CERTIFY- aCtive sEcurity foR connecTed devIces liFecYcles

List of participants

Participant No. *	Participant organisation name	Short name	Country
1 (Coordinator)	Universidad de Murcia	UMU	ES
2	Trust Up SRL	TUp	IT
3	STMicroelectronics SRL	ST-I	IT
4	Engineering - Ingegneria Informatica SpA	ENG	IT
5	Digital Worx GmbH	DWG	DE
6	United Technologies Research Centre Ireland Limited	Collins	IE
7[1]	Advanced Laboratory on Embedded Systems SRL	Collins	IT
8	Red Alert Labs	RAL	FR
9	Gioumpitek Meleti Schediasmos Ylopoiisi Kai Polisi Ergon Pliroforikis Etaireia Periorismenis Efthynis	UBI	EL
10	Fundación Instituto Internacional de Investigación en Inteligencia Artificial y Ciencias de la Computación	DIH-IoT	ES
11	European Cyber Security Organisation	ECSO	BE
12	Universität Zürich	UZH	CH
13	modum.io AG	MOD	CH

1. Excellence

1.1. Objectives and ambition

1.1.1.1. Project scope and vision

Countless Internet of Things (IoT) devices get connected to the Internet every day, while people need to gather and process massive amounts of information from the real world. The advent of 3GPP 5G, allowing for massive information exchange, is a game-changer in IoT. However, enhanced connectivity and IoT's low security led to vast attacks, hindering a wide-spread adoption of IoT[2]. Marriot Cyberattack[3] and Colonial Pipeline[4] are perhaps the most known examples of IoT deficits. Cyber-attacks get more sophisticated every day, thus affecting a large number of IoT-related infrastructures

[1] This partner is affiliated of Collins, within the proposal both are considered as a single partner (Collins, number 6) in this document.
[2] https://www.dw.com/en/millions-of-marriott-guests-exposed-in-new-data-breach/a-52975464
[3] https://stansberryinvestor.com/media-article/240009412
[4] https://www.gartner.com/smarterwithgartner/the-iot-effect-opportunities-and-challenges-2/

Figure 1 CERTIFY overview

and raising security and privacy concerns of consumers and businesses. It is estimated that the total cost of data breaches will increase by 70% from $3 trillion (2019) to over $5 trillion (2024). This highlights the importance of proper IoT security management, enhancing IoT infrastructures with continuous security improvements integrated into IoT lifecycle management. This is not a trivial task considering IoT device heterogeneity, the dynamism of the security landscape, and the number of IoT stakeholders. Any security change caused by a new vulnerability or an insecure update (e.g., patch) on a single device can put the whole IoT system at risk. Security management of IoT infrastructures encompassing the full lifecycle of products and continuous certification are fundamental tools to guarantee a high-level security, as emphasized by the European Union Agency for Cybersecurity (ENISA) Cybersecurity Act (CSA)[5]. Indeed, an effective security framework must stimulate collaboration among IoT stakeholders (e.g., auditors, manufacturers, users) as pointed out by the Network and Information Security (NIS) directive[6].

CERTIFY provides IoT stakeholders with mechanisms achieving high-level security. CERTIFY will detect and respond to a wide spectrum of attacks, in a collaborative/decentralized fashion. CERTIFY will validate the architecture through cutting-edge use-cases and pave the way towards innovative security in a broad spectrum of IoT environments.

To ensure security compliance throughout the lifetime of the device, we propose the design and implementation of a cybersecurity lifecycle management framework for IoT devices. The framework is intended to support device security management by collecting and sharing relevant security information both internally (via monitoring and self-assessment services) and externally, e.g., by interacting with device manufacturers, threat databases, certification authorities, Information Sharing and Analysis Centres (ISACs), and more. The received information is meant to support the local decision making with respect to the security, monitoring, updating and configuration of the device. Moreover, this information sharing will enable a continuous risk assessment, gathering evidence that could agile future certifications.

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 IoT Over-The-Air (OTA) updating, and (v) continuous security information sharing.

1.1.1.2. Project objectives

CERTIFY SMART (Specific, Measurable, Achievable, Realistic and Timely) Specific Objectives – SOs - tackled coherently by the project work plan are reported in Table 1 whereas their pertinence to the call is in Table 2

Table 1 Specific Objectives

Specific objectives
SO1. Cybersecurity awareness for IoT-enabled environments through a multi-stakeholder sharing of threats and mitigations. *Information sharing plays a key role in CERTIFY. It provides infrastructure, mechanisms, and tools to share security information in a secure, trusted, and protected way among IoT stakeholders. The shared information enables CERTIFY to improve security management in the IoT lifecycle accelerating protection against zero-day threats through blockchain-based device inventorying, updating, and dynamic sharing of mitigations (**WP3**). CERTIFY will continuously refine IoT security in the face of a changing security landscape, speeding up recertification. When target security cannot be met, CERTIFY will repurpose/decommission the device.*
KPI1.1: Infrastructure sharing security information among ≥ 4 stakeholders (D3.2), **KPI1.2**: ≥ 1 extended threat behavioural profile developed (D3.2, D5.2), **KPI1.3:** Automatic management of vulnerabilities and mitigation requiring <= 3 user interaction (D3.2)
SO2. Secure reconfiguration and maintenance of customizable embedded devices by means of open hardware primitives and services. *CERTIFY will explore customized, software-based Trusted Execution Environments (TEEs) (**WP4**), relying on open hardware initiatives and using RISC-V running a secure monitor at the highest privilege level. CERTIFY will provide hardware (HW) security primitives and formally proved solutions and components, which guarantee device bootstrapping and data management supporting integrity & confidentiality. CERTIFY will exploit the*

[5] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[6] https://digital-strategy.ec.europa.eu/en/policies/nis-directive

Secure Element (SE), implemented in HW/SW (software), supporting key provisioning, secure storage, secure boot, and encryption. CERTIFY will align with the Global Platform[7], an open ecosystem for secure-by-design digital services
KPI2.1: Design ≥ 1 dedicated RISC-V architectural component for TEEs (D4.2)**, KPI2.2:** Demonstration ≥ 3 CERTIFY Pilots (D2.2)**, KPI2.3:** Formal verification of CERTIFY security properties ≥ 3 (D4.2)**, KPI2.4:** Protection IoT device against ≥ 10 areas of cybersecurity attacks on secure devices[8] (D4.2)
SO3. Perform security operational management based on bootstrapping and monitoring of attacks and malicious behaviours. *CERTIFY will develop a bootstrapping mechanism (**WP5**) using flexible/lightweight protocols. CERTIFY's secure device authentication will allow only approved devices to join the network. CERTIFY executes only trusted SW/FW (firmware) with secure configuration expressed by behavioural profiles. Secure enclaves ensured at boot will be maintained at run-time. Network fingerprints will be prepared at design time and compared with those collected at runtime. CERTIFY will ensure an increased ability to detect attacks thanks to monitoring and intrusion detection (**WP5**) adapted to computational capacities and tolerance of behavioural changes of devices.*
KPI3.1: Discovers complex/cascaded threats[9] ≥ 8 (D5.2), **KPI3.2**: Device-behavioural analysis accuracy ≥90%; device-behavioural analysis at runtime ≥ 4 device types (D5.2), **KPI3.3**: Runtime protection technologies developed ≥5 (D5.2), **KPI3.4**: ≥ 3 secure enclaves supported (D5.2), **KPI3.5**: Bootstrapping time reduced ≥ 10% (D5.2)
SO4. Runtime security compliance and continuous certification methodology via objective metrics. *CERTIFY will follow ENISA CSA in IoT lifecycle management (**WP1**) by developing a dynamic security evaluation methodology to verify lifecycle-wide IoT device security. CERTIFY will use testing techniques that enable automated, objective, and empirical verification, facilitating (re-)certification. The methodology will feed on the received security information and monitor security violations. Behavioural profiles will be created with security recommendations for the IoT device (re-)configuration, addressing known security issues. (**WP3**).*
KPI4.1: Cybersecurity tests executed ≥ 10 (MS5, MS8), **KPI4.2**: Behavioural profiles created ≥ 3 (D1.2, D3.2), **KPI4.3**: Number of defined security recommendations for IoT device (re-)configuration ≥ 10 (D1.2, D3.2)
SO5. Foster knowledge delivery via wide dissemination, capacity building and supporting standardization activities. Build a robust exploitation plan to boost ROI by optimizing current and future EU cybersecurity capabilities. *CERTIFY will support "European trustworthy platforms", strengthening "EU cybersecurity capacities" and "European Union sovereignty", providing "resilient digital infrastructures" and processes for "smart and quantifiable security assurance and certification". CERTIFY aims to accelerate the adoption of advanced technologies by European (EU) manufacturing small to medium enterprises (SMEs) in all sectors and support them in building competitive advantages in global markets. This will be accomplished through scientific dissemination and generation of IoT know-how, Business to Business (B2B) events for improvement of communication capacity, and direct communication among different organisations (**WP6**).*
KPI5.1: Facilitate ≥ 20 cross-border experiments in ≥ 3sectors with SMEs (M36) **KPI5.2**: Events for knowledge sharing and dissemination ≥ 2, Networking events ≥ 1, B2B matchmaking (M36), **KPI5.3**: Number of change requests in main European standardization committees ≥ 2 (M36)
SO6. Industrial validation of the CERTIFY framework in IoT ecosystems. *CERTIFY will demonstrate its results in three application fields (aircraft, micro-factory, and artworks tracking), validating CERTIFY's advances from a technological and business perspective (**WP2**). The project will demonstrate advances on how to ensure security across the whole IoT lifecycle. However, the scope of the project is wide-reaching and aims at the continuous improvement of the cybersecurity of interconnected IoT systems in general.*
KPI6.1: Technological and methodological assets validated in CERTIFY ≥ 10 (MS9)**, KPI6.2**: Number of validation cases ≥ 3 (MS9), **KPI6.3**: Number of detection technologies validated ≥ 6 (MS9), **KPI6.4**: Number of complex/cascaded attacks adopted for validation purposes ≥ 3 (D2.2)

Table 2 Relation of the project objectives to the work programme topic

HORIZON-CL3-2021-CS-01-02 topic description (in blue) and relevant project Objectives/Results (in white)
The quality of hardware and software, notably open source, for IoT and connected devices is improving. However, the restricted environment of many IoT devices does not allow the deployment of more complex protection schemes (e.g., Trusted Platform Modules (TPM), Sandboxing applications in managed memory partitions) and similar approaches that

[7] https://globalplatform.org/
[8] https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-0.pdf
[9] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

often rely on operating system (OS) support to ensure cybersecurity (**SO2**, **SO5**)
CERTIFY will be based on open HW/SW by exploiting TEE based on the open HW RISC-V architecture and SE. SE will support enhanced cryptography currently unavailable in IoT platforms. CERTIFY will develop complex yet generic algorithms, methodologies, protection schemes, and strategic components for secure lifecycle management of all IoT platforms, including the ones natively less secure.
Open-Source designs are frequently used in IoT technology and become more reliable and efficient with the number of developers that deploy them. The management of this large collaborative development environment that Open Source represents is a real cybersecurity challenge. (**SO1**, **SO5**)
CERTIFY is a blend of IoT HW/SW. CERTIFY integrates open-source RISC-V and promotes the development of an open-source collaborative environment among all the stakeholders involved in the IoT device lifecycle. CERTIFY is committed to developing an open-source security information sharing environment to accelerate the responsiveness towards zero-day attacks. CERTIFY will create an ISAC and use thread-descriptors (threat behavioural profile) to alert about new threats and mitigate security risks on affected devices improving EU cybersecurity.
The aim is to support European trustworthy platforms by methods, tools and technologies that foster a stronger Cybersecurity, which can serve in a variety of connected devices. (**SO1-SO5**)
CERTIFY promotes trustworthy platforms developed by EU manufacturers, i.e., CERTIFY explores solutions based on open ecosystems developed by ST-I. A set of open-source tools, technologies, and methodologies supports the IoT security lifecycle, e.g., continuous cybersecurity evaluation, (re-)certification, secure deployment, (re-)configuration, monitoring, patching, repurposing and decommissioning in IoT infrastructures.
The proposed action should integrate formal security models and verified and scalable cryptography that can be used in future key system components (operating systems) (**SO2**, **SO5**)
CERTIFY includes the development of an architecture and methodologies based on high-assurance and formal security proofs. CERTIFY develops strategic components for IoT security using SE scalable cryptography. CERTIFY encompasses symbolic modelling and analysis to formally verify protocols.
Proposals should cover one or more of these research activities: (i) development of verifiable implementations of cryptographic solutions, authentication schemes, and, as relevant, software libraries that implement them securely in operating systems; (iii) development of security auditing for connected devices (vii) development of the security upgrading and (…) life cycle (bootstrapping, commissioning, operational, upgrade etc.) (**SO1-SO4**)
CERTIFY focuses on (vii) a security framework managing the full lifecycle of IoT devices including bootstrapping, (de)commissioning and upgrading. CERTIFY covers also (i) by exposing the HW/SW SE security features through an Application Programming Interface (API) and developing formally verifiable authentication schemes and cryptographic solutions. Finally, CERTIFY develops security evaluation for IoT devices, supporting an agile certification (iii).
The participation of SMEs is strongly encouraged. (**SO1-SO6**)
CERTIFY consortium includes 5 SMEs and 3 industrial partners. Moreover, the developed solutions will consider the requirements and constraints of 3 use cases (smart micro-factory, aircraft, tracking), including complex IoT ecosystems.

1.1.1.3. Ambition and innovation potential

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: CERTIFY general ambition is to define a sound methodological (aligned with current frameworks, legislation, sectoral directives and standards), technological (aligned with current cybersecurity enablers, such as TEE based on open hardware platform, embedded software and formally proved solutions) and organizational (aligned with current skill development and stakeholders needs) approach towards IoT security lifecycle management. The CERTIFY approach integrates into a single framework a set of interoperable tools, mechanisms and methodologies to enable: i) security by design support; ii) continuous security assessment and monitoring; iii) timely detection, mitigation, and reconfiguration; iv) secure updating of the IoT; v) continuous security information sharing. Furthermore, relevant security experience gathered in Pilots will serve as input in the design of the CERTIFY solutions.

B) Certification & security evaluation: CERTIFY aims at the IoT certification by supporting dynamic IoT environments, the whole lifecycle of embedded devices and their operational context and configuration. CERTIFY will improve the state of the art by automating the process and verifying the compliance of security properties, both at design

and runtime, including security and privacy in open hardware. Towards this end, CERTIFY will follow a risk-based security testing approach[10].

C) Enhanced open hardware security: CERTIFY builds upon RISC-V, an Open HW architecture considered a security pillar according to the European Processor Initiative (EPI). CERTIFY will integrate SEs, Physical Memory Protection (PMP), and TEEs in the IoT design, aligned with the Global Platform's Open Ecosystem for Secure-by-Design Digital Services and Devices. This solution will constitute the CERTIFY ecosystem featuring, e.g., NIST-specified bootstrapping mechanisms and patching.

D) Secure integration of IoT devices: CERTIFY will enhance bootstrapping with attestation tokens providing device model, ID, behavioural profiles, associated threats, secure configuration, etc. This will allow for enhanced automatic IoT identification and configuration providing increased domain security. The CERTIFY secure bootstrapping will be based on the National Institute of Standards and Technology (NIST) approach[11] and Direct Anonymous Attestation (DAA), covering device attestation, network/application layer onboarding, and configuration. To provide interoperability in already deployed environments (e.g., Low Range-personal area network), the CERTIFY authorization and authentication solutions will be used in conjunction with EAP/IoT-related portable light-weight protocols.

E) Behavioural profiles: CERTIFY will extend the usage of behavioural files based on the Manufacturer Usage Description (MUD) standard from the Internet Engineering Task Force (IETF) to express configuration policies that the deployment domain could apply during the bootstrapping to configure the device in an intended secure way. In particular, a more expressive behavioural profile beyond current approaches and standards will be designed. The profile will include information related to the device, e.g., vulnerabilities associated so that the network could decide whether the device is secure. Moreover, CERTIFY will integrate the usage of these profiles in lifecycle management, using them to prevent threats associated with the dynamicity of IoT environments.

F) Security monitoring & detection: CERTIFY will combine Security Information and Event Management (SIEM) technologies with an insightful correlation of the security information monitored from different sources to enhance the detection of novel security threats. By combining different techniques (including Machine Learning (ML)), CERTIFY will improve the currently available solutions for anomaly detection in traffic/activity of the IoT system. ML will be used to analyse protocols, vulnerabilities, the effectiveness of IoT related security mechanisms, (e.g., through behavioural IoT profile verification) and will support the discovery of zero-day attacks while reducing false positives.

G) Information sharing and upgrading: CERTIFY will explore binary patching as well as components written in higher level script languages to modify software components on-the-fly without recompilation. For software patches, CERTIFY will leverage blockchain and Distr-buted Ledger Technology (DLT) to keep track of software updates and relevant security aspects, e.g., vulnerabilities, device information, etc. The developed security mechanisms will materialize a holistic and automated approach for dynamic patching, software updates, and policy management. Behavioural profiles will be also explored to dynamically adjust network policies when new vulnerabilities are detected, but patches are yet unavailable.

Table 3 CERTIFY R&I maturity

Asset	Domain	TRL	Partner
Security lifecycle management	A	2→4	ALL
IoT Security evaluation and certification framework	B	3→5	RAL/UMU
IoTSTrust[12] tool for automating security by design and evaluation	B	2→5	RAL
Modular solution for building TEE and enforcing security policies at HW level	C	3→5	Collins/TUp
Secure Microcontroller with static secrets stored on peripheral nodes	C	4→6	ST-I
Security monitoring and device execution introspection engine	C	2→4	UBI
Direct Anonymous Attestation for privacy-preserving platform authentication	D/E	3→5	UBI
FIDO-IoT secure onboarding	D	2→4	RAL
Secure and smart bootstrapping mechanism	D	2→4	UMU
Extended MUD and threat MUD	E	3→4	UMU
Fingerprint-based network bootstrapping and runtime integrity monitor	F/E	2→4	Collins
Secgrid tool for automatic detection of attack and abnormal activities	F/E	2→4	UZH

[10] https://www.sciencedirect.com/science/article/abs/pii/S0920548918301375
[11] https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding
[12] https://www.iotstrust.com/

Machine learning SIEM	F	2→4	ENG/TUp
Signature-based detection tool	F/E	3→6	ENG/TUp
Remote device inventorying for secure management	G	3→5	DWG
Dynamic Trust Scoring based on DLT	G	3→5	DWG
Smart Contract-based protocols to define rules for updated and patch management	G	5→6	DWG
BC4CC[13] blockchain scalable agnostic implementation for information sharing	G	2→4	UZH/MOD

1.2. Methodology

1.2.1. Approach and proposed infrastructure

The CERTIFY project aims at designing and implementing a novel framework (Figure 2) for managing the cybersecurity of network-connected IoT devices throughout their whole lifecycle. Indeed, we advocate that only a holistic way of managing device security can strengthen cybersecurity resilience while providing an opportunity for cost reduction.

