

# CERTIFY NEWSLETTER #3

[WWW.CERTIFY-PROJECT.EU](http://WWW.CERTIFY-PROJECT.EU)



June 26, 2024

## Top News

Technical advancements in  
the project

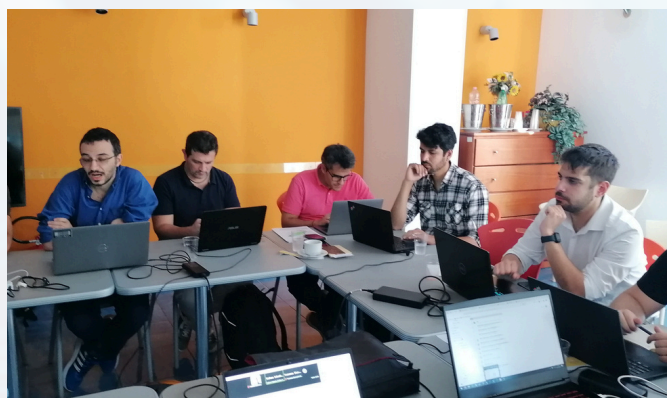
---

Certify Framework, Life-cycle  
Management, Risk Assessment  
and Recertification

## 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 2nd plenary meeting of the project on 03-04 October 2023 organized by Trust Up in Procida. 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

- The CERTIFY framework for managing cyber security of network connected devices
- Advancement Over Current Practices to Security Lifecycle Management
- Security Assessment and Recertification
- A researcher's and a reader's view on CERTIFY

### Featured Reader

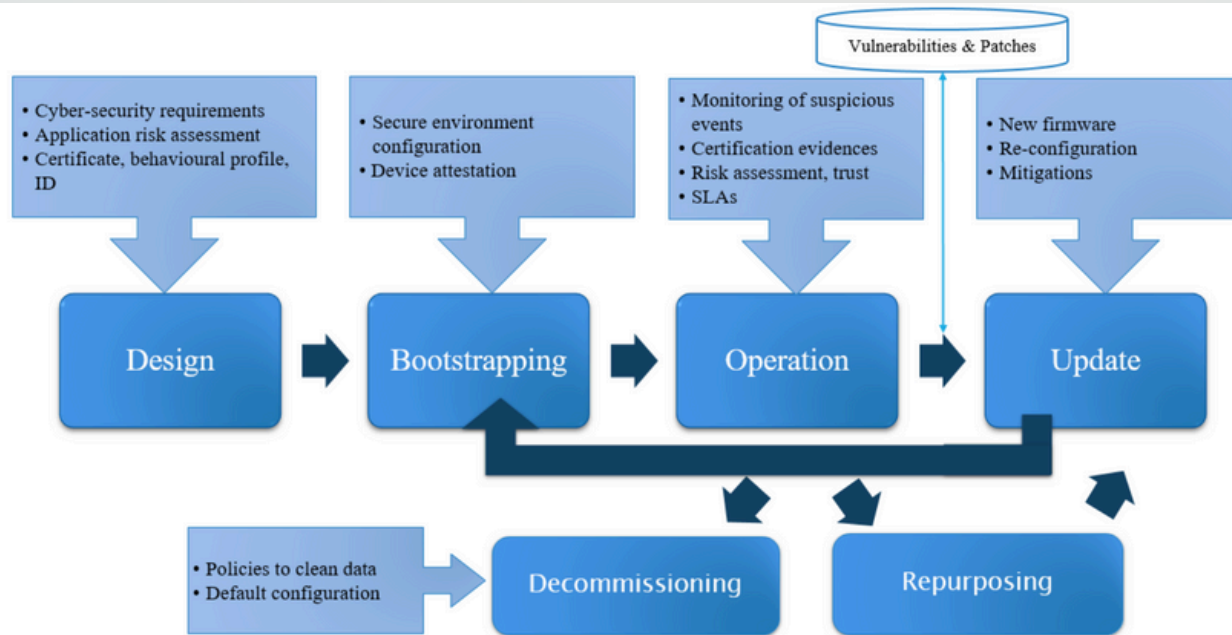


### Kai Michael Hermesen

He is an expert in cybersecurity, digital responsibility, trust in digital technologies, ecosystem building and leadership within this space. He is also a member of the World Economic Forum "Digital Trust" working group.



