ETSI TR 104 160 V1.1.1 (2025-10)

TECHNICAL REPORT

Cyber Security (CYBER);
Observation from the ERATOSTHENES and CERTIFY projects regarding IoT security lifecycle

Reference
DTR/CYBER-00160

Keywords
conformity, privacy, security, security by default

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Given the increasing proliferation of Internet of Things (IoT) devices, it is paramount to implement a robust cybersecurity framework with the ability to address critical issues such as secure firmware updates and vulnerabilities handling, thanks to an effective sharing of cyber threat intelligence during the product lifecycle. ERATOSTHENES is designed from the ground up to handle such aspects of an IoT device's life cycle, through the development of a distributed, resilient, scalable, transparent, and auditable Trust and Identity Management framework. CERTIFY offers a comprehensive framework that aligns with the objectives of the Cyber Resilience Act (CRA), enabling IoT stakeholders to manage cybersecurity from initial design to decommissioning. The present document outlines these projects' frameworks and delves into their various components, evaluating their purpose as for the cybersecurity posture, first through the lens of lifecycle management and further along to verify the architecture's adequacy regarding the CRA. Pilot activities are then described and used to demonstrate the deployment processes in real-life scenarios. Finally, the present document includes an analysis of the identified challenges in standards, regulations and best practices, such as the CRA, and recommendations based on the projects' results.

1 Scope

The present document will focus on presenting the results, observations and lessons learnt from the ERATOSTHENES and CERTIFY projects that tackle the complex security challenges of the Internet of Things (IoT) with a focus on managing the entire lifecycle of these networks, with a specific focus on distributed trust management and digital identity solutions, and the certification process.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.4] ETSI TS 103 097 (V2.1.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[i.5] Common Criteria for Information Technology Security Evaluation.

[i.6] IETF RFC 9019 (2021): "A Firmware Update Architecture for Internet of Things".

[i.7] IETF RFC 8520 (2019): "Manufacturer Usage Description Specification", E. Lear, D. Romascanu, and R. Droms.

[i.8] IETF RFC 7950 (2016): "The YANG 1.1 Data Modeling Language", M. Bjorklund.

[i.9] IETF RFC 8259 (2017): "The JavaScript Object Notation (JSON) Data Interchange Format", T. Bray.

[i.10] "CVE vulnerabilities by date", May 2022, [Online].

[i.11] NIST SP 1800-15: "Securing Small-Business and Home Internet of Things Devices", Gaithersburg, MD, USA, 2019.

[i.12] S. N. Matheu-García and A. Skarmeta: "Defining the Threat Manufacturer Usage Description Model for Sharing Mitigation Actions", 2022 1st International Conference on 6G Networking (6GNet), Paris, France, 2022, pp. 1-4, doi: 10.1109/6GNet54646.2022.9830415.

[i.13] S. N. M. García, A. M. Zarca, J. L. Hernández-Ramos, J. B. Bernabé, and A. S. Gómez: "Enforcing behavioral profiles through software-defined networks in the industrial Internet of Things", Appl. Sci., vol. 9, no. 21, p. 4576, October 2019.

[i.14] Elliot, Mark & Domingo-Ferrer, Josep (2018): "The future of statistical disclosure control".

[i.15] UN Regulation No. 155: "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system".

[i.16] UN Regulation No. 156: "Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system".

[i.17] AC 20-168: "Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment (CS&E)", 2010, Federal Aviation Administration.

[i.18] RTCA DO-313: "Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems and Equipment", 2008, Radio Technical Commission for Aeronautics.

[i.19] ETSI EN 303 645 (V3.1.3): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.20] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[i.21] ENISA: "EUCS - Cloud Services Scheme EUCS, a candidate cybersecurity certification scheme for cloud services", 2020.

[i.22] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive (RED)).

[i.23] ENISA: "Good practices for security of IOT; Secure Software Development Lifecycle", 2019.

[i.24] "Product Security and Telecommunications Infrastructure (PSTI) Act", 2024, United Kingdom.

[i.25] IETF RFC 3748 (2004): "Extensible Authentication Protocol (EAP)", B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz.

[i.26] NIST: "NISTIR 8259 Series".

[i.27] IETF: "A summary of security-enabling technologies for IoT devices", 2024.

[i.28] Global Platform: "Security Evaluation Standard for IoT Platforms (SESIP)".

[i.29] ETSI TS 103 645 (V3.1.1): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.30] ETSI TS 103 701 (V2.1.1) (2025-05): "Cyber Security (CYBER); Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.31] IoT Security Foundation: "IoTSF Security Assurance Framework", Release 3.0, 2021.

[i.32] H. Kaur, and K. Kaur: "Secure elements for IoT devices: A survey", vol. 176, no. 102918, 2021.

[i.33] S. P. and N. Santos: "Demystifying Arm TrustZone: A Comprehensive Survey", ACM Comput Surv., vol. 51, no. 6, pp. 1-36, 2019.

[i.34] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini: "A Survey of Cybersecurity Certification for the Internet of Things", ACM Comput. Surv. CSUR, vol. 53, no. 6, pp. 1-36, 2.

[i.35] S. N. Matheu, A. Robles Enciso, A. Molina Zarca, D. Garcia-Carrillo, J. L. Hernández-Ramos, J. Bernal Bernabe, and A. Skarmeta: "Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems", Sensors, vol. 20, no. 7, p. 1882, January 2020.

[i.36] S. N. Matheu, J. L. Hernandez-Ramos, S. Perez, and A. F. Skarmeta: "Extending MUD profiles through an Automated IoT Security Testing Methodology", IEEE Access, pp. 1-20, 2019.

[i.37] H. Cavusoglu, H. Cavusoglu, and S. Raghunathan: "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge", IEEE Trans. Softw. Eng., vol. 33, no. 3, pp. 171-185, March 2007.

[i.38] S. E. Jaouhari and E. Bouvet: "Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions, Internet of Things", Internet Things, vol. 18, 2022.

[i.39] "ENISA Baseline Security Recommendations for IoT | OWASP IoT Top 10 2018 Mapping Project".

[i.40] TÜV SÜD: "ETSI EN 303 645 Cybersecurity for Consumer Internet Of Things: What It Is and Why It"s Important".

[i.41] EUROCAE.

[i.42] Federal Aviation Administration (FAA).

[i.43] European Union Aviation Safety Agency (EASA).

[i.44] Australian Government- Australian Cyber Security Centre: "IoT Code of Practice - Guidance for Manufacturers".

[i.45] ENISA: "Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis", 2024.

[i.46] CISA: "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default", 2023.

[i.47] CISA: "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software", 2023.

[i.48] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[i.49] ISO/IEC 15408-1:2022: " Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model".

[i.50] J. L. Hernández-Ramos et al.: "Defining the Behavior of IoT Devices Through the MUD Standard: Review, Challenges, and Research Directions", in IEEE™ Access, vol. 9, pp. 126265-126285, 2021, doi: 10.1109/ACCESS.2021.3111477.

[i.51] IEEE 802.11™: "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 7: Enhanced Broadcast Services", in IEEE Std 802.11bc™-2023 (Amendment to IEEE Std 802.11™-2020 as amended by IEEE 802.11ax™-2021, IEEE 802.11ay™-2021, IEEE 802.11ba™-2021, IEEE 802.11az™-2022, IEEE 802.11™-2020/Cor 1-2022, IEEE 802.11bd™-2022, IEEE 802.11bb™-2023, and IEEE 802.11™-2020/Cor 2-2024), pp.1-117, 28 February 2024, doi: 10.1109/IEEESTD.2024.10456575.

[i.52] ECMA-368: "High Rate Ultra Wideband PHY and MAC Standard", 2007.

[i.53] IEEE 802.15.3™: "IEEE Standard for Wireless Multimedia Networks", in IEEE Std 802.15.3™-2023 (Revision of IEEE Std 802.15.3™-2016) , vol., no., pp.1-684, 22 February 2024, doi: 10.1109/IEEESTD.2024.10443750.

[i.54] ETSI EN 304 632: "CYBER; CRA; Essential cybersecurity requirements for smart home products with security functionalities; Including smart door locks, security cameras, baby monitoring systems and alarm systems".

[i.55] ETSI EN 304 633: "CYBER; CRA; Essential cybersecurity requirements for Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features".

[i.56] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys.

[i.57] ETSI EN 304 634: "CYBER; CRA; Essential cybersecurity requirements for personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply; Or personal wearable products that are intended for the use by and for children".

[i.58] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[i.59] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

commissioning: process in which the device boots and connects to the target security context, establishing the necessary security verifications and materials for operating within the context

cyber intelligence: information gathering and analysis activity aimed at identifying, tracking/predicting capabilities and intentions/activities of hostile actors in the cybersecurity domain

Cyber Threat Intelligence (CTI): evidence-based knowledge (including context, mechanisms, indicators, implications, and actionable advice) about an existing or emerging threat that can be used to make decisions regarding similar threats

pre-provisioning: process in which the device undergoes initial configuration and security material installation during its first boot at the manufacturer's premises

security lifecycle: continuous process that encompasses identifying, protecting, detecting, responding to, and recovering from cybersecurity threats

zero-trust: approach that avoids inherent trust assumptions, but instead relies on the continuous evaluation and consideration of the entities' trustworthiness, e.g. for authorization processes

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Accounting
ACL	Access Control Lists

API	Application Programming Interface
ARM	Advanced RISC Machines
CA	Certification Authority
CAV	Connected and Automated Vehicle
CC	Common Criteria
CCS	Connected Cabin System
CERT	Computer Emergency Response Team
CERTIFY	aCtive sEcurity foR connecTed devIces liFecYcles
COPD	Chronic Obstructive Pulmonary Disease
COTS	Commercial Off the Shelf
CP-ABE	Ciphertext Policy Attribute-Based Encryption
CRA	Cyber Resilience Act
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVSS	Common Vulnerability Scoring System
DAA	Direct Anonymous Attestation
DID	Decentralized IDentifiers
DLT	Distributed Ledger Technologies
EAP	Extensible Authentication Protocol
ECU	Engine Control Unit
ENISA	European Union Agency for Cybersecurity
ERATOSTHENES	sEcuRe manAgemenT of iOt deviceS lifecycle THrough idENtities, trust, and distributEd ledgerS
EUCS	European Cybersecurity Certification Scheme for Cloud Service
GB	Gigabytes
GDPR	General Data Protection Regulation
GLOSA	Green Light Optimized Speed Advisory
HW	HardWare
IdM	Identity Management
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IoT	Internet of Things
IoTSF	IoT Security Foundation
ISACs	Information Sharing and Analysis Centers
low-SWaP-C	Size, Weight, Power and Cost
MSPL	Medium-level Security Policy Language
MUD	Manufacturer Usage Description
NIS	Network and Information Systems
NIST	National Institute for Standards and Technology
OBU	On-Board Unit
OTA	Over-The-Air
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PHG	Personal Health Gateway
PKI	Public Key Infrastructure
PP-CTI	Privacy-Preserving Cyber Threat Intelligence
PSTI	Product Security and Telecommunications Infrastructure
PUF	Physical Unclonable Function
RED	Radio Equipment Directive
SaaS	Software as a Service
SDC	Statistical Disclosure Control
SE	Secure Element
SESIP	Security Evaluation Standard for IoT Platforms
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOCs	Security Operations Centres
SSI	Self-Sovereign Identity
SW	SoftWare
TB	Terabytes
TEE	Trusted Execution Environment
TMB	Trust Management and Broker
TMRA	Threat Modelling and Risk Assessment

UN	United Nations
URL	Uniform Resource Locator
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VC	Verifiable Credentials
VM	Virtual Machine
VP	Verifiable Presentations
W3C	World Wide Web Consortium
YANG	Yet Another Next Generation

4 Introduction

4.1 Key IoT Security Challenges

The widespread adoption of Internet of Things (IoT) devices has introduced a complex security landscape. With a vast number of interconnected devices, the attack surface expands significantly, demanding robust security on both individual devices and the entire network. However, many IoT devices have limited processing power and memory, hindering the implementation of strong security measures. Additionally, the lack of built-in security features and outdated firmware make them susceptible to unauthorized access, data breaches, and manipulation. The heterogeneity of devices, protocols, and platforms interweaved in IoT scenarios leads to interoperability challenges and makes it difficult to establish consistent security processes. Weak regulations and the tendency of some manufacturers to prioritize functionality over security exacerbate these issues. Beyond these foundational challenges, securing IoT networks and devices requires addressing several critical areas, such as:

- Security visibility: Security gaps are extremely hard to be detected, to remediate, and to address on time. This is especially true in IoT ecosystems as the large variety of devices, specifications, and vendors makes it difficult to gain clear views into their security posture.
- Effective information sharing: The effectiveness of information sharing with incident response teams (CERTs/CSIRTs) falls short, hindering collective efforts to address threats. This compounds with other security challenges, as the complexity of the systems make the building of collective defences critical to achieve meaningful security levels.
- Lifecycle management: IoT devices present specific challenges in terms of their lifecycle management (shown in Figure 1). A comprehensive solution should cover the distinct phases, from initial pre-provisioning of security mechanisms during device manufacturing, to its secure deployment, operation, and decommission in target systems.
- Common trust enforcement mechanisms: Trust relies on the different expected behaviours of people, data, information, or processes. However, establishing trust is not easy in autonomous systems like IoT, and it becomes critical to be able to model, monitor and quantify trust and its related events in a way that can be understood by artificial agents becomes critical.
- Identity and privacy framework: managing the identities of IoT devices presents challenges due to their hardware characteristics, autonomous functioning, and complex lifecycles. Current practices often lack information in terms of how device and user privacy is protected, and how this interacts with the security of the system through fine-grained access control.
- Firmware updates: Firmware and security updates are infrequent, difficult, or even impossible in large IoT networks. The outdated firmware and exploitable vulnerabilities that attackers may leverage exacerbates the difficulty of addressing other security challenges.
- Training and automated protocol adoption: Humans are the weakest point in the lifecycle chain, as they build, test, deploy and use IoT.

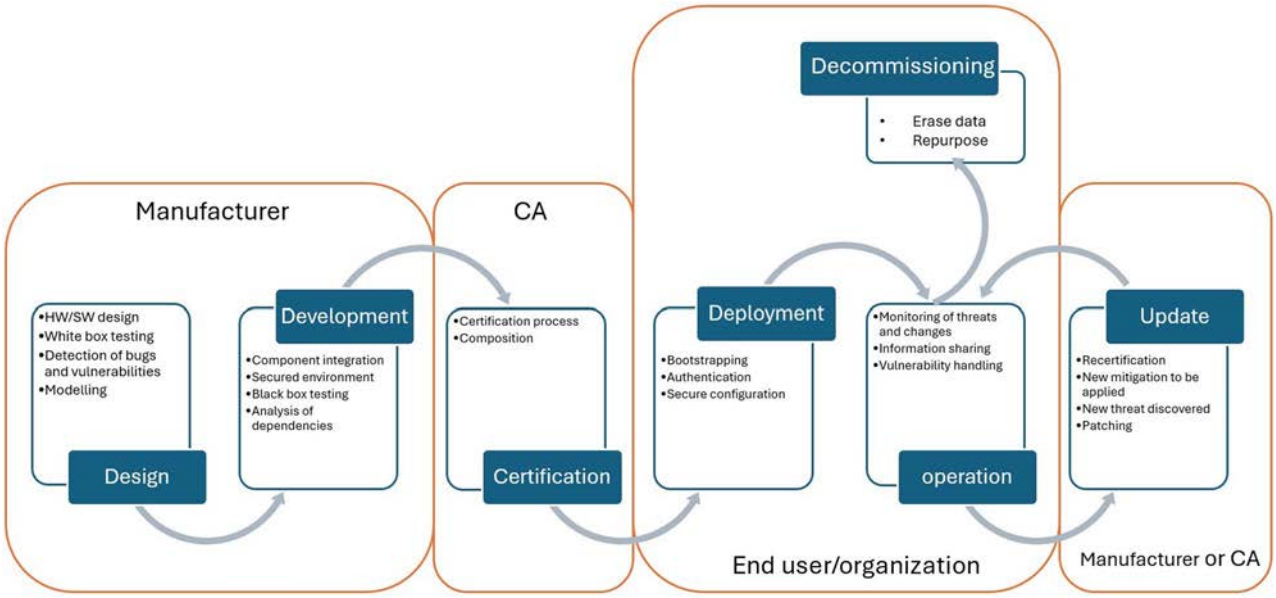

Figure 1: Lifecycle phases

5 ERATOSTHENES

5.1 Overview

The ERATOSTHENES project tackles the complex security challenges of the IoT with a focus on managing the entire lifecycle of these networks through distributed trust management and digital identity solutions. The focal point is the development of a Trust and Identity Management Framework for IoT devices, distributed and operating across the entire network, addressing different steps of the lifecycle of the participant devices. Additionally, the framework is auditable, enabling transparent tracking and verification of actions. Finally, it is privacy-respectful, prioritizing user data privacy and control. By effectively managing the lifecycle of IoT devices, this framework aims to strengthen trust, identities, and overall resilience within the IoT ecosystem. Importantly, the framework is aligned with relevant regulations such as the NIS2 Directive [i.1], the GDPR [i.2], and the Cybersecurity Act [i.3], addressing topics such as CTI sharing for improved cyber-threat handling, privacy-aware identity management and data processing, or device cybersecurity profiles. Overall, the objectives of the project can be summarized as follows:

- Design a reference architecture, components, and protocols for IoT lifecycle management, through the pillars of identity and trust in security domains, suited for resource-restricted environments, critical and industrial applications.
- Design of a decentralized, scalable, efficient and privacy-preserving IoT identity management to conciliate the requirements of self-sovereignty and privacy preservation in a distributed, interoperable, and transparent trust model.
- Design and development of a lightweight, distributed, and dynamic Trust Management solution to enhance the trust in large-scale distributed networks of heterogeneous IoT devices, covering each layer and cross-layer of the network.
- Support the solution and build the overall governance layer of the trust network on novel Distributed Ledger Technologies, enabling decentralization of the solution within domains along with trustworthy information sharing (such as CTI data) in the whole ecosystem.
- Integrate and validate the approach through real-world pilots relevant to the tackled challenges, namely intelligent transport systems, e-health scenarios, and Industry 4.0.
- Deliver knowledge via dissemination and capacity building, supporting the enforcement of the Cybersecurity Act and standardization activities.