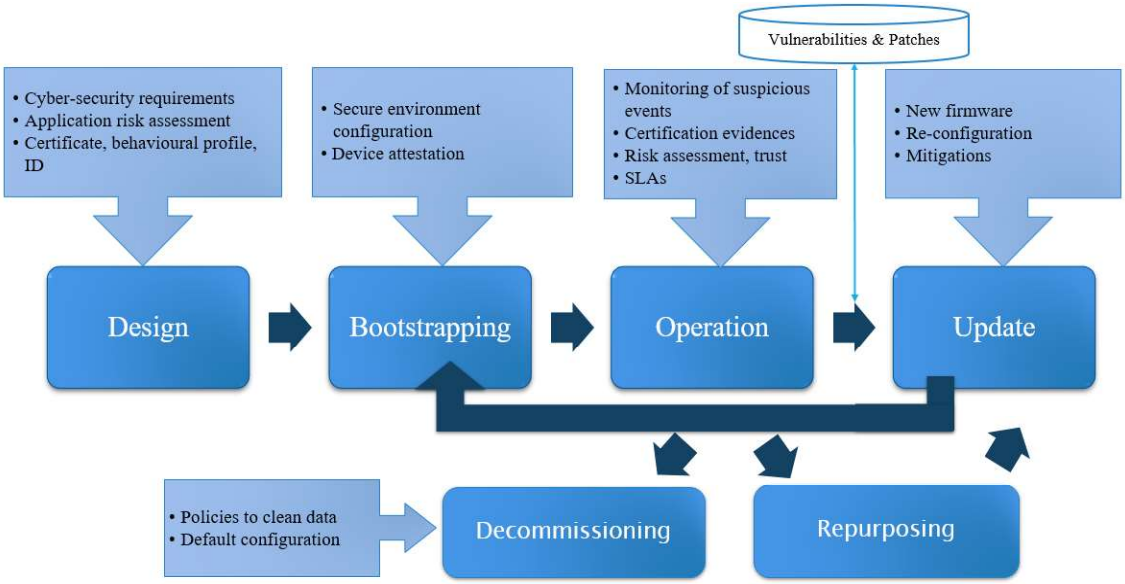


Figure 2 The enhanced cybersecurity lifecycle in CERTIFY

In the first phase of the secure lifecycle, the **design phase**, cybersecurity requirements are collected, and a risk assessment approach is defined for all the connected components according to the envisioned application. Here, and aligned with the CSA, it is important to validate the security properties of the device and ensure that it has an adequate security level. To achieve this goal, CERTIFY will design a security evaluation methodology (based on the one proposed in[14] the ARMOUR project) that is sensitive to possible changes in the security requirements/threats. Then, CERTIFY will provide a generic IoT device with the use of formally proven authentication and cryptographic protocols and robust isolation mechanisms enabled by open hardware architectures and trusted computing standards. We will exploit symbolic modelling and analysis considering the capabilities provided by the HW or SW implementation of the SE, enabling formal reasoning on the correctness and operational assurance throughout the device lifecycle. The secure enclaves will be based on RISC-V architectural features to build pure-software and customizable TEE whose security properties are guaranteed by a high-assurance design (SO2, O1, O6). Continuous assessment will be also performed during the whole lifecycle of the device, gathering empirical evidence needed to validate the certification and perform an agile recertification process (SO1, SO4, O1, O5). The results of such an evaluation will be used to create a behavioural profile, linking design and operational phase of the device (e.g., between the Certification Authority (CA), the Manufacturer and the customer and its device), providing information about the device, its correct use, the expected behaviour and possible security recommendations that can be applied in the deployment phase (SO1, SO4, O1, O5). The **bootstrapping phase** characterizes the change of the device state to operational. At this stage, the design-time configurations are exploited to enrol 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. Further credentials may be issued by the network for subsequent secure communication. In this sense, CERTIFY will develop network and device bootstrapping mechanisms

[13] https://www.csg.uzh.ch/csg/en/research/BC4CC.html
[14] https://www.sciencedirect.com/science/article/abs/pii/S0920548918301375

based on the approach defined by the NIST and Trusted Computing Group (TCG), covering the device attestation (especially the use of DAA), the network layer on boarding, the application layer on boarding and the secure configuration of the device. In particular, the DAA platform authentication mechanism will enable the secure onboarding of a device only if it can attest to the following two enablers of trust: *authenticity* and *integrity* of the computing platform (SO3, O1, O6). TEE will be used as the underlying SE for supporting the execution of DAA and will also be configured and instantiated by exploiting open HW solutions to allow code and data isolation. Such an approach allows one to deploy multiple applications with different security requirements on the same device while preserving confidentiality, integrity, and attestation (SO2, O1, O6).

In the **operational phase,** the devices must be protected from threats and vulnerabilities not foreseen at design time. For this reason, the CERTIFY framework envisions the adoption of an intrusion detection system and runtime monitoring components (SO2, O5). Runtime integrity protection can be ensured by monitoring the device's runtime behaviour (through novel tracing and introspection mechanisms) for identifying any deviation from the expected model provided by the behavioural profile (MUD). Here, techniques for the recognition of attack patterns in the IoT device, in a discrete node of the IoT environment, will be considered. CERTIFY will perform a continuous security assessment, starting a recertification process if needed and providing the needed evidence to support an agile process. The framework will also incorporate a local component, the trust and Service Level Agreement (SLA) manager, in charge of dynamically computing the trust score and ensuring that all SLAs agreed between the customer and the manufacturer are fulfilled (SO1, SO4, O1, O5). Moreover, the adoption of a local ISAC allows the CERTIFY framework to take advantage of the threat intelligence service: identifying novel threats on the IoT devices and strengthening the security of the devices by applying patches, reconfigurations and mitigation strategies (SO1, O1). In this sense, the threat MUD proposed by the NIST will be considered. CERTIFY will also support the information sharing between local ISACs of different manufacturers and sectors, creating a collaborative network to react efficiently against new threats (SO1, O1, O3, O5, O6) including threats with cascading effects. In this context, data protection and privacy must be addressed: CERTIFY will adopt privacy-preserving techniques, anonymization and authorization policies to ensure that data are protected, and their access is controlled. Network and device security changes are performed in the **update phase.** However, it is worth remarking that such operations may affect the digital cybersecurity evidence used for obtaining the previous security certifications. Therefore, once an update is performed, new digital cybersecurity evidence is automatically built by the CERTIFY framework to support a continuous assessment and re-certification processes. The same evidence is also shared with the consumer and the CA. To resolve a new vulnerability, the manufacturer can release an update or patch to mitigate it. To deal with this process and following the IETF recommendations, CERTIFY will develop a Platform as a Service (PaaS) to facilitate remote inventory (including both devices and security requirements) and OTA security patching for IoT devices using new decentralised and distributed technologies. Blockchain will be leveraged for software updates by providing a transparent ledger to manage the different versions of the software elements composing an IoT device or system (SO1, O3). The mitigation strategies suggested by the local ISAC will comply with the cybersecurity requirements and risk plan defined at the design stage. In some scenarios, device resources and capabilities may prevent the update process. In such scenarios the CERTIFY framework identifies a subsystem with different cybersecurity requirements and the device can be repurposed. In such a stage the device is reconfigured at network and secure environment layers. On the other hand, if the device cannot respect the required cybersecurity requirements, or if the discovered vulnerability raises the security risks and the mitigation process suggested by the local ISAC cannot take place, the device is **decommissioned** (SO1, SO2, O5). Both stages are covered by the CERTIFY framework. Decommissioning is needed to avoid information leaks that could potentially affect the cybersecurity of the whole environment: the framework ensures that i) no confidential data is exposed (e.g., intellectual property of the running applications, digital certificates and keys, or data stored in the memory), ii) appropriate clear policies specified for the device are enforced and iii) manufacturer or default device's configuration is restored.

1.2.2. Architecture

In Fig. 3 the architecture of the CERTIFY framework is represented. It is logically constituted by three layers, which are designed and implemented in proper Work Packages (WP) of the project work plan (i.e., WP3, WP4 and WP5). The bottommost provides services built on top of hardware functionalities available in RISC-V and ARM MCUs (micro-controller units) to build and maintain a secure environment. In the second tier, software-based solutions provide monitoring functionalities at both device and network layers. Transversely, a third layer groups the services offered by a remote centre, in charge of the inventorying, patching and securely deploying CERTIFY-powered IoT devices. The next subsections detail the components and services, developed in proper tasks of the work plan.

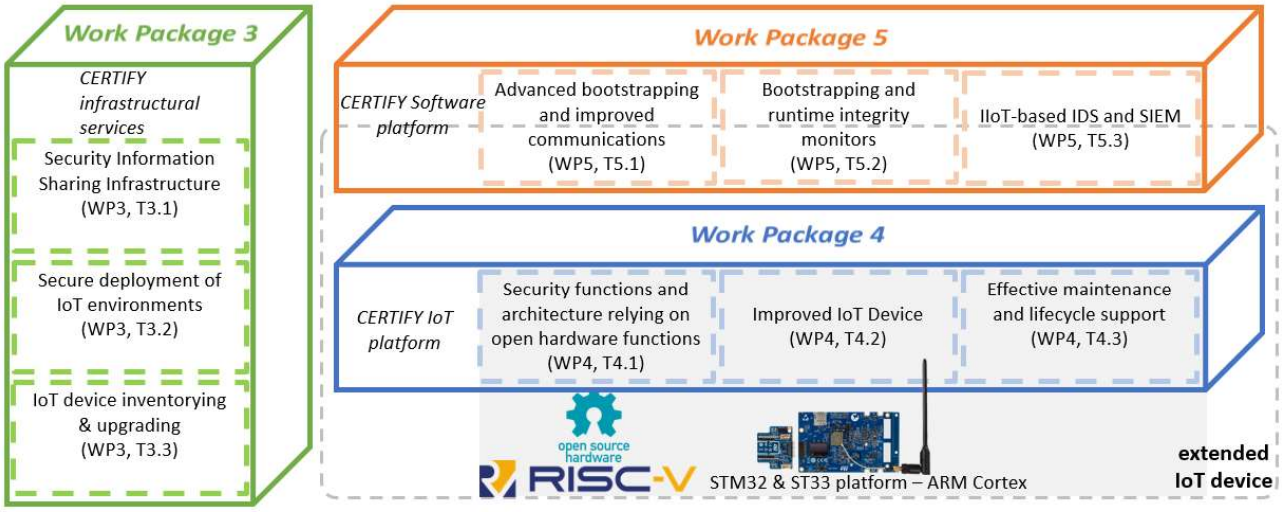


Figure 3 The logical architecture of the CERTIFY framework

A. Security information sharing infrastructure (WP3, T3.1)

In a hyper-connected world, cyberattacks have a borderless nature, and their impact could affect critical infrastructures in different institutions or countries. Therefore, providing access to the corresponding cybersecurity information is crucial to foster the realization of a more homogeneous perspective on cybersecurity at EU level. Both the CSA and NIS Directive promote strategic cooperation among the involved stakeholders to support and facilitate sharing of information. This approach helps to respond to large-scale incidents by creating synergies, which can act more effectively against cybersecurity vulnerabilities. Beyond the requirements for the process itself, a key issue is how to make this information available, considering the scale of the number of ICT artefacts. An important aspect of this platform is to enable a responsible vulnerability disclosure[15] allowing manufacturers/providers to prepare patches and notify users in a timely and reliable way.

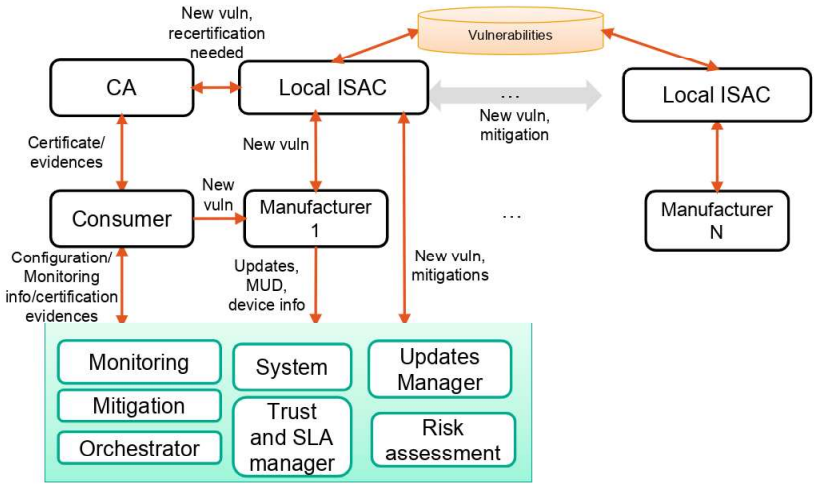


Figure 4 The CERTIFY information sharing workflow

CERTIFY will develop a service to support security information sharing between the different stakeholders to support the continuous security assessment throughout the device lifecycle. For this, CERTIFY will consider DLTs technology as a promising approach to enable a trustworthy and transparent platform for sharing cybersecurity information among stakeholders that do not share a common trusted third party[16]. We foresee the presence of several entities owing different responsibilities and roles in sharing knowledge. An overview of the information flow envisioned in the CERTIFY project is pictorially represented in Fig 4. At provisioning time, the customer is in charge of generating evidence for the cyber-security certifications required by the specific application. During operations, customers keep monitoring the deployed IoT devices for compliance with the specified security requirements. Throughout its lifecycle, the device could be reconfigured to accommodate it to the changing threat landscape or requirements. Indeed, even the original manufacturer of the device may publish secure updates and accordingly modify the MUD file when necessary. Therefore, it will be required to collect new evidence to support the recertification process, which is shared with the CA. While performing its security monitoring activities, consumers may detect vulnerabilities that will be shared with the manufacturer for

[15] https://ieeexplore.ieee.org/document/4084135
[16] https://www.researchgate.net/publication/319047604_A_Blockchain-based_Approach_for_Data_Accountability_and_Provenance_Tracking

further investigation and prompting mitigations or resolutions. The local ISAC is in charge of collecting vulnerabilities from different manufacturers and products to build common knowledge and understanding ongoing and historical vulnerabilities along with the possible mitigations and resolutions, reacting in an efficient way against zero-days threats. Once a new vulnerability is discovered and enumerated, the local ISAC will be also in charge of propagating such information to the CA and manufacturer. In such a way, the CA can rectify the cybersecurity certification requirements according to the ever-modifying and discovered threats, and the manufacturer can provide the required patch.

B. Secure deployment of IoT environments (WP3, T3.2)

Beyond the use of traditional cryptographic and access control techniques, the security aspects of IoT devices should be properly managed through a governance approach to ensure devices behave as expected. However, the specification and enforcement of such aspects can be challenging in environments where a huge number of IoT devices can communicate with each other and, sometimes, without the explicit consent of their owners. To address this issue, the MUD[17] is an IETF standard aimed to define the intended behaviour of the device through Access Control Lists (ACLs), to restrict the communication to/from a certain device. While MUD was recently standardised (March 2019), it has received strong interest from the research community and standardisation entities worldwide. The NIST has also recommended MUD files to complement security credentials to reduce the attack surface[18]. MUD is focused on the definition of network access control policies. Therefore, these restrictions can be straightforwardly enforced through the Software-Defined Networking (SDN) paradigm. However, beyond aspects of the network level, the MUD semantics does not provide the possibility of defining security properties to provide a more fine-grained approach that determines how IoT devices should communicate.

CERTIFY aims to extend the usage of behavioural files to express configuration policies that the deployment domain could apply during the bootstrapping to configure securely the device, reducing the device's attack surface. A more expressive behavioural profile will be designed to provide a higher expressiveness, allowing to specify different types of policies at different layers beyond the network one. This profile will also include useful information related to the device, for example, vulnerabilities associated. On the one hand, CERTIFY will use MUD files to deliver policy requirements for a device joining the network and then translate them to network access specific policies. These policies, together with the device's information previously mentioned, will be used to decide if the device is secure enough to join the network and to configure it securely according to the defined policies. Finally, CERTIFY will exploit the information of the MUD files during the bootstrapping process to obtain the security policies before the device has access to the network and therefore, configure it before any attack could be performed.

C. IoT device inventorying and upgrading (WP3, T3.3)

The secure updating/patching process of IoT devices is essential to ensure security throughout their lifecycle. Manufacturers and software providers will need to update the device's software to increase their functionality, or to fix a security issue after an attack or vulnerability detection. However, most of the current upgrading proposals are based on centralized models using client-server architectures suffering from different issues related to scalability, availability, and efficiency, and in which servers become a single point of failure. The constraints of devices and networks, and the increasing complexity of the IoT deployment raises the need for an efficient and scalable approach. As IoT components present dependencies between components, a corrupted update can affect the whole system. Finally, confidentiality of software updates is crucial since they can disclose information about specific libraries or configurations that can be leveraged by attackers. However, current efforts such as the Lightweight Machine to Machine (LwM2M) Technical Specification (developed by the OMA)[19] or the Software Updates for Internet of Things (SUIT) working group[20] are mainly focused on communication security aspects, and they must be combined with additional techniques to manage the complexity of IoT systems and deployments.

CERTIFY will design a scalable and secure approach for disseminating software updates in scenarios with a huge number of heterogeneous IoT devices. The upgrading will be decentralized, robust and efficient, bringing the upgrading functionality closer to the end devices by means of edge/fog nodes, in such a way that the update/patching process can be carried out through secure and efficient mechanisms to reduce latency and network overhead. CERTIFY will also

[17] https://datatracker.ietf.org/doc/rfc8520/
[18] https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/10/17/iot-trust-concerns/draft/documents/iot-trust-concerns-draft.pdf
[19] www.openmobilealliance.org/release/LightweightM2M/V1_1_1-20190617-A/HTML-Version/OMA-TS-LightweightM2M_Core-V1_1_1-20190617-A.html
[20] https://datatracker.ietf.org/doc/html/rfc9019

explore software components written for IoT devices in higher-level script languages such as Python[21,22] or JavaScript[23] so they could run software functions and ii) replace software files and references to script functions on the fly by just including a software function from a remote location. This allows instant component instantiation by running an initial configuration setting references to external scripts libraries, while no binary firmware preparation, transfer and installation are needed in this case. But this also raises security issues concerning running untrusted software libraries and new attack vectors such as malicious script injections or cross-site scripting. Such a solution of on-the-fly modification of software components requires trusted communication channels between the device, manufacturer, software developer, and security auditor and a process to validate the integrity of software resources and script libraries. To guarantee confidentiality in the distribution of software packages, CERTIFY will integrate a lightweight object-based security approach by implementing and extending recent COSE-based mechanisms[24], which are considered in the scope of the IETF SUIT WG. Blockchain technologies will be leveraged by providing a transparent ledger to manage the different versions of software elements composing an IoT device or system as well as to share other relevant security aspects (e.g., vulnerabilities and device information). As interoperability is crucial, CERTIFY will analyse the use of *Bifröst*[25]*/interledger*[26] approaches to interconnect different blockchain implementations. Finally, the developed security mechanisms will be integrated to come up with a holistic and automated approach for the deployment of mitigations and update of IoT devices using the notion of Threat MUDs proposed by the NIST[27], providing a flexible and dynamic way to alert about a new threat and the mitigations to apply before an update or patch is released. Threat MUD is intended to complement MUD files, dynamically reconfiguring the device when a new vulnerability is detected.

D. Security functions and architecture relying on open HW functions (WP4, T4.1)

In practical instantiations of IoT system architectures, some levels such as the IoT peripheral nodes are replicated in a high number of copies and layers that are less numerous or even unique, as a backend system without redundancy. Differences in attack surface, processing capability, unit costs and number of copies, imply that different approaches are needed at different layers of the architecture. IoT nodes leverage on architectures where the node is developed using HW & SW Open Development Environment (e.g., ST ODE[28] or ST STM32CubeMX[29]). In current best approaches, processing functions less sensitive to security are embedded in a general micro while the security relies on the presence of a Hardware Security Module (HSM) with a core a secure microcontroller (possibly certified) that acts as a companion secure chip with a secure OS. However, this poses some usability problems for developers of IoT nodes, whose competencies focus on sensing/acting/communication and not on security. When we move from the remote node toward the centre of IoT architecture, physical security barriers are more available, the cost of a single unit can be increased (as less devices are used) and the countermeasures target mainly logical attacks. In these upper layers of the IoT hierarchical network, the security problems tend to become like the ones normally faced in other Information and communications technology (ICT) applications not based on embedded devices.

CERTIFY will build security solutions for embedded devices based on the reprogrammable generic node platform and customized with the introduction of a SE designed in alignment with the Global Platform's open ecosystem for secure-by-design digital services and devices. Such SE, in charge of hosting and providing confidential cryptographic data and keys will be built exploiting chips devoted to mobile connectivity (i.e., the SIM card) or software-based solutions to avoid the higher cost and complexity associated with devoted TPM hardware. On the other hand, such a scenario makes the security attestation harder (including integrity and confidentiality) as the devices can be physically accessible to an attacker or the device may need to operate in harsh environments. In CERTIFY, the SE (implemented either in hardware or software) will be able to detect and automatically mitigate a wide set of side-channel attacks. The CERTIFY-augmented IoT architecture will be inherently based on an open hardware approach, with emphasis on the open processor architecture RISC-V, considered in European roadmaps and projects such as the EPI. RISC-V provides a rich privileged architecture along with flexible primitives like a PMP unit, which are an enabler for the establishment of robust isolation mechanisms. In line with current trends, CERTIFY will introduce new approaches for the definition of customized,

[21] https://micropython.org/download
[22] https://www.unibw.de/code-events/huber_code21-3.pdf
[23] https://www.espruino.com
[24] https://www.rfc-editor.org/info/rfc8152
[25] https://ieeexplore.ieee.org/abstract/document/8990860
[26] https://research.aalto.fi/en/publications/interledger-approaches
[27] https://www.nccoe.nist.gov/library/securing-small-business-and-home-internet-things-iot-devices-mitigating-network-based
[28] https://www.st.com/en/ecosystems/stm32-open-development-environment.html
[29] https://www.st.com/en/development-tools/stm32cubemx.html

software-based TEEs, relying on features offered by RISC-V and a pure-software secure monitor running at the highest privilege level in the RISC-V-based platform. Fitting the philosophy of the CERTIFY lifecycle management framework, the customizable TEE will support trustworthy monitoring of continuous compliance with given cybersecurity requirements as well as NIST-specified bootstrapping mechanisms along with enhancements proposed by CERTIFY. Ultimately, the customizable TEE will allow designers to i) rely on open HW development, enabling full transparency of IoT design flows and verifiable implementations of security-sensitive components, ii) exploit the flexibility of the SW trusted environment to develop custom self-monitoring and self-intrusion detection systems, auditing support, decommissioning mechanisms, etc., iii) enhance the credential security level, guaranteeing that the set of credentials stored on IoT will not leave the device even when malicious software is installed, iv) enhance the HW security allowing for certified software components executed on the device, in which the trust is spanned from the HW security module, and v) perform effective maintenance mechanisms, e.g. trustworthy channels for OTA security patches, which will fully match the vision of CSA towards comprehensive IoT lifecycle management.