# CERTIFY FRAMEWORK



The CERTIFY framework provides a comprehensive approach to securing IoT devices throughout their lifecycle. In the **design phase**, it meticulously collects cybersecurity requirements and devises a sensitive evaluation methodology, ensuring devices are equipped with proven authentication and cryptographic protocols. The **bootstrapping phase** characterizes the change of the device state to operational. At this stage, the design-time configurations are exploited to enroll the device in the network and build a secure environment for running the applications. Network and device identities defined in the design phase are used for mutual authentication. For the **operation phase**, CERTIFY implements intrusion detection systems and continuous security assessments, with local trust management dynamically computing trust scores and ensuring adherence to service level agreements. Threat intelligence services and privacy-preserving techniques bolster data protection and response capabilities. Throughout the **update phase**, remote inventory and over-the-air (OTA) security patching are facilitated, with blockchain ensuring transparent ledger management of software updates. If devices cannot meet security requirements or pose significant risks, they are **decommissioned** to prevent information leaks and restore default configurations. The CERTIFY framework's adaptability allows it to address evolving threats and vulnerabilities, with continuous assessment ensuring devices remain resilient.



12

Research Partners

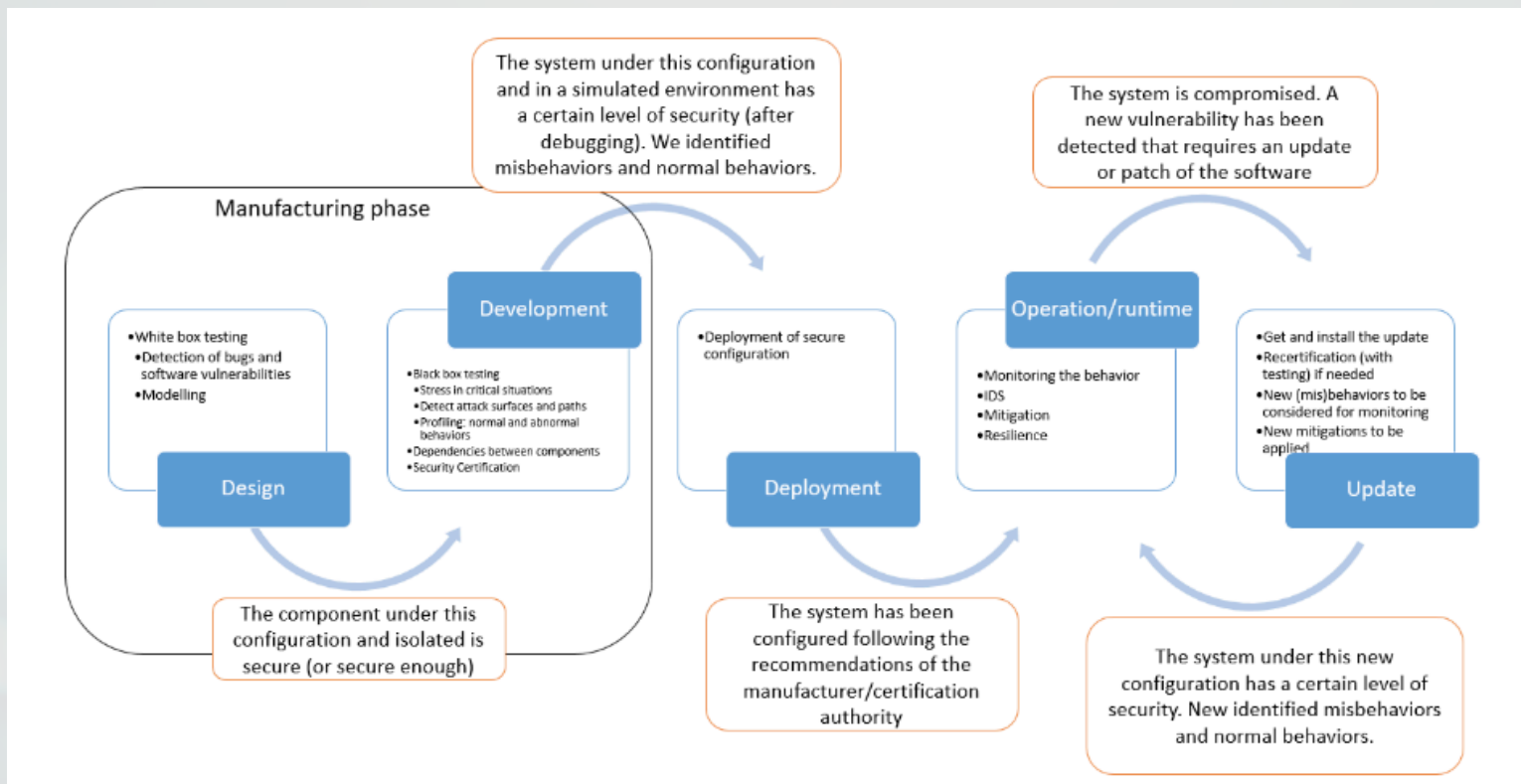
8

Countries

36 M

Project duration

# LIFECYCLE MANAGEMENT



The development of IoT-enabled services requires a comprehensive management of security aspects throughout the lifecycle of IoT devices. Because of recent technological advancements, such devices are composed of an increasing number of software components to provide advanced functionality and to create new data-driven services. Therefore, such devices should be equipped with mechanisms to adapt themselves to security changes throughout their lifecycle. Indeed, the new regulation named EU Cybersecurity Act emphasizes the need for security approaches addressing the lifecycle of any ICT product, service, or process for the definition of a cybersecurity certification framework.

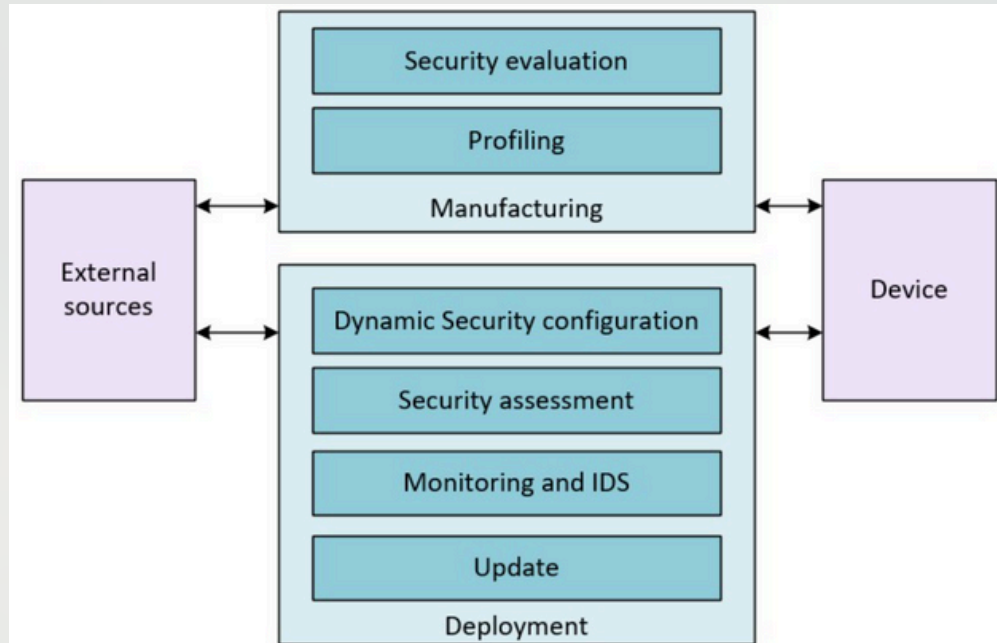
To ensure the security compliance throughout the lifetime of the device, we propose the design and implementation of the CERTIFY cybersecurity lifecycle management framework for IoT devices. The framework is intended to monitor, update, assess and configure the device security according to the security information received both internally (self-assessment, monitoring) and externally (e.g., manufacturer, threat databases, certification authority). At the same time, the framework will share the relevant security information with the external sources, in a symbiotic way.



