DOI: 10.1561/9781638285076.ch13

Chapter 13

Towards a Framework and Methodology Adherent to the EU Cyber Resilience Act – The CERTIFY Project (Extended Version)

By Sara Nieves Matheu Garcia, Stefano Sebastio, Matteo Molé, Roberto Cascella and Antonio Skarmeta

The rapid expansion of the Internet of Things (IoT) has led to a critical increase in the volume of connected devices, introducing significant security and privacy challenges across industries. As devices become embedded in essential systems and daily life, their inherent vulnerabilities can have far-reaching impacts. Addressing these risks, the European Union's Cyber Resilience Act (CRA) proposes rigorous requirements for establishing a baseline for the cybersecurity of IoT products through their entire lifecycle. The CERTIFY project offers a comprehensive framework that aligns with CRA's objectives, enabling IoT stakeholders to manage cybersecurity from initial design to decommissioning. The CERTIFY's lifecycle methodology encompasses phases such as secure design, bootstrapping, continuous monitoring, update management, and eventual decommissioning or repurposing. A key element of the CERTIFY's approach is the use of standardized security practices and tools, including the extended Manufacturer Usage Description (MUD) framework and advanced cryptographic solutions. These elements ensure that device behavior adheres to security policies and that updates are both transparent and traceable, facilitated by blockchain and other distributed ledger technologies. The CERTIFY architecture also enables real-time risk assessment, with dynamic threat detection

and rapid response to vulnerabilities, helping maintain a secure operational state. Through the deployment of active monitoring and security intelligence sharing, CERTIFY improves resilience against emerging cyber threats and promotes compliance with evolving regulations like the CRA. This chapter examines the CERTIFY's methodology and highlights its application through use cases, such as a connected cabin system, to illustrate the framework's effectiveness in addressing CRA regulatory and operational challenges. The CERTIFY project represents a proactive, holistic approach to IoT security, empowering stakeholders to respond to the demands of an interconnected world and establish lasting, lifecycle-oriented security for IoT ecosystems.

13.1 Introduction

Envisioned decades ago, ubiquitous computing [1] is now a consolidated reality, as digital products are no longer confined to business settings but are seamlessly integrated into consumer and critical application environments. Smart and Internet of Things (IoT) devices are not only embedded in homes and workplaces, but they also underpin essential functions across sectors like healthcare, transportation, and energy. Given the widespread role of these devices and the rapid development cycles focused on cost reduction, they have become prime targets for cyber threats. High-profile attacks—such as those affecting the Colonial Pipeline oil system [2], Marriott hotels [3], and major hospital systems in the United States [4]—are stark examples of the vulnerabilities that connected devices introduce when security practices are inadequate. These incidents underscore the need for robust regulatory frameworks and security protocols that protect devices and systems throughout their lifecycle.

In fact, cyber incidents were historically not disclosed unless they were causing major impacts to the public until the entry into force of recent regulations [5, 6] and [7]. From that point on an already galloping trend manifested more openly, also allowing the appearance of public reporting services (e.g., [8] and [9]). Cybercrime continues to grow, with global annual costs projected to exceed 15.63 trillion euros by 2029 [10]. In response to this alarming trend, the European Commission proposed the Cyber Resilience Act (CRA) [11] in September 2022, with the goal of strengthening cybersecurity and resilience across all products with digital components. 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.

In this context, the Horizon Europe CERTIFY project [12]—active security for connected device lifecycles—presents a cohesive approach to managing IoT device

security. The CERTIFY's mission is to provide a methodological, technological, and organizational framework that ensures security throughout the lifecycle of connected devices. The project's efforts align closely with current EU regulations, particularly the CRA, by developing and testing practical use cases that support regulatory objectives. This regulatory alignment is crucial, as it positions CERTIFY to not only demonstrate compliance but also to address real-world security challenges by fostering coherence with the evolving EU policy landscape.

The CERTIFY's methodology encompasses the entire lifecycle of a connected device, from its initial design and risk assessment to secure decommissioning or repurposing. The project's approach is based on the security by design principle, which incorporates security protocols and cryptographic controls at the outset. By embedding these measures during the design and development stages, CERTIFY ensures that devices are prepared to handle threats before deployment. Once a device is deployed, CERTIFY facilitates secure bootstrapping, continuous monitoring, and adaptive reconfiguration to maintain device integrity and security, even as new vulnerabilities emerge. This approach mitigates risks in real-time and minimizes the need for costly and complex retroactive measures.

A defining aspect of the CERTIFY's framework is its collaborative approach, allowing multiple stakeholders—such as auditors, manufacturers, and end-users—to contribute to a shared security ecosystem. The framework supports ongoing communication and feedback loops that improve risk assessment and response times. Through advanced technologies such as the extended Manufacturer Usage Description (MUD) [13] files and Zero Trust Architecture principles, CERTIFY provides stakeholders with a secure, and standardized method for managing device interactions and enforcing access controls. This integrated approach allows stakeholders to monitor, update, and reconfigure devices as needed, creating a flexible security model that adapts itself to changes in the threat landscape. Furthermore, the CERTIFY's architecture enables Distributed Ledger Technology (DLT), such as blockchain, which records every event, update, or configuration change related to the device, providing an immutable and transparent record that reinforces trust among users and regulatory bodies.

The project's engagement with policy and standardization activities throughout the EU demonstrates its commitment to regulatory alignment. The CERTIFY's consortium actively participates in discussions on cybersecurity regulations, ensuring that the project's solutions and use cases reflect current legal requirements and contribute valuable feedback to the regulatory process. This approach not only strengthens the project's alignment with EU policies but also enables sharing challenges linked to their practical roll out, for instance the broader industry's need for guidance on implementing the CRA's requirements in practical settings. The CERTIFY's use cases demonstrate a variety of scenarios, from connected cabins in

aviation to smart manufacturing systems and tracking of artworks, where high levels of connectivity and data sensitivity demand rigorous security practices. Each scenario illustrates how the CERTIFY's lifecycle management can support compliance and protect devices from real-world threats.

In this chapter, we delve into the CERTIFY project's lifecycle methodology and its alignment with the objectives of the CRA. Section 13.2 outlines the CERTIFY framework, detailing its structured approach to IoT lifecycle management. In Section 13.3, we present a comprehensive use case—the connected cabin system in aviation—as a demonstration of the CERTIFY methodology in a high-connectivity, high-security environment. Section 13.4 discusses initial observations on the feasibility of deploying CERTIFY as a pilot framework aligned with CRA requirements, exploring how its approach addresses regulatory and operational challenges. Finally, Section 13.5 concludes with insights into the broader implications of CERTIFY for IoT security, regulatory compliance, and the advancement of secure, resilient IoT ecosystems.