E. Improved IoT Device (WP4, T4.2)

The methodology designed in CERTIFY considers that the security of the IoT peripheral nodes is probably the most critical, being the node distributed in the field and physically in the hands of potential attackers. Special care and advanced methodologies need to be applied in any step of the life cycle of the secure node. From the IoT node architecture selection to its detailed design, functional and secure evaluation, secure keys/application/data management at personalization level in the enrolling stage and operational phase. Also, not trivial is the necessity to update securely in the operational phase.

CERTIFY architecture foresees the presence of a Secure Microcontroller based on a Secure Core: e.g., the latest member of the ST33 family embedding an ARM® SecurCore® SC300™ 32-bit RISC or an equivalent advanced component selected among the best secure silicon supplier. Such a Secure Micro will host a strong Secure OS based on the evolution of the most advanced OS for Smart Card applications. The presence of this separated single secure chip at the core of the node is a first fundamental methodology choice. Nowadays, all payment schemes based on Smart Cards or Mobile Phone transactions use Secure Micro to securitize payment transactions; all mobile phones use Secure Micro (e.g., a SIM, an embedded SIM) to secure connectivity authentication; PCs local security leverages on TPM based on Secure Micro; Electronic Passport, electronic ID card are based on Secure Micro. The secure micro solution at the heart of hundreds of successful secure cases at a maturity stage higher than the relatively new IoT deployment. Therefore, it will be worthy to start from the results of these successful technologies to make the right architecture choice at the node level and work for further improvements tailored to IoT needs. Secure Micro, its related secure SW technology and smart card life management protocols will permit CERTIFY to leverage the possibility of secure personalization at any stage. The Secure Micro will also monitor locally the presence of physical attacks by intercepting abnormal environmental parameters such as low/high temperature and low/high/glitch on the voltage (e.g., due to laser lights attacks). Moreover, a solution based on the secure micro will permit not only to identify at run time security attacks but also to use active countermeasures based on the synergy of mechanisms at HW/SW levels. The security assessment methodology of this solution will be based on the most advanced security evaluation schemas, the latest research results, internal knowledge, and experience from the CERTIFY partners. All design methodology will be based on a risk analysis approach using the most advanced techniques, e.g., Design failure mode and effect analysis (DFMEA) aimed at zero defect/fail/breach in the field. The evaluation techniques will be based on advanced models coming from the latest evolution of assessment methods such as the Common Criteria (CC) approach to assure the highest reachable level of information security

F. Effective maintenance and lifecycle support (WP4, T4.3)

There is an increasing interest to establish a general basis for European security certification and labelling led by the ENISA through the CSA, which explicitly requires managing the cyber risks, validating the security of the device from the design phase, standards, and schemas for managing the risk of IoT devices have shortcomings that make it difficult to meet these requirements. Whereas the high interdependence of devices, makes security assessment even more difficult, requiring mechanisms to manage dependencies, the wide variety and heterogeneity of methodologies and devices makes hard to describe how security evaluation must be done and which aspects should be considered to guarantee an adequate security level. In this context, comparability is unfeasible, as different schemes uses their own metrics, some of them subjective or difficult to calculate (e.g., likelihood). Finally, the dynamism inherent to security makes necessary agile and dynamic approaches to manage the security of a device throughout its lifecycle. Current approaches are not aware of this dynamism: CC, Commercial Product Assurance (CPA) or Certification de Securité de Premier Niveau (CSPN) requires a complete re-evaluation in case of a security change, requiring a lot of money and time. Moreover, existing

hardware evaluation approaches leverage independent testing laboratories to test COTS modules supplied by industry vendors, use manual testing techniques and a validation based on human-readable test report[30].

To cope with the identified challenges, CERTIFY will design a security assessment methodology for the IoT context. The methodology will be based on[31] and consider activities to identify, assess, categorise, test, and treat risks, as well as activities to monitor, detect and respond to cyber-attacks, cyber threats, and vulnerabilities. In particular, the methodology will combine well known standards such as ISO 31000 standard for Risk Management and the ISO 29119 standard for Security Testing, in such a way that the security assessment can be carried out in a more objective and empirical way, also favouring the automation of the process. Furthermore, the proposed methodology will consider safety as an important aspect, so that these two concepts (security and safety) are considered jointly, and not independently. The main purpose will be to carry out a continuous security assessment of devices as the technical baseline for the development of a cybersecurity certification approach for the IoT context following the requirements and guidelines of the recent EU regulation CSA.

G. Advanced bootstrapping and improved communications (WP5, T5.1)

Current standardization organizations, such as the IETF, the Institute of Electrical and Electronics Engineers (IEEE), Internet Protocol for Smart Objects (IPSO), Zigbee and Open Mobile Alliance (OMA) have devoted efforts towards the progress of the secure IoT deployment and bootstrapping. However, all the established approaches have major challenges. On the one hand, using the same pre-shared credential for every device is the simplest approach, but it does not identify each device, nor does it give devices a way to verify they are connecting to the correct network. On the other hand, manually provisioning a unique credential for each device often makes the bootstrapping process complex, resource-intensive, error-prone, and insecure. Even if credentials are needed so that only authorized devices can connect to and use an organization's networks, having manufacturers assign a unique credential to each device during the manufacturing process is expensive and inefficient. Other characteristics are also desirable for a bootstrapping mechanism. It should be i) scalable, by using protocols and infrastructures designed to manage a large number of devices and ii) lightweight, to suit the needs of the more constrained devices with different capabilities (CPU, memory, network bandwidth, etc.).

As reviewed, the bootstrapping service needs to provide a lightweight bootstrapping protocol, reuse (certifiable and attestable) code whenever possible, allow flexible authentication, support different authentication methods depending on the device's characteristics and provide key management. Considering these properties and the mentioned challenges, CERTIFY will develop a bootstrapping mechanism based on the recent NIST[32] draft recommendation and the TCG for network on boarding for IoT devices, covering device attestation, network layer onboarding, application layer onboarding and the secure configuration of the device. In particular, we will take into account the usage of DAA for the authorization and authentication phase and the Authentication, Authorization, and Accounting framework, already considered by the new set of technologies known as LPWAN. This infrastructure is robust and in conjunction with the EAP protocol, they provide a secure framework for flexible authentication, authorization, and key distribution, especially when it is used with an IoT suitable protocol such as CoAP[33]. Moreover, the bootstrapping will be enhanced with a preliminary phase in which DAA will allow verifying the correct state of the device based on verifiable evidence (e.g., certificates, MUD) that will help to decide whether the network allows or not to enter the device. After the authentication and identification, obtained information will be used to configure in a secure way the device before it is able to access the network in which it is deployed, taking the appropriate measures to guarantee the security of the entire ecosystem.

H. Bootstrapping and runtime integrity monitors (WP5, T5.2)

IoT environments are built by heterogeneous smart devices produced by a variety of manufacturers and characterized by very diverse resources and constraints. The bootstrapping process covers the process that allows an embedded device to join and operate in the network. Many secure bootstrapping protocols rely on pre-shared authentication keys (or attestation tokens) supported by a third party (running either online or offline). Such an approach turns out to not be flexible enough in many resource-constrained environments due to the complexity introduced by the presence of this additional entity. Furthermore, this over complicates the runtime assurance of the deployed edge devices since possible software and firmware updates need to be vendor-specific, thus, limiting the vision towards open-source solutions where

[30] https://www.nist.gov/programs-projects/cryptographic-module-validation-program-cmvp
[31] https://www.sciencedirect.com/science/article/abs/pii/S0920548918301375
[32] https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding
[33] https://pubmed.ncbi.nlm.nih.gov/29149040/

authenticated encryption of such updates can be agnostic to specific types of pre-established keys. The large use of commercial off the shelf (COTS) peripherals in embedded systems also pose security challenges at runtime, especially in high-critical/safety-critical scenarios. Indeed, COTS specifications are often hard to verify due to limited details disclosed by the manufacturer.

CERTIFY aims at proposing flexible solutions for controlling the secure on-boarding process of new embedded devices and assuring their runtime integrity. Open attestation solutions leveraging the underlying hardware and/or firmware level security primitives exploiting the assumed behavioural specifications can allow a flexible reconfiguration of the attestation objectives at a low runtime overhead. For the runtime integrity, CERTIFY will leverage device runtime data and execution stream monitoring and introspection capabilities necessary for tracing the control- and information-flow execution paths needed by the runtime integrity (attestation) enablers. In CERTIFY, dynamic tracing functionalities will be provided, as programmable components, enabling the continuous monitoring (of kernel shared libraries, system calls, shared data and memory address space, etc.), and the in-depth investigation of the systems' behaviour for detecting obfuscation attempts if any type of exploits to the program and data memory. This provides the trusted anchor with the compiled control- and information-flow graphs (CFGs & DFGs) that represent the runtime state of a remote device, against the configuration and execution properties of safety-critical components, to be compared against software- and firmware reference values through the CERTIFY explainable AI features. CERTIFY advanced tracing techniques will be based on the novel use of (i) lightweight Extended Berkeley Packet Filters (eBPF) execution hooks capable of providing near real-time low-level code inspection, thus, capturing the strict constraints of IoT environments, and (ii) embedded OS introspection agents capable of traversing the entire physical memory of a device, via Direct Memory Access, for known execution signatures. These tracing functionalities will be fully programmable, enabling the priority of the CERTIFY framework towards dynamic adaptation of tracing. The execution environment of the tracer varies and can be either a software environment running on the same CPU, out-of-band co-processor, or in-band co-processor within the CPU. These three different flavours allow supporting different security and safety requirements. For example, software solutions may hinder the performance, thus, an out-of-band or in-band co-processor will be able to provide dedicated acceleration and isolated execution. Unlike software solutions, relying on a co-processor to collect data allows engineering a "trusted data acquisition method" without being influenced by malware running on the same device (e.g., when using software solutions). In CERTIFY, the endmost goal is to use the customizable TEE for supporting this runtime tracing process, thus, getting the benefits of both extremes - HW and SW-based solutions.

I. IIoT-based IDS and SIEM (WP5, T5.3)

Real-time security monitoring typically relies on the definition of taxonomies of events which cover the detection of botnets, denial of service, brute force, port scanning, malware signatures in traffic, data tampering, Structured Query Language (SQL) injections, attacks against SCADA systems or rootkits, to name a few. To this end, intrusion prevention and detection systems (IPS and IDS), honeypots, network sniffers or vulnerability scanners become several of the most relevant sensors to gather security-related information from a system. The current detection techniques can be divided into two categories: signature and behaviour-based techniques. Signature-based intrusion detection approaches seek runtime features that match a specific pattern of malicious behaviour, and they have a low false-positive rate. On the other hand, behaviour-based intrusion detection approaches look for runtime features that are out of the ordinary. However, the latter approaches are more susceptible to false positives. While it is true that IDS technology has gone a long way, some important limitations persist; In particular, detection accuracy is (relatively) poor, the rate of false positives is still high, which is unacceptable to several application domains (e.g., Telco), they have limited scalability, the growing evasion (current techniques often fail to detect emerging attacks) and they have very limited diagnostic facilities.

CERTIFY will combine SIEM technologies with an insightful correlation of the security information monitored from different sensors, enhancing the detection of security threats. In the context of IoT, the amount of traffic data generated by the devices constitutes a possible obstacle due to resources and computational constraints. Many recent studies and experiments aim at enhancing IDS and their use in IoT environments. The usage of ML techniques is widely recognised as useful, especially to perform automated data analysis and provide meaningful readings and foresight on the system. Studies show that when ML is combined with other techniques, accuracy can increase, and detection capability is enhanced[34]. In particular, the adoption of ML can help to detect outliers from normal traffic/activity in the system. Still, IDS in IoT-based environment is in an early stage and CERTIFY contribute to this field by defining a solution suitable

[34] https://ieeexplore.ieee.org/document/7568495

for these resource constraint environments. Approaches based on ML techniques[35], which have been analysed and studied in other contexts, could potentially be applied for outlier detection. CERTIFY will innovate IoT-based IDS with highly effective and near real-time detection capability, without slowing down or introducing network latency and taking into account IoT limitations and requirements. The proposed solution will consider IoT related protocols and vulnerabilities, monitoring the effectiveness of IoT security mechanisms (e.g., behavioural profiles verification), and will be integrated with the CERTIFY solution to enable a continuous security assessment process. The designed solution will support zero-day attacks' discovery and reduce the number of false positives.

1.2.3. Pilots

The methodologies and tools provided by CERTIFY's framework will be evaluated in 3 use cases from different sectors:

Secure Management of Devices Enabling an Intelligent and Connected Aircraft Cabin	
Use-Case Partner	Collins (lead), TUp, ST-I
Challenge: The deployment of a multitude of IoT connected devices supporting many in cabin components will usher in an era of intelligent aircraft cabin, encompassing a personalized experience for the passengers and opportunities for airlines in delivering targeted retail offers and optimizing operations. Aligned with that vision, in 2019 Airbus started its first in-flight trial for connected cabin technologies[36]. New generation aircrafts are equipped with thousands of sensors generating GBs of data per second[37]. Such IoT devices are arranged in (sub-) systems, communicate using wired[38] or wireless[39] connectivity, and are characterized by a mix set of processing capabilities, sensors and actuators.	
Innovation: The adoption of IoT devices opens up for a Maintenance, Repair and Operations (MRO) cost reduction where modifiable off-the-shelf (MOTS) devices are integrated in the cabin. On the other hand, cybersecurity covers a pivotal role as more IoT devices are integrated and security flaws (e.g., on Boeing's 787[40]) can even reach safety-critical systems. In light of the fast-progressing digitalization of the aircrafts and harmonizing with the Federal Aviation Administration (FAA) in the United States[41], the European Union Aviation Safety Agency (EASA) in the ED Decision 2020/006/R has introduced amendments[42] for airworthiness certification to protect on-board electronic networks and systems against cybersecurity threats. Therefore, it is critical that cybersecurity of these devices is assured throughout their whole lifecycle. In particular, it is crucial that availability, integrity and confidentiality are preserved. All in all, it is required that the various elements are monitored throughout their operations, tested against security requirements, robustness and vulnerability, and can be reconfigured as necessary to detect and mitigate cyber threats in a preventive, corrective or restorative fashion. To reduce maintenance cost and support a continuous certification, a remote prognostics and health management (PHM) supporting also security is envisioned. In 2018, the unplanned maintenance operations reached a global airline cost of 20 billion dollars[43]. Future aircraft maintenance will exploit data analytics and PHM to leapfrogging in efficiency reaching a "zero aircraft on ground (AOG)[44]". The availability of a dynamic monitoring, inventorying, risk assessment, re-configuration and patching will pave the way for reducing unscheduled grounding and making the same maintenance process more reliable.	
Results: A multitude of **edge nodes** equipped with sensors and actuators are installed in the next generation intelligent aircraft cabin, requiring customization and (re-)configuration according to the applications carried out in the cabin, identity verification and runtime integrity protection. In the Pilot use case, these devices are exemplified by considering the ST-I's generic node platform equipped with the SE and based on the ARM open architecture. Nodes' sensors, interfaces and security features are customized and tailored to the application domain. The edge devices are managed by a **master node**, which is a computationally more powerful device based on the RISC-V open hardware devoted to coordinate the airplane services, building isolated execution environments that protects confidentiality and integrity of code and data. The **remote management centre** supports enforcement of and compliance to cybersecurity	

[35] https://pubmed.ncbi.nlm.nih.gov/32400262/
[36] https://www.airbus.com/newsroom/press-releases/en/2019/09/airbus-commences-inflight-trials-of-connected-cabin-technologies.html
[37] https://www.industryweek.com/technology-and-iiot/systems-integration/article/22006020/internet-of-aircraft-things-an-industry-set-to-be-transformed
[38] https://ieeexplore.ieee.org/document/7575375
[39] https://www.researchgate.net/publication/261269790_Fly-By-Wireless_for_next_generation_aircraft_Challenges_and_potential_solutions
[40] https://www.wired.com/story/boeing-787-code-leak-security-flaws/
[41] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3033898
[42] https://www.easa.europa.eu/newsroom-and-events/news/easa-takes-important-step-increase-cybersecurity-aircraft
[43] https://ww2cdn.frost.com/wp-content/uploads/2020/01/White-Paper-Navigating-through-operational-turbulence.pdf
[44] https://aviation.report/trending-news/airbus-sees-big-data-delivering-zero-aog-goal-within-10-years

requirements through OTA reconfigurations, patches and updates of the IoT devices deployed, as domain requirements and threats evolve. Two main scenarios are envisioned:
Scenario #1 - IoT node commissioning, deployment and decommissioning: Cybersecurity must be ensured from the device initial testing and verification. Devices are registered in the remote control centre and configured appropriately. At deployment time the master node in the aircraft continuously verify identity and integrity, and reconfigure the edge devices as needed, managing data flows according to the security requirements of the applications. Once the device reaches its end-of-life, it is decommissioned securely in a compliant and sustainable manner[45].
Scenario #2 - PHM, continuous assessment and (re)configuration of cybersecurity requirements: Throughout their operations, edge devices collect a rich set of data for which integrity and confidentiality must be preserved in all the communications. As new vulnerabilities and threats are identified during the device operations, continuous security PHM, patching and re-configurations must be in place. To reduce operating costs, devices not satisfying the cybersecurity level required by a certain service, can be repurposed through network reconfigurations.

Pilot 2: Smart Micro-Factories	
Use-Case Partner	DWG (lead), UMU
Challenge: Smart Production are IT environments where OT (operational technology) and IT (information technology) are merged into an internet technology based pervasive computing system. Usually in such connected shop floors the machines and tools are connected via robust industrial specific bus-systems (e.g., MODBUS[46] or PROFIBUS[47]) protocols designed in 1970s and 1980s, with no cybersecurity layers for internet connected communication in the design. Additionally, data is often aggregated via additional sensor networks (e.g., retrofitting) in separated network layers using their own LAN or Wireless (RF) connections[4849]. These complex settings and systems are coming along with an increased attack surface, while industry needs comply with the cybersecurity regulations of the NIS directive. Even if OT and IT is segmented, cybersecurity risks from IT are propagating into OT systems with serious risks on operational safety and security of industrial facilities and production. IT standards such as ISO27000 and OT cybersecurity standards such as IEC61508 are in need to be harmonized in the EIC 62443 set of standards. For managing supply chain risk mitigation of devices, in 2021[50], the NIST has published the proposal SP 1800-34 on Validating the Integrity of Computing.	
Innovation: The smart micro-factory represents an ongoing evolution from traditional factories to fully connected, flexible and reconfigurable systems that can self-adapt to frequently changing product and production requirements. As well, the design of smart factories can reduce the attack surface from an entire production site towards a smaller compartment and unit with lower complexity. Smart micro-factory compartments can be arranged to a mesh, where data and production tasks are flowing between the compartments as a dynamic network to fulfil production tasks. New tasks from the Manufacturing Execution System will lead into dynamic rerouting of material, data and building instructions between compartments, requiring secure decentralized architectures, technologies, and protocols to be managed. The smart micro-factory use case will set up novel procedures and protocols. For this, we will consider the flexible, lightweight and robust authentication and device bootstrapping solutions of CERTIFY. The CERTIFY framework able accommodate and manage billions of devices, store their firmware, and respond to device requests of updates in a strict timely manner can support the security requirements of the smart micro-factory.	
Results: Smart Micro Factories dynamic architecture will be set up and tested in an industrial Pilot testbed. This testbed allows to improve and strengthen architecture in iterative development cycles together with industrial customers and along their specific production requirements and needs. The testbed procedures can be controlled and managed by an online management user interface to add assets, group them to compartments, control API access and monitoring the security status of the entire grid of compartments as well to initiate risk mitigation. The testbed infrastructure will result in highly resilient and secure decentralized architecture with interfaces and tools to manage the security of assets during lifetime, strengthening the cybersecurity in industrial production processes and set a foundation to secure industry 4.0. These results will be validated with industrial end users.	

