

RESEARCH PROJECT



www.certify-project.eu

aCtive sEcurity foR connecTed devlces liFecYcles



WHAT IS “CERTIFY”?

CERTIFY is a consortium research project with 12 partners from 8 countries. It offers a comprehensive approach for managing the IoT security lifecycle, including security by design, continuous assessment and monitoring, timely detection and mitigation, secure OTA updating, and information sharing. CERTIFY ensures high-level security for IoT stakeholders.

CERTIFY defines a methodological, technological, and organizational approach towards IoT security lifecycle management based on (i) security by design support, (ii) continuous security assessment and monitoring, (iii) timely detection, mitigation, and reconfiguration, (iv) secure Over-The-

Air (OTA) update, and (v) continuous security information sharing.

The CERTIFY project will validate IoT architecture against state-of-the-art use cases and pave the way for innovative security throughout the lifecycle of IoT environments.

OBJECTIVES

CERTIFY has SMART (Specific, Measurable, Achievable, Realistic and Timely) specific objectives:

- Cybersecurity awareness for IoT-enabled environments through a multi-stakeholder sharing of threats and mitigations.
 - Secure reconfiguration and maintenance of customizable embedded devices by means of hardware primitives and services.
 - Perform security operational management based on bootstrapping and monitoring of attacks and malicious behaviors.
 - Run time security compliance and continuous certification methodology via objective metrics.
 - Foster knowledge delivery via wide dissemination, capacity building and supporting activities. Build a robust exploitation plan to boost ROI by optimizing current and future EU cybersecurity capabilities.
 - Industrial validation of the CERTIFY framework in IoT ecosystems.
-



AMBITIONS

The main contributions of CERTIFY are as follows, going beyond the state of the art:

- A) Novel framework to manage security throughout the lifecycle of the IoT device.
- B) Certification & security evaluation.
- C) Enhanced open hardware security.
- D) Secure integration of IoT devices.
- E) Behavioural profile
- F) Security monitoring & detection.
- G) Information sharing and upgrading.

PILOTS

PILOT II:
Smart Micro-Factories

Pilot Partners:
DWG (lead), UMU

PILOT I:
Secure Management
of Devices Enabling an
Intelligent and
Connected Aircraft Cabin

Pilot Partners:
Collins (lead), TUp
ST-I

PILOT III:
Tracking and monitoring
of artworks

Pilot Partners:
ST-I (lead), UZH
MOD

PROJECT COORDINATOR

Name : Antonio Skarmeta

Email : skarmeta@um.es

About Coordinator : Full Professor at University of Murcia in the Department of Information and Communication Engineering

FUNDING



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



CERTIFY PARTNERS



Universität
Zürich^{UZH}

TrustUP
A PARTHENOPE UNIVERSITY SPIN-OFF



LinkedIn



Website



Twitter



YouTube