5.2 ERATOSTHENES Architecture for IoT lifecycle management

5.2.0 Introduction

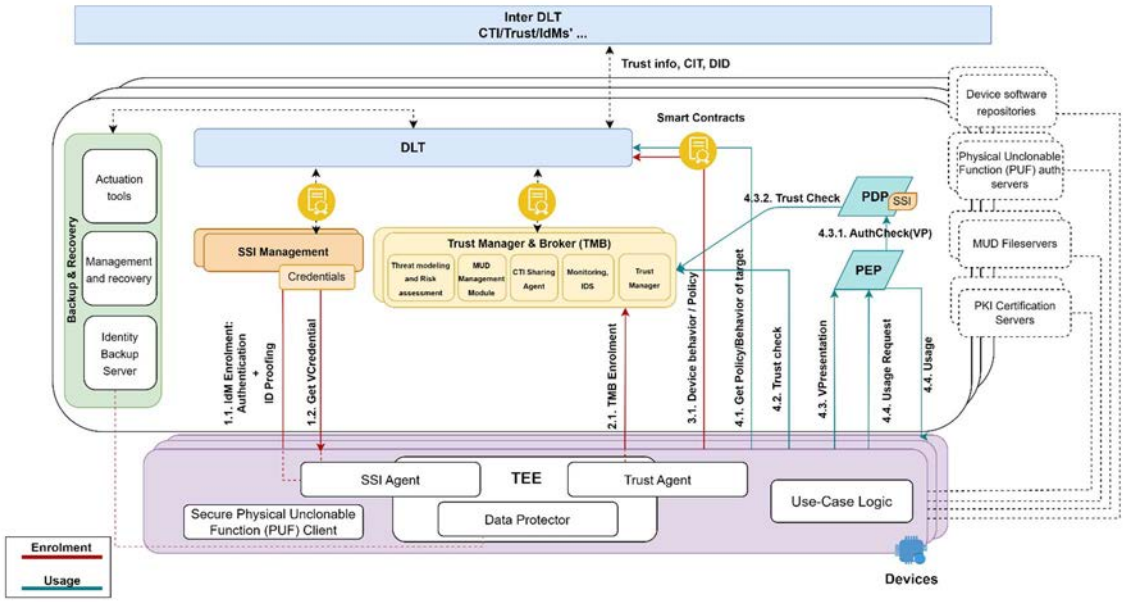

Figure 2: ERATOSTHENES architecture

The ERATOSTHENES architecture and concept have been carefully developed to be adaptable across multiple industrial domains. The architecture is designed to accommodate different use cases, specific requirements, and unique characteristics of each application environment. This flexibility enables its implementation in various scenarios, including transport infrastructures and vehicles, smart devices, personalized health devices, and more. The architecture envisions an environment with multiple independent (but potentially collaborating through information exchange) domains, serving to group operations depending on physical or logical criteria. The components related to the architecture will act within the device, pertain to a specific domain, or operate across multiple ones to enable global functionalities.

ERATOSTHENES establishes identity management based on self-sovereign principles, with SSI Agents in devices managing credentials to enable security and privacy and supporting infrastructural components like SSI Management. Physical Unclonable Function (PUF) based authentication is considered to further enhance the security of identification and cryptographic fingerprinting.

The Trust Management & Broker (TMB) groups key components for achieving a trust framework based on zero-trust principles. Devices will interact with the trust framework through Trust Agents and the TEE will be an anchor of trust for devices along with their identity. The TMB's components for IDS, monitoring, threat modelling, and risk assessment will perform the necessary monitoring and evaluation tasks for maintaining an updated trust network for devices. The use of services will require continuous authorization both through identity and trust policies, with the PDP and PEP serving to delegate the process to the domain infrastructure when necessary.

Along with the identity and trust, the architecture also tackles the management of devices' lifecycles through supporting tools like those for backup, recovery, secure data storage, and management (actuation tools, management and recovery, data protector) and the use of MUD files and CTI sharing both for device's security configurations and coordinated responses to cyber-threats.

The whole ecosystem is enabled by Distributed Ledger Technologies (DLTs) acting as verifiable data registries enriched with smart contracts. Particularly, specific information (such as related to CTI, identity, etc.) can be carried out across domains through inter-DLT to allow collaboration that helps achieve a global ecosystem with enhanced security.

With this series of components, the architecture tackles challenges in the pre-provisioning, commissioning (or enrolment), and operational phases. In the former, providing a root of trust for the identification of the device, i.e. a root identity, and additional identity and security configuration data. Then, during commissioning these artifacts will be used to enrol a device in the security context of operation. The enrolment process enables privacy-preserving authentication and authorization processes, monitoring, and trust evaluation of devices during their operational phase. This is expanded in the following subsections.

5.2.1 Pre-provisioning

The device undergoes initial configuration and security material installation during its first boot at the manufacturer's premises. This process has three key outcomes. First, the device receives and securely stores its root identity material, which serves as a foundation for authentication. This material can range from a simple pre-shared key (e.g. as used in EAP AAA) to a hardware-based root of trust for Trusted Execution Environments or advanced techniques like Physical Unclonable Function (PUF)-based fingerprints. Second, the device is provisioned with security-related configurations, including supported technologies and potential security profiles. Finally, device certificates are generated and installed, providing attributes that define the device's characteristics and identity. These certificates can be linked to the device's root identity, ensuring a secure and verifiable authentication process.

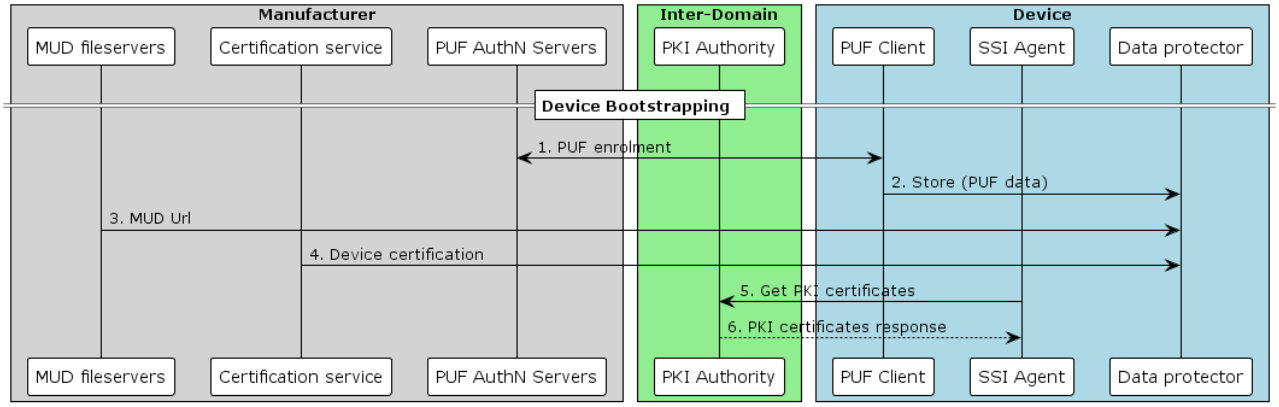

Figure 3: Schematic view of fist pre-provisioning process

In ERATOSTHENES, the Identity Management (IdM) solution uses Physical Unclonable Functions (PUFs) as the primary mechanism for device identification, acting as a root of trust for cryptographic fingerprinting. Figure 3 illustrates the initial pre-provisioning process. During this phase, the device undergoes PUF-based authentication enrolment, which involves installing a PUF authentication client and generating the corresponding cryptographic fingerprint. The device is then registered with the manufacturer's PUF authentication servers, establishing its root identity. Additionally, the device's security configurations are set up by creating an extended Manufacturer Usage Description (MUD) file. This file is stored on the manufacturer's MUD file server, and the device receives a URL linked to its identity through the PUF key material. Traditional identity certificates from PKI certification services are also installed, serving as an attribute source. The specific details of these certificates will vary based on the use case. For example, in scenarios like Intelligent Transport Systems, one of the project's pilots, the certificates may adhere to ETSI TS 103 097 [i.4].

5.2.2 Commissioning

The next phase begins when the device first boots and connects to the target security context. To interact with the domain infrastructure, the device should perform a bootstrapping process that authenticates its root identity. The domain should have a trust relationship with the manufacturer, either directly through its identity service or implicitly, such as by trusting a public signing key. During this step, a domain identification key may be generated, acting as a root identity for use exclusively within the security context. Another important aspect of Identity Management (IdM) is enabling privacy-preserving authentication and authorization. In many use cases, authorization does not only require identification, but also the proof of certain identity attributes. Access control typically depends on conditions tied to these attributes. The framework follows self-sovereign identity principles, where subjects retain control of their identity. Therefore, the device's enrolment includes the issuance of credentials for attribute verification in the security context. This is done through identity proofs, typically in the form of certificates obtained during the initial manufacturer pre-provisioning. The final steps to be carried out during enrolment depart from the field of identity but are crucial for collaborative IoT scenarios and data spaces. Devices may publish their planned behaviour within the security context, such as offering services, data, or associated policies. This enables interactions during the operational phase and may influence how the authorization process is conducted. The result will be the full integration of the device into the trust management framework in the domain, enabling its monitoring and trustworthiness evaluation.

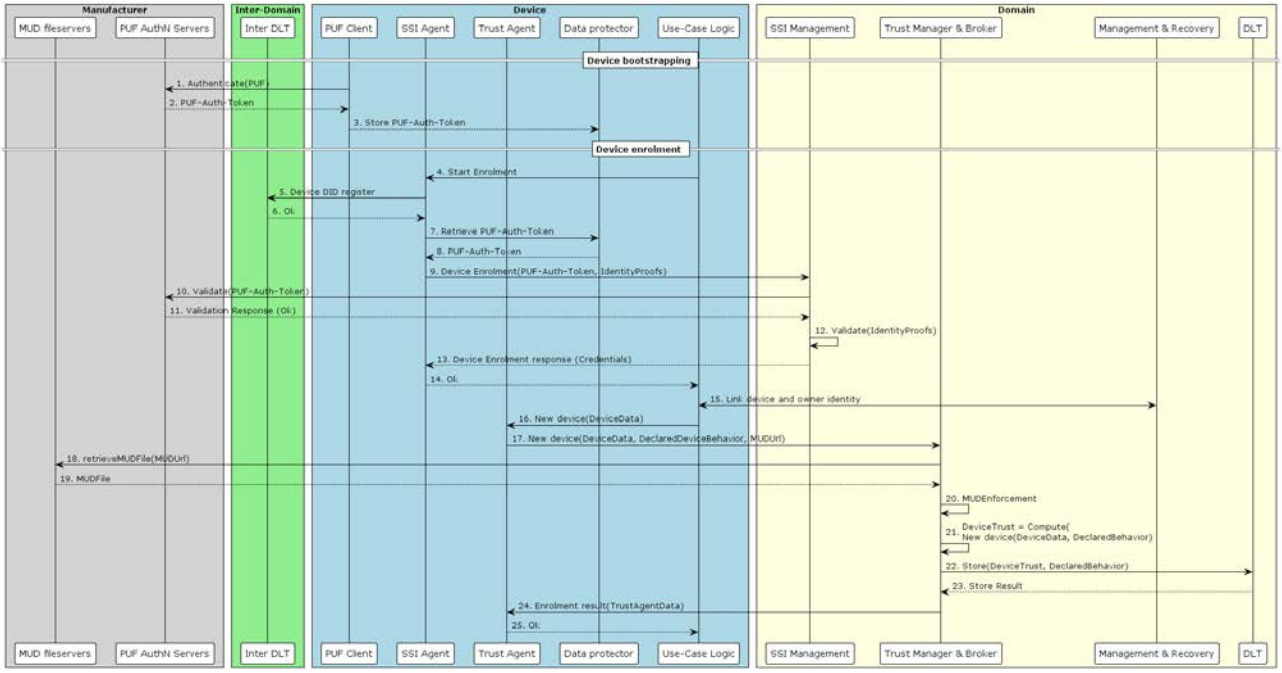

Figure 4: Commissioning, enrolment in a security domain

In ERATOSTHENES, the initial boot in the security domain (see Figure 4) is performed through the PUF authentication process. In this case, the process requires active involvement of the PUF authentication servers in the manufacturer's premises. As a result of this process, the device, through its **SSI Agent**, generates an identity for use within the domain and registers a Decentralized Identifier (DID) for identification. The SSI Agent interacts with issuers in the **SSI Management** infrastructure to facilitate the issuance process. This includes the identity proofing of the device, which may use the PKI certificates obtained by the device. After this, the device will have Verifiable Credentials (VCs) stored in its wallet. These VCs can be generated using a **p-ABC** scheme, that provides the opportunity for devices to later present them through the derivation of zero-knowledge proofs that reveal only the specific data necessary for an authentication process, improving the privacy achieved by the solution. To ensure secure usage and storage, the device's **Trusted Execution Environment (TEE)**, particularly the **Data Protector** component, is used (note that sensitive material such as VCs or secret keys will be stored within the Data Protector, which is omitted from the diagram to avoid cluttering). At this point, the device has completed the identity enrolment process, but it may be necessary depending on the use case to link the device identity with the identity of its owner or manager within the domain (e.g. the security manager of a shop floor).

However, there is an additional process to complete the full enrolment within the ERATOSTHENES domain, involving the trust framework and particularly the Trust Manager & Broker. First, the security configurations are retrieved, analysed, and applied within the trust management component. This step initiates trust score calculations, risk assessment, monitoring, and other processes within the component. Note that the component is comprised of multiple subcomponents that will carry out the complex processes, such as Intrusion Detection Systems for monitoring, Risk Assessment and Threat Modelling engines, and a MUD Management module. The results, such as the initial trust score calculations and their rationale, are published on the DLT, which serves as the project's verifiable data registry.

5.2.3 Operational Phase

Once the enrolment has been completed, devices are ready to interact with other entities in the security context. The framework defined in ERATOSTHENES follows the principles of self-sovereignty. That is, devices are in control of their identity materials, and no other parties should play an active role during an authentication process. As for the actual authorization, the project considers two scenarios that are common in practice. In both cases, the authentication check is equivalent: the device generates a Verifiable Presentation containing the information requested by the attribute-based policy. Outside the policy check, the process varies depending on who oversees verifying the result.

