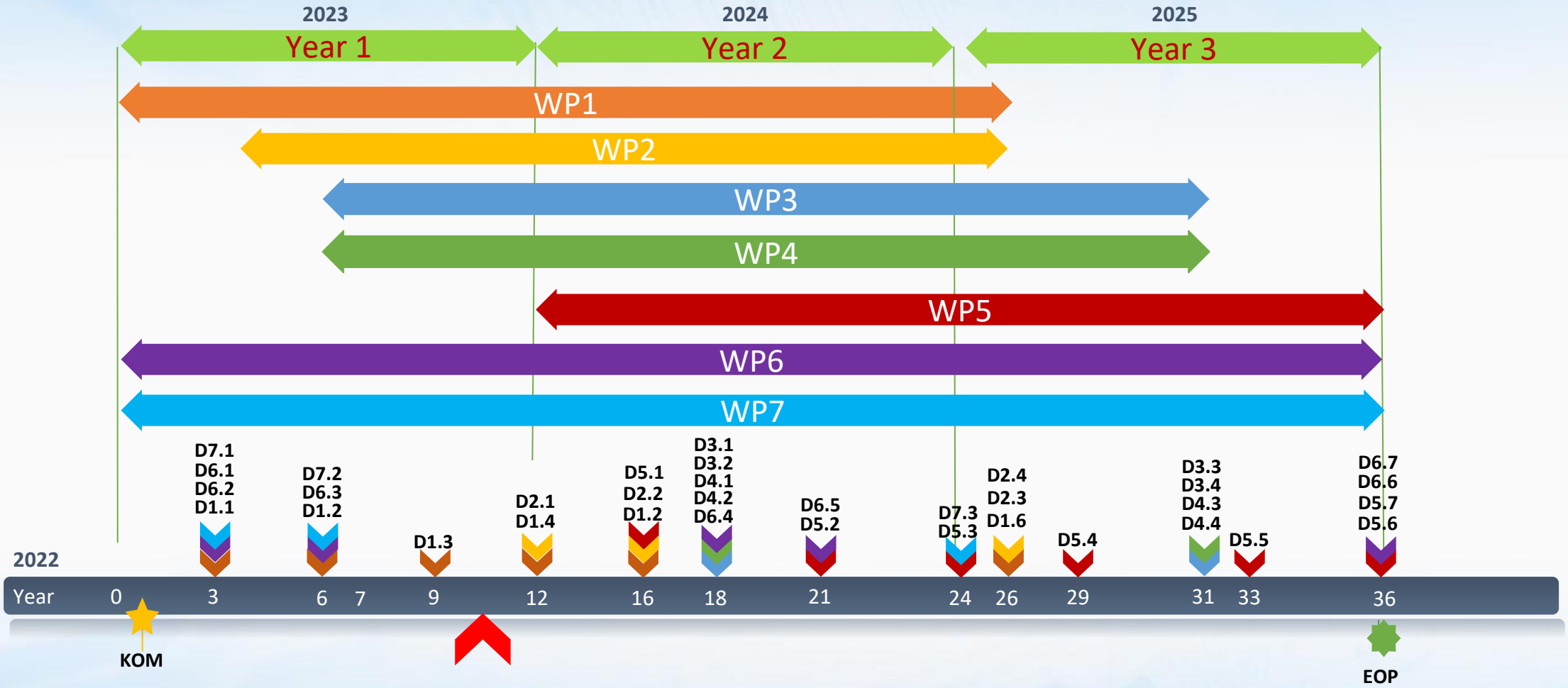
7 Work Packages (WPs) allocated to different leaders:

- WP1 Leader: ATOS
- WP2 Leader: UNITN
- WP3 Leader: UMINHO
- WP4 Leader: BEYOND
- WP5 Leader: SLAB
- WP6 Leader: ATOS
- WP7 Leader: ATOS



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Project Roadmap



Check progress and Deliverables: https://crosscon.eu/library/deliverables

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Get in touch:

contact@crosscon.eu

in/crosscon

www.crosscon.eu

@crosscon_eu

SCAN FOR MORE!

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Cross-platform Open Security Stack

CROSS-CON for Connected Devices

Thank You!

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537