[45] https://www.simslifecycle.com/2020/02/13/e-waste-safety-and-sustainability-in-the-airline-industry/
[46] https://modbus.org/
[47] https://www.profibus.com/download/profibus-standard-dp-specification
[48] https://lora-alliance.org/
[49] https://zigbeealliance.org/solution/zigbee/
[50] https://csrc.nist.gov/publications/detail/sp/1800-34/draft

Pilot 3: Tracking and monitoring of artworks	
Use-Case Partner	ST-I (lead), UZH, MOD

Challenge: Transporting exhibit masterpieces and artworks is a critical activity, which requires the utmost attention. Damaging ancient archaeological finds, paintings, or sculptures by great masters of the past would cause incalculable damage to the heritage and history of a country. The tracking and monitoring of the artworks during the transportation and during the exhibition time is a concern for all the stakeholders interested to the masterpieces, owner, transport and insurance company, Public Institution or Museum[51]. Information like: "persons (who), things, ideas (what), spatial (where), temporal (when), procedural (how) and causal (why)" need to be tracked, secured and stored. Cybersecurity is a crucial matter for the monitoring and protection of artworks and concerns issues like user/administrator role authentication and the integrity and confidentiality of sensitive data. Only entities with authenticated roles should have access to the monitored data and when transmitted only an enciphered and signed format should be used.

Innovation: Many initiatives and projects having as target the tracking and monitoring of masterpieces are now running around the world led by private organizations and/or universities in collaboration with public institutions, ministers of culture etc. The devices used for tracking and monitoring are like a **"black box"** acting as a **"data logger"**. Their task is to monitor the entire phase of movement/restoration/conservation of the masterpieces and periodically communicate a summary of the data to a remote server. In general, in case of movement of artworks the logged data are the microclimatic parameters[52], the shocks and vibrations suffered by the artwork and the geographical position. Nowadays, very few of these data logger devices available on the market are addressing the cybersecurity issues of such a critical application with the right approach. In the proposed Pilot, the cybersecurity issues are addressed by two technologic solutions:

- The first approach introduces the tracking and monitoring device (the IoT node device) a SE as a dedicated cryptographic processor[53]. The SE is certified at a high level of security. The key pairs for digital signature are generated and stored by the SE and used by authorized and authenticated administrator/user to sign data. The generated private key cannot be readout of the SE.
- The second approach use a dedicated HSM for key storing. The data is being signed with the help of the private key and included in the DLT[54] for immutable storage. The public/private key pair should never leave the device even under malicious software modifications. This shall be guaranteed by a HSM storing keys. Those are then not accessible to firmware components running on the IoT device. The IoT device only asks the HSM module for signature, the HSM signs the DLT Transaction, and the transaction equipped with the corresponding signature is sent to a DLT for permanent storage.

Results: An IoT node device, with an embedded dedicated cryptographic processor based on a SE certified at a high level of security attached to a masterpiece/artwork and to its crate/package, can measure and record mechanic vibrations and variations in temperature, humidity, pressure and provide, throughout the journey, the current geographic position of the artwork. A data view of the logged data is available to the stakeholders after authentication to the monitoring device, view and scan the recorded data, plot the data on the time scale and analyse out range conditions if any. CERTIFY will provide an effective alarm system reporting when pre-set thresholds for critical values of microclimatic and vibration are met or exceeded and performance analysis of the two proposed technical approaches to cybersecurity.

1.2.4. Project methodology

CERTIFY is divided into 7 WPs and 3 Pilots. Project activities will be driven by the overall project objectives and the collected requirements. The project will be executed over two iterations (Fig. 5) linked to the project Milestone (MS) with multiple feedback and learning loops such that the Pilot results will inform technical development of components based on agile development techniques. This means that will get functional Pilot complements faster, through which real-world feedback will be provided to drive the development in the next cycles.

- First iteration: This iteration starts with the **baseline** step, which marks the beginning of CERTIFY, extracting the needs of the IoT security management focusing on the foreseen use cases and the involved stakeholders always incorporating the citizens' view [T1.1]. In parallel, we will identify the main attack scenarios and threats [T1.2]. All this information

[51] https://ur.booksc.eu/book/62845735/dc74ab
[52] https://www.zora.uzh.ch/id/eprint/136294/
[53] https://ieeexplore.ieee.org/abstract/document/9110379
[54] https://ieeexplore.ieee.org/abstract/document/7987376

will be translated into requirements and technical specifications. These requirements will guide the first development of the CERTIFY components (Infrastructural services [WP3], IoT platform [WP4] and Software platform [WP4]) and its integration [T2.2], providing a first version of the CERTIFY framework [T2.1] (**innovation spark and flames** steps). The first iteration ends with the **demonstration spark** step, in which the framework and its technologies will be demonstrated through comprehensive scenarios and validation campaigns [T2.3]. The validation campaigns that have been chosen highlight the social, environmental, technological and financial impact of data operations in various domains. They will be based on the following use cases: aircraft, microfactories and tracking of artworks. Objective and subjective feedback collected from **CERTIFY** internal (consortium) and external stakeholders attending the campaign events will be analysed, to provide feedback for the design of the CERTIFY security lifecycle methodology [T1.3] and a consolidated architecture [T2.1] (**innovation fire**).

- Second iteration: The second iteration follows a similar process, collecting the previous feedback to guide the final development of the CERTIFY components [WP3, WP4, WP5] and the second version of the CERTIFY integrated framework [T2.1] (**demonstration flame**). As before, the framework is validated in the **demonstration fire** step [T2.3]. The iteration ends with three key aspects (**consolidation**), namely (a) the engagement of relevant stakeholders [T6.1] (b) the communication and dissemination activities to ensure wide results visibility [T6.2] and (c) the exploitation and financial sustainability of the CERTIFY innovations during and after project lifetime, including standardisation activities and contributions to relevant fora [T6.3].

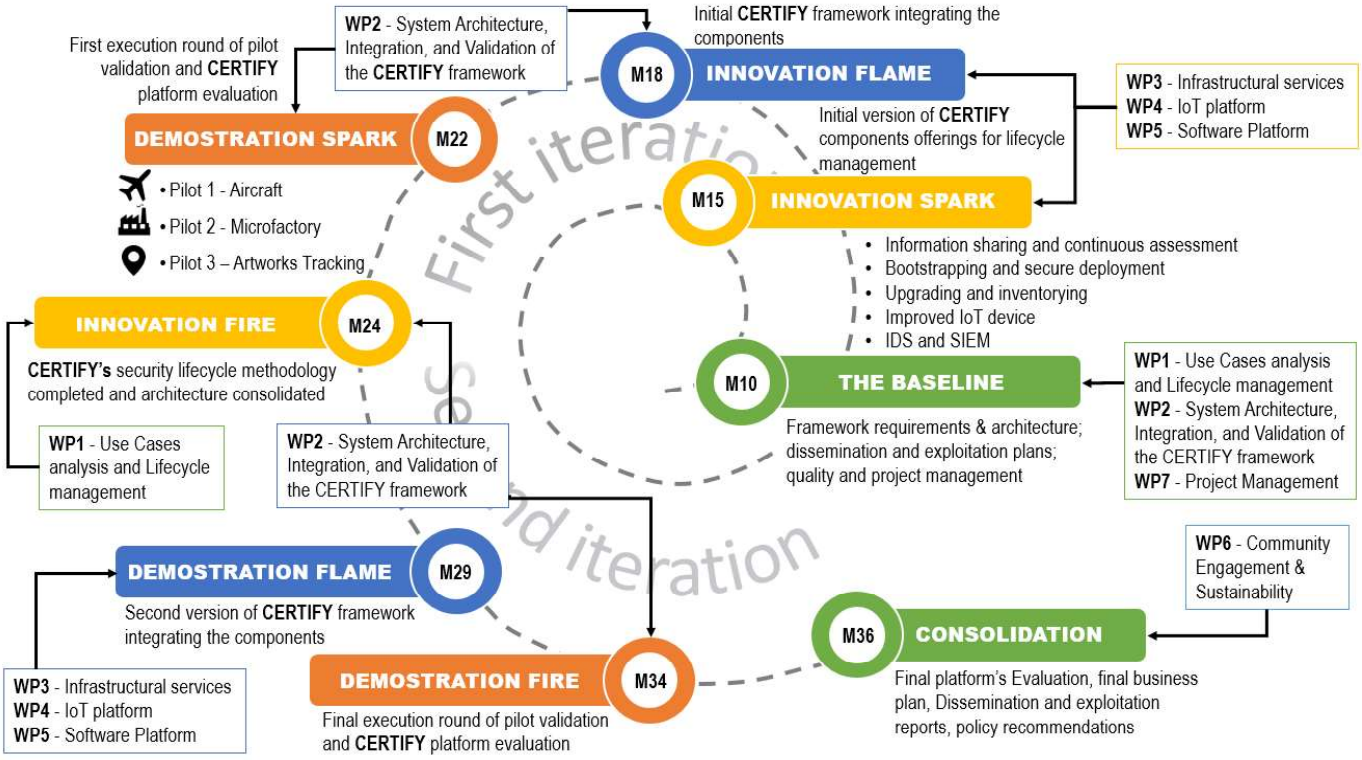


Figure 5 CERTIFY methodology

1.2.5. National and international innovation related activities

CERTIFY has considered the following National or International Initiatives in the project definition and will take them into account in the following areas for the project execution. Some of them are already participated by CERTIFY partners, which can act as 'linking partners'. Some others will be contacted through the activities foreseen in Section 2.2.1 [WP6] to make sure that potential synergies among them are considered in the project execution.

Table 4 National or international research and innovation activities linked with CERTIFY

CyberSec4Europe	It brings to CERTIFY results of interest related to cybersecurity certification and security information sharing. Partners: **UMU**
BIECO	Supply chain security lifecycle management, MUD files and security evaluation. Partners: **UMU**
CyberSEAS	Cybersecurity aspects of the energy supply. Partners: **ENG**

ANASTACIA	Dynamic orchestration and deployment of security policies and actions within complex and dynamic Cyber Physical Systems (CPS) and IoT architectures. Partners: **Collins, UMU**
COLLABS	Cyber intelligence solutions for collaborative manufacturing in the Industry 4.0 enabled by the Industrial Internet of Things (IIoT). Partners: **Collins**
ASSURED	Formally verified operational assurance in Cyber Physical Systems. Partners: **Collins**
CONCORDIA	It brings to CERTIFY results on the use of multiple blockchains (e.g., Bifröst), blockchains on IoT devices, and platforms for threat visualizations. Partners: **UZH**.
BC4CC	It brings results on multi chain interoperability to CERTIFY. Partners: **MOD, UZH**
IRIS	It brings to CERTIFY high impact solutions and policy recommendations to facilitate public-private collaboration on information-sharing and cyber threat intelligence. Partner: **ECSO**
2019 and 2020 -EU-IA-A4CEF	It brings a full set of processes set up to build and run an IoT Certification Scheme and the first andidates' cybersecurity certification scheme (EUCC and EUCS) under the CSA. Partners: **RAL**
CNECT/2020/ OP/0069	It aims at creating a European hub to foster the interaction among EU cybersecurity certification stakeholders, bringing a platform to exchange best practices, tools and services with relevant stakeholders and also to enhance the visibility of the CERTIFY results. Partners: **ECSO**
EPI-SGA1 and EPI-SGA2	Solutions for the supply of the rails of the High Performance core processing unit and the hardware accelerators based on RISC-V architecture. Partners: **ST-I**
HECTOR	Efficient, secure and robust implementation of cryptographic algorithms. Partners: **ST-I**
DIH-World	European project for the transfer of disruptive technologies to SMEs brings CERTIFY convening power to events. Partners: **IoT-DIH**

1.2.6. Interdisciplinary approach and Integration to Social Sciences and Humanities

CERTIFY also adopts an inter-disciplinary approach, integrating assets, information, expertise, techniques, tools, methodologies and concepts from diverse disciplines and further develop their application. The inter-disciplinary elements include IoT security evaluation, security monitoring, Information sharing and upgrading, secure IoT Bootstrapping, Open HW based IoT security and security management tools. The project's consortium has the relevant expertise (as evidenced in Section 3) to carry out the interdisciplinary aspects of the project, integrating knowledge from several stakeholders beyond academic disciplines. This scheme will be applied to several vertical solutions [Aircraft Cabin, Micro-Factories, artworks] to address different markets: manufacturing, construction, heritage, etc. And it is also expected that it can be the key for future efficient technologies like Internet of Medical Things, smart homes, sensors for guided vehicles, smart monitoring sensors, etc. CERTIFY integration of multiple disciplines will be complemented by its multisector approach. The concept of CERTIFY, as the development of a security management framework for IoT, does not include, raise or prescribe any concerns related to social sciences and humanities (SSH). In CERTIFY, the social sciences are involved as an integrated part of the development of the framework to support the system industrial/social integration as well as feedback. As a basis for this work there is a responsible research and innovation (RRI) approach which has boosted the Pilots approach, applied in WP1. RRI as such emphasizes the role of societal actors such as researchers, citizens, policy makers, business, and third sector organisations that collaborate in research and innovation processes, with the aim to support and enrich the process as well as its outcomes with the values, needs and expectations of society. On top of the impact towards social benefits from CERTIFY is outlined in Section 2.1.

1.2.7. Gender dimension

CERTIFY is well aware of gender issues in the digital society, and how it is especially visible in science and technology areas, where in fact females are underrepresented in the EU ICT sector: only 18.5% of all ICT specialists employed in the EU are female[55]. Hence, the consortium is fully committed to the integration of the gender dimension and gender equality in research, and how it can affect the final project results. In that sense, in addition to encourage women participation and support their working conditions, it is essential the involvement of female colleagues in all phases of the project development and encouraging gender balanced Pilots and deployments as a guarantee of an appropriate and inclusive design and implementation, adapted to all the peculiarities, of a key area such as privacy. The CERTIFY consortium will participate in international initiatives aimed at reducing the gender gap in ICT and especially cyber sectors. As an example, it will carefully follow, and possibly participate in initiatives proposed by Women4Cyber (W4C),

[55] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

of which ECSO is a founding member. Additionally, several on-going initiatives will be continuously monitored, including the European Institute for Gender Equality[56], and national activities such as awareness raising activities promoted at national and regional levels. With regard to the dissemination and exploitation of activities, the participation of women should also be encouraged in order to reach a wider audience and convey the details that have been taken into account during the project and in its results. For this reason, in order to advance from the roots, the groups have in-house regulations preventing discrimination of employment opportunities for women and will adhere to the Non-discrimination Principle and Gender Balance stated in the European Charter and Code for Researchers. Finally, the groups will ensure that none of the components in the CERTIFY platform, including, but not limited to, modelling, composition, simulation, orchestration, optimisation, proof-of-concepts and their implementations, will be gender-specific. In the context of machine learning, special emphasis will be given to mitigate and eventually completely counter discriminatory practices that lead to unfair data-driven model design. A steady stream of empirical findings has shown that data-driven methods can unintentionally both encode existing human biases and introduce new ones. CERTIFY will adopt a "fairness, accountability and transparency" approach to address off-the-shelf machine learning techniques that produce behaviour that is intuitively unfair. Finally, gender considerations will be deeply integrated in the personal data protection compliance and validation approach to be deployed in the CERTIFY project, particularly throughout the performance of regular Data Protection Impact Assessments, which will consider the views of end-users towards validation of trust in the proposed solutions. This exercise will incorporate specific safeguards to ensure these end-user consultations are performed in a non-discriminatory, gender-balanced manner which ensures relevant inputs obtained are raised to the attention of the consortium's Data protection Officer (DPO) for its integration into the data protection by design and by default approach followed by CERTIFY.

1.2.8. Open Science Practices

Resonating with the principle 'as open as possible', CERTIFY wholeheartedly supports the goals of the Open Science Policy under Horizon Europe and thus, appropriate open science practices will be implemented as an integral part of its proposed methodology as described below. In particular, the project aims at contributing to the EC European Open Science Cloud initiative by identifying services, resources, and use cases that will be contributed in accord to FAIR (Findability, Accessibility, Interoperability and Reusability) management policies. Inspired by Responsible Research and Innovation (RRI) and Open Innovation, CERTIFY will follow a co-creation approach to define tailored and contextualised engagement strategies and agile methodologies for maximising the sustained social acceptance of the CERTIFY open innovation package. The objective is to bring additional experiences and perspectives to the decision-making processes, while also enabling stakeholder accountability in the development of solutions to emerging issues they are called to answer. It is worth noting that all data gathered from involved end-users during the co-design process and the demonstrations will be pseudo-anonymised prior to processing, to ensure General Data Protection Regulation (GDPR) compliance. Furthermore, the project has dedicated part of its budget to cover the fees associated with open-access publication to facilitate dissemination and reuse of the project's results. Project participants, for various reasons, may need to submit articles to journals (or proceedings) that only offer a lower level of open-access, requiring either parallel publication or an embargo period. The need for this will be evaluated on a case-by-case basis and will balance benefits against the less convenient or delayed access to the result. In any case, at least the final author's version of every accepted paper will be made publicly available, in accordance with the rules posed by many journals. In this respect, the project will use widely self-archiving (or green open access) services for research communities like Zenodo or OpenAire which will balance traditional publications and open-access. Moreover, the project will consider to contributing to the Pilot on open access to research data in Horizon 2020: the Open Research Data (ORD) Pilot and will pursue its researchers to use the Open Research Europe[57]. To facilitate the access to the results, CERTIFY will publish on major Podcasts platforms a recurring Podcast format targeting researchers, economy and developers covering topics on hardware security, open hardware and IoT lifetime security in Europe. Furthermore, CERTIFY is committed to an open-source model of exploitation of the technologies that will advanced and proposed as part of the project and that will bring citizens from several parts of Europe: Germany, Italy, Spain, France, Greece, Belgium, Ireland and Switzerland by utilizing links with school networks, local government, active citizen groups, hacker/makerspaces as well as artistic communities across Europe.

1.2.9. Data Management

CERTIFY project will generate and consume research data through the implementation of the use cases. Therefore, the Data Management Plan (DMP) will be generated and maintained during the whole lifetime of the project by WP7, as a

[56] https://eige.europa.eu
[57] https://open-research-europe.ec.europa.eu/

deliverable following the Horizon Europe Data Management Plan template. The CERTIFY DMP (D7.3) will describe plans for creating, organizing, documenting, storing, and sharing data. It will consider issues such as data protection and confidentiality, data preservation and curation, methodologies and standards applied, and will provide a framework that will support researchers and their data throughout the course of their research and beyond. This plan will be delivered in M3 and will be constantly updated through the project lifespan, including what happens to project data after the contractual obligations. The project fully commits to follow and foster FAIR principles among its use cases. During the project lifetime, the project office will enforce and monitor that all project outputs and research activities are following those principles and will ensure and promote that adequate actions are taken upon their fulfilment (like deposit of research outputs in relevant repositories, use of adequate metadata, etc.). DMP is regularly updated by UMU who is responsible for data management and quality assurance. The DMP covers the FAIR principles as follows:

- **Findability** of data/research outputs: CERTIFY data have unique identifiers - DOI (Digital Object Identifiers)[58]. Data and their metadata are hosted on open data repositories satisfying requirements of data providers. Among the repositories we will consider for data sharing are EOSC, EU Open Data Portal, PCQC and AO Spine. The other research results (models, publications, technical reports etc.) are stored in the same way. Extensive metadata, including descriptive information about the context, quality and condition, and characteristics of the data in human and machine-readable format will be attached to the datasets, including the unique identifier.
- **Accessibility** of data/research outputs: The consortium is fully committed to the European Commission requirements to support **open access for published articles**. All scientific publications of the project's results will be granted open access according to publisher and law regulations as set out in the grant agreement, with a specific budget allocated to cover the open access article processing fees whenever appropriate. To access the data free and open protocols such as HTTPs will be used. The Free Datasets will be published under Creative Commons Licenses (CC-BY and CC-BY-NC, depending on the requirements of partners).
- **Interoperability** of data/research outputs: The project will engage to deliver in a timely manner and as appropriate, standards, specifications and methodologies from project activities with the other EOSC relevant projects (especially those awarded under the same topic) in order to foster to the maximum extent interoperability between the different services and tools being developed.
- **Reusability** of data/research outputs: The CERTIFY project aims to adopt (whenever possible and upon agreement with partners) the following default licenses for the research outputs: Creative Commons CC-BY 4.0 for documents, reports, presentations and training material; Apache License Version 2.0 (Open Source Initiative (OSI) approved) for any software development; Gold Open Access to all scientific and technical publications in journals.