On the one hand, the project envisions a fully decentralized approach, where the service provider is the one that assesses the requesting device. On the other hand, the service provider may delegate the authorization check to the infrastructure with the traditional roles of Policy Decision Point (PDP) and Policy Enforcement Point (PEP). Slight variations, like the service provider acting as its own PEP, are easily adapted from the framework. The main advantage of the centralized approach is that the more resource-intensive authorization process is carried out less frequently, with the verifier delegating the task to the infrastructure. This enables service providers with limited resources, or those that prefer to rely fully on the infrastructure, to integrate seamlessly into the framework. Additionally, it maintains backward compatibility with many existing IoT scenarios that already use a PDP/PEP infrastructure. However, this approach places a greater burden on the server-side and diverges from decentralization, as it requires stronger trust assumptions in the infrastructure. Despite this, both approaches can typically coexist, offering a range of viable options.

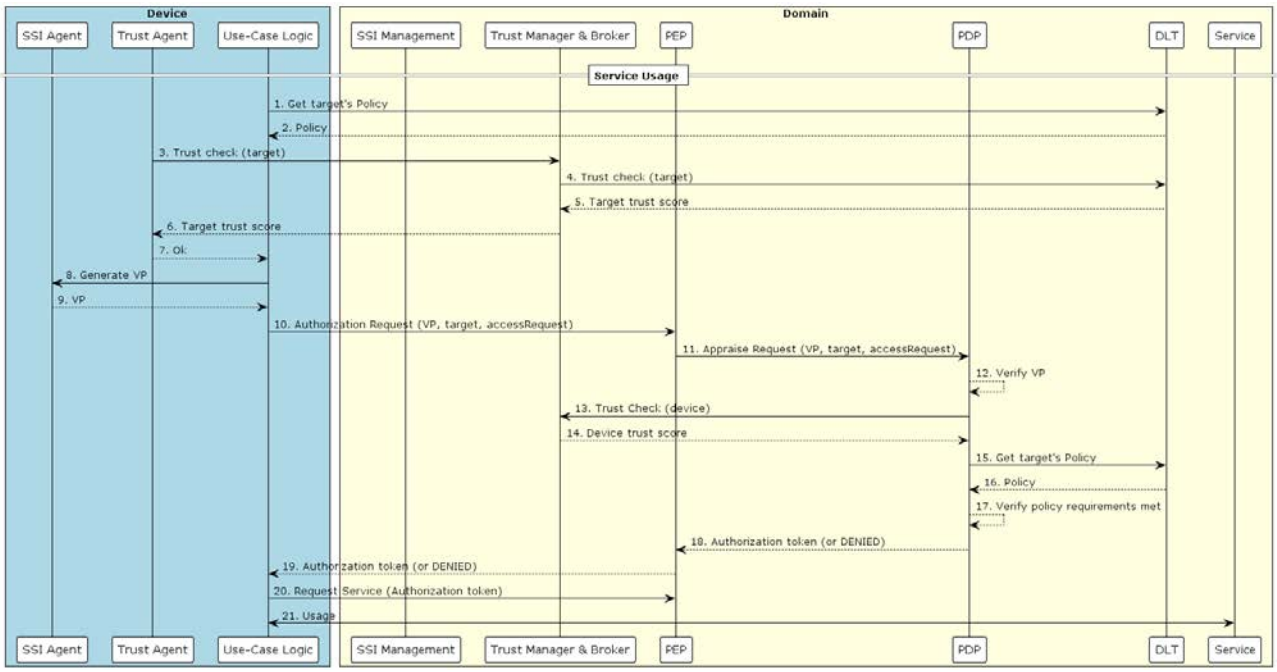

Figure 5: Service usage authorization check

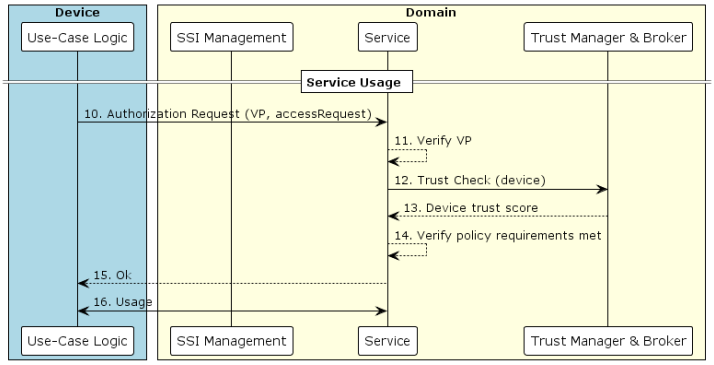

Figure 6: Service usage decentralized authorization alternative schematic view

Thus, in ERATOSTHENES (see Figure 5) devices can perform authentication/authorization processes using the VCs retrieved during enrolment. Participants can retrieve policies from the DLT and generate Verifiable Presentations (VP) that include the necessary information to fulfil the policy through their SSI Agent. Additionally, they may check the current trust evaluation of the target service to inform the decision on continuing with the process or not. Due to the p-ABC scheme, the authentication process can be done in a zero-knowledge fashion, ensuring minimal disclosure and non-link-ability of the revealed data. By generalizing the process by enabling the PDP to generate authorization tokens that are valid for the mid to long term, reducing the frequency of complete authorization processes. These tokens are then checked by the PEP when accessing a service. Alternatively, the use of a direct communication flow is also supported by the solution, as shown in Figure 6. In both cases, according to the zero-trust approach of the framework, the current trust score of the involved parties is checked as an additional source of information for authorization decisions. The DLT plays the role of a verifiable data registry for identity and trust information, serving as a decentralized enabler for the trustworthiness in the process.

Note on flexibility of the presented flows: The previous subsections present a solution covering the steps identified in the ERATOSTHENES framework up to device's actively participating in the domain. Throughout the discussion, it has established specific solutions, but it is worth noting that there exist alternatives with trade-offs. For instance, the adoption of a full-fledged p-ABC scheme brings remarkable privacy advantages but also introduces limitations e.g. in terms of efficiency. In some scenarios, selective disclosure might be enough to cover the privacy requirements. In other cases, it might not be possible to rely on schemes more complex than plain forwarding of credentials because of limiting resource constraints of the involved devices. Similarly, PUF-based authentication gives high guarantees against forgery or attacks on devices but imposes strict requirements on hardware that simpler solutions like pre-shared keys or plain certificates avoid.

This need for flexibility is not only important for instantiations of the framework in different use cases. The vast heterogeneity within IoT environments in terms of conditions or device types makes the flexible application of technologies a key requirement in every deployment. Otherwise, solutions will achieve poor security or privacy results or become impractical as many devices will not be able to participate. This means the ideas of protection profiles enforced for specific targets (ISO/IEC 15408-1 [i.49]) are a compelling avenue for comprehensive solutions. It enables the creation of "flavours" of security/privacy, which will be applied depending on the characteristics or needs of each device and domain of use.

Accordingly, while the flows presented are the main solution in the ERATOSTHENES architecture, some variations are foreseen and planned. Precisely, the application of specifications such as the W3C VCs allows organizations to achieve transparent interchangeability between different solutions that offer trade-offs on security, privacy, and efficiency during an attribute-based authorization process without changes to flows, implementations, or models. Similarly, not all devices will be PUF-enabled, so alternative approaches for the root identity like pre-shared keys may be considered as an alternative. In this sense, the zero-trust approach of the framework helps to accommodate such changes more smoothly. The device's trustworthiness will be continuously evaluated and considered for authorization. Particularly, during enrolment, their characteristics and supported technologies will be considered to assign trust scores. A key tool for moving towards the security profile paradigm and aligning with Cyber Resilience Act (CRA) [i.20] is the extended MUD files, which can be assigned to each device to establish some security configurations that will be considered during enrolment and operation (see clause 9 for more information).

Particularly, the recovery processes in ERATOSTHENES cover multiple scenarios related to a device's lifecycle such as partial compromise or malfunction, actuations against potential threats even before they are realized, or substitution for a new device. The process may be triggered internally by the monitoring tools, or coming from the threat and mitigation sharing framework of the project as expanded in clause 7. Then, depending on the specifics of the issue, a multi-stage recovery process will be carried out. First, if necessary, new software will be securely deployed on the device (e.g. an upgraded version of a firmware that patches a known vulnerability). Then, recovery of identity material will be carried out, protected through the use of Data Protector and advanced cryptographic techniques such as proxy re-encryption. Lastly, the trust context of the device within the security domain will be updated and configured in the device to ensure its readiness to participate in the domain as part of its operation. The DLT is used as a verifiable registry to support these processes in a decentralized way.

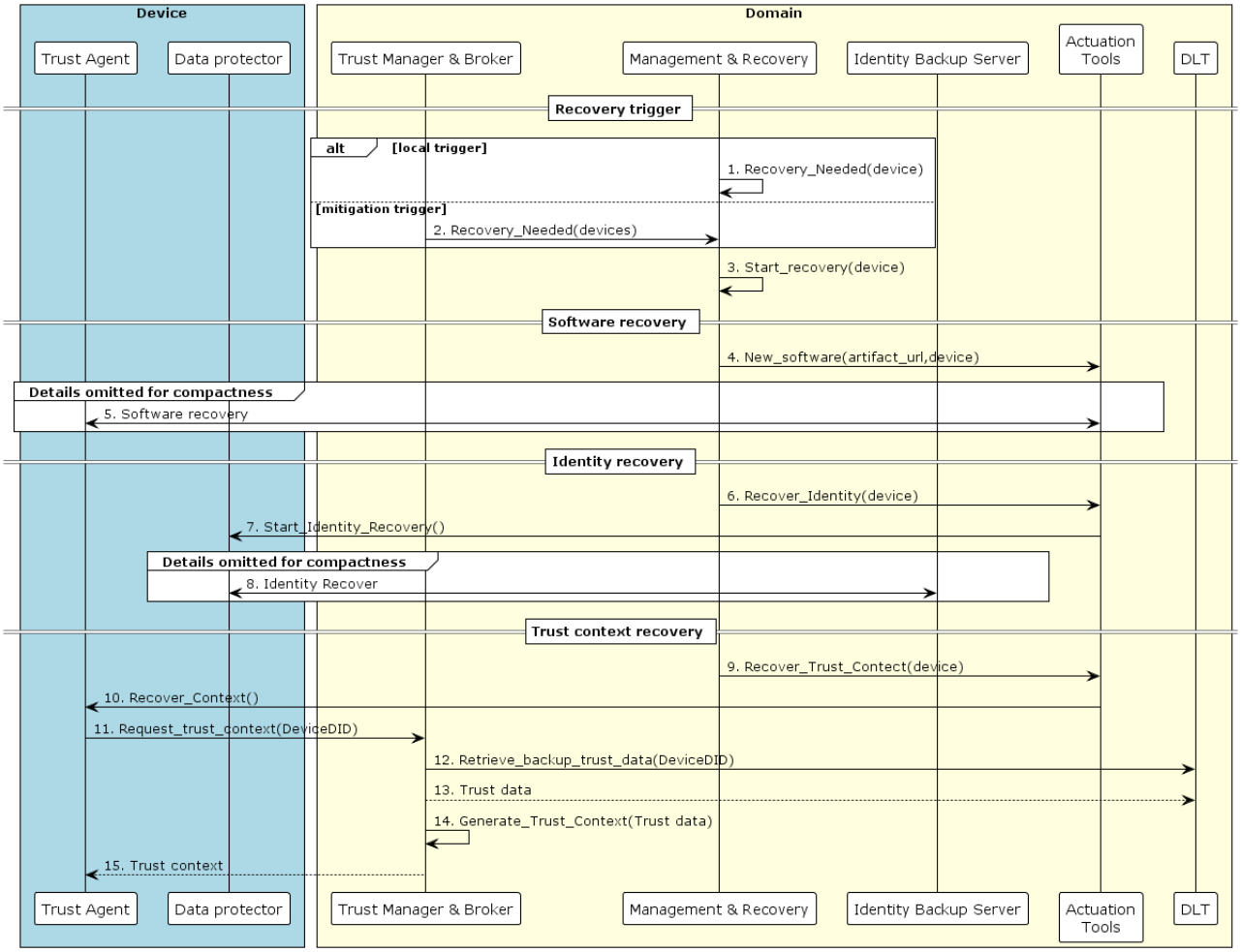

Figure 7: Generic device recovery process

6 CERTIFY

6.1 Overview

The Horizon Europe project CERTIFY (active security for connected device lifecycles) aims to provide a methodological, technological, and organizational framework that ensures security throughout the lifecycle of connected devices. These efforts align with current EU regulations, particularly the CRA, positioning the project to not only demonstrate compliance but also to address real-world security challenges.

CERTIFY's goal is to provide to IoT stakeholders (e.g. auditors, manufacturers, users, Information Sharing and Analysis Centers (ISACs), with tools and strategies that foster a high level of security. The project takes a collaborative and decentralized approach, helping stakeholders identify, assess, and respond to security threats throughout the lifecycle of connected devices. A key point of the CERTIFY approach is the sharing of security information and evidence among relevant parties, allowing for continuous risk assessments and faster responses to new vulnerabilities.

CERTIFY's methodology addresses the full lifecycle of connected devices - from initial design and risk assessment to secure decommissioning or repurposing. Rooted in the principle of security by design [i.46], [i.47], the approach integrates security protocols and cryptographic controls from the beginning. By embedding these measures early in the design and development phases, CERTIFY ensures that devices are equipped to resist threats before they are deployed. After deployment, the framework supports secure commissioning, continuous monitoring, and adaptive reconfiguration to preserve device integrity and resilience against emerging vulnerabilities. This proactive strategy reduces real-time risks and limits the need for costly, reactive fixes.

6.2 CERTIFY Framework

6.2.0 Introduction

The CERTIFY architecture, as depicted in Figure 8, is organized into six "domains" or "planes" with dedicated functionalities.

The embedded device plane provides security services built on top of hardware functionalities to instantiate and maintain a secure environment. It characterizes the IoT platform through the CERTIFY API and services, including for instance support for operations such as configuration, bootstrapping, upgrading, and monitoring. These high-level services are offered by the low-level security enablers for the IoT device, the Secure Element (SE) [i.32] and the Trusted Execution Environment (TEE) [i.33]. The access to such enablers is abstracted and made accessible through a low-level API.

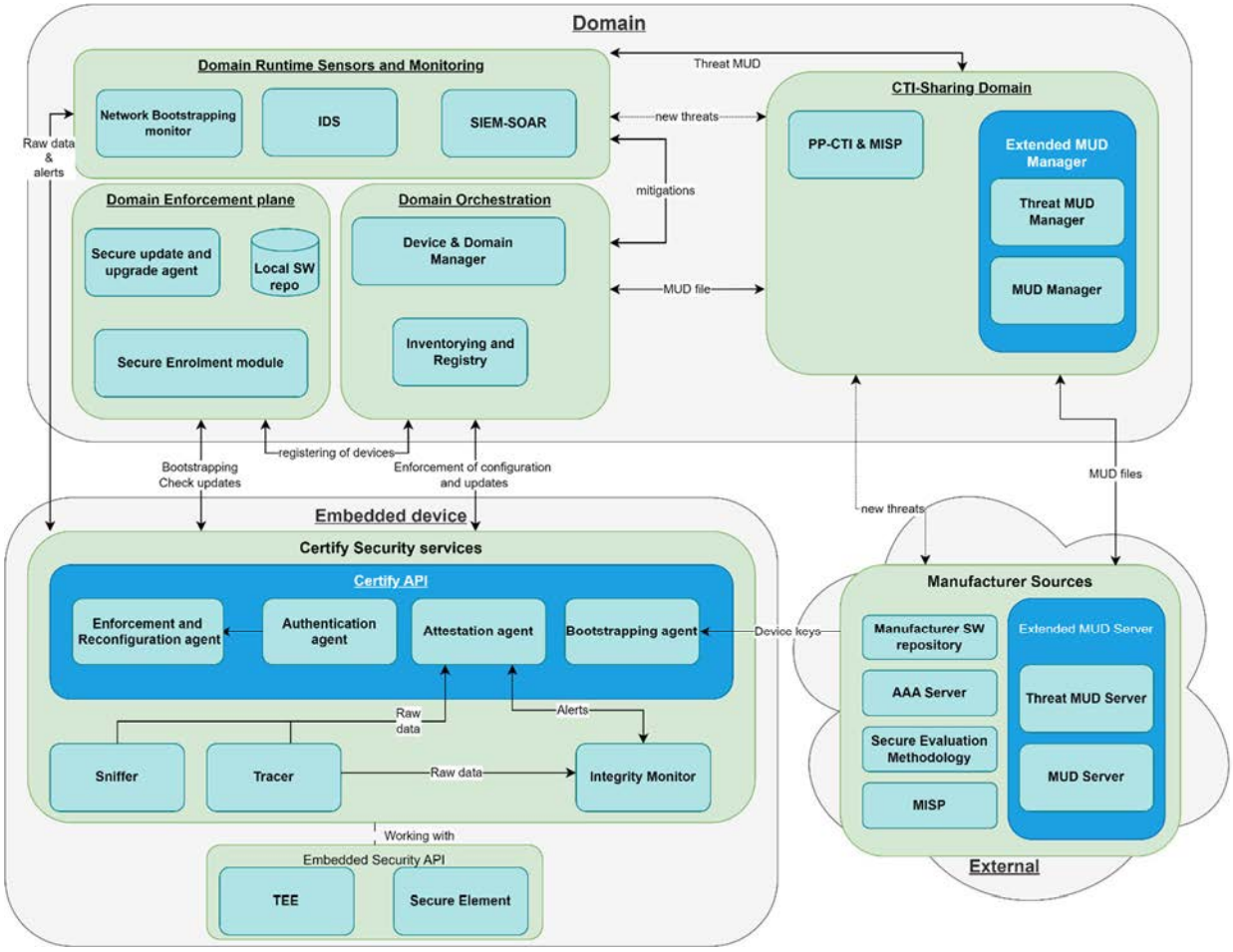

Figure 8: CERTIFY Architecture

The Domain enforcement plane includes services for the secure deployment of the device within the domain and the application of updates on the device. One core component of this plane is the Secure Enrolment module, responsible for the registration of the devices in the domain and the issuance of cryptographic material as the basis for domain identities. The secure update and upgrade agent provides a graphical user interface where security administrators can visualize registered software and devices, upload the software to the repository, and trigger the secure Over-The-Air (OTA) software update process.