# LIFECYCLE MANAGEMENT

## Design and Development:

The device's lifecycle begins when it is manufactured to be later installed and commissioned within a network. In this phase, the device is designed, created, programmed and tested, so the initial level of security is established.



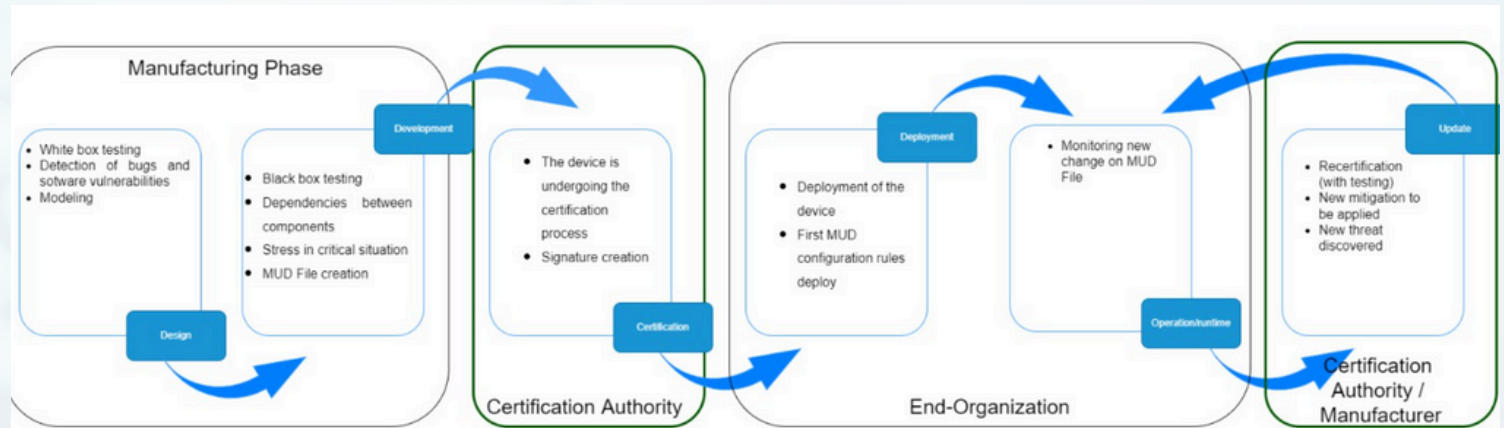
**Bootstrapping/Deployment:** The bootstrapping phase starts when the device is installed and configured in a certain context. This process usually consists of a set of procedures in which a device joins a network in a certain domain (health, house, industry etc.). During the bootstrapping, the cryptographic material statically configured during manufacturing in the device is used to derive dynamic credentials and keys to be used during its operation.

**Operation:** During the operation stage, the device is providing the functionality for which it was manufactured. In this phase, the device should be monitored, since new security vulnerabilities can be discovered or a new patch/update can be installed, and consequently, the device's security level can be modified.

**Update:** This stage may involve procedures related to software updates or patches proposed by the manufacturer, as well as configuration tasks requested by the owner, also influencing the security level offered. In particular, the realization of a secure update/patching process requires suitable protection of software images, so that only legitimate and authorized software providers are enabled to update a certain device through a secured software.

# SECURITY ASSESSMENT AND RECERTIFICATION

The methodology and associated framework proposed by CERTIFY covering the complete lifecycle management of the IoT security, will allow a dynamic security assessment covering from the generation of the behavioral profiles as a result of the manufacturer testing and risk analysis and the certification process, the bootstrapping with the enforcement of the security context and associated policies derived from the profile, up to the monitoring of the behavior of the IoT and possible mitigation in operational phase that could be based on reactive actions or possible updates, or in the worst case the decommissioning to request a re-certification process.