2. Impact

2.1. Project's pathways towards impact

2.1.1. Expected Outcomes and Impacts

2.1.1.1. CERTIFY contribution to HORIZON-CL3-2021-CS-01-02 Expected Outcomes

CERTIFY's results represent a unique contribution to the expected outcomes:

O1: Reduced security threats of open source hardware for connected devices. *Linked to objectives 1, 2 & 3 (WP1, WP4, WP5).*

Challenge: The restricted environment of many IoT devices and constraints on cost and/or to limitations on power consumption, does not allow the deployment of more complex protection schemes (e.g., TPM, Sandboxing applications in managed memory partitions) and similar approaches that often rely on OS support to ensure cybersecurity.
Expected contribution: **Scientifically,** CERTIFY will advance the state of the art by introducing new approaches for the definition of customized, software-based TEEs and the SE implemented either in hardware or software. Such solutions will be based on functionalities provided by open hardware architecture and ecosystems. CERTIFY will develop novel self-monitoring, self-intrusion detection, network bootstrapping and security auditing mechanisms adapting and extending current techniques to the computational capacities of IoT devices. **Economically and technologically**, the above-mentioned SE solutions allow a manufacturing cost reduction (not requiring dedicated hardware components) and ease the secure deployment, being based on the reprogrammable generic node platform and customized with the introduction of a software/hardware SE designed in alignment with the Global Platform's open ecosystem for secure-by-design digital services and devices. **Societally**, CERTIFY allows a timely sharing of security relevant information among all the stakeholders involved in the device lifecycle management (e.g., manufacturer, consumer) raising security awareness on IoT products and services across different domains. As consortium we have

[58] https://www.doi.org/

a well-established network throughout the broad European Innovation Ecosystem, due to long-term business-partnerships with intermediaries such as the Enterprise Europe Network (EEN), and we will maximise our reach within the broad EU manufacturing sector, targeting collaborative experiments between DIHs, SMEs and mid-caps.

Scale & significance: Two billion industrial IoT & utility connected devices will be deployed by 2022 and the IoT security services market will be > $10 billion in 2021 and with > 90 million new 5G IoT connections in 2026. More and more solutions are adopting the RISC-V architecture, whose organization currently has one third of its members in Europe. Mainly thanks to its open-source Instruction Set Architecture (ISA) and a better power consumption performance, such an open architecture is expected to reach by 2025 a penetration rate of 28% in IoT, 12% in industrial and 10% in automotive environments. To further foster the adoption of these open solutions even in safety critical environments CERTIFY aims at strengthening their security and providing evidence supporting an agile certification process.

Target groups: Researchers, industry, consumers, manufacturers, Integrators, Network Operators, SP.

iKPI 1.1: Validation of the framework in 3 use cases; **iKPI 1.2:** >6 seminars/events/expo to showcase the technology demonstrator; **iKPI 1.3**: adherence and contribution to >= 2 open standard initiatives

O3: **Effective management of cybersecurity patches for connected devices in restricted environments such as IoT devices.** *Linked to objectives: 1, 3 & 4 (WP3, WP4)*

Challenge: The software/firmware update process for IoT devices faces different challenges related to the constraints of IoT devices and networks. Often different software versions and dependencies between components are running. , There is a need for distributed updating approaches able to minimize the resource impact while considering dependencies among the deployed components.

Expected contribution: **Scientifically,** CERTIFY will explore a collaborative and decentralized patching management for a robust and efficient dissemination mechanism of software updates based on rapidly evolving solutions such as blockchain technologies. Moreover, patching will be complemented by extending the notion of threat MUD files, to provide fast mitigations before a patch is released. **Economically and technologically**, CERTIFY will bring patching functionality closer to the end devices to reduce latency and network overhead. Moreover, updates will be managed through a distributed cloud platform to manage billions of devices thanks to a security Configuration Management Database (CMDB). CERTIFY will enhance current software update standards (e.g., IETF SUIT WG, LwM2M), focusing on communication security aspects, to manage the complexity of IoT deployments, and the different software versions. **Societally,** CERTIFY will foster the collaboration between all the stakeholders involved in the IoT lifecycle throughout its cybersecurity information sharing secure configurations, threats and mitigations via MUD files. As smart embedded devices interact with humans and the environment through sensors and actuators, benefits of more secure products are propagated to the whole society (from producer to consumer, including users simply interacting with IoT environments). By reducing the exposure to cyber risks even online privacy concerns related to IoT solutions can be mitigated (e.g., baby monitors).

Target groups: Researchers, industry, consumers, public authorities, manufacturers, Conformity Assessment Bodies (Labs and Certification bodies), National Schemes (NCCA), Integrators, Network Operators, SP.

Scale & significance: Security companies report astonishing numbers on security breaches ascribable to unpatched systems and on the use of outdated software, respectively 27% of the surveyed companies (37% in Europe) and 70% of the systems. This scenario opens up for severe security breaches that, along with the hyper interconnectivity of modern systems, could lead to cascading incidents. IT professionals mention lack of knowledge about the vulnerability/patch, incompatibilities found in the patching process, trust in external threat detection and late inventorying of new hardware/software among the main causes for the delayed patching. Surveys estimate an average cost of 7.9M$ per data breach. Solutions designed in CERTIFY can improve the security posture of IoT environments.

iKPI 3.1: One extended MUD model generated for 3 devices (WP3); **iKPI 3.2:** Security information sharing solution targeting the requirements of >= 4 stakeholders; **iKPI 3.3:** Extension/contribution to at least 1 standard related to SW updates; **iKPI 3.4:** IoT user and community engagement initiatives >= 3

O5: **Effective mechanisms for inventory management, detection of insecure components and decommissioning.** *Linked to objectives: 1, 2 & 4 (WP1, WP3, WP4, WP5)*

Challenge: Due to the increasing interconnectivity and complexity of IoT systems, vulnerabilities in one device could affect other devices deployed in the same environment. Therefore, in addition to the evaluation of the security level of the device. Dependencies should be tracked in order to identify potential risks derived from cascade effects. Insecure

components and corrupted updates could affect the security of other components in a certain device, so it should be detected and reconfigured in an efficient way.
Expected contribution: **Scientifically,** CERTIFY will evaluate CMDB inventorying solutions in IoT and embedded environments to store security requirements and security level associated with each device (e.g., the security patches that need to be installed to keep using the device for a given function, or the identity certificates of the trusted devices). In such a way, CERTIFY will also provide mechanisms to repurpose/reconfigure untrusted devices unable to meet the cybersecurity requirements. Coupled with the dynamic and semi-automated security assessment of CERTIFY checks if, in a mutated security setting (due to new vulnerabilities discovered, updates and patches applied), the security properties are still fulfilled. **Economically and technologically,** CERTIFY will reduce recovery time and costs by capturing device interdependencies performing security assessment and disseminating mitigations. Moreover, repurposing the device to cope with the mutated threat landscape provides a further opportunity for cost savings. **Societally,** CERTIFY will provide a basis towards the deployment of the CSA and the NIS directive, providing mechanisms and tools for continuous information sharing and agile reaction against new vulnerabilities and managing the security of the IoT device throughout its lifecycle.

Target groups: Researchers, industry, consumers, manufacturers, Integrators, Network Operators, SP.

Scale & significance: The CMDB market is estimated to be USD 13,2 Bn in 2021 with a CAGR growth of 8.3% reaching USD 19.67 Bn by 2026[59] due to its ability to lower operational cost and collecting accurate configuration evidence.

iKPI 5.1: Device-behavioural analysis on 3 devices executed at runtime; **iKPI 5.2:** Demonstration of an inventorying solution able to consider >=10 security specifications of 3 devices; **iKPI 5.3:** Dissemination of the lifecycle management to >= 5 scientific conferences

O6: **Methods for secure authentication and secure communication for connected devices in restricted environments such as IoT devices**. *Linked to objectives: 1 & 3 (WP4, WP5)*

Challenge: The process of bootstrapping involves authentication, authorization, and key management operations, vital to control and protect network resources and data communications. Nevertheless, traditional bootstrapping is not adapted to the features of recent wireless technologies (e.g., NB-IoT) formed by IoT devices with limitations in computing and networking capacities to implement complex security protocols.
Expected contribution: **Scientifically,** CERTIFY will evaluate the use of secure, flexible, lightweight and robust bootstrapping mechanisms with the design of novel solutions for identification, authentication and secure configuration deployment based on the usage of behavioural profiles and enhancements to the generic IoT Device Node Architecture for integrity and data confidentiality. **Economically and technologically,** CERTIFY will support the standardization work developed within the IETF, NIST, IEEE, IPSO, Zigbee or OMA, which have devoted efforts towards the progress of bootstrapping mechanisms in the IoT. **Societally,** the transparent device authentication and secure configuration of the devices automatically provided by CERTIFY will enhance the security of IoT devices without requiring additional knowledge and expertise to the consumer.

iKPI 6.1: Less than 1 second to mechanisms to compute heavy cryptographic primitives (e.g., for signature, signature verification, hashing) through SE on IoT devices (WP4); **iKPI 6.2:** Design of solutions usable in compliance with 2 standards; **iKPI 6.3:** Secure reconfiguration solution requiring <= 1 user actions

Target groups: Researchers, industry, consumers, manufacturers, Integrators, Network Operators, SP.

Scale & significance: The Mirai attack in 2016 marked a turning point in security showing how security misconfiguration, and/or identification and authentication failures can cause catastrophic effects due to the direct internet connectivity of embedded devices. In 2021 the same factors are still listed in the top 10 security risks[60]. And while secure boot and authentication are listed among the best practices[61], nowadays vulnerabilities of embedded devices are still exploited to build botnets each constituted by more than 30 million zombie endpoints allowing malicious actors to have profits > 100,000$ per month[62].

[59] https://finance.yahoo.com/news/global-configuration-management-markets-2021-185100312.htm
[60] https://owasp.org/Top10/
[61] https://blackberry.qnx.com/en/embedded-system-security/ultimate-guide/
[62] https://www.ustelecom.org/wp-content/uploads/2021/03/USTelecom-CSDE-2021-Botnet-Report.pdf

2.1.1.2. CERTIFY contribution towards the wider impacts, expected impacts in the long term

In the long term, these expected outcomes will contribute to the following Expected Impacts:

Impact 1: Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
In accordance with the principles and objectives of the relevant EC communications on the topic, the CERTIFY will be constituted by a mix of methodologies, tools and technologies enabling cyber-resiliency for European entities - by protecting and timely reacting to cyberattacks, and by increasing the cybersecurity situational awareness for the networked devices. The project also supports maximisation of the EU's digital capacities through promotion of standards, events, cybersecurity training, empowering communities and capacity building achieved through the technological demonstrator developed in T6.1. **Target groups**: European industry and SMEs, public actors, policy makers, Cybersecurity professionals. **Scale & significance**: CERTIFY will strengthen EU ambitions and increase EU cybersecurity capacities in strategic technologies by increasing SW, (open solutions) HW and supply chain security. Fully aligned with the priorities identified by the EU's Cybersecurity Strategy for the Digital Decade to improve the cybersecurity of connected devices on the market and increase resilience, and ECSO for future challenges to strengthen European society, CERTIFY can also contribute to reduce the dependence of the EU on non-EU cybersecurity solutions. The participation to EU based events in the context of the (Industrial) IoT environment will increase the visibility of the EU cybersecurity capabilities enabled by CERTIFY endorsing the application of technological innovation designed and developed in Europe.
Impact 2: More resilient digital infrastructures, systems and processes
The CERTIFY framework will focus on ensuring security by design and by default for IoT devices and, throughout its security information sharing, further developing the European IoT community by maintaining an active and collaborative ecosystem of stakeholders. Furthermore, the CERTIFY solutions can detect and react to abnormal and/or out of range running conditions. The CERTIFY authentication, integrity, confidentiality and secure configuration mechanisms will increase the resilience of the digital infrastructures, systems and processes to security attacks. **Target groups**: Researchers, industry, public security authorities, manufacturers, CA, ISACs. **Scale & significance**: CERTIFY framework will lead to improved defence against focused attacks, e.g., by increasing the share of attacks and breaches that are prevented (~87% in 2018) while decreasing the time needed to detect security breaches (55% of breaches detected within a month in 2018), resulting in decreasing the economic and reputational cost of incidents[63].
Impact 3: Increased software, hardware and supply chain security
The CERTIFY innovation approach provides a number of features that effectively and efficiently support the management of security throughout the IoT supply chain (SC), including: hardware and software cybersecurity management at different abstraction levels; identification and sharing of risks in heterogeneous, complex and dynamic ecosystems; tools for enforcing security mechanisms at hardware and software level; tools for detecting and mitigating violation; reconfiguration of IoT devices; secure deployment and upgrading. The availability of the CERTIFY solution will boost the productivity of security component providers - as well as the quality of the delivered products - thus ultimately improving their market offering at the EU level. **Target groups**: Researchers, industry, SMEs, public security authorities, manufacturers. **Scale & significance**: ENISA estimates there will be 4 times more supply chain attacks in 2021 than in 2020[64], mainly due to Advanced Persistent Threat actors, with devastating large-scale and ripple cross-border effects. CERTIFY may help in reducing or containing the rise of supply chain attacks and reaching a common level of security across all supply chain actors by developing solutions for continuous monitoring and patch management to increase cyber resilience.
Impact 4: Secured disruptive technologies
The project builds upon a number of cutting-edge technologies, such as distributed ledgers (DLT), dedicated cryptographic processors, TEE, ML, smart contracts, OTA updates, etc. CERTIFY will significantly contribute to their adaptability to IoT scenarios increasing their current TRL. To show specific examples, CERTIFY results will increase the use of DLTs in the IoT sector, providing an efficient platform to engage with researchers and industry, increasing profitability and generating investments in longer-term technological competitiveness. CERTIFY will also develop a dedicated SW toolkit facilitating the use of the cryptographic functionalities and it will make feasible the integration of a dedicated cryptographic processor in constrained IoT devices. Moreover, via its support to the device repurposing, CERTIFY will be a contributor to green results. Enhancements on reprogramming, OTA management and patching for

[63] https://www.accenture.com/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf
[64] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

security and functional reasons will extend the life of physical IoT devices reducing costs and environmental impact. Finally, CERTIFY will support and enhance pioneering approaches from well-known entities such as the NIST regarding onboarding and lifecycle management and cryptographic module validation, or the IETF regarding behavioural profiles[65] and upgrading[66].

Target groups: European industry and SMEs, public actors, Cybersecurity professionals.

Scale & significance: CERTIFY project will directly impact the evolution of the development and prototyping boards for IoT thanks to the ST-I worldwide mass market. Moreover, trusted events triggered by secure IoT devices can be directly used in blockchain solutions automating currently manual business processes. Such automatization can speed up the digital transformation, thus, having a large impact on the European economy.

Impact 5: Smart and quantifiable security assurance and certification shared across the EU

The CERTIFY framework will ease verifiability and tracking of the cybersecurity requirements throughout the whole device lifecycle and therefore potentially ease the way to the re-certification - with a potentially high impact of cost savings. The security evaluation methodology will take into account current certification schemes, standards and regulations such as the CSA, and the automation of the process will improve the efficiency of the CABs (Conformity Assessment Bodies). The number of features left to be manually re-evaluated during the recertification process will be significantly reduced allowing faster recertification. Finally, CERTIFY is intended to improve the level of collective resilience and allows a wider adoption of common European cyber security standards for IoT devices that are placed on our market which is exactly the purpose of the European Cyber Resilience Act announced recently.

Target groups: Researchers, industry, consumers, public authorities, manufacturers, Conformity Assessment Bodies (Labs and Certification bodies), National Schemes (NCCA), Integrators, Network Operators, OES, SP.

Scale & significance: CERTIFY will support the practical and comprehensive implementation of both the CSA and the NIS Directive providing evidence of continuous compliance with the specified cybersecurity requirements. The decentralized security information architecture between manufacturers, local ISACs, consumers and certification authorities, can increase transparency, reduce response times in presence of threats and setting up a baseline for security certification. This is intended to cope with the expected large adoption of connected devices which is putting a huge pressure on manufacturers to meet time to market. CERTIFY is expected to find the right balance between security and business needs while helping manufacturers implement baseline security requirements in the most cost-efficient way and scale to address the big market demand.

Impact 6: Reinforced awareness and a common cyber security management and culture

Cybersecurity does not only challenge researchers and industry. It is a major concern for European societies at large. It is, therefore, of paramount importance that cyber security experts will be made aware and kept updated about the major threats, and new technologies reducing risks through certification, live upgrades, and reconfiguration. In this sense, CERTIFY will empower users, manufacturers, CA and experts, among others (target groups), through specific tools and mechanisms to facilitate cybersecurity management. CERTIFY also provides a collaborative framework for security management, reinforcing a common knowledge and action against zero-day threats.

Scale & significance: Our ambition at CERTIFY is also to bring our advances in cyber security to SMEs. To disseminate our results, we will build experiments, demonstrators, and offer holistic support (cybersecurity mentoring, technological advice, etc.). CERTIFY has planned different sessions for the assessment of the impact caused by its solution and to gather direct information about end-users/stakeholders' interests and feedback, in order to have a realistic estimation of their cybersecurity potential. These sessions will include different activities and seminars to attract the interest of different audiences and will perform some live evaluation sessions to gather the opinion of real end-users carrying out an impact assessment based on an ad-hoc methodology developed to evaluate the level of accomplishment reached for the objectives set in CERTIFY, having in mind the KPIs set for the project.

2.1.1.3. CERTIFY contribution to key strategic orientations of the HE strategic plan Strategic Plan 2021-2024, Cluster 3 - Civil security for society in the long term

KSO A: Promoting an open strategic autonomy by leading the development of key digital, enabling and emerging technologies, sectors and value chains

Different key sectors of the economy are going through a new digital transformation (e.g., transportation, factories and art gallery). With the use case demonstrations, CERTIFY equips them with solutions for a comprehensive cybersecurity awareness and protection throughout the whole IoT lifecycle: pioneering tools, mechanisms and technologies for the

[65] https://datatracker.ietf.org/doc/html/rfc8520
[66] https://datatracker.ietf.org/wg/suit/about

management of the IoT device from design to decommissioning are introduced. The technology demonstrator (WP6) will also pave the way for future innovation efforts and experimentation in the value chain of other industries.
KSO D: Creating a more resilient, inclusive and democratic European society
CERTIFY will contribute to bridge the gap between the EU-wide cybersecurity research and industrial communities, promoting sharing of best practices, development of skills, best use of resources and innovation with the intent to increase capacities and competitiveness in Europe, thus supporting the objectives of the European Cybersecurity Competence Centre (EUCC). Moreover, protection, detection, mitigation, and resolution technologies of the CERTIFY framework increase the resilience of digital infrastructures, supply chains, systems and processes making them more resistant and reactive to security attacks. CERTIFY promotes a cultural shift in sharing security information and best practices across organizations and countries, in full respect of GDPR and other regulations, strengthening the EU cybersecurity and creating a more secure, resilient, open and democratic EU society prepared for emerging threats.

2.1.2. Barriers/obstacles and framework conditions

Cybersecurity is traditionally suffering from issues concerning misalignment incentives (e.g., who's responsible for a security breach, conflicting interests), lack of information on the actual cost/impact of cyberattacks, and externalities (networked and interdependent systems). CERTIFY aims to build a lifecycle security management by bringing together all the different stakeholders in charge of the device maintenance in a common security information sharing environment. Moreover, the industrial technological demonstrator (T6.1) will showcase the CERTIFY methodologies and technologies and continuously incorporate market feedback.
Insufficient stakeholders' involvement in the following of the CERTIFY results at communication and dissemination events. Tailored actions have been defined in the WP6 for the commitment of stakeholders from different sectors and industries. Workshops (mainly), conferences and demonstrators (for other audiences but able to gather important information for stakeholders) will look for the attendance of relevant actors in the interactive industries to put the focus in the market engaging technology and content providers. CERTIFY will also engage with the Core Service Platform for EU Cybersecurity Certification Stakeholders of the European Commission at the early stage of the project to align objectives and promote the CERTIFY lifecycle security management approach. Cybersecurity technologies develop rapidly, and it is difficult to foresee their evolution, which may influence technical design decisions. CERTIFY will be engaged in a continual technology watch effort and safeguard that the development process will comply with all related standards and that new security requirements that may arise will be properly and timely gathered and processed.
Varying EU states regulations may pose challenges in the adoption of the proposal. Governmental regulations of data privacy present the concern of significant legal consequences. CERTIFY will fully comply with all European policies relating to Data protection, respecting and incorporating possible modifications that regulation may suffer

2.2. Measures to maximise the impact

2.2.1. Plan for the dissemination, exploitation and communication activities (D&C&E)

The impact of the project is supported by the implementation of a comprehensive D&C&E plan, released in month M9, and maintained until M36 (Deliverable D6.3).