The Domain orchestration plane provides coordination functionalities within the domain, and its main component is the Device and Domain Manager, that provides high-level management IoT devices within a security domain. In particular, it coordinates the enforcement and reconfiguration of IoT devices. All the configurations (e.g. policies applied, version of updates) are stored in the Inventorying and Registry, which provides trustworthy data storage e.g. through DLTs.

The Domain runtime sensors and monitoring plane offers software-based solutions for monitoring, detection, and decision functionalities based on the information received from the device and other domain components. The Network Bootstrapping Monitor and the Intrusion Detection System (IDS) receive data from the CERTIFY API in the IoT device regarding the network activity in different phases of the lifecycle (bootstrapping and operation). Alerts are sent to the SIEM-SOAR (Security Information and Event Management - Security Orchestration, Automation and Response), which aggregates data and carries out complex analysis.

The Cyber Threat Intelligence (CTI) plane provides services for ensuring privacy-preserving sharing of security information, such as vulnerabilities, mitigations or recommended configurations. The Privacy-Preserving CTI (PP-CTI) system is a central tool here, anonymizing sensitive data and attributes in cyber threat reports. For responding to identified threats, the CTI plane combines the MUD [i.7] with the Threat MUD server [i.11] respectively as default secure configuration, and threat and mitigation signalling mechanisms.

Finally, the external plane integrates all the manufacturer services that, even if not strictly part of the framework, are exploited by CERTIFY. In particular, it includes services for security assessment and certification, CTI sharing, device authentication, and MUD generation and storage.

6.2.1 Pre-provisioning

6.2.1.1 Design Phase

In this phase, the device is designed, developed, programmed, and tested, establishing its initial security posture. All actors in the supply chain - component designers, integrators, and software developers - are involved, while the manufacturer conducts the initial security evaluation. However, as new threats and vulnerabilities continue to emerge, defining a fixed, standardized cybersecurity evaluation and certification process becomes increasingly difficult. This evolving threat landscape demands agile and dynamic approaches to maintain product security throughout its lifecycle. As a result, continuous assessment and the use of dynamic labels that reflect a device's current security status in real time are essential. While current certification schemes [i.48] acknowledge this need for adaptability, frameworks like Common Criteria (CC) [i.5] still require full recertification for any security change, leading to significant time and financial costs [i.34].

To support security by design and enable dynamic certification, CERTIFY proposes a model-based evaluation and certification approach. This method allows security to be tested from the early design stages and supports automation of the evaluation process by integrating security testing with risk assessment. The approach is implemented through the Cyberpass tool (https://www.cyber-pass.eu/) - a cloud-based platform that interprets security requirements and guides the evaluation process. It begins with a self-declaration or self-assessment step, enabling manufacturers to respond to a tailored questionnaire based on relevant security criteria.

6.2.1.2 Pre-provisioning of security material

While security assessment results are typically used only for device certification, CERTIFY leverages this information to enhance device deployment and operation. Specifically, the evaluation results are embedded into a behavioural profile that maps different security levels to recommended operational policies. This profile limits the device's behaviour to a defined set of actions, thereby reducing its attack surface and enabling the detection of anomalous activity during runtime. CERTIFY's behavioural profile extends the Manufacturer Usage Description (MUD) standard [i.35] and [i.36]. The extended MUD profile is digitally signed by the Certification Authority (CA) and hosted on a MUD server, making it accessible to clients that buy and deploy the device. The MUD URL and root cryptographic identity material are stored in the device to facilitate secure deployment. To support this process, CERTIFY utilizes strong isolation mechanisms - such as Secure Elements (SE) and Trusted Execution Environments (TEE) - enabled by open hardware architectures and trusted computing standards.

6.2.2 Commissioning

The commissioning phase starts when the device is installed and configured in a certain context. This usually consists of a set of procedures in which a device joins a network in a certain security domain. During the process, the cryptographic material installed during the previous phase is used to derive dynamic credentials and keys to be used during its operation. Extended MUD files were integrated into CERTIFY's enhanced commissioning to enable the safe deployment of configurations prior to the device joining the domain. Therefore, the device will not be allowed to interact with other components or to access network resources until it is not properly identified, configured, and authenticated, ensuring that the network will not be compromised once the device will access to it.

In the first stages, the device requests to start the bootstrapping in the domain. CERTIFY leverages the Extensible Authentication Protocol (EAP) [i.25] to authenticate the device and generate domain keys. Moreover, CERTIFY relies on the extended MUD of the device, which is securely retrieved and translated in the MUD manager during the authentication process, to securely configure the device. The results are used during the security configuration of the device. Additionally, CERTIFY also checks that the device type is authorized based on its fingerprint. While attempting to join an IoT network, each device type exhibits a characteristic fingerprint. The network bootstrapping monitor exploits such a behavioural feature of the device to build a monitor that can pose constraints on the devices that can join the network, as well as request the enforcement of specific rules. This behavioural fingerprint can be created by the manufacturer and included as part of the extended MUD file designed in CERTIFY.

For completing the enrolment in the domain, high-end devices need to verify their correct state based on the policies defined in the MUD. CERTIFY leverages the DAA (Direct Anonymous Attestation) protocol to authenticate the high-end device and generate appropriate policies for attestation. The DAA allows verifying the correct state of the device based on this verifiable evidence and helps to decide whether the network should allow or not the device to join. Once deployed, the device can generate dynamic credentials based on its identity for securely communicating with the entities inside the domain. All the information about authorized network devices, configurations, identity certificates and upgrades are stored in the Device Inventory and Registry.

6.2.3 Operational Phase

6.2.3.0 General

In the operational phase, continuous monitoring of the device is essential due to evolving security threats and vulnerabilities that were not anticipated at design time. As a device's security posture evolves, it may require reassessment and even recertification. Within the CERTIFY framework, monitoring components collect data from IoT devices to detect vulnerabilities and trigger appropriate mitigation actions. Runtime attestation and the Integrity Monitor verify that certified security properties are maintained, while an IDS analyses network traffic in real time to identify potential threats. Detection rules are regularly updated with new signatures and can be tailored to specific user or customer needs.

More complex analysis is handled by the Security Information and Event Management (SIEM) - Security Orchestration, Automation, and Response (SOAR) component, which processes events from both the network and the device, correlating them to detect sophisticated threats. The Device and Domain Manager then coordinates enforcement of mitigations and updates, linking runtime detection to recommended actions from manufacturers, threat databases, or certification authorities. CERTIFY uses an extended Threat MUD to support this process, enabling the system to block network access or reconfigure the device in response to critical risks.

CERTIFY fosters continuous information sharing among stakeholders. It integrates external intelligence on vulnerabilities, patches, and zero-day threats with domain-specific insights. This is done through the Privacy-Preserving CTI (PP-CTI) component [i.37], which securely shares data with manufacturers and Cyber Threat Intelligence (CTI) providers, enabling bidirectional exchange of alerts, threat information and even mitigation actions.

6.2.3.1 Updating

Over-The-Air (OTA) software updates are vital for maintaining the long-term security of IoT devices. This need is underscored by standards and recommendations from organizations such as the European Union Agency for Cybersecurity (ENISA), which highlights regular updates as key to improving the security and reliability of connected systems [i.38], [i.39] and [i.40].

CERTIFY aligns with these recommendations by incorporating OTA components based on the IETF RFC 9019 [i.6] framework. To strengthen security and trust, CERTIFY integrates DLTs to log every event related to firmware updates and device metadata. This provides transparency, immutability, and a continuous chain of trust across the OTA process. Secure cryptographic algorithms are used to verify firmware integrity and sign updates, ensuring authenticity and protection against tampering.

The update phase in CERTIFY includes both the deployment of software patches from manufacturers and configuration adjustments needed to counter emerging threats. These tasks are carried out by a coordinated set of components - such as the enforcement and reconfiguration agent, secure update and upgrade agent, and the device and domain manager - and may be initiated manually by administrators or automatically in response to detected threats or anomalies.

6.2.3.2 Decommissioning & Repurposing

The decommissioning phase in the CERTIFY lifecycle marks the final stage of a connected device's life, where it is either retired from operations or repurposed. This phase is crucial to ensuring that devices no longer in service do not pose residual security risks. Proper decommissioning protects the network by securely managing all sensitive data and configurations, preventing potential vulnerabilities that could arise from improper disposal.

The process begins with an assessment to determine whether the device can be safely repurposed for a less security-sensitive role or should be fully retired. For devices being decommissioned, CERTIFY prioritizes secure data erasure - permanently deleting cryptographic keys, certificates, logs, and configurations. To ensure transparency and policy compliance, the framework uses DLT to create a verifiable, immutable record of the decommissioning process.

If a device is deemed suitable for repurposing, CERTIFY provides a secure reconfiguration framework. This may involve assigning the device to a lower-security domain or adjusting its functionality to handle less sensitive tasks. While repurposing can extend device lifespan and reduce costs, it should be done in a way that maintains appropriate security standards for the device's new role.

7 Design of the continuous cybersecurity posture management and relation to CRA and certification

7.1 Introduction

In both projects, two technologies rise as a key cornerstone for achieving the continuous cybersecurity posture and certification goals.

7.2 Manufacturer Usage Description (MUD)

7.2.0 General

To achieve effective detection and mitigation of security threats in specific IoT environments, it is useful and sometimes necessary to know the expected behaviour of devices beforehand. However, the heterogeneity of IoT environments (from critical infrastructures to home) and of devices themselves, based on various technologies and communication protocols, and the restrictions inherent to certain IoT devices (e.g. the lack of a user interface) make the management of IoT devices cumbersome for non-expert users. To cope with these challenges, one key aspect is to standardize the identification and management of device behaviour.

The Manufacturer Usage Description (MUD) standard was published in 2019 by the Internet Engineering Task Force (IETF) [i.7]. The MUD specification's major goal is to limit the threat and attack surface of a certain IoT device by allowing manufacturers to establish network behaviour profiles for their devices. Each profile is specified through Access Control Lists (ACLs), which establish policies for communication endpoints. They are defined using Yet Another Next Generation (YANG) [i.8] to model network restrictions, and JavaScript Object Notation (JSON) [i.9] as the serialization format. Since its adoption, MUD has been the object of interest both from researchers and standardization bodies. In particular, the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA) consider the use of MUD as part of future IoT security good practices to increase security against cyberattacks in IoT domains.

The protection of security in environments with IoT devices does not end with the initial device installation. Many vulnerabilities and attacks can, and indeed are, discovered during the operational phase. For instance, only in 2022, more than 25,000 vulnerabilities were detected [i.10]. Manufacturers cannot always deal with vulnerabilities quickly enough through updates, which follow a complex process, and in many cases the relationship with third-party services makes this even harder. While MUD files can be updated, this process does not cover most vulnerable scenarios. In this sense, security-information-sharing systems enable fast and collaborative sharing, and analysis and mitigation of vulnerabilities or attacks, which may also be applied before a patch is released. The sharing of cyber-threat information for building cybersecurity capabilities has also been a big focus of the NIS2 Directive of the ENISA [i.1].

In this direction, the NIST proposed a threat Manufacturer Usage Description (threat MUD) [i.11], to share vulnerability information and its mitigations. It is based on the MUD standard for device behaviour specification and follows a similar structure. However, despite the close relationship, the threat MUD is conceived as a mitigation mechanism. However, the NIST only gives some indications about the threat MUD model and its functioning, leaving some details undefined but framed in the guidelines. In the following clause, the present document overviews the threat MUD model as presented in [i.12], which the present document uses as a basis, though with differences on how the flows are integrated into the architecture (e.g. receiving threat identifiers for which to search associated files through the TMB). The present document takes NIST guidelines and the MUD standard as a starting point.

A key element to have in mind for the threat MUD is that, even if its structure and operation are similar that of the regular MUD, its purpose is to serve as a mitigation method against a specific threat, particularly through network communication rules for sites that have been associated to a threat. Therefore, a threat MUD does not need to be strictly related to a specific device, nor specify expected behaviour. As a result, rather than being developed by the manufacturer, the threat MUD might be created by a threat intelligence provider.

As with the standard MUD, the threat MUD model has two modules. The first module reflects information about the threat MUD itself. It contains equivalent fields to the MUD standard, such as version, URL, cache-validity, signature, etc. However, some fields have to be modified (manufacturer name is changed to intelligence provider, and device model name is changed to threat name), removed (information about device to which the MUD is associated like system or firmware is no longer needed), or added (CVSS and documentation fields for additional information about the threat) to fulfil the new mitigation goal. The second module is again related to the ACLs that specify the conditions and restrictions. In this case, as the file is tied to a threat and its mitigation and not to a specific device, the configuration to apply should be as generic as possible. Thus, unnecessary fields like "same-manufacturer", "local-networks", "controller", and "my-controller" (which established conditions specific to the device) are removed.

MUD is integrated into ERATOSTHENES and CERTIFY as a source of behavioural information of the devices that enrol in a domain. The MUD file servers are outside of the end user domains, e.g. on the manufacturer premises. MUD components from all domains may communicate with them to retrieve MUD files. The main functional components of the MUD standard and threat MUD proposal will be active in each domain, as part of the Trust Manager & Broker component.

7.2.1 Key Components of MUD

- **MUD File:** This file, created by the manufacturer, contains a detailed set of instructions that define the anticipated network behaviour of the device. It serves as a blueprint for the device's network interactions and security posture.
- **MUD Manager:** This component acts as the network administrator. It is responsible for retrieving MUD Files using MUD URLs provided by the devices. The MUD Manager ensures that the network policies are updated according to the latest MUD specifications.
- **MUD URL:** Embedded within the device by the manufacturer, this URL points to the location where the MUD file is stored. It allows the MUD Manager to fetch the necessary files for policy implementation.

7.2.2 Extended MUD

The MUD standard [i.50] presents a few limitations to its capabilities and applicability in practice, such as reduced expressivity focused only on networking, insufficient security in the MUD retrieval process, or supporting efficient updates for security information. Both ERATOSTHENES and CERTIFY go beyond the standard and provide "extended MUD", addressing such gaps for an improved impact of the solution in the lifecycle management process.

CERTIFY extends the MUD model to accommodate finer-grained security aspects and diverse security policies. These encompass extended network access control, channel protection, data protection, and authorization policies [i.36]. In this regard, while a standard MUD server offers guidelines for allowed or restricted network activities for each device, a Threat MUD server would allow to incorporate real-time or near real-time threat information as provided by the PP-CTI. Additionally, the extended MUD file is taking advantage of to include behavioural profiles and device fingerprints that can be later used for attestation and monitoring of the device during the initial phases and throughout its operation in a security domain.

