Cross-platform Open Security Stack for Connected Devices

PRESS RELEASE

OCT 2025

Successful Integration of CROSSCON Use Cases

The CROSSCON project has successfully implemented and integrated its five use cases, validating the interoperability and scalability of its open and secure IoT stack. These final demonstrations mark a significant step toward enhancing trust, transparency, and interoperability across heterogeneous connected devices and computing environments.

Advancing Security Across IoT Domain

Using the project's results, partners have validated a comprehensive set of security mechanisms across five diverse use cases, showcasing the adaptability of the CROSSCON stack to real-world conditions.

- UC1 - Device Multi-Factor Authentication: Demonstrates trusted second-factor authentication for IoT devices with varying capabilities. Two scenarios were implemented: a PUF-based factor for verifying low-end to high-end devices and Context-Based Authentication (CBA) for high-end ones. Both highlight the adaptability of CROSSCON's multi-factor authentication mechanisms.
- UC2 - Firmware Updates of IoT Devices: Showcases authenticated and tamper-proof firmware delivery in heterogeneous environments. A dual-environment design separates update logic from cryptographic operations, ensuring both integrity and confidentiality throughout the device lifecycle.
- UC3 - Commissioning and Decommissioning of IoT Devices: Illustrates secure onboarding and retirement processes using unique cryptographic credentials. Credentials are protected against unauthorized access and securely erased upon decommissioning, ensuring forward security and reliable lifecycle management.
- UC4 - Remote Attestation for Identification and Integrity Validation of Agricultural UAVs: This use case leverages the payload segregation from the CROSSCON Hypervisor and its integrated Remote Attestation (RA) service to verify the identity and integrity of agricultural UAVs, even under limited connectivity, supporting secure autonomous operations.
- UC5 - Intellectual Property Protection for Secure Multi-Tenancy on FPGA: Demonstrates secure FPGA provisioning in multi-tenant environments. By supporting partial reconfiguration, CROSSCON enables dynamic and trusted sharing of FPGA resources while protecting users' intellectual property.

Integration and Availability

The successful integration of all five use cases confirms the CROSSCON security stack as a flexible, open, and vendor-independent solution applicable to diverse hardware and software environments. Detailed implementation architectures and final descriptions are documented in deliverable D5.5.

[1] **https://github.com/crosscon**

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