13.2 The CERTIFY Project

The CERTIFY's goal is to provide to IoT stakeholders (e.g., auditors, manufacturers, users, Information Sharing and Analysis Centers - ISACs), with tools and strategies they need to ensure 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.

The project is based on international standards and frameworks such as MUD files and Zero Trust architecture [14]. These foundations enable CERTIFY to support ongoing security evaluations, enabling stakeholders to detect threats in real-time, securely update devices, and reconfigure them as necessary. The CERTIFY's focus is on providing security by design and ensuring that it can be monitored and updated securely as new risks emerge. This holistic approach also facilitates future recertification processes by streamlining the collection of security evidence throughout the operational life of a device.

13.2.1 Certify Framework

An abstract representation of the CERTIFY framework is depicted in Figure 13.1, where, for the sake of clarity, only the main interactions are reported.

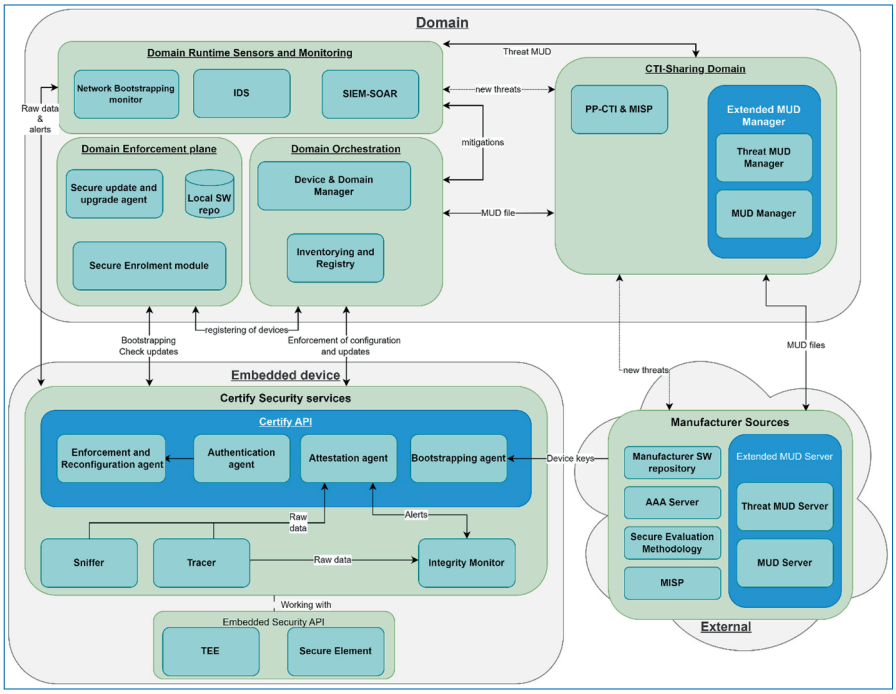

Figure 13.1. CERTIFY architecture.

The CERTIFY architecture is organized into six "domains" or "planes" based on the functionality.

The *Embedded device* plane provides the CERTIFY security services built on top of hardware functionalities to instantiate and maintain a secure environment. It characterizes the IoT platform by means of the API (Application Programming Interface) and services of CERTIFY. The CERTIFY security services include elements needed to support operations such as configuration, bootstrapping, upgrading, and monitoring. Instead, the low-level components part of the embedded security API, i.e., the Secure Element (SE) [15] and the Trusted Execution Environment (TEE) [16], provide the necessary enablers to guarantee the security of the processes inside the IoT Device.

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 Enrollment module, responsible for the registration of the devices in the domain and the issuance of the required cryptographic material to enable the creation of Direct Anonymous Attestation (DAA) [17] signatures. Instead, 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 software update process. It

also provides features to check for available updates. This component has a close relationship with the Inventory and Registry, as it is used to record every event, firmware, and device metadata. This integration ensures security, transparency, and an unbroken chain of trust in the over-the-air (OTA) process, incorporating secure cryptographic algorithms for firmware integrity and signing.

The *Domain orchestration* plane provides coordination functionalities within the domain, and its main component is the Device and Domain Manager. It focuses on the high-level management of groups or domains of IoT devices. These groups could be based on various criteria, such as location, functionality, or other attributes. In particular, the Device and Domain Manager coordinates enforcement and reconfiguration of IoT devices based on the information received from other components such as the MUD manager or the SIEM-SOAR (Security Information and Event Management - Security Orchestration, Automation and Response). All the configurations (e.g., policies applied, version of updates) are stored in the second component part of this plane, i.e., the Inventorying and Registry, which is managed by the device and domain manager.

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 phase of the lifecycle. They generate an alert if the network bootstrapping behavior differs from the expected one or if a threat has been detected at runtime, respectively. Alerts are sent to the SIEM-SOAR component for aggregation and correlation analysis with other raw data and alerts. Also, this plane interacts with the Cyber Threat Intelligence plane, since discovered threats can be shared with the MISP (Malware Information Sharing Platform), and possible mitigations can be received in the form of threat MUD files.

The *Cyber Threat Intelligence (CTI)* plane provides services for ensuring privacy-preserving security information sharing like vulnerabilities, mitigations or recommended configurations. A central pillar of this plane is constituted by the Privacy-Preserving CTI (PP-CTI) system, which is responsible for anonymizing sensitive data and attributes in cyber threat reports. For responding to identified threats, the PP-CTI combines the MUD [7] with the Threat MUD server [10] as threat signaling mechanism. The MUD is a standardized software description defined by the Internet Engineering Task Force (IETF) Request for Comment (RFC) 8520, that allows IoT manufacturers to advertise device specifications and supported communication patterns. In particular, 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,

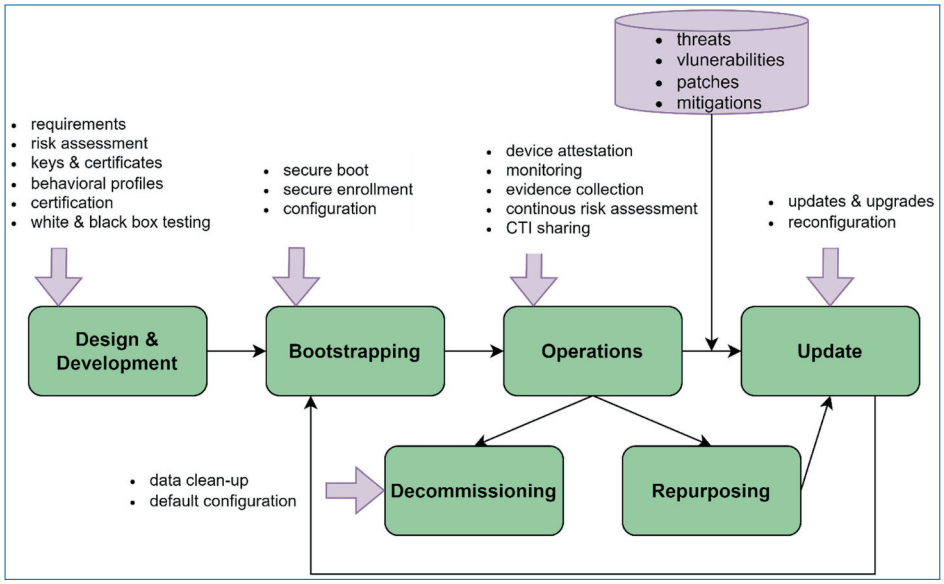

Figure 13.2. CERTIFY lifecycle methodology.

and authorization policies [8]. 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.