One of the key innovations in ERATOSTHENES over the standardized MUD obtaining process comes from the integration of the MUD processing into a full-fledged trust framework. Now, using the ERATOSTHENES domain enrolment phase to get the MUD URL from the device, through the publish/subscribe approach used for communication between TMB components. The integration in such a flow, and within the ERATOSTHENES ecosystem, also allows the exploration of further improvements for the MUD flow.

For instance, while the communication with the MUD fileservers can be easily secured in any usual way for webservers (e.g. HTTPS), there is a glaring gap in the standard regarding the possible spoofing of a MUD URL by the device. This authentication of the URL during MUD file obtention can be tackled through the ERATOSTHENES identity framework. Specifically, the manufacturer (at pre-provisioning time, along with PUF and MUD URL installation) will associate the PUF of a device (as a root of trust for identity) to the respective URL. Alternative approaches can be explored in the case of not having PUF available as a root of trust, following the project's general approach for tackling this case, e.g. by taking it into account when threat models, risk and trust for the device are evaluated. This is addressed, for instance, in CERTIFY with the securitization of the process through the secure element of the device during the bootstrapping phase.

Of course, network elements will still have to be considered in specific instantiations, but this will be partly solved by the own MUD mechanism: MUD files will be associated to devices that are relevant to the application domain, which will make the rules included in them relevant to the deployment domain by default. What is more, the advantages of the extension of the MUD model with higher-level concepts, like software updates or cryptographic parameters restrictions, will be even more relevant through this abstraction.

Lastly, both projects tackle the issue of efficient and scalable MUD updates and the dynamicity of security contexts, with the inclusion of update flows, threat MUDs and other means for sharing threat information. The approach taken in the projects for lifecycle management through MUD files thus innovates by providing comprehensive mechanisms at multiple levels (e.g. not only network level, or one-time configurations) that tackle multiple challenges identified in the MUD standard and other recent works and ensure the continuous management throughout the lifecycle including collaboration through sharing of cybersecurity information from many sources.

7.2.3 MUD management in ERATOSTHENES

7.2.3.0 General

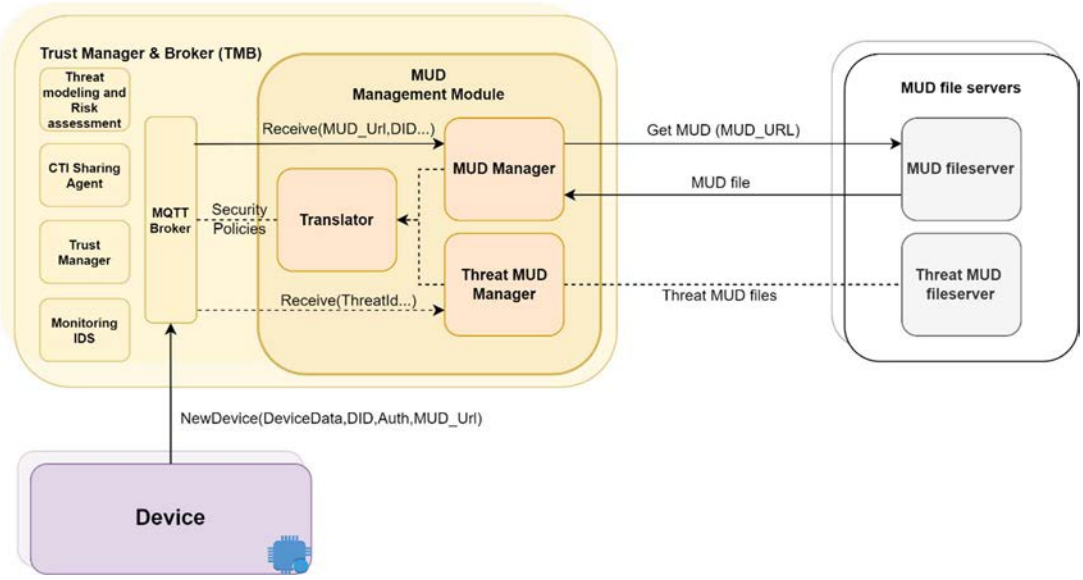

Figure 9: Instantiation of MUD components in ERATOSTHENES

As a detailed example of the described tools and processes, Figure 9 shows the instantiation of the MUD components in the ERATOSTHENES architecture. Note that the MUD management module in ERATOSTHENES is an aggregation of subcomponents, including the functionalities of both standard MUD and threat MUD managers, plus a translation module for the interaction with other ERATOSTHENES components, e.g. by transforming MUD files into corresponding security policies.

7.2.3.1 MUD Manager / Threat MUD Manager

The central components of the MUD Management Module architecture. The MUD Manager oversees the retrieval of MUD files associated to devices that enrol in an ERATOSTHENES domain. The threat MUD manager carries out the equivalent functionality for threat MUD files.

7.2.3.2 Policy Translator

For inter-component communications, ERATOSTHENES introduces a service to translate MUD files into intermediate security policies. ERATOSTHENES currently utilizes Medium-level Security Policy Language (MSPL) [i.13], a security policy language with medium level of abstraction, that provides a set of actions suitable by the most common applicable security settings. The MSPL's structure is defined in a YANG model, which allows using XML or JSON as encoding format. This allows flexibility when applying the information contained in MUD files. Other components will take the medium-level policy from the topic and take advantage of it for their purposes, potentially with another translation into their own structures. For instance, the TMRA may use the policy directly to increase its knowledge base for building models, while the IDS may translate policies into rules that detect related events and further enforcement policies may be derived by PDPs.

7.2.3.3 MUD File Servers

The source for all MUD/Threat MUD files. MUD file servers are located outside the ERATOSTHENES deployment, belonging instead to the device manufacturers. MUD components from all domains may communicate with them to retrieve MUD files. Threat MUD file servers, on the other hand, are controlled by threat intelligence actors (which may not necessarily be manufacturers).

7.3 Continuous Assessment

In today's interconnected digital landscape, cybersecurity is no longer an afterthought; it is a strategic imperative. Organizations should proactively defend against cyber threats, adapt to evolving attack vectors, and ensure the resilience of their systems. This is critical to achieving cybersecurity resilience in the face of constant risks and threats.

Referring to the cybersecurity environment, an organization's continuous efforts to monitor, assess, and improve its security measures are necessary. Unlike a static approach, where security is treated as a one-off event, the continuous posture recognizes that threats are dynamic and require constant vigilance. The following key components are recognized:

- **Threat Intelligence:** Organizations collect and analyse threat intelligence to stay informed about emerging risks. This includes monitoring vulnerabilities, tracking threat actors, and understanding attack patterns.
- **Security Monitoring:** Real-time monitoring of network traffic, system logs, and user behaviour helps detect anomalies and potential breaches. Security Operations Centres (SOCs) play a crucial role in this process.
- **Incident Response:** Having a well-defined incident response plan ensures that the organization can swiftly address security incidents. Timely detection, containment, eradication, and recovery are essential steps.
- **Patch Management:** Regularly and consistently applying security patches and updates is fundamental. Unpatched vulnerabilities are often exploited by attackers.
- **Employee Training:** Educating employees about security best practices reduces the risk of insider threats and social engineering attacks.

The European Union's Cyber Resilience Act (CRA) aims to protect consumers and businesses that buy or use products or software with a digital component. This law establishes mandatory cybersecurity requirements for manufacturers and retailers of such products, ensuring that inadequate security features become outdated. The CRA addresses two key issues:

- **Inadequate level of cybersecurity:** Many products have an insufficient level of inherent cybersecurity or poor security updates. The CRA establishes harmonised standards when placing products or software with a digital component on the market.
- **Inability to determine secure products:** Consumers and businesses are often unable to determine which products are secure from a cyber perspective. The CRA introduces a framework of cybersecurity requirements that governs the planning, design, development, and maintenance of such products.

More descriptions on these regulations and needs, and how ERATOSTHENES and CERTIFY technologies may be envisaged as a tool to address them can be found in clause 9 of the present document.

7.4 Cyber Threat Intelligence (CTI)

7.4.1 General

Cyber intelligence is an information gathering and analysis activity aimed at identifying, tracking/predicting capabilities, and intentions/activities of hostile actors in the cybersecurity domain. Cyber-Threat Intelligence (CTI) can be defined as evidence-based knowledge (including context, mechanisms, indicators, implications, and actionable advice) about an existing or emerging threat that can be used to make decisions regarding similar threats. CTI is a compound of attributes that give overall meaning to such a report, e.g. malicious IP addresses or hashes alone are not considered CTI but grouped in context along with other information to form part of a CTI report. One of the most crucial elements of Cyber Threat Intelligence are Indicators of Compromise (IoCs). They are the most easily actionable attributes and the ones that most tools working with this information focus on: IoCs are widely used in applications such as Intrusion Detection Systems, web blockers, identification of compromised hosts or malware. In addition, these indicators can be easily related to other indicators that have occurred previously, taking advantage of big data analysis techniques on stored indicators.

There are some risks involved in sharing CTI. Organizations are reluctant to share information on such platforms because they feel that revealing information about intrusions could damage their reputation. Moreover, this information sometimes carries identifying data, IP addresses, email accounts, names, which in the hands of attackers can be used against the organization that shared it, if they have not fixed the breaches in their system yet. This information, also, can fall into the hands of a dishonest partner, who can make fraudulent use of the data.

For the anonymization of these identifiers values, there exist privacy-preserving and data transformation techniques, such as suppression, generalization, sampling, k-anonymity, l-diversity, t-closeness, d-presence, etc., derived from Statistical Disclosure Control (SDC) [i.14]. SDC, also known as Disclosure Avoidance, is the discipline that manages the balance between the privacy of respondent data and the usefulness of this data for research purposes.

These techniques attempt to minimize data risks related to identity disclosure, (i.e. when an adversary can correctly associate an individual within a dataset), attribute disclosure, (i.e. when an attacker is able to infer the value of an attribute due to the distribution of attribute values in the table) and membership disclosure, (i.e. the ability of an attacker to be able to determine at very high probability whether or not a particular individual is in the dataset).

7.4.2 CTI in ERATOSTHENES

One of the key business challenges for IoT scenarios is the need for increased cybersecurity, as security events incur in many direct and indirect losses. The components developed in ERATOSTHENES and CERTIFY aim to provide a platform for inter-domain Cyber-Threat Intelligence (CTI) sharing, compliant with the guidelines of the NIS directive. The main outcome is the collaboration of the tools developed for a comprehensive scenario that covers the needs for CTI sharing in heterogeneous and large IoT scenarios. To showcase these concepts, this clause provides a detailed description of the CTI sharing components in ERATOSTHENES.

ERATOSTHENES supports a comprehensive, resource-efficient, and flexible security analysis of threats based on cyber intelligence sharing across the different domains. The objective is to maintain an update status about vulnerabilities and threats that appears through the architecture elements including the lifecycle management and the trust governance layer. To this end, CTI reports will be generated by monitoring entities and shared through the domains with the support of the inter-DLT infrastructure.

The exchange of security and threat information between the various stakeholders is implemented through CTI integration into DLT and inter-DLT platforms. The CTI Sharing Agent is a key component in the process of communication and threat information sharing between domains, specifically CTI and IDS systems. Besides, its anonymization techniques and along with the MISP platform ensure privacy and reliability, and flexible encryption approaches such as CP-ABE, in addition to privacy-enhancing techniques like k-anonymity or t-closeness provide confidentiality, trust, and privacy enhancement. This approach should provide the necessary confidentiality and flexibility for the tracking and exchange of cyber threat information.

Figure 10 shows the detailed description of the CTI Sharing Agent as part of a Trust Manager and Broker, as well as the main communication flows between the subcomponents, and with other ERATOSTHENES components.

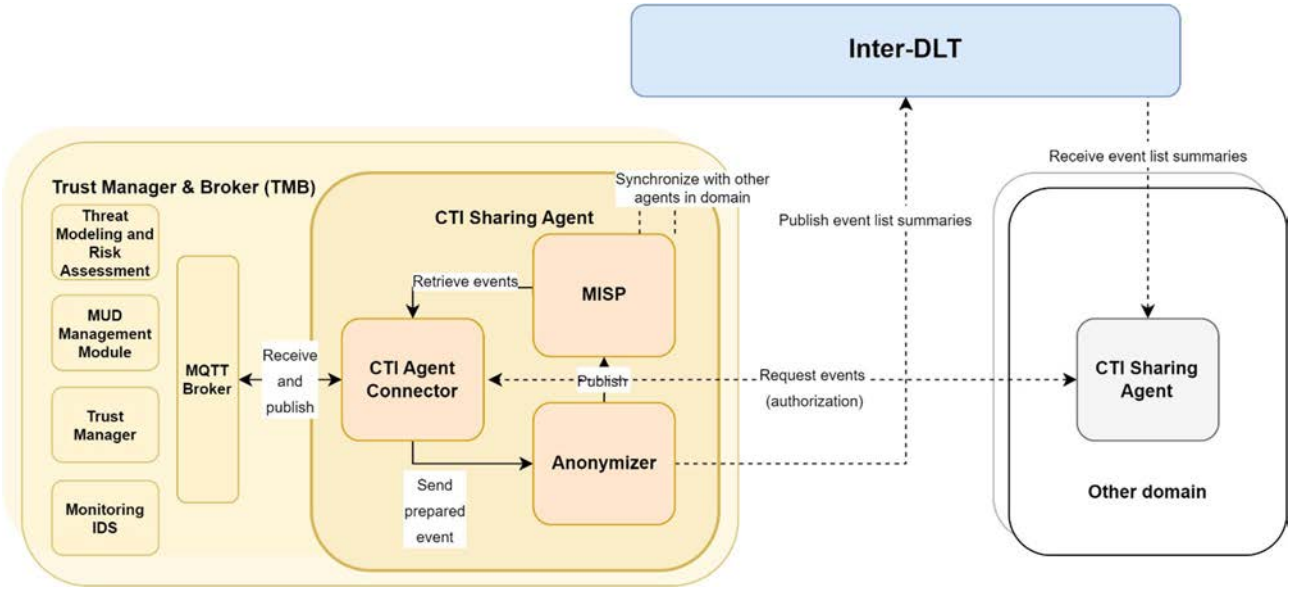

Figure 10: CTI Sharing Agent structure and flows

The information shared through the CTI agent is integrated into the ERATOSTHENES ecosystem through the Trust Manager and Broker. A specific topic is setup so that components interested in threat information will receive the relevant events. One component of particularly close relationship with the CTI sharing tool is the Intrusion Detection System (IDS). The events generated by the IDS after detection of security events are shared with the CTI sharing agent through the MQTT broker. This is received by the CTI Agent Connector, which parses and prepares it and sends it to the next step in the pipeline, the Anonymizer, from which the events processed according to privacy policies are published. From the other direction, events received in the CTI agent from other agents will be prepared and published to the MQTT broker by the CTI Agent Connector. The IDS will be able to use that information to improve its detection capabilities, for instance by including rules in its detection engine that cover the newly discovered events. Another component whose interaction with the CTI Agent brings important security gains is the MUD Management module. One key element that may be shared through CTI are events that convey the publication of new mitigations, particularly new Threat MUD files, by manufacturers or security teams. Thus, the MUD Management module can retrieve them, translate them into a Medium-Level Security Policy Language (MSPL) object that is shared through the MQTT broker so that mitigations can be applied by the ERATOSTHENES components.

7.4.3 CTI Sharing Agent Components

7.4.3.1 CTI Agent Connector

This component handles communication with other components of the TMB by subscribing to the broker's threat sharing MQTT topic. The CTI Agent Connector receives threat alerts coming from the Monitoring IDS component. It also retrieves events from the MISP instance for later forwarding them to TMB components through the MQTT broker. Lastly, it governs the authorization of sharing processes with CTI Sharing Agents from other domains, relying on the project's identity management solution (e.g. authentication through DIDs).

7.4.3.2 Anonymizer

Receives a threat-related event coming from the CTI Agent Connector and applies anonymization techniques that are specified in the privacy policy file related to that type of event. After the anonymization process the resultant event is published on the MISP domain's instance, and additionally, the DLT is used for auditability and signalling of this publication process. The techniques implemented in this component are generalization, suppression, k-anonymity, l-diversity, and noise addition via Differential Privacy.