CERTIFY proposes to inherit from actual EU cybersecurity certification framework and enhance its procedures in different areas:

- Usage of the certification information as a baseline for the secure bootstrapping and enrollment of components in customer's premises
- Integrate the certification process associated to the component with its lifecycle and the security management in the IoT device
- Contribution to the (re)certification process as consequence of the operational behavior of components in the daily life of the IoT device
- Propose an enrichment of the certification process creating an extended MUD (behavioral profiles) framework solution that can be used for different assets and that provides:
  - Security context/behavior in which the assets need to be deployed to fulfill the security properties already certified by a certification authority.
  - A solution to allow the distribution of future mitigation mechanisms in case a new vulnerability emerges, providing access to MUD updates using the Threat MUD mechanism.
  - A procedure to be proposed as part of the EU cybersecurity certification framework with recommendations based on the experience.

In a nutshell, CERTIFY is like a watchdog that makes sure that certified IoT devices are maintaining their level of assurance during the whole lifecycle. Since the onboarding phase, CERTIFY provides to domain owners the information to securely configure the device and use it in the intended operational environment. During operations, it does so by collecting threats and dispatching mitigation (through the extended MUD file) in case a change occurs. In case such a change impacts the certification status, authorities and manufacturer can exploit the information sharing enabled by CERTIFY.



# Baseline for a Security (Re-)Certification

---

In the context of IoT devices by following the approach outlined above, a baseline for security (re)certification could include the following:

**Current Certification Status:** The initial state of the IoT device's certification is essential. The baseline needs to consider if the device is currently certified and under what standard or requirements and profile. This would include any existing certification documentation or reports, including the security controls and policies currently implemented. In CERTIFY, an extended version of the MUD file will be used to describe security profiles and the context where the device is expected to be used.

**Behavioral Profile:** The baseline should detail the security requirements and standards that the device is supposed to comply with. These could be industry standards or specifications, regulatory requirements, or best practice guidelines. The specific requirements will likely vary based on the type of device and its intended use. Therefore, CERTIFY will provide different behavioral profiles according to the required security level.

**Threat Modeling and Risk Assessment:** A threat model for the IoT device placed in an operational environment should be created, which outlines potential threats, their severity, and the controls in place to mitigate them. The risk assessment should also be part of the baseline, documenting the risks associated with the IoT system and how they are managed. In CERTIFY, the threat MUD will be adapted to share security information on threats and mitigation.

**Change Impact Analysis:** As changes occur, an impact analysis should be conducted to understand how these changes might affect the security of the IoT device. This analysis should examine the potential impact of any change on the security controls and policies in place. The CERTIFY methodology envisions a continuous impact assessment by including knowledge external and internal to the domain.

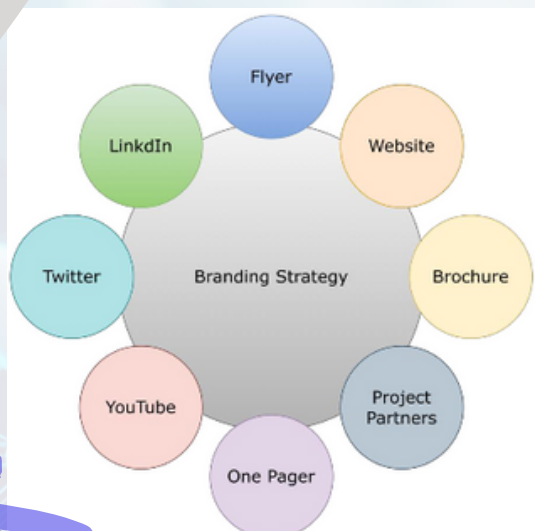
**Security Testing Results:** Finally, the baseline should include the results of any previous security tests conducted on the IoT device. The information sharing between manufacturer, certification authorities and domain owner enabled by CERTIFY allows a more complete assessment of the reached security level.