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.

13.2.2 Certify Lifecycle Methodology

The CERTIFY lifecycle (pictorially represented in Figure 13.2) starts with the design and deployment of the device. At that time requirements are considered, the risk assessment is performed considering the target application domain, and a certification may be requested. Moreover, keys, certificates and behavioral profiles used during the enrollment are built and securely stored by the manufacturer (some information is stored on the device while others remotely). Once deployed, the device bootstrapping takes care of the secure boot, enrollment, and configuration in the domain. During operations, device attestation and monitoring are performed to identify the presence of any suspicious event. New threats, vulnerability and patches may be identified by exploiting internal and external information. These may summon update, upgrade and reconfiguration. Changes performed on

the device and an evolved threat landscape are also considered while collecting the evidence needed for a continuous risk assessment and the potential need to trigger a device re-certification. A complete lifecycle includes also the case of device repurposing (i.e., when it no longer fulfills a given purpose) and decommissioning (requiring the proper application of data cleaning policies and default reconfiguration).

13.2.2.1 Manufacturing: Design and Development

In this phase, the device is designed, created, programmed, and tested, so the initial level of security is established. In this stage, all the actors in the supply chain (i.e., component designer, integrator, software and library developer) are part of the process, while the manufacturer is responsible for carrying out the initial security evaluation of the device. Adoption of the best security practices for design, production and testing can ensure adequate implementation.

In this area, there is vast research and documentation effort to summarize all existing attacks. Nonetheless, many more are found continuously. Furthermore, there is difficulty in defining a common standard methodology to describe how security evaluation and certification must be done. The wide variety and heterogeneity of methodologies, mechanisms, standards, and products generates a complex landscape of solutions. Therefore, it is quite unclear which security aspects should be considered to guarantee an adequate security level. In this context, performing a comprehensive comparison is unfeasible, as different schemes use their own metrics, especially when products are evaluated under different national schemes or approaches, or when they include some subjective or difficulty calculating metrics (e.g., Common Weakness Scoring System, CWSS, uses likelihood). The Cybersecurity Act (CSA) and the CRA present a pioneer initiative to foster a European Cybersecurity assessment of product and services. These regulations, in addition to the directive on security of network and information systems (NIS) [18] and the General Data Protection Regulation (GDPR) represent the four main pillars for cybersecurity in Europe.

However, as new vulnerability and threats are continuously discovered, defining a comprehensive and common standard methodology for cybersecurity testing, evaluation and certification becomes cumbersome. On the one hand, the wide variety of standards, certification schemes, and requirements hardens the goal of an objective comparison on the security achieved by products and a comparison between certified products. On the other hand, the intended use and context (regulation, domain, etc.) determine the security level required for a particular product and requirements to be considered. This problem is exacerbated by the out-of-date certificates offering a false sense of security due to zero-day vulnerabilities and evolving threats. The dynamism inherent to security makes necessary agile and dynamic

approaches to manage the security of a product throughout its lifecycle. Consequently, it is also necessary to consider continuous assessment and adopt dynamic labels capable of showing in real time the actual security level. Current certification schemas and approaches are not neglecting this dynamism, however Common Criteria (CC), Commercial Product Assurance (CPA) or Certification de Sécurité de Premier Niveau (CSPN), to name a few, require a complete recertification in case of a security change, involving high money losses and time [19].

Toward this end, CERTIFY considers a security evaluation and certification approach based on modelling, allowing to test the design of the device from the very beginning and automating the security evaluation process as indicated in previous section, combining security testing and risk assessment towards an objective and automated assessment. In CERTIFY, the secure evaluation methodology is supported by the Cyberpass tool,[1] a cloud-based platform taking as input security requirements and suggesting an evaluation methodology that starts with the self-declaration/self-assessment, allowing the manufacturer to answer the questionnaire based on these security requirements.

Although in general the results of the security assessment are used only to certify the security of the device, CERTIFY explores approaches to benefit from this information during the deployment and operation of the device. In this sense, the evaluation results can be embedded in a behavioral profile associated to different levels of security with some recommendations (polices) to consider during the operation phase of the product. This profile reduces the attack surface to the allowed behaviors, and it can be also used to monitor suspicious behaviors during the operation phase. This activity interoperates and makes use of the results of the previous evaluation. Indeed, the behavioral profile designed in CERTIFY, which is based on extending the MUD standard [20, 21] is generated from the security results containing both security recommendations from the manufacturer and from the security certification to perform a secure deployment. In particular, the use of MUD is being extended to create augmented security profiles, to govern the intended communications of IoT devices throughout their lifecycle.

Once the certification process is finished, the MUD is signed by the Certification Authority (CA), and the manufacturer can publish it on its MUD server to be accessible to any buyer of the product. The MUD URL together with the device identity is then stored inside the device for its secure deployment.

To provide support for the following phases of the lifecycle, CERTIFY adopts formally proven authentication and cryptographic protocols and robust isolation mechanisms enabled by open hardware architectures and trusted computing

1. https://www.cyber-pass.eu/

standards. The architecture of the IoT device includes three strategic enablers: the SE, the TEE, and the Embedded Security API acting as an interface for these low-level components. The SE is a dedicated secure and physical tamper-resistant microcontroller allowing protection against high-level software and hardware attacks. Such an element, when present, will constitute the hardware engine, assuring support for the securitization at a high level of the IoT device. While the SE provides PKCS11 functions [22] to be used by the agents to interface and invoke crypto functionalities, the TEE provides a trusted world for those applications that need it, supporting cryptographic functions and secure operations. This is necessary to execute and protect CERTIFY processes such as IoT authentication, derivation of keys or data integrity protection. The embedded security API aims to abstract access to the low level IoT security components such as the SE and the TEE. Thanks to these enablers, high-level components described in the following subsections can securely enforce certain configurations inside the IoT device, not only policies, but also software images (enforcement and reconfiguration agent), perform the secure bootstrapping and authentication of the device (bootstrapping and authentication agent), and monitoring of the IoT device behavior and configuration (attestation agent).