7.4.3.3 MISP

An instance of the MISP platform for publishing and sharing security events. It acts as the repository of threat events received. Its synchronization capabilities are useful to keep instances within a domain synchronized (i.e. from the multiple instantiations of the distributed TMB). What is more, it can be synchronized with external MISP instances, such as those of manufacturers or public CSIRTs/CERTs, so that the database of threats reaches relevant people in the security sector and improves the security of the overall ecosystem.

8 Deployment strategies in the projects with examples of the pilots

8.1 Introduction

The ERATOSTHENES and CERTIFY solutions are of interest in many scenarios where heterogeneous IoT devices play a key role. The various technologies and procedures for managing devices' lifecycles in such scenarios have been displayed through piloting activities in several scenarios in both projects. In this clause, this present document provides examples of such scenarios and the deployment strategies in the fields of Intelligent Transport Systems, Smart Health, Industry 4.0 scenarios and next generation Aircraft Systems.

8.2 Example 1: Connected Vehicles

The number of connected devices in the automotive industry has grown over the years, and this increase comes along with the evolution of the HW and SW that is integrated into vehicles and infrastructures. Over the last years, the electronic architecture of vehicles has been continuously developed to adapt to the new requirements of the users. Modern vehicles can interact with other connected devices to retrieve information about other vehicles or infrastructures (e.g. vehicles, smart traffic lights, smart speed signs) to make driving more comfortable and advise for the best possible decision while supporting smart-city and smart-connectivity trends.

These short-range interactions with other vehicles or infrastructure are not the only benefits those modern vehicles can provide to the users. Also, software updates can be executed remotely, eliminating the need to bring the vehicle to the manufacturer facilities, allowing the improvement of the software installed in the ECUs integrated in the vehicles. However, this progress is also accompanied by concerns of the automotive industry about possible cyber threats and the safety reduction of pedestrians or drivers. This connection can be exploited by cyber criminals to carry out attacks remotely, modifying the vehicle behaviour or hindering its function. The 155 [i.15] and 156 [i.16] UN Regulations are proof of this worry, standardizing cybersecurity, and a software update process that the manufacturers should follow on their products.

For this situation, this present document presents a scenario (Pilot 1) for the interaction of the vehicle with the infrastructure devices, where a vehicle will be the victim of attacks. This illustrates the deployment methodology followed in a highly distributed scenario, as well as the way in which the technologies developed during the ERATOSTHENES project can detect bad behaviours in the network, identify the potential malicious actors and finally, be able to deal with a cyber-attack.

This scenario takes advantage of the solutions ERATOSTHENES provides in fields such as decentralized identity management and device monitoring. Pilot 1 makes use of Physically Unclonable Functions (PUF) to generate uniquely identifying hardware fingerprints, which are then handled by the SSI agent to manage enrolment and identification. The SSI solution is then used to ensure that participants are authorized to perform actions, such as traffic lights sending updates that affect vehicles' driving decisions. The TMB plays a significant role in the deployment by analysing vehicle behaviour, maintaining a trust database for all vehicles and performing monitoring actions to detect potential threats and attacks. Within the TMB, the CTI Sharing Agent is used to record threat events reported in the network and to share anonymized CTI with CERT/CSIRTs of the automotive industry. MUD files are leveraged to apply security configurations and react against threats through mitigations such as critical software updates developed by manufacturers, with file integrity checks performed to protect against tampering attacks. The DLT acts as a backbone for the trustworthiness and identity data, as it maintains an immutable record of the network/individual device's state, which can then be used to support device recovery.

Vehicles are fitted with an IDAPT to be able to interact with the network, while the infrastructure (smart traffic light) is fitted with Raspberry Pi devices. To support complex and innovative projects, extend testing capabilities, and bridge the gap between them, Applus+ IDIADA has developed a vehicle On-Board Unit (OBU), which can be used independently or integrated into a vehicle's electronic architecture. IDAPT (IDIADA ADAS Platform Tool) is a multi-purpose, flexible prototyping/development tool for Connected and Automated Vehicle (CAV) activities. This tool encompasses several individual CAV components into one single unit with one single power supply, allowing easy installation and removal from a vehicle.

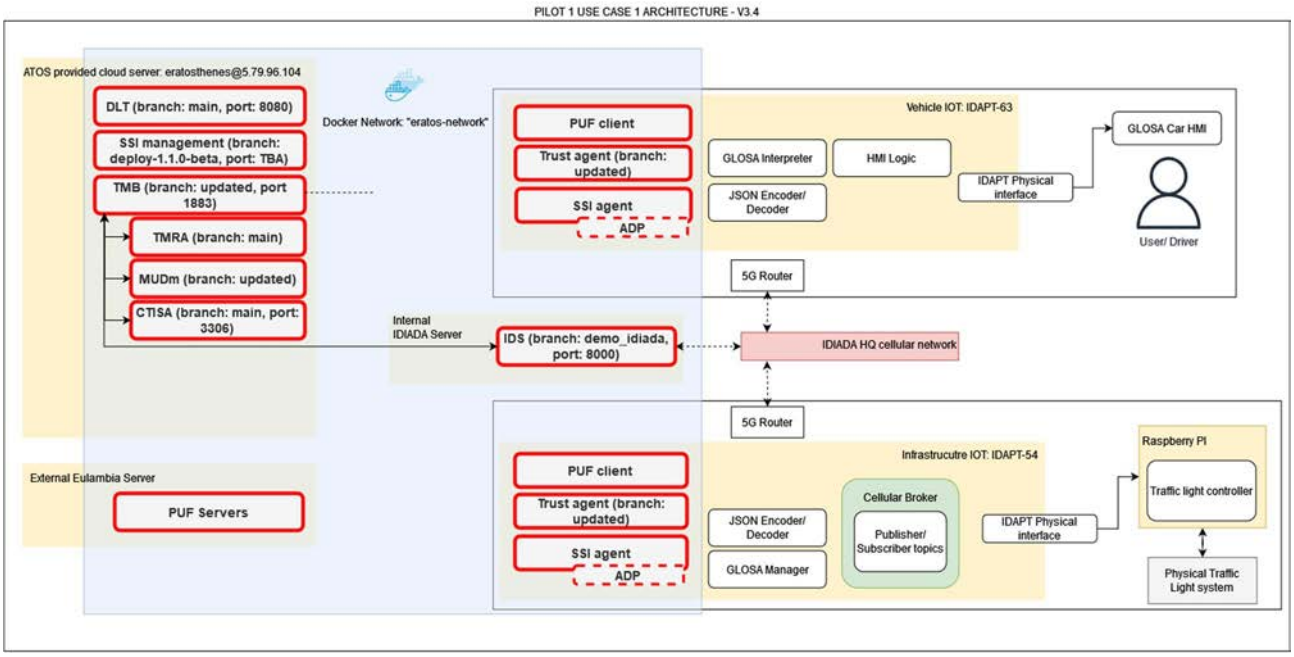

Figure 11: Pilot 1 deployment instantiation

The first use case is focused on the communication between the vehicle and its exterior devices on the road. This present document considers two types of communications for this case: a) Vehicle-to-Infrastructure (V2I) and b) Vehicle-to-Vehicle (V2V), covering both scenarios that can be carried out in a situation where the vehicles and the infrastructure can be connected to each other.

The exact scenario uses a vehicle that communicates through an OBU with a smart traffic light. The vehicle will act according to the inputs that it receives from this infrastructure device. Green Light Optimized Speed Advisory (GLOSA) is an example used in such situations where the vehicle would adapt its speed depending on the state of the cycle the traffic light is in. A second vehicle fitted with an OBU is also present. The aim of this additional vehicle, and the third actor in the scenario, is to send conflicting/malicious messages to the first vehicle, trying to destabilize the previous established communication between the first vehicle and the infrastructure (smart traffic light).

The second use case faces one of the most challenging and newest worries of the automotive world, which is the remote software updates. A server is set up to be able to send and receive messages. This packet exchange is done with a vehicle in the test field fitted with an OBU (able to communicate with the server). The intention of this communication is to simulate that one of the ECUs placed in this specific vehicle needs to update its software, and instead of going to the manufacturer's facilities to update it manually, the code will be downloaded from the cloud and installed autonomously.

8.3 Example 2: Smart Health

Tellu is an IoT application provider in the eHealth market with an Edge-based SaaS for remote patient monitoring and assistance product. The Tellu Health Gateway, which is deployed in every patient's home, is at the core of the service and is responsible for collecting data from various medical sensors and sending them to the back-end cloud services. The services analyse the data and record them in the patient's electronic health journal. Abnormal situations, such as fell-down and abrupt increase of blood pressure, are notified to the healthcare team. The gateway also hosts logics for pre-processing the raw data, to:

(i) limit data exchange between the gateway and the Cloud with the aim of preserving bandwidth;

(ii) increase security and privacy; and

(iii) ensure continuity of service even in case of no Internet connection.

Driven by the market trends, Tellu is aiming at transforming their product from a closed remote patient monitoring service to an open platform for home assistance, with two major extensions:

1) The healthcare gateways will be able to collect data from not only the standard IoT devices distributed by Tellu, but also the patient's own devices;

2) Third-party developers will be able to provide value-added services on top of the Tellu platform, integrating and utilizing the sensor data and the standard Tellu services in innovative ways.

Tellu will transfer to a platform provider and build an ecosystem around its Edge platform.

Pilot 2 is focused on the Remote Patient Monitoring system used by Tellu to facilitate remote assistance to follow up on patients suffering from chronic diseases such as diabetes, COPD or Covid-19, allowing patients to stay home during treatment, care, and foster self-care. It includes a Personal Health Gateway, which is deployed in every patient's home that is responsible for collecting data from various medical sensors and sending them to the back-end Cloud services. The services provide data to health personnel, allowing remote patient monitoring. Data is recorded in the patient's electronic health journal and normalized according to standard eHealth ontologies to allow performing various analysis. The objective of the pilot is to demonstrate secure enrolment, identity management, and trust monitoring of critical zero-touch devices.

Use Case 1 is aimed at the trusted and secure onboarding of PHGs on the Tellu system. This achievement is realized through the integration of three key technologies developed in the ERATOSTHENES project: Physically Unclonable Function (PUF), Self-Sovereign Identity (SSI), and Distributed Ledger Technology (DLT).

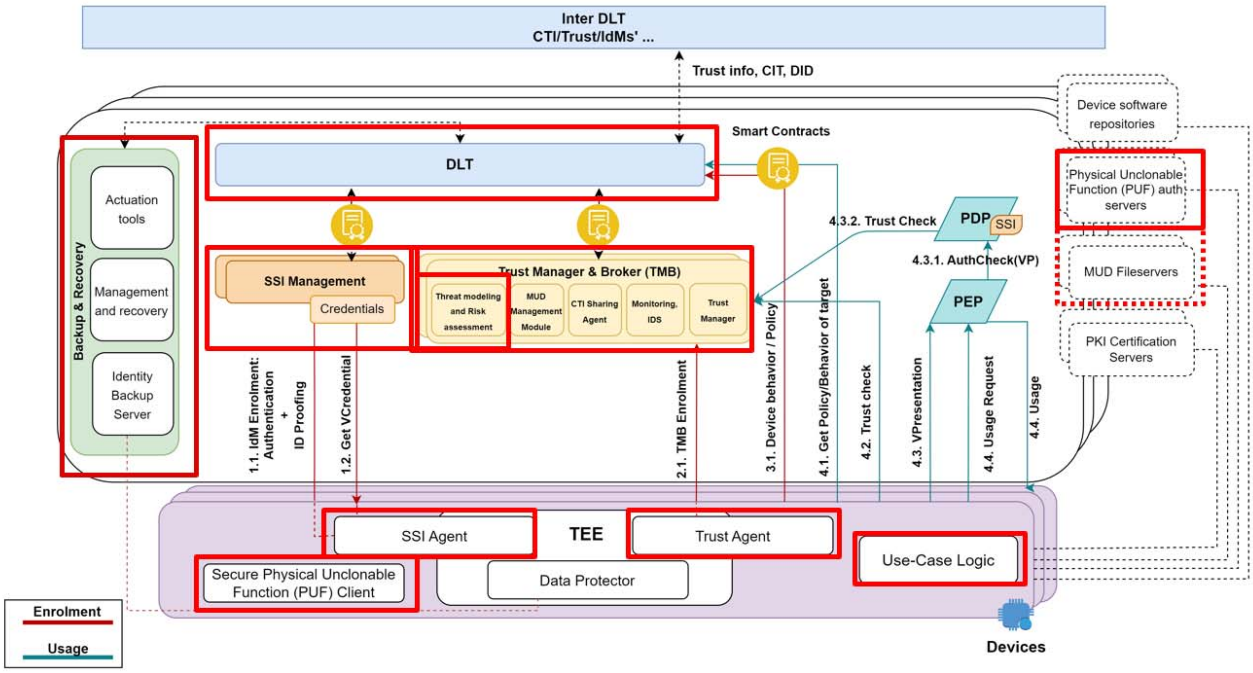

Figure 12: Key ERATOSTHENES components in pilot 2

Use case 2 is about the trust management of devices and services and is building on Use Case 1. The main device is the Personal Health Gateway (PHG), which manages a set of medical sensors attached to it. The PHG is responsible for sending the patient's medical data over the gateway to the Tellu backend service. The PHG can be compromised and exploited to send fake data, so the device should be continuously monitored to ensure that data from the gateway can be trusted.

This pilot saw the deployment of the ERATOSTHENES components through a containerized setup on both the Personal Health Gateway (IoT layer) and the cloud server. A Raspberry Pi 3 with a Debian image (version 11) is installed as the gateway - all client-side components are deployed on the Raspberry Pi, together with an MQTT client capable of sending data to the server. The deployment server is launched on an Ubuntu-based Virtual Machine (VM) on AWS.

8.4 Example 3: Industry 4.0

Digital Worx (DWG) is a provider for Industry 4.0 solutions with a focus on integration IoT into customized shop floor and productivity systems. DWG provides solutions for retrofitting sensor and cloud interfaces in machining, tracking production assets, and mobile solutions to optimize human workflows in industrial productions. The solutions operate in high security sensitive areas such as industrial automotive production, where connected systems, assets, and communication should be protected from malicious attacks or failures to prevent production downtimes. Thus, process related industry and production have a strong incentive to avoid downtimes. With Industry 4.0 reliability and security of manufacturing in such industry has become more complex. Industry 4.0 offers new opportunities for optimizing production but as well is increasing the attack surface of production systems. Ransomware infiltrated by PC workplaces has become a common threat for production systems. DWG is aiming to increase security by design in industrial IoT network and communication by introducing novel approaches on IoT Asset Identification and the use of disposable IDs to identify trustworthy entities in communication networks. The system should implement a level of trust and resilience in industrial communication networks to prevent, defend and isolate malicious attackers hiding or faking their true identities.

Currently, string-based static identifiers are used for IoT asset management and authorization. Identifiers are shared between communication parties in the network, processed and stored in sub-systems of the manufacturing process, operating apps, and vendor databases. The sharing and usage of identifiers cannot be effectively supervised in such complex environments. Thanks to the ERATOSTHENES solution, the PUF-based authentication will allow univocal authentication of devices throughout their lifetime, while the identity framework will enable the use of disposable identities specific for scopes, contexts, and time limits, allowing fine-grained authorization and access control. This will allow operators and devices to carry out the processes required on a shopfloor, like sharing machines' sensor data to perform analysis and maintenance. The strong authentication mechanisms will reduce potential attacks on the system through, e.g. data poisoning, by means of forgeries or impersonations. The identity system will be complemented by reputation and trust management and intrusion detection and protection mechanisms, improving the security of the system to reduce and mitigate cyber-attacks that jeopardize the factory's well-functioning.

