

# CERTIFY NEWSLETTER #4

WWW.CERTIFY-PROJECT.EU



July 30, 2024

## Top News

Collaborations with EU funded research projects and Deliverables.

## CERTIFY

defines a methodological, technological, and organizational approach towards IoT security lifecycle management based on

- security by design support
- continuous security assessment and monitoring
- timely detection, mitigation, and reconfiguration
- secure Over-The-Air software update
- steady security information sharing





## Newsletter Highlight

We had our 3rd plenary meeting of the project on 21-22 February 2024 organized by Collins Aerospace in Cork. The meeting was chaired by our project coordinator and joined by all partners physically and remotely. Each Project partner presented its relevant tasks, deliverables and milestones.

## Inside The Issues

- 3rd Plenary project meeting in Cork organized by Collins Aerospace

---

- Collaboration with the EU research projects

---

- Deliverables submitted since the last newsletter

---

“Many IoT devices come with the username “admin” and a common, guessable password. That means any preset password needs to be changed. This issue must be addressed by manufacturers but will also require more vigilance on the part of consumers”

**Ryan Barnett**

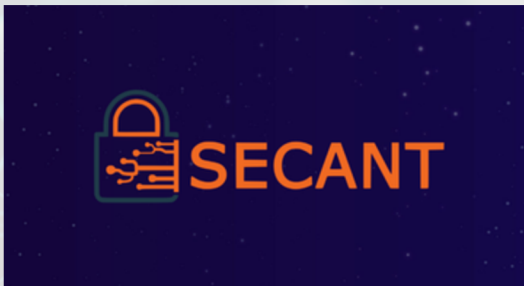
# COLLABORATION

Collaboration among R&D projects is crucial to optimize effect, foster innovation, and expedite advancement in the R&D ecosystem. When researchers work together with other efforts to pool diverse perspectives, resources, and talents, they can better handle challenging situations. Our goal in working together with other EU-funded initiatives has been to take advantage of synergies and jointly communicate outcomes.



PUZZLE is a project funded by the EU's Horizon 2020 research and innovation programme, which consists of thirteen partners representing research institutes, universities, technology providers, infrastructure providers (and users) and industrial partners (including eight SMEs & MEs) from eight EC member states and associated countries. PUZZLE will implement a highly usable cybersecurity, privacy and data protection management marketplace targeted at SMEs & MEs that enables them to monitor, forecast, assess and manage their cyber risks through targeted cybersecurity services, increase their cybersecurity awareness.

The vision of CONNECT is to address the convergence of security and safety in CCAM by assessing dynamic trust relationships and defining a trust model and trust reasoning framework based on which involved entities can establish trust for cooperatively executing safety-critical functions. The CONNECT Trust Management framework is the basis that models and captures the trust relationships of the next generation CCAM systems. CONNECT's new safety paradigm is a key element in bringing autonomous driving to a completely new level of trustworthiness and is expected to lead to long-term consumer acceptance as a result.



The SECANT platform will enhance the capabilities of organisations' stakeholders implementing (a) collaborative threat intelligence collection, analysis and sharing; (b) innovative risk analysis specifically designed for interconnected nodes of an industrial ecosystem; (c) cutting-edge trust and accountability mechanisms for data protection. Ultimately, SECANT will contribute decisively towards improving the readiness and resilience of the organisations against the crippling modern cyber-threats, increasing the privacy, data protection and reducing the costs for security training in the European market.

The ECCO project, responding to the call for tenders CNECT-2022-OP-0033, received funding from the Digital Europe Programme (Cybersecurity WP2021-22) to support the activities necessary to develop, promote, coordinate and organize the work of the Cybersecurity Competence Community at European Level, within the scope and operations of the ECCC and National Coordination Centres Network. ECCO held its first kick-off meeting to delve deeper into ECCO's core tasks and to present its execution and achievement strategy on Wednesday the 25th January.



"SecOPERA aims to provide a one-stop hub for complex OSS/OSH solutions delivering to a connected device designer, implementer and operator as well as any open-source software/hardware developer, the means to analyse, assess, secure/harden and share open-source solutions as those are integrated in an overall complex product developed for a networked connected environment. The SecOPERA hub offers to the open-source community a framework supporting the open-source DevSecOps lifecycle and generates secure open-source solutions along with appropriate, verifiable security guarantees."



# DELIVERABLES

## Deliverable D3.1

Deliverable 3.1 introduces the core components of the CERTIFY infrastructure services, primarily aligned with the requirements of WP3, which is dedicated to designing and implementing tools and services essential for ensuring the secure operation and lifecycle management of the system. A central pillar of this infrastructure is the Privacy-Preserving Cyber Threat Intelligence Sharing (PP-CTI) system, responsible for anonymising sensitive data attributes in cyber threat reports. It provides an interface for the Malware Information Sharing Platform (MISP) for secure and private threat information sharing.



## Deliverable D4.1

WP4 aims to enhance IoT security by designing and implementing solutions that improve authentication, data authentication, and secure storage. It utilizes a Secure Element (SE) and the Embedded Secure IoT Development Toolkit API. Additionally, it leverages the RISC-V open ISA for comprehensive IoT security lifecycle management. These enhancements target a generic IoT device, with the goal of bolstering its security services and reducing vulnerability to cyber threats. WP4's approach integrates cryptographic support and utilizes the RISC-V open ISA for enhanced security throughout the device's lifecycle.

## Deliverable D5.1


Deliverable D5.1 outlines the architecture of the CERTIFY Software Platform and the design and initial implementation of modules within the CERTIFY Security Domain. It integrates contributions from WP5 tasks: T5.1 Advance Bootstrapping and improve communication, T5.2 Bootstrapping and runtime monitors, and T5.3 IIoT-based Intrusion Detection System and Security Information and Event Management (SIEM). The design phase begins with activities in WP1 (Use Cases analysis and Lifecycle management) and WP2 (System Architecture, Integration, and Validation), establishing functionalities, requirements, and use cases.



# ABOUT US



## aCtive sEcurity foR connectEd devlces liFecYcles

OCT 2022 | SEP 2025 

### Project Partners



### FIND US ON

- [WWW.CERTIFY-PROJECT.EU](http://WWW.CERTIFY-PROJECT.EU)
- [WWW.TWITTER.COM/CERTIFY\\_PROJECT](https://WWW.TWITTER.COM/CERTIFY_PROJECT)
- [WWW.LINKEDIN.COM/COMPANY/CERTIFY-PROJECT](https://WWW.LINKEDIN.COM/COMPANY/CERTIFY-PROJECT)



This project has received funding from the European Union's Horizon CL3 Increased Cybersecurity 2021 under grant number agreement number 101069471 and from the Swiss State Secretariat for Education, Research and Innovation (SERI) under grant agreement numbers 22.00165 and 22.00191