13.2.2.2 Bootstrapping/Deployment

The bootstrapping phase starts when the device is installed and configured in a certain context. This process usually consists of a set of procedures in which a device joins a network in a certain domain (health, house, industry…). During the bootstrapping, the cryptographic material statically configured during manufacturing of the device is used to derive dynamic credentials and keys to be used during its operation. In recent years, different botnets (e.g., Mirai [23]) have shown that the deployment of IoT devices can compromise critical infrastructures with huge economic losses. This is especially critical in certain scenarios (e.g., involving eHealth devices), which can affect users' safety. To address such security concerns, there is a need to define approaches to reduce the attack surface of the devices from the very beginning. Beyond the use of traditional cryptographic (and more recently towards post-quantum cryptographic algorithms) and access control techniques, the security aspects of IoT devices should be properly managed through a governance approach to ensure devices behave as expected. However, the specification and enforcement of such aspects can be challenging in environments where a huge number of IoT devices can communicate with each other and, sometimes, without the explicit consent from their owners.

Extended MUD files were integrated into the CERTIFY's enhanced bootstrapping 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.

Following this strategy, CERTIFY divides the bootstrapping into three subphases, each of them involving a subset of the components reported in Figure 13.1:

1. **The factory bootstrapping.** In this phase, the cryptographic material (device keys) and the MUD URL are statically configured and securely stored in the IoT during manufacturing (if available, in the SE).
2. **The domain bootstrapping.** In this phase, the device requests to start the bootstrapping in the domain (bootstrapping agent). CERTIFY leverages the Constrained Application Protocol (CoAP) - Extensible Authentication Protocol (EAP) [24, 25] to authenticate the device and generate the keys. In particular, the bootstrapping agent acts as the EAP peer, the secure enrollment module acts as EAP authenticator, the Device and Domain Manager acts as an Authentication, Authorization and Accounting (AAA) domain server [26] and the AAA manufacturer server acts as EAP server. Moreover, CERTIFY relies on the extended MUD to securely configure the device. For this, CERTIFY adapts the IETF architecture to the MUD extension and the interactions with other components. In this sense, the Extended MUD Manager is the main entity of the CERTIFY MUD architecture. It aggregates the functionality of the MUD manager and threat MUD manager, in charge of the processes required for obtaining and parsing the MUD and threat MUD file. This component has been extended from the IETF standard and the NIST proposal. In this way, the MUD, which is stored by the manufacturer in the Extended MUD Server, is obtained and translated to MSPL policies by the Extended MUD Manager using the URL provided by the device. While the Device and Domain manager orchestrates at domain level the enforcement of the MSPL policies, the Enforcement and Reconfiguration Agent is the component responsible for the internal IoT orchestration of the activities that need to be performed. 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. Such a fingerprint changes by device type (hardware) and firmware version. The network bootstrapping monitor exploits such a behavioral 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. As fingerprints are characterized by device type (and firmware version), we envision that the manufacturer builds such a behavioral fingerprint and includes it as part of the extended MUD file designed in CERTIFY.

3. **The domain enrollment.** In this phase, high-end devices need to verify their correct state based on the policies defined in the MUD. CERTIFY leverages the DAA protocol to authenticate the high-end device and generate appropriate policies for attestation. In the CERTIFY architecture, the Authentication agent is responsible for the creation and management of the DAA key, and the Secure Enrollment module is the DAA issuer, responsible for the issuance of the cryptographic material required to enable the creation of DAA signatures. While the extended MUD file is retrieved from the server and enforced, enhancing device security in alignment with the manufacturer's certification, 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. All in all, these processes allow CERTIFY to leverage the extended MUD file information during device bootstrapping to enable the configuration of security policies before granting network access, enhancing the security posture.

Once deployed, the device can generate dynamic credentials (authentication agent) 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. In essence, this repository serves as a pivotal tool in safeguarding the security, functionality, and integrity of network devices while maintaining a comprehensive inventory of their attributes by enabling monitoring and securing device-related information.

13.2.2.3 Operations

During the **operational** phase, continuous monitoring of the device is essential due to evolving security threats and vulnerabilities that were not anticipated at design time. The device's security level changes over time, requiring re-assessment and potentially re-certification.

In the CERTIFY framework, monitors are in place to send information about the IoT device (Sniffer and Tracer). Therefore, whenever a vulnerability is detected, CERTIFY can select and apply a mitigation. This information is processed by runtime attestation (Attestation agent) and by the Integrity monitor to check the fulfillment of the security properties certified (i.e., the ones contained in the MUD) during the operational phase. Network traces are also processed by the IDS that analyses the traffic in real-time and alerts about potential threats. Detection rules are periodically updated with new known signatures and new rules can be added to customize the solution to customers' and users' needs. The detection is enriched with an anomaly detection procedure that analyses offline datasets of network traffic

to identify potential misbehavior and anomalies in the usage of the network. These events can be further processed with more advanced, and computationally expensive, solutions by the SIEM-SOAR that could also correlate multiple events identified in the network and on the device under analysis.

The SIEM-SOAR tool combines the typical functionalities of Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) systems. While the SIEM allows for the collection and analysis of security events and contextual data, the SOAR enables the centralized handling of threat intelligence and automates responses to security incidents, significantly reducing reaction times and limiting potential damage. Given alerts details, the SIEM-SOAR identifies and applies the most appropriate reaction (e.g., publish information, request an update, apply a mitigation by reconfiguring system, network or device, or even check for threat MUD file from the Extended MUD Server). Then the Device and Domain Manager coordinates the mechanisms to enforce mitigations and updates on the IoT Device. If an update is required, the secure update and upgrade agent orchestrates the software update based on the information contained in the local software repository, Manufacturer software repository, and Inventorying and Registry. In any case, the Enforcement and Reconfiguration agent is in charge of enforcing the configuration on the IoT device.

By linking runtime detection with mitigation actions suggested by manufacturers, threat databases, or certification authorities, CERTIFY ensures timely protection against identified vulnerabilities. This is facilitated by an extended threat MUD. CERTIFY combines manufacturing-phase security evaluation with runtime metrics to continuously assess security. The system can deny network access if critical risks are detected, and adjust device configurations as needed to maintain security.