# DELIVERABLES

## Deliverable D7.1

This deliverable outlines project management, quality procedures, and data management strategies aimed at ensuring CERTIFY compliance with excellence standards. It begins with a brief overview of the project, its partners, and the work plan to establish the document's framework. Project management procedures cover organizational structure, reporting processes, decision-making mechanisms, and risk management. Quality management processes include template definitions for document production and quality reviews. Communication tools, notably the CERTIFY Repository, are highlighted, providing a centralized platform for document sharing. Lastly, the Data Management Plan outlines data types, standards, and GDPR compliance measures. It was submitted in M3 of the project.



## Deliverable D6.1

The primary aim of the deliverable is to outline a comprehensive strategy for disseminating, communicating, exploiting, and standardizing CERTIFY's concepts and achievements to a diverse range of identified targets, both within the project's scope and beyond. This strategy will employ a combination of tools and media, ensuring a balanced approach that integrates online and offline activities and actions. By leveraging a variety of communication channels and engagement methods, the goal is to maximize the impact and reach of CERTIFY's outcomes across its intended audience and broader stakeholders. The deliverable was submitted in M9 of the project

## Deliverable D1.1

This deliverable provides an overview of the initial version of the CERTIFY security lifecycle methodology and delves into the specifics of three distinct use cases integral to the project: the connected cabin system, smart micro-factories, and the tracking and monitoring of artworks. These use cases were thoughtfully selected to encompass a broad spectrum of applications involving embedded devices within complex systems. Each use case is meticulously described, drawing upon operational scenarios and requirements analysis. Additionally, comprehensive threat scenarios and associated risks have been identified through thorough secondary research, ensuring a robust understanding of the security landscape surrounding each use case. The deliverable was submitted in M10 of the project.





# CERTIFY IN WISP

## About Workshop

WISP was founded with the goal of drawing in and showcasing the most recent findings in security and privacy research on IoT and continuous computing. The best papers will be chosen through a rigorous peer review procedure. In order to promote a deeper knowledge of how to shape the future of the Internet, WISP encourages submissions from researchers, developers, and practitioners working at the intersection of intelligent connected devices and security and privacy problems.



The workshop underscores the crucial function of Privacy Enhancing Technologies (PETs) in mitigating privacy hazards associated with Internet of Things (IoT) systems and instigating an exhaustive exploration of plausible remedies for a secure and privacy-aware IoT ecosystem in the times ahead. WISP is a one-of-a-kind event that will include panel discussions, scientific paper presentations, keynote addresses, and themed workshops. In addition to organizing a panel discussion with stakeholders to analyze the demands and expectations of the industry, WISP will accept scholarly papers in response to a call for papers. Furthermore, we are inviting position papers from the community and industry to be presented in a pitch format during a unique session (not related to publications).

## Scope of Workshop

The primary obstacles to the design and development of IoT-enabled scenarios are generally acknowledged to be the enforcement of security and privacy concepts. As wireless communication technologies are widely used and IA techniques are integrated, the Internet of Things (IoT) is becoming more and more autonomous in our surroundings. Further driving the need for a standardized security and privacy layer, including the inclusion of privacy-enhancing technologies (PETs), is the rapidly growing number and heterogeneity of IoT devices. The incorporation of 5G technologies will strengthen this element in order to achieve a society that is driven by data. In this scenario, potential attackers will target present physical and digital infrastructures in an attempt to gain access to the data these devices supply. The rise in security and privacy threats that comes with this hyperconnectivity trend is a result of IoT systems that frequently act as their owners' agents by releasing potentially sensitive data. To boost confidence in the next digital society, producers, regulators, legislators, and end users must work together to address these issues. To encourage the widespread use of cutting-edge connected devices and related systems, it is necessary to create collaborative methods that address the detection and mitigation of security and privacy issues.

## About Workshop Committee

Experts from various EU projects focusing on cross-layer issues related to user-centric security, privacy, and trust in connected devices and its interactions with the continuum computing paradigm are to be brought together for this workshop.

This workshop is made possible by EU initiatives: ERATOSTHENES, CERTIFY, CROSSCON, COBALT, ENCRYPT, REWIRE, DOSS, ENTRUST, TRUSTEE.