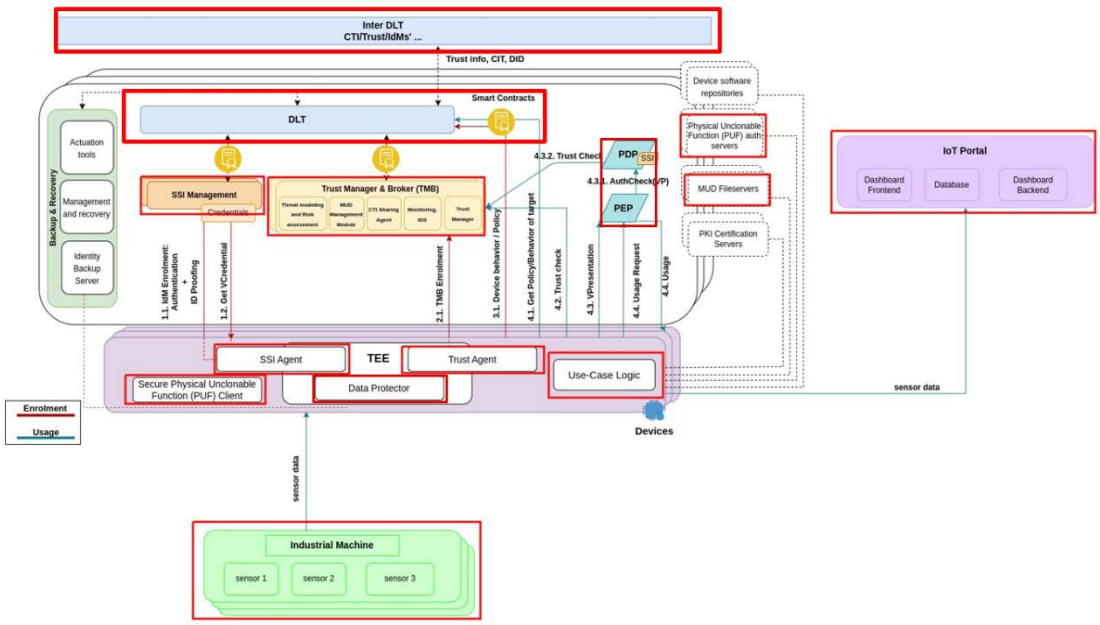

Figure 13: Key ERATOSTHENES components in pilot 3

Pilot 3 aims to solve and assess identification problems in industrial IoT setups. In the first use case, a PUF-based solution is developed to generate hardware fingerprints for assets. PUF makes use of micro variations that occur during the semiconductor manufacturing process. A service-oriented solution is developed to identify and register assets using secure disposal ID. IDs are created based on state-of-the-art cryptographic algorithms.

In use case 2, a ledger ID is implemented as a distributed service on the industrial edge. The service helps to carry out operations using an Application Programming Interface (API) exposed by an application. The tasks of the service range from generating disposal IDs to store them in a distributed ledger. The ledger facilitates authorized access using Access Control Lists (ACL) managed by a smart contract.

Use case 3 concerns itself with trust and permission systems through disposal identifiers. The use case is well suited for an industrial customer who employs several types of IoT devices and wants to create another layer of protection. A disposal ID is multi-faceted, empowered by processes, data, and communication links. Each aspect of a disposal ID is controlled by a smart contract. The trust and permission service API provides a mechanism to exchange information. It regularly checks the validity of the disposal ID and its cryptographic keys. An asset is deregistered in a suspicious event or if it is under attack, by revoking its disposal ID. It ensures that a malicious actor does not affect other assets of a critical network.

Use case 4 is about open-sourcing the disposal ID solution. It needs to be integrated with every modern IoT solution in its final form. Therefore, making it open source will encourage IoT developers to adopt and standardize it. Use case 5 employs distributed and decentralized technologies for asset identification. The solution is scalable by design since it incorporates distributed technologies. The overall concept, architecture and application services are tested and approved in an industrial IoT testbed, embedding industrial manufacturing sites.

The physical deployment uses a Raspberry Pi Model 4B1 for the client-side deployment, whereas the server-side components are deployed on a private server hosted by DWG on their premise. The server is based on Linux® Container (LXC) technology and maintained by Proxmox.

NOTE: Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

8.5 Example 4: Connected Cabin System

Next-generation aircraft are expected to use many IoT-connected devices supporting new and improved services in the cabin.

The shift promises:

i) personalized experience for passengers, e.g. through customized In-Flight-Entertainment (IFE);

ii) new revenue streams for airlines, such as delivering targeted retail offers; and

iii) smarter operations like Prognostics and Health Management (PHM) applications through a detailed view on the evolving status based on the connected sensors.

This will lead to a high volume of data GBs up to TBs per second and by the heterogeneity of devices. Devices will be connected through wired (e.g. the Ethernet-based AFDX-ARINC 664, CAN bus, ARINC429) or wireless technologies (e.g. IEEE 802.11 [i.51], ECMA-368 [i.52], IEEE 802.15.3 [i.53]). The heterogeneity is also manifested in the different computational capabilities to host services.

Although these cabin systems are classed as non-essential to flight safety, they still fall under aviation airworthiness guidance, certifications and regulations (e.g. from RTCA, EUROCAE [i.41], FAA [i.42] and EASA [i.43]) such as the AC 20-168 [i.17] and the RTCA DO-313 [i.18]. These require verification of the security of the wired and wireless systems preventing any unintended change to the systems during operations. Hardware, software, network traffic, and data all require scrutiny, especially when Commercial Off-The-Shelf (COTS) components are integrated and alternative test methods are needed. All in all, there is a clear need to protect these devices throughout their lifecycle and generate appropriate evidence.

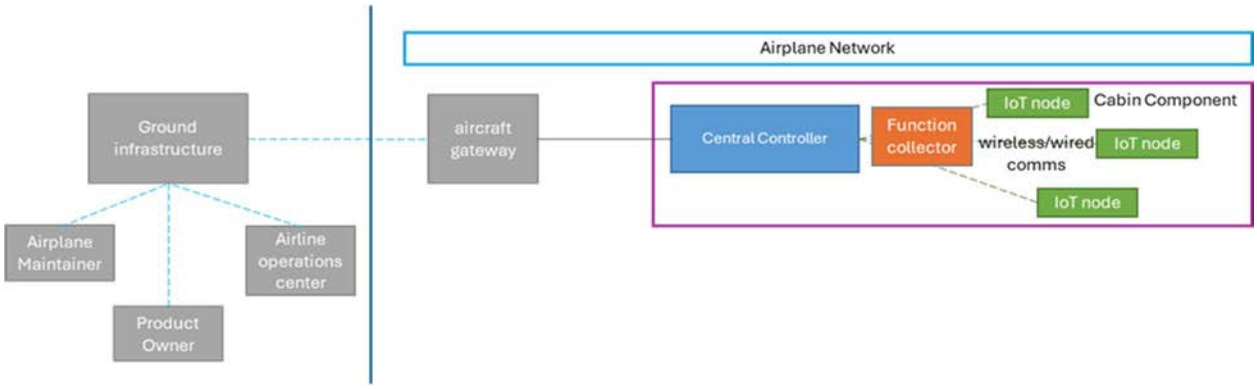

Figure 14: High-level block diagram of the CERTIFY use case for the connected cabin system

As shown in Figure 14, CERTIFY use case considers an environment constituted by IoT devices deployed in the connected cabin and infrastructural remote services hosted by the component and system manufacturer, and the airline.

In the cabin, the devices will belong to two classes:

i) IoT node devices having a small footprint in terms of "Size, Weight, Power and Cost" (low-SWaP-C); and

ii) high-end embedded central controller devices able to host more complex software services and manage entire functionalities in the cabin.

In the pilot, these devices have been instantiated by a custom RISC-V based node and an off-the-shelf high-end embedded board based on the ARM instruction set, respectively. Additionally, an aircraft gateway oversees the communications to/from the aircraft. This heterogeneous architecture requires a trade-off analysis on the cybersecurity services and functionalities of the CERTIFY framework that can be deployed.

The pilot is divided in three different scenarios covering multiple stages of the lifecycle:

Scenario 1 - Installation of a new component. A new component needs to be installed in the cabin. This could exemplify the adoption of a new smart component (e.g. a smart coffee machine). The process should be carried out without compromising the cybersecurity posture of the system. Thus, it will include secure bootstrapping, initial update, and customization for the specific deployment environment by considering the security configuration defined by the product owner/manufacturer during evaluation for the original certification. Moreover, if the new component is a replacement for a previously installed one, secure decommissioning, including reset and wipe out of any sensitive data, should be performed by the maintenance operator.

Scenario 2 - Operations and monitoring. Data is periodically collected in the cabin with a frequency that is dependent on application and services, e.g. for monitoring, optimization, and preventive maintenance. Additionally, passengers' devices and the usage of a wireless network generate a wider attack surface. External infrastructures may also upload data for onboard connectivity experience and In-Flight Entertainment (IFE) services, and the product owner may also need the availability of a remote connectivity to perform device reconfigurations. An environment that requires such operations demands vulnerability management and anomaly detection throughout the entire operational phase.

Scenario 3 - Replacement and repurposing. When a cabin system component fails, a compatible replacement Line-Replaceable Unit (LRU) could be repurposed for the specific target system to minimize downtime. Airline, maintainer, product owner, and maintenance operator are all involved to manage different steps of the process. It is important to check that the device has all the characteristics needed to be repurposed before using it. Indeed, the new deployment may require different capabilities to host services and security features. Therefore, the new usage should be among the ones foreseen and certified by the manufacturer so that proper reconfiguration can be implemented.

9 Gap Analysis and Recommendations

9.1 Introduction

The rapid growth of the IoT has drastically increased the number of connected devices, bringing significant security and privacy challenges across various industries. As these devices become deeply integrated into critical systems and everyday life, their vulnerabilities can have widespread consequences. To address these risks, the European Union's Cyber Resilience Act (CRA) introduces strict requirements to establish a cybersecurity baseline for IoT products throughout their entire lifecycle. By placing responsibility on manufacturers to secure devices throughout their entire lifecycle, the CRA seeks to ensure that devices are secure by design, fit for purpose, and protected against emerging threats. Additionally, cyber incidents and cyber-threat intelligence should be shared across ecosystems, aiming for a widespread improvement on the security of solutions and the achievement of a collaborative cyber-shield. To achieve this, the CRA sets out to:

- Facilitate the secure development of digital products and their components;
- Define cybersecurity rules for placing products on the market;
- Define requirements for the design, development, and production of products;
- Define requirements for the processes for handling vulnerabilities;
- Establish rules on market surveillance and enforcement;
- Establish different proof of conformity processes (self-declaration, third-party assessment, etc.) depending on the category the products fall in.

The CRA's scope and impact on IoT devices makes it truly relevant to ERATOSTHENES and CERTIFY and the contents discussed in the present document. Lifecycle management, threat detection, sharing and mitigation techniques, secure identification, timely security updates, to name a few, are all relevant to the goals of the regulation. In the following, this present document overviews desirable properties from such security standards and regulations that are challenging to achieve and provide recommendations through the solutions developed in the two projects and the experience obtained in the piloting activities.

Apart from the mentioned standards and regulations, the contents in this clause are relevant to, and will be related to, several CRA-aligned standards still in development, such as:

- ETSI EN 304 632 [i.54], which will provide security requirements and assessment criteria covering elements defined in CRA Annex I for smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems.
- ETSI EN 304 633 [i.55], which will provide security requirements and assessment criteria covering elements defined in CRA Annex I for Internet connected toys covered by Directive 2009/48/EC [i.56] that have social interactive features (e.g. speaking or filming) or that have location tracking features.
- ETSI EN 304 634 [i.57], which will provide security requirements and assessment criteria covering elements defined in CRA Annex I for personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 [i.58] or Regulation (EU) 2017/746 [i.59] do not apply or personal wearable products that are intended for the use by and for children.

9.2 Desirable properties in standards, regulations and best practices

9.2.0 Introduction

There exist several desirable properties that are discussed in relevant IoT standards, regulations and best practices documents, and particularly the CRA. Achieving these principles presents challenges derived from the inherent requirements of such properties and the characteristics of IoT environments such as heterogeneity of devices, large numbers of participants or hardware constraints. In this clause, the present document gives an overview of some of these relevant properties, their relationship to standards, and recommendations on how it could be possible to tackle them coming from the solutions of ERATOSTHENES and CERTIFY.

9.2.1 Security by Design

Security by design approaches aim to make cybersecurity a primary perspective in the design, development, and production of products, in contrast to the addition of security characteristics at later stages. The CRA aims to apply this notion to products with digital elements. This sentiment is also reflected in multiple requirements established in relevant standards, from basic security requirements for any device to the provisions of risk assessment, secure development or safety features for the products. These are summarized in the following table.

Requirements	Standards and regulations
Basic security requirements	CRA, ETSI EN 303 645 [i.19], EUCS [i.21]
Securely store sensitive security parameters	ETSI EN 303 645 [i.19] (Provision 5.4-1) + RED [i.22] + CRA (I.1-3c I.1-3d), IoT security codes Australia [i.44], ENISA Good practices for IoT devices [i.23]
Comprehensive Cybersecurity Risk Assessment	CRA (10-2. I.1-3h I.1-3i), CRA (I.1-1)
The product should be built with effectively implemented safety features	EUCS
Facilitate the secure development of products with digital elements and their components	CRA

To address this, CERTIFY introduces the automation tool CyberPass, which streamlines the conformity assessment process based on ETSI EN 303 645 [i.19]. This standard was highlighted by the CRA Requirements Standards Mapping study conducted by ENISA and the European Commission's Joint Research Centre since it maps to most of the CRA essential requirements. The tool provides a model-based evaluation and certification approach, allowing security to be tested from the early design stages and supporting automation of the conformity assessment process to ensure scalability.

9.2.2 Identity Generation and Management

To achieve cybersecurity notions such as confidentiality, integrity and authenticity it is paramount to establish robust identity management mechanisms. The CRA and other IoT security regulations highlight the needs for strong access control mechanisms that ultimately should also be based on authentication and identity management solutions:

Requirements	Standards and regulations
Tamper-Resistant Implementation of Unique Device Identity	ETSI EN 303 645 [i.19] (Provision 5.4-2) + RED + PSTI (C3.6) [i.24]
Unique device identification	NISTIR 8259 [i.26], CRA
Identity Validation for Secure Access Authorization	RED + CRA (I.1-3b, I.2d)
Implement Key management and authentication mechanisms	ENISA and IETF good practices for IoT DEVICES [i.23], [i.27], SESIP [i.28]

To **address** this, ERATOSTHENES sets up the device with identity material during the development phase, based on strong root identity material such as Physical Unclonable Functions (PUF). During deployment, the identity of the device is checked, and the identity material for the security domain is generated. The result of this process is the creation of attribute-based identity material that is later used during operation for access control to resources and services, based on attribute-based policies that can be managed in a decentralized way or using traditional PEP/PDP approaches. Apart from the security obtained from the strong PUF root identity, sensitive material (such as keys) is always managed in the Trusted Execution Environment of the device, improving security through isolation.

9.2.3 Secure Deployment

The CRA emphasizes the importance of a Secure by Default Configuration, ensuring that products with digital elements are designed to be secure from the moment they are deployed, without requiring users to apply additional security measures. This means manufacturers should provide default settings that prioritize security, minimizing vulnerabilities and reducing the risk of cyber threats.

Requirements	Standards and regulations
Secure by Default Configuration	RED + CRA (I.1-3a)
Minimize exposed attack surfaces	ETSI EN 303 645 [i.19] (Provision 5.6-1) + RED + PSTI (C6.1)
Define cybersecurity rules for placing products on the market	CRA
Make installation and maintenance of devices easy	ETSI EN 303 645 [i.19] (Provision 5.12-1) + PSTI (C2.5)

To **address** this challenge, both CERTIFY and ERATOSTHENES on the extended MUD files generated during the design phase and continuously updated by the manufacturer. The MUD file is used to automatically reconfigure the device during deployment, and the enrolment process only finishes after the proper security controls are applied. Additionally, this process is linked to the strong identity management approach, ensuring the security of the MUD profile itself.

9.2.4 Vulnerability Handling

Part of the CRA essential requirements insist on processes and not only on products: they call for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the product is expected to be in use. In particular, there should be clear processes and formal policies showing that the manufacturer can immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or recall the product, as appropriate. NIS2 Directive [i.1] also promotes cooperation and information exchange among EU Member States to prevent and respond to cybersecurity incidents.

Requirements	Standards and regulations
Implement a means to manage reports of vulnerabilities	ETSI EN 303 645 [i.19]
Transparent Vulnerability Disclosure Policy	ETSI EN 303 645 [i.19] (Provision 5.2-1) + CRA (I.2-5) +PSTI (C4.1) + EUCS + NIS2 (e.g. 18, 26)
Timely Response to Disclosed Vulnerabilities	ETSI EN 303 645 [i.19] (Provision 5.2-2) + CRA (I.2-2 10-6.)
Continuous Monitoring and Remediation of Security Vulnerabilities	ETSI EN 303 645 [i.19] (Provision 5.2-3) + CRA (I.2-1 10-4. 10-6. 10-12.) PSTI (C4.2 C4.4 C4.5 C4.6), ENISA baseline requirements for IoT
Protecting sensitive data	NIS2 (121)

To **address** this challenge, both CERTIFY and ERATOSTHENES apply a multi-technology approach where sharing of cyber-threat information is the cornerstone. Particularly, both projects rely on a privacy-preserving CTI sharing component for the anonymized sharing of security alerts, applying data mining and privacy enhancing technologies (Suppression, Generalization, K-Anonymity) to the sensitive attributes in the alerts. External threat alerts and mitigation strategies can be recovered through the same means as a source of information for the security domain. This process is supported by DLT (instantiated as blockchain), that act as a secure and decentralized source for public information storage and IoT event verification. Lastly, the extended MUD, and particularly the Threat MUDs, are used to share mitigations associated with vulnerabilities, which are applied automatically in the security domains, for instance triggering a software update that patches the vulnerability.

9.2.5 Continuous Assessment

Even if a device is certified as secure, new threats and vulnerabilities may still emerge over time, potentially compromising its security and invalidating the certificate. The time required for certification can be reduced if detailed and up-to-date information from the manufacturer is available, allowing for a more efficient recertification process when new vulnerabilities arise. CRA requires organizations to maintain a proactive approach to emerging threats, making it crucial to have verifiable documentation and evidence to support the security of devices throughout their lifecycle.

Requirements	Standards and regulations
Security Anomaly Examination for Telemetry Data	ETSI EN 303 645 [i.19] (Provision 5.10-1) + PSTI (7.6), IoT security codes Australia
Continuous Conformity Assessment Procedure	CRA (10-7.)
Proactive Consideration of Changes in Device Conformity	CRA (10-9.)

To **address** this, the CERTIFY methodology includes collection, identification, and decision coupled with its real-time monitoring capabilities (e.g. SIEM-SOAR, IDS, runtime attestation, MUD). Security events are securely stored in the Inventory and Registry component. This allows for the identification and handling of any anomalous behaviour while placing its user in a better spot to comply with cybersecurity regulations. ERATOSTHENES follows a zero-trust architecture where trustworthiness of devices is continuously evaluated and taken into account for security decisions. The process includes real-time monitoring, threat modelling and risk assessment based on digital twins that are updated according to events happening in the domain. This results in the dynamic assessment of devices' conformance to the security profiles specified through MUD files and trustworthiness, which are reflected in the digital twin models and persisted in the DLT in an auditable way.

9.2.6 Secure Update

The CRA places significant emphasis on software upgrading to ensure the long-term security of products with digital elements. It mandates that manufacturers provide regular security updates to address vulnerabilities, ensuring that devices remain protected against emerging cyber threats. Updates should be delivered in a timely and reliable manner and installed with minimal user intervention.

Requirements	Standards and regulations
Keep software updated	ETSI EN 303 645 [i.19]
Ensure software integrity	ETSI EN 303 645 [i.19] (Provision 5.3-9 Provision 5.3-10) + RED + CRA (I.2-7) + PSTI (C5.2), ENISA and IETF good practices for IoT [i.23], [i.27]
Timely Delivery of Security Updates	CRA (I.1-3k I.2-2 I.2-7), PSTI (C5.11), IoT security codes Australia
Automated SW updates	ETSI EN 303 645 [i.19] (Provision 5.3-4) + RED + CRA (I.1-3k) + PSTI (C5.5), IoT security codes Australia
Periodic Security Update Checks	ETSI EN 303 645 [i.19] (Provision 5.3-5) + PSTI (C5.5)

To **address** this challenge, both projects provide secure device registration based on credentials created after the pre-provisioning process. Along this process, and throughout the operation of the device, a software update process may be automatically triggered because of the availability of a new version or directly enforced as a mitigation (extended MUD) that involves an upgrade to remove a vulnerability. The process will then consist of the recovery of images from a software repository, their automated deployment through the use of digital twins, and the secure installation, including integrity checks.

9.2.7 Repurposing and Decommissioning

As cybersecurity threats evolve, devices may require updates, reconfigurations, or upgrades to maintain security standards. However, some changes might exceed the device's capabilities, such as requiring more storage than available or hardware modifications beyond its design. When a device can no longer meet security requirements, it can either be repurposed for a different use case with lower security demands or decommissioned if no viable reuse is possible.

Requirements	Standards and regulations
Use secure data removal techniques	ETSI EN 303 645 [i.19]/ ETSI TS 103 645 [i.29]/ETSI TS 103 701 [i.30]
Secure Equipment Disposal and Replacement	RED
Orderly decommissioning	IoTSF Security Assurance Framework [i.31]
Make installation and maintenance of devices easy	ETSI EN 303 645 [i.19] (Provision 5.12-1) + PSTI (C2.5)

For repurposing, CERTIFY ensures that when a device is repurposed, it is securely reconfigured to meet its new environment's security needs through the application of security profiles in the MUD file. For decommissioning, CERTIFY and ERATOSTHENES enforce strict data erasure policies, ensuring that all stored information, including digital certificates, DIDs, and encryption keys, is completely removed.

9.3 CRA in ERATOSTHENES and CERTIFY pilots

9.3.0 Introduction

Clause 9.3 develops further the applicability of ERATOSTHENES, CERTIFY and their pilots as a reference for the CRA. As the CRA recently came into force and its obligations are still further away in the future, even though the text is stable, many aspects will be delegated to implementing acts. Thus, the analysis presented herein might need to be revised when the details and the actual application of the CRA will occur after a transition period. In addition, this present document is dealing with research projects, and it does not claim to perform any conformance test, nor does it plan to undergo a certification process within the context of this exercise. The complex issue of conformity assessment of such solutions remains a gap in the regulatory context.

Thus, this present document discusses here one pilot - and its use cases or scenarios - per project in the context of the CRA to bring a better understanding of their impact being developed in close alignment with the reality of the industry, the law, and its evolution, to facilitate the adherence to such regulatory context. The components, architectures and frameworks developed in ERATOSTHENES and CERTIFY can be a step toward alignment with the CRA and its implementation, and particularly for the core roles covered by lifecycle management and information sharing.

9.3.1 ERATOSTHENES illustrative use case

To illustrate the implications of the CRA in the project, this present document uses the Intelligent Transport System pilot as a reference. The CRA is a very horizontal piece of legislation with common cybersecurity requirements for all products, regardless of sector or field of application. Most of the devices involved in the pilot would fall under the CRA scope (e.g. IoT nodes, OBUs and roadside units, gateways, etc.). Indeed, Article 2 of the CRA text [i.3] says that the regulation applies to products with digital elements made available on the market, which includes a direct or indirect logical or physical data connection to a device or network.

The CRA aims to embed cybersecurity as a fundamental consideration in the design, development, and production of products with digital components. As emphasized in various policy discussions, its successful implementation would ensure a security-by-design approach for all manufacturers selling products in the EU market. This goal can be achieved by enforcing essential cybersecurity requirements and ensuring that products are free from known vulnerabilities before reaching consumers. The first scenario in the pilot starts with the secure bootstrapping and enrolment of the devices involved in Vehicle-to-Everything (V2X) communication into a security domain. Similar to the essential requirements of the CRA, the certifications and security assets introduced during manufacturing will be key during this process and serve as a root of trust for the process. Additionally, the scenario focuses on the operation and monitoring of such devices in a secure way, leaning on the results of such enrolment. This relates to several pillars and topics within the CRA, but especially on the provisions about lifecycle and vulnerability management. If, for instance, a rogue device injects false traffic control data in aims of performing harmful actions to the connected vehicles, the ERATOSTHENES framework, particularly as part of the TMB's duties, will be able to detect it and inform about it in a privacy-preserving manner through the exchange of CTI. Of course, when a vulnerability is detected, one or more digital products within the systems might no longer be compliant with the CRA or at least be impacted by a "known exploited vulnerability". As the CRA requires market operators to act throughout the product's lifecycle, providing support, updates, or mitigation measures, the automated CTI sharing will be key in starting (and completing) such processes.

What is more, the scenario goes a step further, covering the vulnerability handling process. It considers the essential requirement established by the CRA on the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the product is expected to be in use. Once a vulnerability is identified, the manufacturer should take immediate action to address the issue. This may involve bringing the product or manufacturing processes into compliance or, if necessary, withdrawing or recalling the affected product. The ERATOSTHENES framework allows for not only the detection and notification of vulnerabilities, but also automated collection and application of mitigation measures, thanks to the application of CTI sharing techniques and the application of the extended MUDs. This enables the identification and handling of any anomalous behaviour while helping security domains comply with cybersecurity regulations.

The second scenario involves remote software updates in the automotive sector and is particularly one of the key potential outcomes of a vulnerability handling process. Again, the CRA is explicit in the obligation to support and update digital products, especially in the case of vulnerabilities. The ERATOSTHENES framework provides tools for addressing these processes, and particularly for the management of the lifecycle of the device in a secure manner, taking advantage of secure execution, monitoring, trust, and strong identity management. Particularly, as mentioned above, the usage of the extended MUD file emerges as a key solution for many of the challenges established. Each actor can collaboratively contribute, update, and provide a state of the security of the system.

The application of the MUD file (and its expressiveness extensions along with Threat MUDs as proposed in ERATOSTHENES and detailed in the present document) meets the spirit of many of the regulatory provisions contained in the CRA text. Such a tool would help with the dispatching of newly discovered vulnerabilities as well as their mitigation. The enforcement of the latest MUD file policies would support the creation of evidence of a secure state of the system, providing a basis to build on for notification and reporting purposes.

The legislation emphasizes that market operators should systematically document key cybersecurity aspects of products with digital elements, including any known vulnerabilities and relevant information from third parties. They are also required to update the cybersecurity risk assessment of their products as needed. Additionally, the CRA introduces detailed notification and reporting requirements for exploited vulnerabilities and major incidents, featuring new elements such as a Single Reporting Platform and a Single Point of Contact for manufacturers. The extended MUD file further strengthens collaboration among stakeholders, promoting a more cohesive approach to IoT security. These measures align with the need for cooperation among key entities involved in vulnerability management and incident response, such as Computer Security Incident Response Teams (CSIRTs), ENISA, and Single Points of Contact. Ideally, the extended MUD file could also serve as a foundation for conformance documentation, whether self-assessed or verified by a third party.

9.3.2 CERTIFY illustrative use case

To illustrate the implications of the CRA in the project, this present document uses the Intelligent Transport System pilot as a reference. In a similar vein to the previous clause, most of the devices involved in the pilot would fall under the CRA scope according to [i.20], Article 2 (e.g. IoT nodes, central controllers, aircraft gateway).

The CRA sets an ambitious goal: to embed cybersecurity as a fundamental consideration throughout the design, development, and production of products with digital elements. As emphasized in multiple policy discussions, its effective implementation would establish a security by design approach for all manufacturers placing products on the EU market. This could be achieved by making sure that several basic cybersecurity requirements are respected and that products made available do not have any known vulnerability. In the CERTIFY project, this objective is supported through CyberPass, an automation tool that streamlines conformity assessments based on ETSI EN 303 645 [i.19]. Notably, ETSI EN 303 645 [i.19] was highlighted in the CRA Requirements Standards Mapping study [i.45] by ENISA and the European Commission's Joint Research Centre for mapping closely with most of the CRA's essential requirements. The **first scenario** addressed here involves the secure bootstrapping and integration of a cabin component into a network. As with the CRA's essential requirements, a baseline set of security measures is pushed to the device to be able to join the network. CERTIFY then issues a certificate attesting to the component's secure state, facilitating further demonstration of regulatory compliance.

The **second scenario**, centred on operations and monitoring, is probably the most well-suited for a CRA pilot as it showcases several pillars and angles of the CRA, particularly regarding lifecycle and vulnerability management. If a rogue device were to inject false data or perform harmful actions inside the cabin, CERTIFY's monitoring plane would detect the anomaly. Once a vulnerability is flagged, any affected digital product might stop being compliant with the CRA, or at least be classified as having a "known exploited vulnerability." Under the CRA, market operators should take action in such cases, providing continuing product support, security updates, or mitigation measures throughout the product's entire lifecycle.

Furthermore, this scenario also highlights the CRA's process-oriented requirements, which require manufacturers to maintain robust vulnerability-handling procedures to ensure the cybersecurity of a product during its expected use. Policies and processes should show that manufacturers can act immediately: once a flaw is found, they should either fix the product or their own processes or, if necessary, withdraw or recall the product. The CERTIFY methodology includes collection, identification, and decision, and coupled with its real-time monitoring capabilities (e.g. SIEM-SOAR, IDS, runtime attestation, MUD), allows for the identification and handling of any anomalous behaviour while placing its user in a better spot to comply with cybersecurity regulations. These processes are enhanced through continuous collaboration through the projects' PP-CTI sharing mechanisms.

The **third scenario** focuses on the Line-Replaceable Units (LRUs) and further illustrates the CRA's clear mandate for ongoing support and updates of digital products. A peculiarity of this scenario is the possibility of repurposing a device within the network for a different function than originally intended. The CRA explicitly requires manufacturers and operators to assess not only the intended use of a product with digital elements but also its "foreseeable use and misuse". Repurposing a component within a system is therefore a perfect test-based scenario to assess the emergence of new intended uses. Operators should adopt a risk-based approach to continuously evaluate such changes to ensure they do not introduce harmful or unforeseen consequences. This proactive assessment aligns directly with the CRA's lifecycle and risk management obligations.

Figure 15 represents a visual summary of the link between the use case, the CRA and the CERTIFY project.

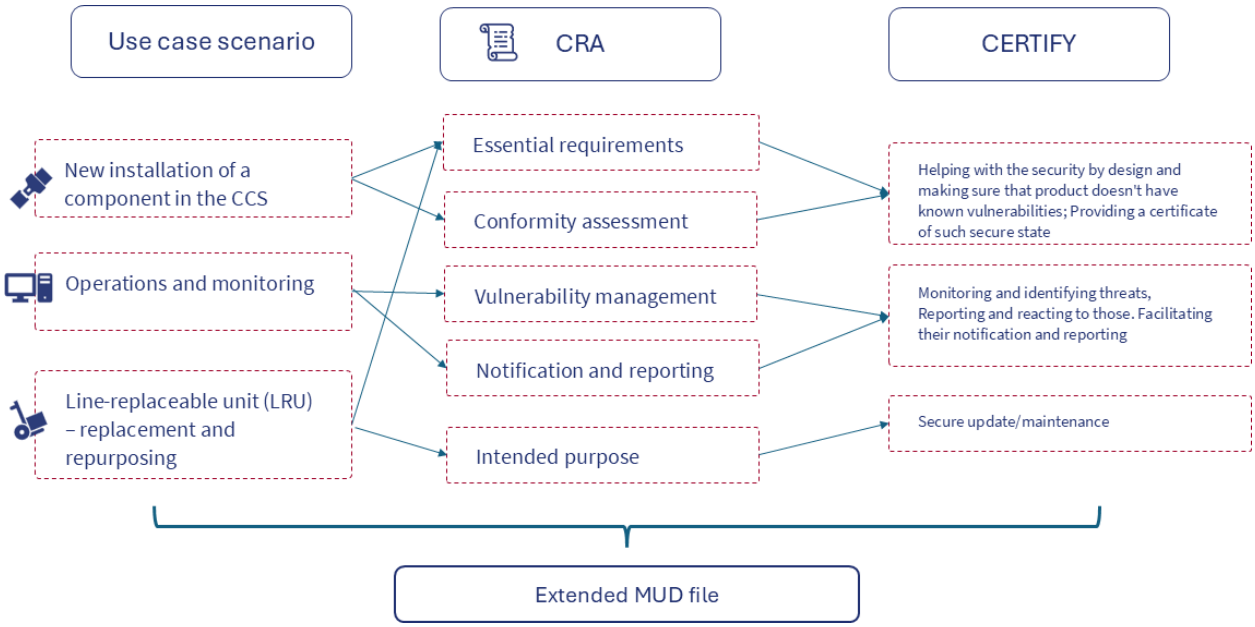

Figure 15: The CERTIFY cybersecurity lifecycle methodology and framework aligned with recent EU Regulation: the CRA example

History

Document history		
V1.1.1	October 2025	Publication