CERTIFY also promotes continuous communication among stakeholders by integrating external security information about new vulnerabilities, updates, patches, and potential zero-day attacks with domain-specific data. The framework integrates mechanisms to share security information with manufacturers and other interested parties in a privacy-preserving (PP) way through the PP-CTI component [27]. In particular, the PP-CTI includes data mining techniques such as suppression, generalization, K-Anonymity, T-Closeness, L-Diversity and Differential Privacy [28–30]. PP-CTI interfaces with the Malware Information Sharing Platform (MISP)[2] where vital threat information is shared, and other valuable cybersecurity insights. Furthermore, PP-CTI & MISP integrates an access control layer, featuring identity management software such as Fiware Keyrock [31]. This

2. https://www.misp-project.org/

allows CERTIFY to decide which entities can send or receive specific data, further enhancing data security and privacy. The information could then be accessed by other CTI providers and the manufacturer (MISP manufacturer). In the same way, new threats and alerts can be received and exchanged among these sources.

13.2.2.4 Updating

Traditionally, IoT security has been hindered by a "set and forget" approach, where manufacturers and service providers configure devices but rarely update their firmware. This practice represents a significant obstacle to long-term IoT security. To overcome this, OTA [32] software updates are essential for maintaining the security of IoT devices over time. This necessity is reinforced by various standards and recommendations, including those from the European Union Agency for Cybersecurity (ENISA), which has emphasized the importance of regular software updates in enhancing the security and reliability of connected devices [33, 34].

However, the process of updating software on IoT devices introduces its own set of cybersecurity challenges [35–37], particularly for devices with limited resources. In response to this, the IETF published RFC 9019 [38], which defines a standardized architecture for firmware updates in IoT environments. CERTIFY builds on these guidelines, incorporating OTA components that adhere to RFC 9019's framework. To further enhance security, CERTIFY integrates advanced blockchain technology, which records every event related to firmware updates and device metadata. This ensures transparency, immutability, and a continuous chain of trust throughout the OTA process. Secure cryptographic algorithms are employed to verify firmware integrity and to sign firmware updates, ensuring that the software is authentic and untampered.

The updating phase in CERTIFY encompasses the procedures for deploying software updates or patches provided by manufacturers, as well as configuration tasks required to address newly identified threats. These procedures involve multiple components, including the enforcement and reconfiguration agent, secure update and upgrade agent, device and domain manager, inventory and registry, and software repository. The secure update-and-upgrade agent provides a graphical user interface (GUI) where security administrators can manage registered devices and software. This interface allows administrators to upload new software to the software repository, register it with the Device and Domain Manager, and trigger updates. It also includes features to check for available updates and initiate the upgrade process, making the management of software versions straightforward and efficient. The software repository serves as a storage hub where software packages are stored, organized, and managed. This repository allows users to access, download, and update applications and libraries, facilitating the distribution of software across devices. By centralizing the management of software packages, the repository

ensures that updates are delivered efficiently and securely to all connected devices within the network.

Finally, to enhance the transparency and traceability of the update process, CERTIFY framework employs DLTs such as blockchain. This provides a transparent ledger that tracks software versions and any known vulnerabilities, allowing manufacturers to be represented as individual blockchain nodes. Through this approach, information about software components can be securely shared between stakeholders. Although interoperability issues with various DLT implementations persist, CERTIFY is exploring the use of interledger technology to link different DLT systems into a cohesive, secure framework for managing updates.

13.2.2.5 Decommissioning & Repurposing

The decommissioning phase in the CERTIFY lifecycle methodology represents the final stage in the life of a connected device, where it is either retired or repurposed. This phase is critical to ensuring that once a device has reached the end of its operational life or it is no longer able to meet security requirements, all security-sensitive data and configurations are effectively and securely handled. The focus during decommissioning is on safeguarding the network and preventing any residual vulnerabilities that might remain if the device were simply discarded without proper protocols.

A device may be decommissioned for several reasons: it may no longer meet the security standards required for its operational environment, it may be incompatible with essential software updates due to hardware limitations, or a vulnerability may have been discovered that cannot be mitigated through available patches. In all these cases, the decommissioning process begins by performing a comprehensive analysis to determine whether the device can be repurposed for a different or less security-critical role, or if it must be fully decommissioned and removed from service.

When a device is slated for decommissioning, CERTIFY emphasizes the importance of secure data erasure. This involves permanently wiping all sensitive data stored on the device, including cryptographic keys, certificates, and any stored configurations or logs. Simply restoring the device to factory settings is not sufficient in most cases, as residual data might remain accessible. CERTIFY ensures that the decommissioning process includes a thorough, verifiable data destruction procedure, employing cryptographic techniques or secure overwriting methods to guarantee that no information can be recovered.

For devices that are repurposed rather than fully decommissioned, CERTIFY provides a framework for reconfiguring the device for a different role within the network. This may involve reassigning the device to a domain with lower security requirements or reconfiguring its functionality to handle fewer sensitive tasks. Repurposing a device can often extend its operational life and reduce costs, but it

must be done in a way that ensures the device is still capable of meeting the security standards necessary for its new role.

If a device is determined to be unsuitable for repurposing, the final step in the decommissioning phase is its secure removal from the network. DLT technology used in the CERTIFY's framework provides a transparent and immutable record that verifies the device's decommissioning and ensures compliance with all relevant security policies. This record could not only include confirmation that all sensitive data was securely erased, but also the steps taken to prevent the device from re-entering the network or being reused in an unauthorized manner.

13.3 Connected Cabin System – CERTIFY Use Case

Next generation aircrafts foresee the presence of a multitude of IoT-based connected devices supporting new and enhanced services in the cabin, e.g., smart screen, galley, lavatory, seat, and light. This evolution will usher in the era of intelligent aircraft cabin. The expected benefits from such a scenario encompass: (i) a personalized experience for passengers, e.g., customized In-Flight-Entertainment (IFE) and seating configurations; (ii) opportunities for airlines in delivering targeted retail offers; and (iii) optimized operations and Prognostics and Health Management (PHM) applications, thanks to a detailed overview on the aircraft status and passenger preferences built through distributed and connected sensors.

This environment is characterized by a high volume of data per second – GBs up to TBs (considering all the sensors in the aircraft) – and by a heterogeneous set of devices. Communications is performed by means of wired (e.g., the Ethernet-based AFDX – ARINC 664, CAN bus, ARINC429) or wireless connectivity (e.g., IEEE 802.11, ECMA-368, IEEE 802.15.3). The device heterogeneity is also reflected in the different capabilities to host services. It is worth noting that the devices considered in this scenario are part of the cabin system and therefore do not require any specific safety assessment. However, they must still meet the related certifications, guidance, and regulations for airworthiness (e.g., from RTCA, EUROCAE [39], FAA [40] and EASA [41]) such as the AC 20-168 and the RTCA DO-313 "Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment (CS&E)". Therein it is required to verify the security of the wired and wireless systems, by adopting a design approach that will prevent any unintended change to the systems during operations. The emphasis is given to hardware, software, network, and data in consideration of the potential challenges related to the inclusion of Commercial Off the Shelf (COTS) components where alternative methods and processes are needed to perform the required tests and evaluations. All in all, there is a clear need to protect these devices throughout their lifecycle and generate appropriate evidence.