Furthermore, a day will be devoted to the Cybercamp-USAL initiative, namely a conference with industry experts where profiles with cybersecurity concerns will be brought closer to the realities of cybersecurity through discussions and workshops.

# FEATURED RESEARCHER

---



## Stefano Sebastio


*R&D Manager  
Collins Aerospace*

### ABOUT

Stefano Sebastio, PhD is a Senior R&D Manager in Cybersecurity at Collins Aerospace (an RTX business) in the Applied Research and Technology (ART) center, located in Cork, Ireland. He and his team (distributed across the US, Ireland, and Italy) design solutions to assure runtime integrity of the system operations, to protect and control the exchange of shared sensitive data in connected environment, to proactively eliminate vulnerabilities at design time, and to ensure resilience and availability of critical systems. In CERTIFY, Stefano is the scientific and technical coordinator (supporting Prof. Skarmeta) and the principal investigator for Collins Aerospace.

### ON CERTIFY

CERTIFY lays the foundation for a holistic cybersecurity management of IoT systems encompassing the entire lifecycle of the device. Its innovative methodology and framework can constitute a leap forward in protecting novel interconnected digital environment. The designed solutions are also well aligned with the prominent security paradigm of Zero Trust ("never trust, always verify") and its tenets.



As embedded and IoT devices get more and more adoption in civil aviation solutions, cybersecurity covers a pivotal role. Thus, we are proposing in CERTIFY a pilot aligned with the Connected Ecosystem initiative at Collins Aerospace, namely the connected cabin system. In CERTIFY we are focusing on remote attestation of the device in two stages of the lifecycle: network bootstrapping and operations. The proposed monitoring solutions can be configured with the device behavior specified by the manufacturer and are meant to work in orchestration with other components of the CERTIFY architecture.



# READER'S VIEW

He is an expert in cybersecurity, digital responsibility, trust in digital technologies, ecosystem building and leadership within this space.

He is currently building the "twinds foundation" concerned with establishing "disposable identities" as a key technical enabler for building trust online. In addition, He advises and coaches on matters of digital trust and cybersecurity. He is a member of the World Economic Forum "Digital Trust" working group.



**Kai Michael Hermesen**

*Co-founder twinds Foundation*

## STATE OF IOT SECURITY

No doubt, modern technology like the Internet of Things (IoT) has revolutionized our lives, enabling new applications and reshaping societal norms. During the COVID-19 crisis, remote work and online education kept economies running. Digital tools also facilitate decentralized energy production, contributing to sustainability efforts.

However, these advancements come with drawbacks such as data exploitation, cybersecurity risks, and negative societal impacts like the digital divide. Unequal access to technology risks leaving communities behind, underscoring the importance of fair and transparent digital practices.

Now, if this wasn't not already a mouthful, along comes AI. With the rise of AI and IoT networks, real-time AI-based decisions are increasingly necessary at the edge. However, traditional cloud-based compute resources cause latency issues, hindering real-time analysis. To address this, AI is moving to the edge, necessitating a flexible and extensible technology stack. This stack must support real-time AI tools like image analysis systems. Organizations will need to shift more data processing to the edge, requiring expanded resources and IT infrastructure to support the growing IoT landscape.

To address these challenges, I believe a shift towards "trust by design" is imperative. Becoming trustworthy and strengthening „trust in tech“ is an up-leveling of the security conversation to include attributes such as transparency, privacy, collaboration and even business ethics. These elements transform the conversation from what "must" a company do to prevent negative outcomes to what "should" a company do.

In many ways, trust in technology will be as important as any innovations in technology itself. For the question of our time is no longer if „technology can do this“ but if „technology should do this“. This entails prioritizing transparency, privacy, and ethical behavior in technology development. Building trust is essential for widespread adoption of digital technologies like IoT and ensuring positive societal outcomes.

## HOW CERTIFY WILL HELP


Certify defines a methodological, technological, and organizational approach for IoT security lifecycle management, including timely detection, mitigation, and reconfiguration of security threats. It enables secure integration of IoT devices through enhanced automatic identification, configuration, and increased domain security based on behavioral profiles and extended Manufacturer Usage Description (MUD) standards.



# 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