2.2.1.1. Dissemination strategy

The project will ensure the correct dissemination of project results defining an effective dissemination strategy, targeting specific groups with predefined objectives, channels and initiatives, as described in Figure 6.

2.2.1.2. Communication strategy

The project identity and the communication strategy will be developed over the lifetime of the project. All promotional and publicity material will specify that the project has received funding from the EU and will display the relevant logos. The potential target audience and their interest in CERTIFY activities is reported in Figure 7.

Figure 7 Dissemination channels and activities

Target groups	Dissemination objective	Channels and actions
Universities, RTOs, in the areas of cybersecurity, privacy, PETs, data sharing, etc.	Advancing own research, training personnel & students on CERTIFY technologies.	Publication of the project results in relevant scientific journals and magazines. Presentation at relevant conferences, workshops and events. Organization of technical workshops (at least 2). Preparation of educational material for M.Sc.s and PhD students on CERTIFY research topics.
Industry, SMEs, solution providers, industrial partners	Fostering use of project results in operations or R&D activities.	Participation in industrial exhibitions, business conferences and trade fairs. Holding of dedicated industry workshops (at least 2 virtual Info Days with European coverage and one Info Day in the city of Valladolid, with the support of the Institute for Business Competitiveness of Castilla y León (ICE). Participation in the DIGIS3 network..
CERTS and CSIRTS	Practically implementing the recommendations of the NIS directive and CSA.	Publication of white papers on security lifecycle management technologies within / across sectors, with emphasis on the case studies. Liaison with ENISA and national CSIRTs for dissemination towards wider network of sectorial CERTs & CSIRTs.
Standards bodies and open source organizations	Contribute to evolutions of standards for secure IoT and influence IoT developers community.	Publication of white papers (at least 2) on standardisation, disseminated to working groups such as ETSI, 3GPP, Global Platform, Trusted Connectivity Alliance, CEN/CENELEC, IoXT, IIC (Industry IoT Consortium), IoTSF (IoT Security Foundation), ANSSI, GSMA.
Policy Makers, Public authorities in charge of digital policy, data protection and cybersecurity	Promoting policies that support cybersecurity information sharing across EU countries.	Dissemination of results to working groups and consortiums such as ECSO, Galactea-plus, Ethereum EIP, Core Service Platform for EU Cybersecurity Certification etc. and to the European Commission, Member States, National Authorities, Regulators, and European Agency for Cybersecurity (ENISA). Presentation of results at (at least 2) ECSO events.
Potential investors	Investing in cutting-edge cybersecurity.	Reaching out to investors, both private organisations and public organisations and European institutions and programmes (European Regional Development Fund, H2020, EUREKA Clusters, etc.) to spur the development and adoption of technologies. ECSO is the promoter of the Cyber Investor Days, already at 10th edition, that could be used as a channel to engage with investors and promote innovative cybersecurity solutions.
Other projects under same or other calls	Advancing own research, training personnel & students on CERTIFY technologies.	Liaisons with the CSAs called upon to cut across topics and establish synergies with other IAs/RIAs in the same or other CS calls as well as other relevant projects. At least 2 common events (webinars, workshops, etc.) will be organised.

Figure 6 Target audience groups for communication

Target groups	Description	Interest in the project
SMEs and industry.	Stakeholders from industry, network operators, SMEs and entrepreneurs, operating in the cybersecurity domain	• Evaluate CERTIFY novel approaches for enhancing cybersecurity in novel IoT-enabled environments. • Use of CERTIFY platform for a enhanced IoT lifecycle management • Promoting CERTIFY in operations and in their R&I activities for IoT security management
Mass media channels.	Non-technical articles to newspapers and magazines, radio, social media (LinkedIn, Facebook, YouTube…)	• Inform of benefits offered to the society • Inform through flyers, banners, videos, podcast, press releases related to the added value of the project and the benefits offered to the society
Clusters & partnerships.	EU initiatives and clusters, research communities, associations, (e.g., Digital Business Innovation, Digital Agenda, Innovation Union)	• Communicate project's results to their members • Participation in project's events for knowledge exchange • Inclusion of project's results to collaborative research activities (roadmap, white papers…)
Target alliances & associations.	Push use case results at ECSO, IETF, ITU, Ethereum EIP and whitepapers	• Promote project's results in various alliances in which the consortium partners are active members
General Public.	General public, end-users and anyone interested in the project	• Promote project's results and stimulate innovation in society through participation in "open days for science" and "Technology days" events. Non-technical articles based on project's results

Communication Channels and Activities. The CERTIFY communication strategy combines a mix of traditional and disruptive communication channels. A project website will be created by M2 and maintained by **DWG** serving to i) promote the project's public image as a main online access point for the different target groups; ii) serve as an information source, highlighting project objectives, activities (**3 video clips** will be produced, which will cover the CERTIFY general ideas, demonstrations and presentations created by **DWG**), outcomes and relevant updates (periodic newsletter, three issues per reporting year). The consortium (with **DWG** coordination) will regularly post announcements and initiate discussions from month M3 onwards through social media sites, such as Twitter, LinkedIn, YouTube, etc. CERTIFY will prepare **3 technical brochures** for technical and scientific achievements and **3 non-technical**, brochure-files, flyers, posters and roll-up banners (created by **DWG)** to be distributed to local universities, schools, town councils, etc. Partners will give at least **2** interviews and participate in technical press conferences organized by local newspapers and local/regional broadcasters. This activity will be undertaken by **UMU**, as it has a university television and associated program in the local television, **IoT-DH, ECSO** and **DWG**. CERTIFY will publish a recurring Podcast (interviews and discussions) covering topics on hardware security, open hardware and IoT lifecycle security in Europe, with the plan to publish **10 episodes** every 4-6 weeks during M13 - M36 of the project (activity carried out by **DWG**). And also whenever possible, at workshops or summits (at least 3+ events), **IoT-DIH** and **ECSO** will encourage the organisation of networking sessions to promote the CERTIFY project. Finally, CERTIFY will participate in at least **3 joint workshops** with related projects, e.g., CyberSec4Europe or Concordia, where partners like **UMU** and **UZH** are members of them, respectively.

2.2.1.3. Exploitation strategy

The CERTIFY Key Exploitable Results (KER), which will form the basis for its exploitation strategy and for the development of appropriate commercial sustainability plans, are indicated in the table below:

Table 5 List of exploitable KER in CERTIFY

KER	TRL		Exploited by partner	Time to market (post project)	Targeted market	Expected Return on Investment (ROI)
	M01	M36				
Remote inventory management	3	4	DWG	2y	Industry 4.0, Mobility, Telecom	40%
Improved IoT evaluation methodologies	3	4	RAL	0.5y	Industrial 4.0, Automotive, Healthcare	> 500K EUR
Automated IoT device re-certification	3	4	RAL	1y	Industrial 4.0, Automotive, Healthcare	> 1 M EUR
Advanced IoT privacy-preserving SIEM	2	4	TUp	2y	Industry 4.0, Mobility, Telecom	40%
Fully Qualified Signature Service for Blockchains	2	4	MOD/UZH	2y	Blockchain	40% (estimate)
Definition of a more secure and connected aircraft cabin	2	4	Collins	>3y	Aerospace	Contribute to reducing Maintenance, Repairs and Operations (MRO) and Unplanned Maintenance costs by ~10%
IoT based IDS/IPS	2	4	ENG	2y	Industry 4.0	35%

The exploitation strategy is at the heart of the CERTIFY project and it is conceived following the EU study reported in "Innovation - How to Research into Commercial Success Story?" Basically, it encompasses a direct connection with commercialization and a transformation of knowledge. By taking into account that part of technologies and tools developed within CERTIFY aims for a TRL 4 (with some of them reaching TRL 5 or 6 maturity as detailed in Section 1), CERTIFY will execute the commercial transformation through further research activities and technology scanning.

Table 6 Individual exploitation of CERTIFY

INDIVIDUAL EXPLOITATION
Collins Aerospace will contribute to innovate the aircraft cabin by providing solutions for personalized passenger

experiences and enhanced airlines services. CERTIFY's approach to manage the entire cybersecurity lifecycle for the IoT devices allows to ease the (re)certification processes throughout the device lifetime with potential cost savings.
UMU will improve its knowledge and expertise by working in cooperation with SMEs, and industrial partners. This experience will help reinforcing the UMU position in the research community, and also will help in creating new employment possibilities for their students. UMU will also be able to transfer the results of the project to its spin-off www.odins.es.
ENG will mainly exploit the results of CERTIFY's outcomes through CyberTech, its 300-strong unit commercial branch for cybersecurity solutions. ENG also deploys a set of digital platforms positioned as enablers of the Digital Transformation (e.g. Digital Enabler1) and CERTIFY's results will be used to extend the platform's capabilities thus promoting a more secure integration within IoT environments.
UZH will exploit its experience of enhanced security in IoT gained through CERTIFY by industrial collaborations, (e.g., technology transfer projects, spin-off companies, etc.) and teaching Bachelor, Master, and PhD courses. UZH backs it up with an excellent record of ICT technology transfer projects and spun-off start-up companies like Modium.io[67], Axelra[68], or AirGap[69].
MOD has successfully completed numerous digitization projects in various industries by adopting a process-focused approach to solving supply chain challenges and leveraging its own industry expertise to industry associations and academia. Modum.io has proven capabilities for realizing solutions using the latest technologies on both hardware and software level. CERTIFY will allow modum.io to verify new use-cases in the market.
RAL successfully developed the first IoT security and certification platform which eases the frictions associated with IoT security certification, standardization and security. CERTIFY's results will be used to extend and automate some features linked to security evaluations and thus improve the efficiency of the pre and post certification processes.
IoT-DIH will strengthen its role as knowledge provider on the IoT by ensuring that the security of devices is integrated into their design; will benefit from the promotion of the activity carried out and from the increased attractiveness of its community of technology providers and start-ups collaborating to develop the technology of the future.
DWG has become an excellent R-&-D and innovation solution provider for industry. DWG is actively contributing to German cybersecurity hubs and security organizations to increase the cybersecurity awareness in industry. CERTIFY will lead into the development of new products to serve the demands of cybersecurity and tools on risk management.
ST-I has an important market share of general and secure microcontrollers, of embedded secure solutions and of other components for IoT nodes. CERTIFY results will be in the short term a competitive advantage for ST-I and in the medium term a new benchmarked reference to be addressed by the whole competition.
TUp is an academic spin-off of the University of Naples (Italy) aiming at exploiting the important research results in the Cyber-Security field. CERTIFY results will lead to the development innovative solutions to monitor the security of IT systems. They will enable widening targeted markets to IoT-related applications, where proper solutions are awaited.
UBI is an active R&D and Software System centre focusing on the provision of security solutions for a multitude of systems and networks. Through CERTIFY, UBI will produce architecture specification and proof-of-concepts that would guide the design of robust and resilient attestation adapters.
ECSO is a not-for-profit association and will consolidate the project outcomes with its own activities, specifically in its WG1. ECSO is well placed to align project outcomes with market demand and relevant EU policies and strategies.

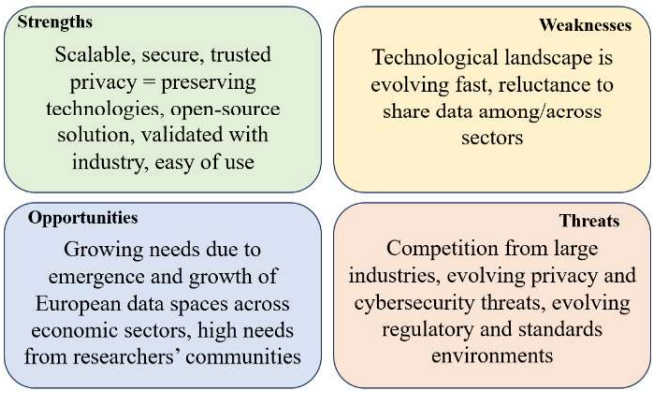
Product/Market Alignment and business model

CERTIFY consortium is composed of a mix of large industries and SMEs cooperating in the use case design to achieve a broad coverage of the current trends and scenarios for complex and market relevant IoT environments. CERTIFY project considers running an "industrial technology demonstrator" in WP6 - T.6.1 with the aim of showcasing the applicability of the CERTIFY technologies to very disparate market scenarios, business needs and application fields. As described by ENISA (PROACTIVE DETECTION - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS), "*proactive detection of incidents is defined as the process of discovering malicious activity*". In this sense, CERTIFY will develop a NIDS for the IoT environment and the market of NIDS is growing. Markets and Markets have reported[70] that "the global cloud IDS IPS market is expected to grow from USD 600.9 Million in 2017 to USD 1,764.7 Million by

[67] https://www.roambee.com/
[68] https://www.axelra.com/
[69] https://airgap.it/
[70] https://www.marketsandmarkets.com/Market-Reports/cloud-ids-ips-market-158051963.html

2022, at a Compound Annual Growth Rate (CAGR) of 24.04% during the forecast period". Big players involved are CISCO, Intel, Trend Micro, etc., open-source products are also available and widely used such as Suricata and Snort, mainly from the US and/or Asia, EU market is almost non-existent. **ST-I** is one of the world's largest semiconductor companies with 2020 revenues of $10.2 B, Signatory of the United Nations Global Compact (UNGC), Member of the Responsible Business Alliance (RBA) and owner of more than 18,000 patents & 557 new filings in 2020. **ST** strategy stems from 3 key long-term enablers: 1) Smart Mobility: ST provides innovative solutions to help customers make driving safer, greener, and more connected for everyone. 2) Power & Energy: ST technology and solutions enable customers to increase energy efficiency everywhere and support the use of renewable energy sources. 3) IoT & 5GIoT & 5G: ST provides sensors, embedded processing solutions, connectivity, security and power management, as well as tools and ecosystems to make development fast and easy for ST customers. Results coming from CERTIFY will sustain the possibility to increase all the 3 ST segment revenues.

Figure 8 SWOT Analysis



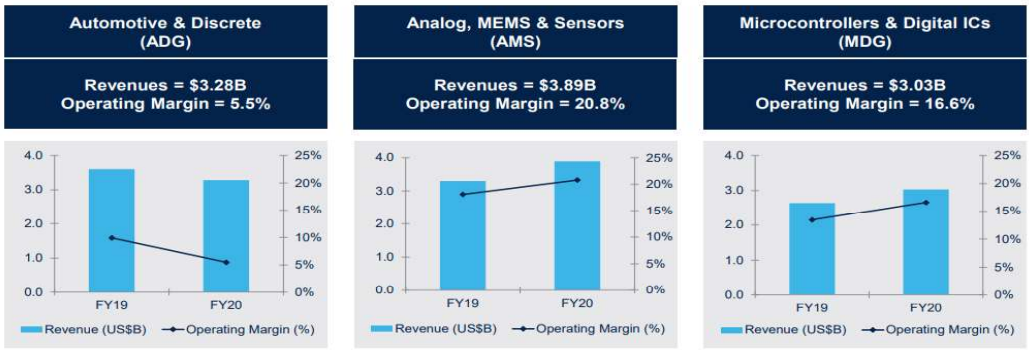


Figure 9 Full Year 2020 ST-I Product group results

Standardization activities

The multiplication of project results across the European automotive industry will mainly be driven by the standardization activities of the project partners. During the R&D phase, relevant standardization bodies will be identified to generate awareness of the project's developments and results. **RAL** will exploit its network in the standardization ecosystem across the EU (ENISA, CEN CENELEC, ETSI, ANSSI, IoTSF, EUROSMART), and other regions of the world (IoXT, IIC, GSMA), to generate interest on the project within the community. In addition, RAL will leverage their contacts and membership/chair of working groups within industry and standardization organisations to trigger engagement and due consideration of CERTIFY's results in shaping the discourse for future publications. **ST-I** as partner in CERTIFY has active participation in various working group set up in globally recognized standardization committees as ETSI, 3GPP, Global Platform and Java Card Forum. CERTIFY is also aligned with the spirit, aim and content of relevant security standards focused on promoting trust and confidence into the Digital Single Market, e.g., eIDAS Regulation, proposal for an e-Privacy regulation, ISO/IEC 27001, ISO 31000 etc. and with the standardization efforts of entities such as ENISA, ECSO and/or Gaia-X. Although all partners are involved in this analysis, a project Exploitation Manager will be in charge to track these activities and continuously update the status.

2.2.2. Outcomes, metrics and quantifiable targets for D&C&E

Table 7 lists the D&C&E metrics and their corresponding target values.

Table 7 Dissemination, Communication and Exploitation outcomes, metrics and quantifiable targets

Activity / Metrics		Target value
Dissemination	Industry	**2** virtual info days; **2** industrial workshops
	Scientific publications	Journals/magazines >**10**; Conferences > **12; 2** technical workshops
	Workshops / surveys	Number of events for knowledge sharing and dissemination: **3+**
	Training / education	Number of PhD thesis: **3**;
	ECSO and standardization	No of WGs to contribute: **2;** ECSO events > **2; 2** white papers
	Other projects	**2** common events

Communication	Social media	LinkedIn followers: >**500**; LinkedIn posts: > **40**; Twitter followers: > **500**; Re-Tweets:>**500;** Facebook followers:>**500**; Number of posts > **10; 3** videoclips; Website visitors> **1,000**
	Press releases/Newsletters	**2** interviews
	Factsheets / Brochures	3 non-technical and **3** technical
	Flyers/posters & roll-ups	Project flyers: >**3**; Posters & roll-up banners: >**3**
	Public engagement	Number of demonstrators: **3** demonstrators in **3** sectors; Number of attendants to demonstrators: more than **200** attendants
	Podcast	10 Episodes
Exploitation	Post project opportunities	At least 3 identified. At least 3 meetings with potential investors / funding agencies

2.2.3. Management of intellectual property

- **Intellectual Property Rights (IPR) Management** during the project. Explicit rules concerning IP ownership, access rights to any Background and Results for the execution of the project and the protection of IPRs will be addressed within the Consortium Agreement (CA) which will be signed by all partners before the project start.
- **Access Rights to Background and Results**. The project partners agree to grant each other royalty-free Access Rights to their Background and Results for the execution of the project.
- **IP ownership**. Results shall be owned by the partner carrying out the work leading to such results. Any joint results, including inventions and all related patent applications and IP will be jointly owned by the contributing parties.
- **Knowledge Management and IPR** activities will be addressed by T7.3, led by UMU. The task will develop and finalize a detailed Knowledge Management and IPR Strategy. An integrated approach will be followed for the identification, capture, retrieval, distribution, sharing, use and reuse of generated information and knowledge assets.

2.3. Summary (Canvas)

Table 8 Key elements of the project impact pathway and maximizing impact measures

SPECIFIC NEEDS	EXPECTED RESULTS	D & E & C MEASURES
• Need for protection for constrained IoT devices • Increasing IoT devices makes necessary usage of share security information • Heterogeneity in IoT and the dynamism difficult their maintenance. Need to manage the whole lifecycle security.	**Scientific advancements for IoT security lifecycle management** **Improved technologies:** • Infrastructure and tools to share security information among stakeholders • Secure reconfiguration and maintenance embedded devices by mean of open hardware primitives and services • Advanced bootstrapping and monitoring of attacks and malicious behaviours • Runtime security compliance and continuous certification methodology • Integration in real systems and Validation in real-life contexts	**Dissemination:** Journals >10; Conferences>12; Scientific workshops: 2, Industry workshops: 2, Standards: contribution in 2 WG, 2 ECSO events, white papers: 2, 3 PhD students, Presence at EU events: >9; 2 common events with other projects **Communication:** Website online, LinkedIn, Twitter; interviews: 2; video clip: 3; Flyers; 3; Posters; 10 podcasts; Presence in Public events >5; **Exploitation:** Open-source version of CERTIFY framework; 6 industrial exhibitions; 3 meetings with potential investors, *3 post-project opportunities*
TARGET GROUPS	**OUTCOMES**	**IMPACTS**
Researchers, industry, consumers, enterprises, end users, public authorities involved security and privacy, manufacturers.	• Faster and increased ability to protect against and detect cyber-attacks targeting IoT. • Collaboration between stakeholders involved in IoT lifecycle.	***Scientific & Technological:*** Empower IoT stakeholders with tools and mechanisms to achieve a guaranteed level of security; Contribute to the adaptability of cutting-edge IoT security technologies

Conformity Assessment Bodies, National Schemes, Integrators, Network Operators and Service Providers	• Support the standardization and regulatory work within the IETF, NIST, IEEE, IPSO, Zigbee, OMA, CSA and NIS. • Authenticating and configuring devices in a secure way • Increase resilience of digital infrastructures, systems and processes to security attacks. • Continued compliance mechanism with the cybersecurity requirements. • Facilitate lifecycle cybersecurity management with tools and mechanisms.	***Economic:*** Maximisation of EU's digital capacities through standards, events, cybersecurity training, empowering communities; Reduce dependence of EU on non-EU solutions; Quantifiable security assurance and certification shared across EU; Increased software, hardware and supply chain security; Improve the collective resilience ***Economic / Technological:*** Increase transparency and response times, set up baseline for security certification; Find right balance between security needs and business needs; Improve defence against focused attacks. ***Societal:*** Bring cyber security to SMEs; Help cyber security expert's awareness about major threats, new technologies reducing risks through certification, live upgrades, reconfiguration and guidance about IoT device lifecycle.

3. Implementation

3.1. Work plan and resources

3.1.1. Overall structure of the work plan

The project work plan has been designed taking into account the objectives set up in Section 1. CERTIFY is structured in 7 WPs, as depicted in Fig. 10. The development of the CERTIFY framework follows an iterative process, where services and components are released, integrated and validated in subsequent versions according to requirements coming from the use cases, as shown in the Gantt chart (Fig. 11). In brief, WP1 will analyse the project Pilots and the state of the art to identify relevant threat models and attack scenarios, resulting in the elicitation of the security requirements. The same WP will also define the lifecycle and the certification methodology and its instantiation to the concrete scenarios identified in the Pilot use cases. WP2 will define the CERTIFY architecture, manage the integration of tools and services also conduct the validation of the overall framework. The technical WPs (i.e., WP3, WP4 and WP5) are oriented to the design and the implementation of the components and services belonging to the CERTIFY architecture and specifically, the Infrastructural Services (WP3), the IoT Platform (WP4) and the Software Platform (WP5). WP6 will take care of all dissemination and exploitation activities, including the planning of the showcases to external subjects, promoting community engagement. At last, WP7 will include all activities related to the project management.

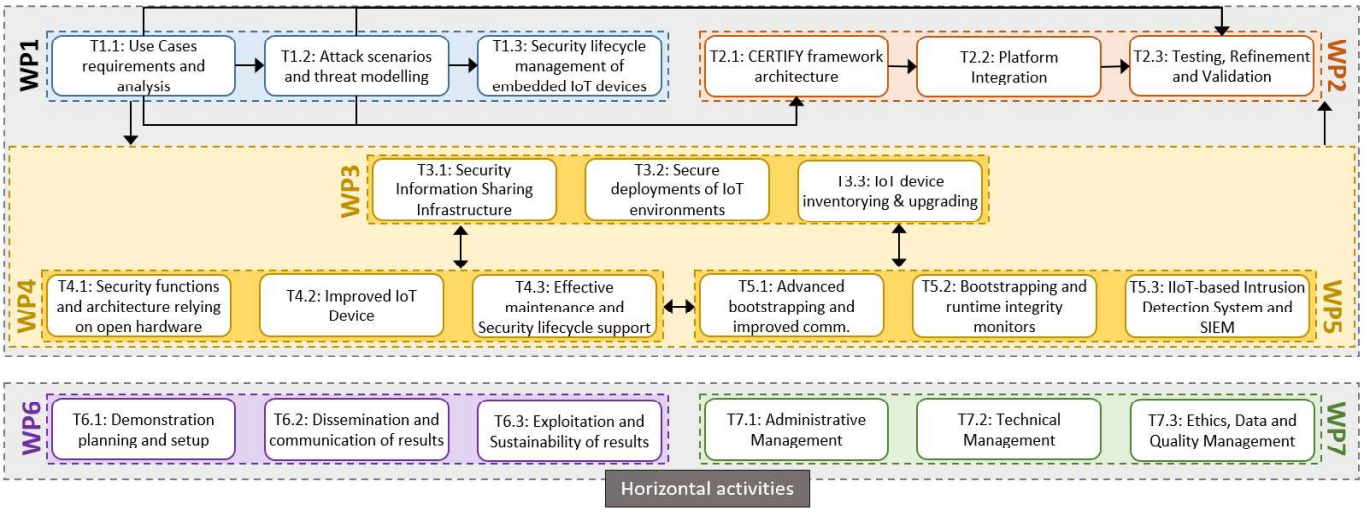


Figure 10 CERTIFY PERT Diagram

	Duration	Start	End
Task 1.1 Use Cases requirements and analysis	24	1	24
Task 1.2 Attack scenarios and threats modelling.	24	1	24
Task 1.3 Lifecycle security management of IoT devices.	17	8	24
WP2 System Architecture, Integration, and Validation of the CERTIFY framework	35	2	36
Task 2.1 CERTIFY framework architecture	23	2	24
Task 2.2 Platform Integration.	31	6	36
Task 2.3 Testing, Refinement and Validation.	27	10	36
WP3 Design and Implementation of the CERTIFY's Infrastructural services	27	6	32
Task 3.1 Security information sharing infrastructure	27	6	32
Task 3.2 Secure deployment of IoT environments	27	6	32
Task 3.3 IoT device inventorying & upgrading	27	6	32
WP4 Design and Implementation of the CERTIFY IoT platform	28	6	33
Task 4.1 Security functions and architecture relying on open hardware functions	28	6	33
Task 4.2 Improved IoT Device.	28	6	33
Task 4.3 Effective maintenance and Security lifecycle support	28	6	33
WP5 Design and Implementation of the CERTIFY Software Platform	29	6	34
Task 5.1 Advanced bootstrapping and improved communications	29	6	34
Task 5.2 Bootstrapping and runtime integrity monitors	29	6	34
Task 5.3 IIoT-based Intrusion Detection System and SIEM	29	6	34
WP6 Community Engagement & Sustainability	34	3	36
Task 6.1 Stakeholders Demonstration	34	3	36
Task 6.2 Dissemination and communication of results.	34	3	36
Task 6.3 Exploitation and Sustainability of results.	31	6	36
WP7 Project Management	36	1	36
Task 7.1 Administrative Management.	36	1	36
Task 7.2 Technical management.	36	1	36
Task 7.3 Ethics, Data and Quality management.	36	1	36

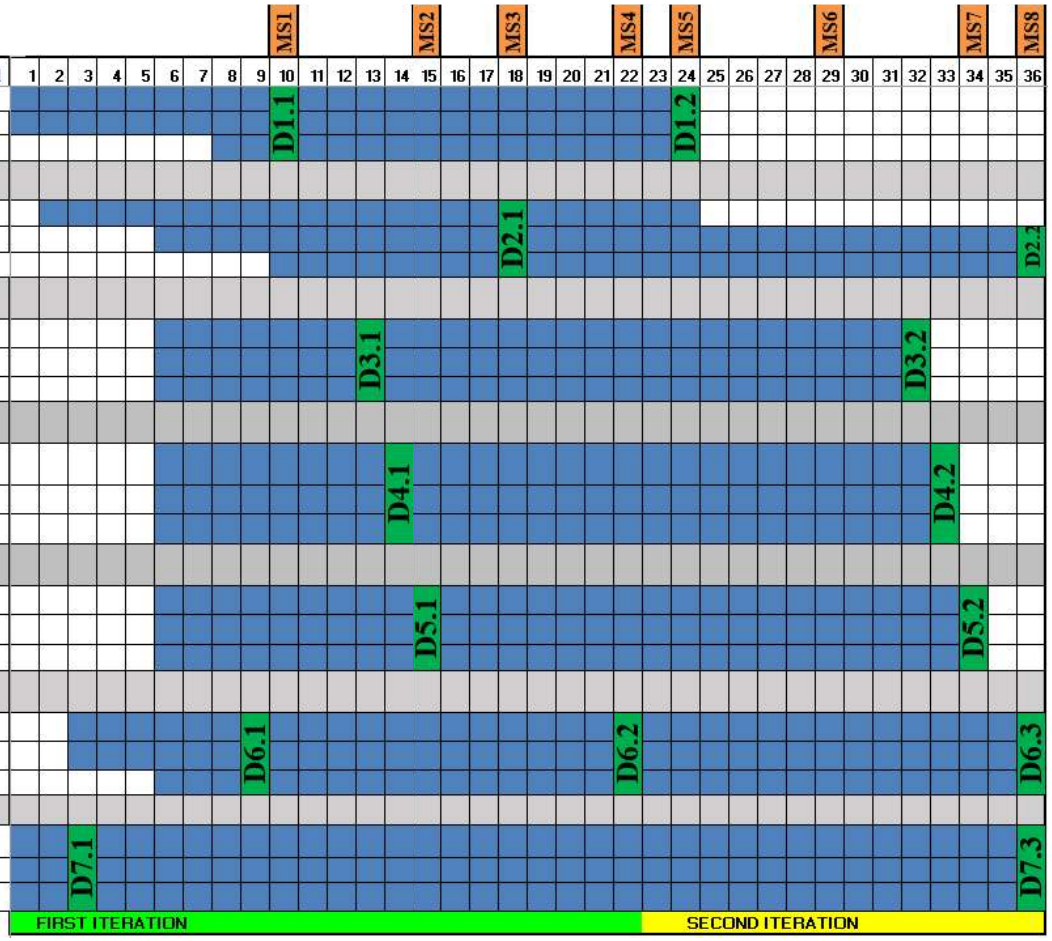


Figure 11 CERTIFY Gantt chart

3.1.2. Detailed work description

3.1.2.1. Work Packages List

Table 9 List of Work packages

WP No	Work package Title	Lead Participant No	Lead Participant Short Name	Person - Months	Start Month	End Month
WP1	Use Cases analysis and Lifecycle management	6	Collins	103	1	30
WP2	System Architecture, Integration, and Validation of the CERTIFY framework	2	TUp	92	2	36
WP3	Design and Implementation of the CERTIFY Infrastructural services	1	UMU	78	6	32
WP4	Design and Implementation of the CERTIFY IoT platform node	3	ST-I	112	6	33
WP5	Design and Implementation of the CERTIFY Software Platform	4	ENG	101	6	34
WP6	Community Engagement & Sustainability	5	DWG	76	3	36
WP7	Project Management	1	UMU	32	1	36
		Total months		**36**		

3.1.2.2. Work packages description

Table 10 Work package description

WP No:	**1**	**Lead Beneficiary**			**Collins**		**Start Month**		**M1**	**End Month**		**M30**
WP title	Use Cases Analysis and Security Lifecycle Management											
Participant No.	1	2	3	4	5	6	8	9	10	11	12	13
Short Name	UMU	TUp	ST-I	ENG	DWG	Collins	RAL	UBI	IoT-DIH	ECSO	UZH	MOD
Persons/month	15	3	13	12	6	12	15	4	10	3	6	4

Objectives

WP1 will lay the foundations for the CERTIFY's holistic security monitoring and analysis, by identifying requirements, constraints, threats and attack scenarios relevant for systems exploiting embedded, connected and IoT devices. A particular focus will be devoted to three project Pilots. Moreover, WP1 will develop the CERTIFY methodology for the security lifecycle management of embedded devices and IoT-enabled environments including security evaluation and definition of effective countermeasures. Such a security evaluation methodology will be based on current standards and will be developed and adapted to encompass hardware vulnerabilities, semi-automated verification of security properties at runtime and collection of objective certification evidence. This work comprises the following objectives: i) security requirements elicitation in three use cases and identification of the most relevant threat models and attack scenarios; ii) collection of KPIs and validation methodology supporting the Piloting activities; iii) definition of the security management lifecycle reference architecture and certification methodology; iv) instantiation of the CERTIFY security lifecycle methodology in the use cases.

Description of work

T1.1: Use cases requirements and analysis (M1-M24) [Leader: ST-I; Participants: UMU, TUp, ENG, DWG, Collins, UZH, UBI, RAL, ECSO, MOD, IoT-DIH] This task will focus on the elicitation of the security requirements to address the specific challenges of the three Pilot use cases describing different application domains of embedded and IoT devices. Moreover, it will include input from the State-of-the-Art (SotA) analysis. The main objectives of the task will be: i) identification of key scenarios characterizing the Pilots; ii) definition of a coherent set of security requirements; iii) identification of the technologies needed for strengthening the security in the use case scenarios. [**Output**: report]

T1.2: Attack scenarios and threats modelling (M1-M24) [Leader: Collins; Participants: UMU, TUp, ENG, DWG, ST-I, UZH, UBI, RAL, ECSO, MOD, IoT-DIH] Starting from the use case requirements identified in T1.1, this task will identify and model vulnerability, threats, and relevant attack scenarios for embedded devices and IoT environments. This task will also include a SotA analysis of physical/cyber/human attack scenarios. Moreover, a

cybersecurity risk assessment will be performed to identify, classify and rank the hazards (including the correlated ones) according to their impact on the identified use cases. [**Output**: report]

T1.3: Security lifecycle management of embedded IoT devices (M8-M24). [Leader: UMU; Participants: ST-I, TUp, ENG, DWG, Collins, UZH, UBI, RAL, ECSO, MOD, IoT-DIH] This task will develop a methodology for the security lifecycle management of IoT devices, with the objective of dealing with security changes (in terms of requirements and threat landscape) and of verifying the level of security reached by a device, establishing a basis towards security certification. The overall methodology is intended to be objective and semi-automated, and it will include a mix of approaches, techniques and tools aimed at enabling cyber-resiliency for European entities, by protecting, identifying and timely reacting to the attack scenarios identified in T1.2. A blended model/experimental based approach will be designed to support the safety/security integrity level certification. [**Output**: report]

Deliverables

D1.1. Security requirements, threats models and initial CERTIFY lifecycle management. Editor: RAL; M10 (Type: R); This deliverable reports on the activities of T1.1, T1.2 and T1.3 and includes the security requirements elicitation and threat models for the use cases and the first version of the CERTIFY security lifecycle methodology.

D1.2. CERTIFY security lifecycle methodology. Editor: UMU; M24 (Type: R&OTHER); This deliverable reports on the CERTIFY security lifecycle methodology. Use case requirements and threat models may be updated if needed.

WP No:	2	Lead Beneficiary		TUp		Start Month		M2	End Month		M36
WP title	System Architecture, Integration, and Validation of the CERTIFY framework										
Participant No.	1	2	3	4	5	6	8	9	10	11	12	13
Short Name	UMU	TUp	ST-I	ENG	DWG	Collins	RAL	UBI	IoT-DIH	ECSO	UZH	MOD
Persons/month	18	12	0	12	8	6	4	5	7	0	12	8

Objectives

WP2 will define the architecture and drive the validation of the CERTIFY framework. Moreover, it takes care of the integration of components developed as part of WP3, 4 and 5. User requirements and analysis performed in WP1 will guide the identification of CERTIFY components and the related interactions as part of the overall CERTIFY logical architecture. The same input will drive the testing and validation of the integrated solution. This work comprises the following objectives: 1) Definition of the main building blocks of the CERTIFY framework, related interactions and data flows; 2) Integration of the components and services developed in WP3, 4 and 5 in a single framework; 3) Evaluation and validation of the CERTIFY framework.

Description of work

T2.1: CERTIFY framework architecture (M2-M24). [Leader: UMU, Participants: TUp, ENG, DWG, Collins, UZH, UBI, MOD] This task will define the architecture of the CERTIFY framework, including components, interfaces, and interactions, based on the requirements surfaced in T1.1 and T1.2. The framework will provide functionalities for cybersecurity data correlation, operations, dynamic response, data for internal evolution of cybersecurity knowledge, etc. From requirements, components, interfaces, and data structures that make up the basic structure of the core CERTIFY framework, taking into account components already provided by partners to be extended and new components to be developed. These will include interfaces, protocols, flows and data models. After the first iteration of activities, and following feedback and inputs also from technical WPs, a second iteration will be made, making adjustments where needed. [**Output**: report]

T2.2: Platform Integration (M6-M36). [Leader: TUp; Participants: Collins, UMU, ENG, DWG, UZH, UBI, MOD] This task will integrate components and services developed in WP3, WP4 and WP5 into a unified platform. The integration will follow an iterative process, in which this task will provide a common integration framework that will be used for the implementation of the reference architecture. It will be done by setting-up and managing a continuous integration/continuous delivery system using state-of-the-art tools and services (e.g., Jenkins, GitHub, Docker). It will also define a quality management process and common development practices. Integration of Pilots 1-3. [**Output**: report and tools]

T2.3: Testing, Refinement and Validation (M10-M36). [Leader: DWG; Participants: UMU, TUp, ENG, Collins, RAL, UZH, UBI, IoT-DIH, MOD] Based on the analysis of the Pilots and elicited user requirements, validation scenarios and acceptance criteria will be identified. The scenarios will be used to test and validate the subsequent

versions of the integrated platform. Acceptance tests will be carried out for both intermediate and final delivery of the CERTIFY platform thus leading to the final validation of the solution. Full evaluation of Pilots 1-3 [**Output**: report]

Deliverables

D2.1. CERTIFY Platform (First version). Editor: UMU; M18; (Type: R); This deliverable releases an interim version of the CERTIFY platform useful to start validation of initial assumptions and choices. As a product of continuous integration approach, it includes already available functionalities, and mockups where components are not available. It also includes acceptance criteria and validation scenarios for the final architecture.
D2.2. CERTIFY Platform (Final version). Editor: TUp; M36; (Type: R&DEM); This deliverable presents the final version of the CERTIFY framework architecture, including the results of the validation campaign.

WP No:	3	Lead Beneficiary		UMU		Start Month		M6	End Month		M32
WP title	Design and Implementation of the CERTIFY's Infrastructural services										
Participant No.	1	2	3	4	5	6	8	9	10	11	12	13
Short Name	UMU	TUp	ST-I	ENG	DWG	Collins	RAL	UBI	IoT-DIH	ECSO	UZH	MOD
Persons/month	18	0	11	8	9	5	3	6	0	0	12	4

Objectives

WP3 will design and implement the core tools and services supporting both the correct operation of the CERTIFY framework and the lifecycle management. Among the infrastructural services, a particular emphasis will be given to setting up and maintaining the list and specification of trusted devices. CERTIFY will take advantage of a hyper ledger accessible by a remote management centre for device inventorying, also identifying the required software patches/updates that must be installed. When a novel security requirement cannot be satisfied, the CERTIFY framework will repurpose the device for a not critical task. This work comprises the following objectives: 1) Identification of infrastructural services and security mechanisms of the CERTIFY framework supporting the whole lifecycle management and 2) Design and setup of the identified infrastructural tools and services.

Description of work

T3.1: Security Information Sharing Infrastructure (M6-M32). [Leader: ST-I; Participants: UMU, DWG, UZH, UBI, MOD] Developing a decentralized security information architecture using hyper ledger technology between the different stakeholders involved in the device lifecycle management (i.e., device manufacturer, consumer, certification authorities, local ISAC). The architecture will allow timely and accurate dissemination of certificate evidence, device configurations, and information on new threats and vulnerabilities. Develops versioning & certification in Pilots 1-2 [**Output**: report and tools]
T3.2 Secure deployment of IoT environments (M6-M32). [Leader: UMU; Participants: ST-I, DWG, UBI, RAL, MOD] Designing an approach for specifying the configuration of the IoT devices through fine-grained policies with a high level of expressiveness at different security layers (i.e., not restricted at the network layer as in the current MUD standard). The designed approach will leverage the information-sharing infrastructure defined in T3.1 by collecting and incorporating, in threat MUD files, known device vulnerabilities, and by exploiting the sharing infrastructure for disseminating in a timely fashion the threat and extended MUD files useful for secure deployment of IoT-enabled environments. Develops Pilot 1-3 in device policy management. [**Output**: report and tools]
T3.3 IoT device inventorying & upgrading (M6-M32). [Leader: Collins; Participants: UMU, ST-I, ENG, DWG, UZH, UBI] Designing a secure upgrading and device inventorying service in the form of a CMDB to store and gather information about the devices allowed in the network as well as the associated requirements e.g., the security patches that need to be installed to keep using the device for a given function, or the identity certificates of the trusted devices. Develops Pilot 1-3 in OTA patching & reconfiguration. [**Output**: report and tools]

Deliverables

D3.1. Implementation of the CERTIFY's infrastructure services (First version). Editor: UZH; M13 (Type: R); This deliverable reports on the requirements, architecture and first implementation of the infrastructural services of CERTIFY.
D3.2. Implementation of the CERTIFY's infrastructure services (Final version). Editor: UMU; M32 (Type: R&OTHER); This deliverable reports on the final implementation of the infrastructural services of CERTIFY.

WP No:	4	Lead Beneficiary		ST-I		Start Month		M6	End Month		M33
WP title	Design and Implementation of the CERTIFY IoT platform node										
Participant No.	1	2	3	4	5	6	8	9	10	11	12	13
Short Name	UMU	TUp	ST-I	ENG	DWG	Collins	RAL	UBI	IoT-DIH	ECSO	UZH	MOD
Persons/month	3	12	55	0	4	11	3	6	0	0	10	8

Objectives

WP4 involves the design and the implementation of solutions able to reduce the exposure to threats of IoT systems. The WP will build improved security functions along with support to maintenance phases, taking a generic IoT device as a model and focusing on functions like authentication, enrolling, data authentication, secure storage, etc. The architecture of this generic IoT device will include two strategic components: the SE (cryptographic support) and the Embedded Secure IoT Development Toolkit API (usage of the cryptographic functionalities in the SE). The WP will target the following specific objectives: i) improve the services of a generic IoT device; ii) leverage also the RISC-V open ISA for the implementation of a comprehensive IoT security lifecycle management, in compliance with the CSA.

Description of work

T4.1: Security functions and architecture relying on open hardware functions. (M6-M32). [Leader: Collins, Participants: TUp, UZH, UBI] This task has the objective of designing security functions and architectures relying on hardware security functions. Such functions will enable the definition of customizable secure and trustworthy open-source secure enclaves whose sets of properties (such as secure processing and logical isolation) are validated by testing and (where applicable) formal verification. The designed modular and reconfigurable solution will be able to reduce the development cost of secure IoT solutions and support common IoT security needs. In line with current trends in IoT-oriented trusted computing, CERTIFY will introduce new approaches for the definition of customized, software-based TEEs, relying on a reduced set of architectural features offered by RISC-V and a pure-software secure monitor running at the highest privilege level in the RISC-V-based platform. This solution will be able to interact with other commercial TEEs (such as ARM TrustZone) for consistent node-to-node security policies management. Develops Pilots 1-3 provided with security features. [**Output**: report]

T4.2: Improved IoT Device. (M6-M32). [Leader: ST-I, Participants: UZH, UBI] The task implements a secure OS and applications running on secure micros designed to be protected against high potential security attacks. The task will focus on the improvement of a generic IoT Device, focusing on the secure device authentication and enrolling, data authentication, data privacy, data secure storage, data encryption/decryption, data exchange protection etc. Two core components of the IoT Device Node Architecture will be implemented: the SE (i.e., cryptographic support) and the Embedded Secure IoT Development Toolkit API (i.e., the cryptographic functionalities in the SE). The SE supports several security features (monitoring, MPU, active shield, true random number generator, etc.) and the embedded software, Secure Micro and cryptographic library implement countermeasures against the state-of-art attacks. The SE implements the Global Platform mechanisms to update remotely and via OTA the embedded application. The secure OS implements a specific internal security auditing mechanism to detect and react to abnormal and/or out range running conditions. Develops Pilots 2-3 in advanced cryptography features, e.g., EAP/DSA. [**Output**: report]

T4.3: Effective maintenance and lifecycle support. (M6-M32). [Leader: TUp; Participants: UMU, DWG, UBI, RAL] This task will leverage the RISC-V based customizable TEE concept foreseen by CERTIFY to support trustworthy monitoring of continuous compliance with given cybersecurity requirements as well as NIST-specified bootstrapping mechanisms along with enhancements proposed by CERTIFY. The CERTIFY-augmented TEE based on RISC V will enable the implementation of effective maintenance mechanisms, consisting of self-checking capabilities and trustworthy channels for OTA security patches, which will match the vision of the CSA towards comprehensive IoT lifecycle management. Develops Pilots 1-3 with PHM, OTA patches, and reconfiguration. [**Output**: report and tool]

Deliverables

D4.1. Implementation of the CERTIFY's IoT platform (First version). Editor: ST-I; M14 (Type: R); Report on the requirements, architecture and first implementation of the infrastructural services of CERTIFY.

D4.2. Implementation of the CERTIFY's IoT platform (Final version). Editor: TUp; M33 (Type: R&OTHER); This deliverable reports on the final implementation of the infrastructural services of CERTIFY.

WP No:	5	Lead Beneficiary		ENG		Start Month		M6	End Month		M34
WP title	Design and Implementation of the CERTIFY Software Platform										
Participant No.	1	2	3	4	5	6	8	9	10	11	12	13
Short Name	UMU	TUp	ST-I	ENG	DWG	Collins	RAL	UBI	IoT-DIH	ECSO	UZH	MOD
Persons/month	20	8	0	37	6	11	3	16	0	0	0	0

Objectives

WP5 will design and implement the CERTIFY Software Platform, which includes the set of tools for the management of IoT devices. These include the continuous security monitoring and assessment, the selection of the most appropriate mitigation strategy, tools supporting the bootstrapping, configuration, repurposing and decommissioning of devices. Among the tools for the continuous security monitoring, a specific emphasis is given to the bootstrapping process of both the network and devices. This work comprises the following objectives: i) improve device bootstrapping process; ii) monitor the network bootstrapping process; iii) provide an integrated and advanced IDS and SIEM solution for privacy preserving security monitoring.

Description of work

T5.1: Advanced bootstrapping and improved communications. (M6-M34) [Leader: UMU, Participants: ENG, DWG, UBI, RAL] The task will improve the bootstrapping process following the NIST approach, that is, integrating a preliminary phase in which the deployment domain obtains relevant security information from the new device (ID, behavioural profile, security policies, certificates, etc.) to evaluate if the device is secure enough to be part of the network, and to configure it in a secure way. The standard MUD will be also integrated as part of the bootstrapping process to configure the device in a secure way. Develops Pilots 1-2 with secure bootstrapping. [**Output**: report]

T5.2: Bootstrapping and runtime integrity monitors. (M6-M34) [Leader**:** Collins**,** Participants: UMU, ENG, DWG, UBI] To control the types of devices allowed to join the network at a given time, this task will build network fingerprints collected at design time and compared with the ones generated at runtime. This task will also design a solution to verify the runtime integrity by means of open attestation solutions leveraging the underlying hardware/firmware level security primitives. Monitors will be tailored to the specific security properties and will allow runtime reconfiguration of the attestation objectives based on the usage of MUD files. Develops Pilot 1-2 with PHM & runtime integrity. [**Output**: report]

T5.3: IIoT-based Intrusion Detection System and SIEM. (M6-M34) [Leader**:** ENG**,** Participants: UMU, TUp, ENG, DWG, UBI] This task will provide an IIoT-based Intrusion Detection System for LoRa LP-WAN protocol, log analysis and privacy-preserving SIEM tools. The activities related to the development of an IoT-based Intrusion Detection System will focus on building an IDS which can detect known and new threats, taking into account IoT's potentials and limitations. Furthermore, new threats will generate a threat MUD to alert other stakeholders using the infrastructure provided in T3.1. The solution will start from known detection techniques and then will discover and apply innovative techniques, based on machine learning, to enhance detection capabilities. Outputs of the IoT-based IDS will feed SIEM tools for further and aggregated analysis. Develops Pilot 1-2 with PHM, threat and security incident detection, investigation and forensics & incident response. [**Output**: report and tool]

Deliverables

D5.1. Implementation of the CERTIFY's software platform (First version). Editor: ENG; M15 (Type: R); Requirements, architecture and first implementation of the CERTIFY's software architecture.

D5.2. Implementation of the CERTIFY's software platform (Final version). Editor: UBI; M34 (Type: R&OTHER); This deliverable reports on the final implementation of the software architecture of CERTIFY.

WP No:	6	Lead Beneficiary		DW		Start Month		M3	End Month		M36
WP title	Community Engagement & Sustainability										
Participant No.	1	2	3	4	5	6	8	9	10	11	12	13
Short Name	UMU	TUp	ST-I	ENG	DWG	Collins	RAL	UBI	IoT-DIH	ECSO	UZH	MOD
Persons/month	6	5	8	8	7	3	3	3	12	12	4	5

Objectives

WP6 aims at preparing, monitoring and supporting all dissemination and exploitation activities: i) Develop and deploy hands-on Pilot for the Pilot case studies; ii) evaluation of user experiences and business opportunities to wider deployment; iii) find, analyse, rank, select and integrate CERTIFY services with respect to privacy and security in the use-cases, seek requirements and disseminate results to target industry and cybersecurity-related organizations and beyond the project through DIHs approaching SMEs to validate the project results; iv) business plans around the exploitation of partners with the sustainability of open-source software components; v) dissemination of the project results, publication of concepts and reports to the research and industry communities as well as to other European stakeholders to create awareness, involvement and update; vi) monitoring of ongoing standardisation activities and contributing by promoting advancements and solutions.

Description of work

T6.1: Stakeholders Demonstration (M3-M36) [Leader: IoT-DIH; Participants: UMU, TUp, ST-I, ENG, DWG, Collins, UZH, ECSO, MOD] Overall planning of the CERTIFY showcases to external subjects, promoting the engagement. Objectives are the identification of target groups and communities of interest to be engaged; the identification of the most representative cases to be demonstrated; the setup of demonstration showcases that effectively impact the target audience contributing to the engagement of a substantial community. Based on the validation Pilots of T2.3 but specifically planned to impress an audience external to the consortium, the demonstration setups will be thus adopted as dissemination and community building tools. [**Output**: demonstration setups]

T6.2: Dissemination and communication of results (M3-M36) [Leader: DWG, Participants: UMU, TUp, ST-I, ENG, Collins, UZH, UBI, RAL, ECSO, IoT-DIH, MOD**]** Bundles all dissemination and communication tasks regarding the project's outcomes: regularly updated website, talks at industry events, public talks for citizen awareness, provision of online resources, training material and the demonstration of the use-cases, scientific dissemination via publications including journal articles, posters and presentation to workshops and conferences. The components and modules developed in the project will be distributed as open-source software to enable the global community to benefit from the developments made, using dissemination through summer schools and co-locating workshops with conferences that project partners co-chair regularly. This will align the CERTIFY results with current regulations and policy recommendations, ensuring compliance with relevant certification schemes. [**Output**: report]

T6.3: Exploitation, Standardization and Sustainability of results (M6-M36) [Leader: ECSO, Participants: UMU, TUp, ST-I, ENG, DWG, Collins, UZH, UBI, RAL, ECSO, IoT-DIH, MOD**]** Cover the effort made towards the definition of the partners' exploitation and standardization plans. This includes the alignment of results with current standards and the definition of a roadmap to exploit relevant results and how the individual partners will benefit from the project outcomes and increase their TRLs. The project partners will develop individual business plans and joint exploitation strategies using business models to show how they will use the outcomes for future products, activities, patents and the generation of IP. This includes all promotional actions (presentations and demonstrations of use-cases and project results) to other companies and stakeholders, who can benefit from CERTIFY, and creation of links with several stakeholders such as device manufacturers, threat databases, certification authorities, ISACs, cybersecurity professionals and policymakers at EU and national level. One of the goals of this task is to contribute to the objectives of the EUCC towards the definition of a comprehensive research and industrial agenda to favour the development of cybersecurity competencies in IoT across EU. Thus, liaison activities within the academic domain and cooperation with related R&D initiatives and other projects will also be pursued, especially with the four pilots of SU-ICT-03-2018 where partners like UMU and UZH are members of CyberSec4Europe and Concordia, respectively. Collaboration with the two projects through the associated partners will create research synergies while addressing the shared focus groups to enhance effectiveness. To achieve the above mentioned activities, this task includes a) the participation in at least 3 international meetings and workshops organized by the EC (EUCNC, ARES, ETSI Security Week) and other security projects, as well as articles in representative journals and magazines; b) collaboration, integration and promotion of EU projects, activities and events via dissemination efforts carried out by partners; c) communication towards consortium, trials, European ICT industry representatives, and third-parties initiatives and vice-versa (e.g., knowledge transfer to SMEs). During the first phase (M1-M17), the main purpose will be to create general awareness about the project and to establish links with stakeholders. The second phase (M18-M36) will aim at increasing the market potential and gather feedback for driving the final development. [**Output**: report]

Deliverables

D6.1. Plan for communication, dissemination, exploitation, standardization and demonstration activities. (Type: report); **Editor:** IoT-DIH; M9 (Type: R); Plans for communication, dissemination, exploitation, demonstration and standardization.
D6.2. Intermediate report on communication, dissemination, exploitation, standardization and demonstration activities and plans. (Type: report); **Editor:** DWG; M22 (Type: R); Completed activities in the first project period and plans for communication, dissemination, exploitation, demonstration and standardization.
D6.3. Final report on communication, dissemination, exploitation, standardization and demonstration activities. **Editor:** ECSO; M36 (Type: R); Report on completed activities for communication, dissemination, exploitation, demonstration and standardization.

WP No:	7	Lead Beneficiary		UMU		Start Month		M1	End Month		M36
WP title	Project Management										
Participant No.	1	2	3	4	5	6	8	9	10	11	12	13
Short Name	UMU	TUp	ST-I	ENG	DWG	Collins	RAL	UBI	IoT-DIH	ECSO	UZH	MOD
Persons/month	17	2	1	2	2	3	0	1	2	0	1	1

Objectives

This WP will implement the project management activities. This work comprises the following objectives: 1) To perform and maintain an efficient overall project government, as well as set up and support the communication, control and reporting infrastructure; 2) To monitor and report development tasks and resource usage, risks, identify deviations and propose corrective actions when needed; 3) To perform administrative coordination including financial reporting supervision and funding distribution; 4) To provide the scientific coordination of the project ensuring excellence of the research activities performed; 5) To assure the required quality standard of the project activities and results; 6) To monitor issues related to ethics, data management, gender & SSH cross-cutting priority.

Description of work

T7.1 - Administrative Management. **(M1-M36)** [Leader: UMU, Participants: TUp, ST-I, ENG, DWG, MOD, IoT-DIH, UBI, UZH]. This task will take care of the global administrative project management, by 1) establishing an effective project management structure, providing overall coordination within the project, taking care of activity planning and monitoring, progress reports, milestone reports, budgetary overview and reviews; 2) handling day-to-day administrative and management functions with the help of other management bodies; 3) providing financial and administrative coordination and financial reports; 4) setting-up an effective online collaboration platform and ensure fast and reliable communication channel; 5) performing the required risk management activities and 6) including mitigation actions if needed and liaising with the EC and with other projects. [**Output**: Progress reports, management procedures, risk assessment and plans]
T7.2 - Technical management. **(M1-M36)** [Leader: Collins, Participants: UMU] This task is dedicated to managing the technical and scientific execution of the project. This includes monitoring the technical progress of the work, ensuring compliance with the defined deadlines and milestones, coordinating the WP leaders' and task leaders' work following the defined task responsibilities, assessment of the exchange of technical information among partners, anticipating potentially critical situations regarding the technical and scientific success of CERTIFY and proposing solutions, liaising with T7.3 regarding quality control and approval of technical deliverables and coordinating the preparation/organisation of periodic technical reports/meetings (physical and/or virtual). [**Output**: report]
T7.3 - Ethics, Data and Quality management (M1-M36) [Leader: UMU, Participants: TUp, ENG, DWG, IoT-DIH] This task will ensure the compliance of the project research and innovation process with EU legal and ethical codes and regulatory framework while supporting consortium partners to address all issues related to the involvement of human participants and their personal data. The task will develop the DMP, containing the types of data that CERTIFY will generate and collect, the standards used to represent it and how partners might exploit it, supporting GDPR compliance. The task will also monitor gender issues, by gathering data on the current state of equality in the consortium, and by monitoring the use of methodological tools aligned with a gendered approach to innovation, particularly in the development, Piloting and evaluation. Finally, the task will evaluate the project's performance in relation to the active integration of socio-economic and social disciplines in the project's work. [**Output**: report]

Deliverables

D7.1. Project management handbook, QA procedures & templates and data management plan. Editor: UMU; M3; (Type: R&DMP); This deliverable establishes the project management and quality procedures and tools for efficient coordination and communication between partners, as well as the project's data management procedures.
D7.2. Ethics, gender and SSH report. UMU; M36. (Type: R&DMP); The deliverable summarises the ethics, gender and SSH monitoring, and provides an update of the DMP.

3.1.2.3. Deliverables List

Table 11 List of Deliverables

No	Name	WP No	Lead Partner Short Name	Type[71]	Dissem. Level	Month
D1.1	Security requirements, threats models and initial CERTIFY lifecycle management	WP1	RAL	R	PU	M10
D1.2	CERTIFY security lifecycle methodology	WP1	UMU	R&OTHER	PU	M24
D2.1	CERTIFY Platform (First version)	WP2	UMU	R	PU	M18
D2.2	CERTIFY Platform (Final version)	WP2	TUp	R&DEM	PU	M36
D3.1	Implementation of the CERTIFY's infrastructure services (First version)	WP3	UZH	R	PU	M13
D3.2	Implementation of the CERTIFY's infrastructure services (Final version).	WP3	UMU	R&OTHER	PU	M32
D4.1	Implementation of the CERTIFY's IoT platform (First version)	WP4	ST-I	R	PU	M14
D4.2	Implementation of the CERTIFY's IoT platform (Final version)	WP4	TUp	R&OTHER	PU	M33
D5.1	Implementation of the CERTIFY's software platform (First version)	WP5	ENG	R	PU	M15
D5.2	Implementation of the CERTIFY's software platform (Final version)	WP5	UBI	R&OTHER	PU	M34
D6.1	Plan for communication, dissemination, exploitation, standardization and demonstration activities.	WP6	IoT-DIH	R	PU	M9
D6.2	Intermediate report on communication, dissemination, exploitation, standardization and demonstration activities and plans	WP6	DWG	R	PU	M22
D6.3	Final report on communication, dissemination, exploitation, standardization and demonstration activities	WP6	ECSO	R	PU	M36
D7.1	Project management handbook, QA procedures & templates and data management plan	WP7	UMU	R&DMP	PU	M3
D7.2	Ethics, gender and SSH report	WP7	UMU	R &DMP	PU	M36

[71] **R**: Document, report (excluding the periodic and final reports); **DEM**: Demonstrator, pilot, prototype, plan designs; **DEC**: Websites, patents filing, press & media actions, videos, etc.; **DATA**: Data sets, microdata, etc.; **DMP**: Data management plan; **ETHICS**: Deliverables related to ethics issues; **SECURITY**: Deliverables related to security issues; **OTHER**: Software, technical diagram, algorithms, models, etc.

3.1.2.4. List of milestones

Table 12 List of milestones

MS	Milestone [MS] name	WP(s)	Month	Means of Verification
MS1	Initial Requirement elicitation and threats modelling	WP1	M10	First identification of use case requirements and modelling of relevant threats.
MS2	First version of the CERTIFY components and approaches	WP3, WP4, WP5	M15	First agile cycle generating a first version of the CERTIFY components
MS3	First version of the integrated framework	WP2	M18	First agile cycle generating a first version of the integrated framework.
MS4	First evaluation cycle of the CERTIFY solutions	WP2	M22	End of first agile cycle executed. Initial software components ready and test performed.
MS5	Security lifecycle methodology completed, and architecture consolidated	WP1, WP2	M24	Second agile cycle started with a consolidated version of the architecture and lifecycle.
MS6	Final version of the CERTIFY framework with all solutions integrated	WP1,WP2, WP3, WP4, WP5	M29	CERTIFY solutions integrated in the framework
MS7	First evaluation cycle of the CERTIFY solutions	WP2	M34	Second round of tests performed.
MS8	Final version of the CERTIFY security lifecycle and recommendations	WP1, WP2, WP6	M36	Report and fully qualified CERTIFY framework validated through use cases, providing the recommendations.

3.1.2.5. Critical risks and mitigation measures

To guarantee the achievement of the objectives targeted by the project it is essential to visibly identify and understand the significant project risks in advance (Task 7.1). Early risk identification is a primary goal within the project, which turns into the definition of a strategy for continuous risk management. The goal is to minimise the uncertainty due to assumptions and the environment in which the project is executed by proactively paying attention to possible obstacles. The continuous risk management process, defined in the project handbook, is implemented through strongly fostering project communication by frequent telcos and regular meetings so that irregularities can be quickly identified and dealt with at a very early stage. Moreover, the frequent meetings of the project bodies will therefore serve as the main forum for risk identification. Possible risks have been identified at the proposal preparation stage (see Table 13).

Table 13 Critical Risks

Risk No.	Description of the risk (Likelihood/Severity)	WP	Proposed risk-mitigation measures
Management			
RM1	Inadequate management (Low/High)	WP7	The PC has extensive experience in the coordination of EU projects and so has the TM and the WP Leaders that complement the Steering Committee. Meetings of the SC will take place regularly to identify potential problems.
RM2	Partners are not reacting as expected or lack communication (Low/High)	ALL	Use more interactive means of communication, e.g., use the phone when email is not enough, and ultimately resorting to the potential penalties to be described in a Consortium Agreement in case of underperformance. Regular SC meetings will prevent partners' isolation.
RM3	Partners leaving consortium in a critical phase (Low/High)	ALL	For each of the activities, more than one competent partner is part of the consortium. In case of partner exit, if it's possible, the partner will be changed with an appropriate substitute or the resources reallocated.