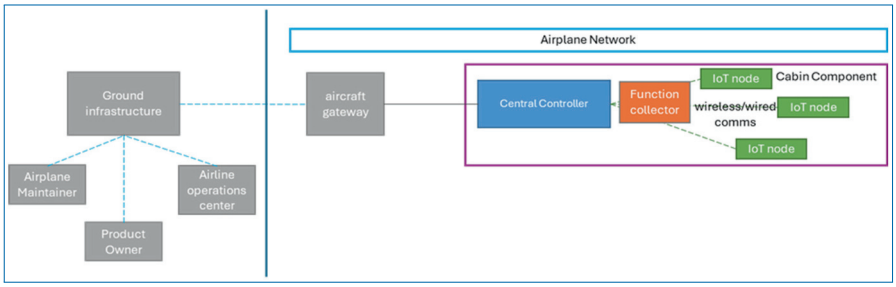

Figure 13.3. High-level block diagram of the CERTIFY use case for the connected cabin system.

The CERTIFY use case considers an environment constituted by two different classes of devices deployed in the cabin, plus a set of infrastructural remote services hosted by the component and system manufacturer, and airline. The onboard devices are: 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. These two classes of embedded devices have respectively been exemplified in the project by a custom RISC-V based node and an off-the-shelf high-end embedded board based on the ARM instruction set. Moreover, 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. Figure 13.3 pictorially represents the use case.

For demonstrating the CERTIFY functionalities, three different scenarios covering multiple stages of the product lifecycle have been introduced. Namely, installation of a new component, operations and monitoring, and replacement and repurposing. In the following, we briefly recall the scenarios later referenced in Section 13.4 where the approach taken by CERTIFY for these scenarios matches the EU CRA.

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) in the cabin. To not compromise the cybersecurity posture of the system the performed process must include bootstrapping, initial update, and customization for the specific deployment environment by considering the secure configuration defined by the product owner/manufacturer during the product evaluation for the original certificate. Moreover, if the new component is a replacement for a previously installed one, secure decommissioning, including reset and wipe out of any sensitive data, must 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. Moreover, it is worth considering that connecting passengers' devices, as well as the presence of a wireless network, generate a wider attack surface. Similarly, external infrastructures can upload data for onboard connectivity experience and In-Flight Entertainment (IFE) services. Moreover, maintainer and product owner may also need the availability of a remote connectivity to perform device reconfigurations. All these operations demands for vulnerability management and anomaly detection throughout the entire operations of product and system.

Scenario 3 – Replacement and repurposing. In case a cabin system component has a failure, to minimize the downtime, a compatible replacement Line-replaceable unit (LRU) could be retrieved from the same manufacturer and repurposed for the specific target system. 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 request a different amount of resources to host services and security features. Therefore, the new usage must be among the ones foreseen and certified by the manufacturer so that proper reconfiguration can be implemented.

13.4 Towards a CERTIFY Pilot for the European Cyber Resilience Act

Looking at the current cybersecurity policy landscape it was quite straightforward to make a connection between CERTIFY and the CRA due to the scope of its application and its strong impact on IoT products. CRA also revolutionizes the cybersecurity ecosystem by imposing requirements, both at the product and process level, with significant implications over the entire product lifecycle.

The CRA could officially enter into force by the end of 2024, after being proposed by the European Commission at the end of 2022, and after being adopted by the European Parliament in March 2024. The objective of the CRA is to establish a minimum level of cybersecurity for all digital devices (both software and hardware) sold in the EU internal market. In order to achieve that, the CRA sets to:

- facilitate the secure development of products with digital elements 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 vulnerability handling process;
- establish rules on market surveillance and enforcement;
- establish more or less stringent proof of conformity depending on the category the products fall in (i.e., self-declaration, third-party assessment, etc.).

To understand the implications of the CRA developments, the Connected Cabin Systems use case of CERTIFY is chosen as a reference with the intent to consider the large scope of its three scenarios, as well as the security challenges, and the complexity of the set of actors involved. It is quite clear that 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 Connected Cabin se case would most likely fall under the CRA scope (e.g., IoT nodes, central controllers, aircraft gateway). Indeed, Article 2 of the CRA text 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 remaining of the section develops further the ambitious and challenging task of trying to pave the way for a pilot on the CRA offered by the CERTIFY project. The challenge is mainly due to the fact that the CRA is not yet adopted, even though the text is stable, many aspects still need to be defined, and quite several key aspects will be postponed to delegated and implementing acts. Thus, the analysis herein presented might need to be revised when the details and the actual application of the CRA will occur after a transition period.

In addition, CERTIFY remains a research project, so both from a product and regulation perspective, we still need to go through complex revision cycles. Moreover, we do not claim to perform any conformance test, nor do we plan to undergo a certification process within the context of this exercise, nor the CERTIFY framework pretends to be an answer to the complex issue of conformity assessment.

In conclusion, we believe we discuss the CERTIFY use case in the context of the CRA to bring a better understanding of the project impact being developed in close alignment with the reality of the industry, the law, and its evolution. In other words, each technical advancement of the project should be performed keeping in mind what regulatory context it will face, facilitating rather than making more difficult the adherence to such regulatory context. The CERTIFY framework can be a step toward alignment with the CRA and its implementation.

13.4.1 Use Case Analysis for the CRA

This section discusses the CRA in the context of the three scenarios discussed in Section 13.3.

Scenario 1: The CRA ambitiously aims to make cybersecurity a primary perspective in the design, development, and production of products with digital elements. In essence, as has been stated in several policy fora, the successful implementation of the CRA would assure a security by design approach for each manufacturer that makes products available in the EU market. This could be achieved by making sure that several basic cybersecurity requirements are respected and that, ultimately, products made available do not have any known vulnerability. In CERTIFY, this step is carried out through the automation tool *CyberPass* which streamlines the conformity assessment process based on the ETSI EN 303 645 standard [34]. It is important to note that this latter standard was highlighted by the *CRA Requirements Standards Mapping study* [42] conducted by ENISA and the European Commission's Joint Research Centre since it maps to most of the CRA essential requirements. Strictly speaking, the scenario in question focuses on secure bootstrapping and customization of a cabin component into the network. Similarly to the essential requirements of the CRA, an initial set of basic requirements is pushed on the component to be part of the network. In addition, CERTIFY provides a certificate of the secure state of the newly added component, which should ideally facilitate further demonstration of regulatory compliance.

Scenario 2: The scenario on *operations and monitoring* is probably the most interesting for a CRA pilot. It touches upon several pillars and angles of the CRA, but more precisely on the provisions related to lifecycle and vulnerability management. If, for instance, a rogue device injects false data and or takes harmful actions within the cabin, the CERTIFY framework will be able to monitor and spot that. It goes without saying that, in case 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". Clearly, the CRA requires market operators to take action, stressing their need to assure support all along the lifecycle of a product (being for product and service support, updates, or mitigation responses).

Moreover, this scenario taps into part of the CRA essential requirements that insist on processes and not only on products: such requirements 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 corrective measures. Indeed, once a vulnerability is discovered, the manufacturer must promptly perform the necessary actions to bring a product with digital elements or the manufacturer's processes into conformity, or alternatively withdraw or recall the product, as appropriate. The CERTIFY methodology includes collection, identification, and decision, and coupled

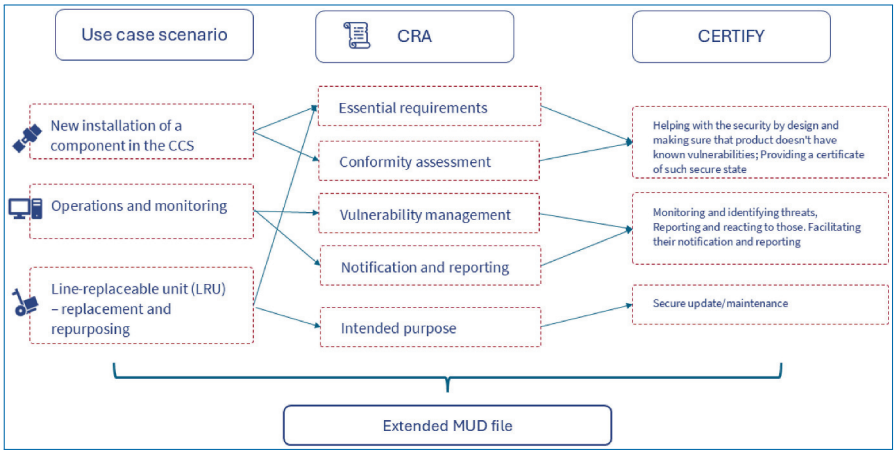

Figure 13.4. The CERTIFY cybersecurity lifecycle methodology and framework aligned with recent EU regulation: the CRA example.

with its real-time monitoring capabilities (e.g., SIEM-SOAR, IDS, runtime attestation, MUD), allows for the identification and handling of any anomalous behavior while placing its user in a better spot to comply with cybersecurity regulations.

Scenario 3: The last scenario is the Line-replaceable Unit (LRU) one. Here again, the CRA is quite explicit in the obligation to support and update digital products. However, one of the peculiar aspects of this scenario is the eventuality of repurposing a device within a network for a different use or functionality. The CRA text calls for an assessment of the intended use of a product with digital elements. In other words, the new potential purpose of a network component should already be foreseen by the market operators as the CRA calls on them to be familiar with the intended use of a product, as well as with 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. Finally, the operator should always adopt a risk-based approach to continuously assess this eventuality and make sure that new device usage does not lead to harmful and previously unforeseen consequences

Figure 13.4 pictorially represents the link between the use case, the CRA and the CERTFIY project.

13.4.2 The Role of the Extended MUD File

During the design of the CERTIFY methodology, the usage of the extended MUD file emerged as the cohesive element for the three scenarios. Each actor can collaboratively contribute, update and provide a state of the security of the system. The usage of the MUD file (and particularly its extension considered in CERTIFY) 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 legislator has underlined several times how market operators should systematically document relevant cybersecurity aspects concerning products with digital elements, including vulnerabilities of which it becomes aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products. In addition, the CRA introduces complex notification and reporting rules concerning exploited vulnerabilities and severe incidents (with some novelty elements such as a *Single Reporting Platform or* a *Single Point of Contact* for manufacturers).

Moreover, the extended MUD file would enhance the possibility of collaboration with all the stakeholders, encouraging cooperation and cohesion toward IoT security. All these ingredients combine well with the need for cooperation with the stakeholders involved in the notification and vulnerability handling procedures, e.g., CSIRTs (Computer Security Incident Response Teams), ENISA, Single Point of Contacts. Ideally, the extended MUD file could also be a good starting point to build the conformance documentation (being itself or third-party-assessed).

13.5 Conclusions

While European regulations advance cybersecurity by imposing measures to manage it throughout the lifecycle of a device, it is still not clear how to implement such cybersecurity lifecycle management in an efficient and coordinated manner. In response to this problem, this chapter provides an introduction and comprehensive overview of the general architecture of CERTIFY.

CERTIFY gets inspiration from recent EU initiatives such as the Cybersecurity Act and the Cyber Resilience Act the core role covered by certification, lifecycle management and information sharing. Indeed, in its framework CERTIFY considers: (i) current certification status and reports, as baseline for describing the security profile of a device including security controls, policies, recommended configuration (by means of the extended MUD) and assurance level according to domain of deployment; (ii) behavioural profile, as a way of describing the expected functioning of the device; (iii) threat modelling and risk assessment, that from a baseline built at design time is continuously updated thanks to the information sharing and the usage of the threat MUD; (iv) change impact analysis, to dynamically understand, from internal and external information, how changes in the threat landscape, and applied security controls and policies may impact the security posture of the

system; v) recertification from testing results, by leveraging a complete assessment of the reached security level and exploiting the artifacts collected throughout the device lifecycle to request and support an agile recertification process in case the device should not meet anymore the requested Security Assurance Level (SAL).

This chapter discusses the CERTIFY project in the context of the CRA. In particular, the Connected Cabin Systems use case is analyzed with the intent to shed some light about the challenges and impact of the implementation of the CRA in a real industrial case.

The holistic methodology adopted by CERTIFY ensures that the CERTIFY architecture is suited to address the complexities of managing the security lifecycle of IoT devices, offering robust security, privacy, and adaptability in an ever-evolving digital landscape.

Acknowledgements

Research partially supported by the EU through the Horizon research and innovation program CERTIFY (grant agreement no. 11069471) and the Swiss SERI (grant agreements no. 22.00165 and 22.00191). The European Commission's and Swiss SERI's support for the production of this publication does not constitute an endorsement of the contents, which reflects the views of the authors only, and neither the Commission nor the Swiss Confederation can be held responsible for any use which may be made of the information contained therein.

References

[1] M. Weiser, "Ubiquitous Computing," *Computer*, vol. 26, no. 10, pp. 71–72, Oct. 1993, doi: 10.1109/2.237456.

[2] Tech Target, "Colonial Pipeline hack explained: Everything you need to know." Apr. 2022. [Online]. Available: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[3] TechCrunch, "Hotel giant Marriott confirms yet another data breach." Jul. 2022. [Online]. Available: https://techcrunch.com/2022/07/06/marriott-breach-again/.

[4] TechHQ, "The way cybercrime can kill." Dec. 2022. [Online]. Available: https://techhq.com/2023/12/hospital-cyberattack-ardent-health-systems-down-er-shut/.

[5] U.S. Securities and Exchange Commission (SEC), "Cybersecurity Disclosure."

[6] European Commission, "What is a data breach and what do we have to do in case of a data breach?" 2016. [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en.

[7] C. Boggini, "Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework," *Comput. Law Secur. Rev.*, vol. 53, p. 105987, 2024, https://doi.org/10.1016/j.clsr.2024.105987.

[8] European Union Agency for Cybersecurity (ENISA), "CIRAS." 2023. [Online]. Available: https://ciras.enisa.europa.eu/.

[9] European Repository of Cyber Incidents, "EuRepoC." Nov. 2022. [Online]. Available: https://eurepoc.eu/.

[10] "Global cybercrime estimated cost 2029," Statista. Accessed: Oct. 31, 2024. [Online]. Available: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

[11] European Commission EUR-Lex – 52022PC0454, "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act)." 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.

[12] CERTIFY, "aCtive sEcurity foR connecTed devIces liFecYcles." [Online]. Available: https://doi.org/10.3030/101069471.

[13] E. Lear, D. Romascanu, and R. Droms, "Manufacturer Usage Description Specification (RFC 8520)." Accessed: Feb. 12, 2019. [Online]. Available: https://tools.ietf.org/html/rfc8520.

[14] Rose, S., Borchert, O., Mitchell, S. and Connelly, S., "Zero Trust Architecture." Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2020. [Online]. Available: 10.6028/NIST.SP.800-207.

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

[16] S. P. a. N. Santos, "Demystifying Arm TrustZone: A Comprehensive Survey," *ACM Comput Surv.*, vol. 51, no. 6, pp. 1–36, 2019.

[17] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proceedings of the 11th ACM conference on Computer and communications security*, in CCS '04. New York, NY, USA: Association for Computing Machinery, Oct. 2004, pp. 132–145. doi: 10.1145/1030083.1030103.

[18] EUR-Lex, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)." 2016. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[19] 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, 2020.

[20] S. N. Matheu et al., "Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems," *Sensors*, vol. 20, no. 7, p. 1882, Jan. 2020, doi: 10.3390/s20071882.

[21] 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, doi: 10.1109/ACCESS.2019.2947157.

[22] "PKCS #11 Specification Version 3.1." Accessed: Oct. 25, 2024. [Online]. Available: https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.html.

[23] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.

[24] F. Bersani and H. Tschofenig, "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol Method (RFC 4764)."

[25] ACE Working Group, "EAP-based Authentication Service for CoAP," *IETF Datatracker*. 2024. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-ace-wg-coap-eap-10.

[26] J. Vollbrecht et al., "AAA Authorization Framework (RFC 2904)." 2000.

[27] 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, Mar. 2007, doi: 10.1109/TSE.2007.26.

[28] D. Slijepčević, M. Henzl, L. D. Klausner, T. Dam, P. Kieseberg, and M. Zeppelzauer, "k-Anonymity in practice: How generalisation and suppression affect machine learning classifiers," *Comput. Secur.*, vol. 111, p. 102488, Dec. 2021, doi: 10.1016/j.cose.2021.102488.

[29] T. Ha, T. K. Dang, T. T. Dang, T. A. Truong, and M. T. Nguyen, "Differential Privacy in Deep Learning: An Overview," in *2019 International Conference on Advanced Computing and Applications (ACOMP)*, Nov. 2019, pp. 97–102. doi: 10.1109/ACOMP.2019.00022.

[30] F. Piccialli and Z. Lyu, "The Security of Medical Data on Internet Based on Differential Privacy Technology," *ACM Trans. Internet Technol.*, vol. 21, Mar. 2020, doi: 10.1145/3382769.

[31] Fiware Keyrock, "Fiware Keyrock API." [Online]. Available: https://fiware-idm.readthedocs.io/en/latest/index.html.

[32] 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.

[33] "ENISA Baseline Security Recommendations for IoT |OWASP IoT Top 10 2018 Mapping Project." Accessed: Oct. 25, 2024. [Online]. Available: https://scriptingxss.gitbook.io/owasp-iot-top-10-mapping-project/mappings/enisa-baseline-security-recommendations-for-iot.

[34] "ETSI EN 303 645 Cybersecurity for Consumer Internet Of Things," TÜV SÜD. Accessed: Oct. 25, 2024. [Online]. Available: https://www.tuvsud.com/en/resource-centre/stories/etsi-en-303-645-cybersecurity-for-consumer-internet-of-things.

[35] N. S. Mtetwa, P. Tarwireyi, A. M. Abu-Mahfouz, and M. O. Adigun, "Secure Firmware Updates in the Internet of Things: A survey," in *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, Nov. 2019, pp. 1–7. doi: 10.1109/IMITEC45504.2019.9015845.

[36] Q. Wang, Y. Zhu, and L. Cheng, "Reprogramming wireless sensor networks: challenges and approaches," *IEEE Netw.*, vol. 20, no. 3, pp. 48–55, May 2006, doi: 10.1109/MNET.2006.1637932.

[37] S. Brown and C. J. Sreenan, "Software Updating in Wireless Sensor Networks: A Survey and Lacunae," *J. Sens. Actuator Netw.*, vol. 2, no. 4, Art. no. 4, Dec. 2013, doi: 10.3390/jsan2040717.

[38] B. Moran, H. Tschofenig, D. Brown, and M. Meriac, "A Firmware Update Architecture for Internet of Things," Internet Engineering Task Force, Request for Comments RFC 9019, Apr. 2021. doi: 10.17487/RFC9019.

[39] "EUROCAE," Eurocae. Accessed: Oct. 25, 2024. [Online]. Available: https://www.eurocae.net/.

[40] FAA, "Federal Aviation Administration." [Online]. Available: https://www.faa.gov/.

[41] EASA, "European Union Aviation Safety Agency." [Online]. Available: https://www.easa.europa.eu/en.

[42] "Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis," ENISA. Accessed: Oct. 25, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping.