Ref. Ares(2021)5190713 - 19/08/2021

# Deliverable 7.1

## Report on the Identified Security and Privacy Metrics and Security Claims to Evaluate the Security of a System

### Technical References

| | | |
|---|---|---|
| Document version | : | 1.0 |
| Submission Date | : | 19/08/2021 |
| Dissemination Level | : | Public |
| Contribution to | : | WP7 – Security and Privacy Claims |
| Document Owner | : | UMU |
| File Name | : | BIECO_D7.1_19.08.2021_V1.0 |
| Revision | : | 2.0 |

| | | |
|---|---|---|
| Project Acronym | : | BIECO |
| Project Title | : | Building Trust in Ecosystem and Ecosystem Components |
| Grant Agreement n. | : | 952702 |
| Call | : | H2020-SU-ICT-2018-2020 |
| Project Duration | : | 36 months, from 01/09/2020 to 31/08/2023 |
| Website | : | https://www.bieco.org |

**This project has received funding from the European Union´s Horizon 2020 Research and Innovation Programme under Grant agreement No. 952702.**

## Revision History

| REVISION | DATE | INVOLVED PARTNERS | DESCRIPTION |
|---|---|---|---|
| **0** | 20/11/2020 | UMU | Creation of the document |
| **0.1** | 20/11/2020 | UMU | First draft of the ToC |
| **0.1** | 10/12/2020 | UMU | Content added |
| **0.1** | 24/01/2020 | IESE | Content added to section 2. |
| **0.1** | 31/01/2020 | UMU | Content added to section 2 and 3 |
| **0.2** | 09/02/2021 | CNR | Content added to section 2.1.9 |
| **0.2** | 12/04/2021 | IESE | Review structure, added small edits and internal review of section 2 and section 3 |
| **0.3** | 12/4/2021 | CNR | Review structure, added small edits |
| **0.4** | 10/5/2021 | UMU | Restructure of claims sections |
| **0.5** | 31/05/2021 | CNR | Claims added to section 7 and section 4.<br>Modified content in section 2. |
| **0.6** | 10/06/2021 | GRAD | Claims added to section 4 and section 7. |
| **0.7** | 14/06/2021 | CNR | Added content (text and table) to Section “Methodology” |
| **0.8** | 16/06/2021 | IESE | Edit and Review and comment Section 1, and parts of Section 3. |
| **0.9** | 16/06/2021 | RES | Claims added to sections 4 and 7 |
| **1.0** | 23/06/2021 | UMU | Review, conclusions and methodology. |
| **1.2** | 01/07/2021 | IESE | Corrected safety-related claims, added references to safety-related standards |
| **1.1** | 01/07/2021 | CNR | Review methodology, section 5.2, and some claims in section 8 |
| **1.2** | 02/07/2021 | UMU | Final review and edition of the deliverable. |
| **1.2** | 07/07/2021 | 7Bulls | Internal review |
| **1.3** | 13/07/2021 | UMU, GRAD, RES, CNR, IESE | Comments from review addressed |
| **1.3** | 14/07/2021 | HS | External Review |
| **1.4** | 20/07/2021 | UMU | Comments from review addressed |
| **1.5** | 23/07/2021 | UMU | Deliverable finished |
| **2.0** | 19/08/2021 | UNINOVA | Final Review by PC and submitting |

## List of Contributors

**Deliverable Creator(s)**: Sara Nieves Matheu (UMU, Editor), Adrián Sánchez (UMU), Emilia Cioroaica (IESE), Said Daoudagh (CNR), Francesca Lonetti (CNR), Eda Marchetti (CNR), Enrico Schiavone (RES), Massimiliano L. Itria (RES), Ioannis Sorokos (IESE), Borja Pintos (GRAD)

**Reviewer(s):** Pawel Skrzypek (7Bulls, Internal reviewer), Oliviu Dorin Matei (HS, External reviewer), José Barata (UNINOVA, External reviewer), Sanaz Nikghadam-Hojjati (UNINOVA, External reviewer)

**Disclaimer:** The information in this document is subject to change without notice. Company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

**All rights reserved.**

The document is proprietary of the BIECO consortium members. No copying or distributing, in any form or by any means, is allowed without the prior written agreement of the owner of the property rights.

This document reflects only the authors' view. The European Community is not liable for any use that may be made of the information contained herein.

BIECO project has received funding from the European Union's Horizon 2020 research and innovation Programme under grant agreement No **952702**.

## Acronyms

| Acronym | Term |
|---|---|
| **AC** | Access Control |
| **CS** | Control System |
| **CSMS** | Cyber Security Management System |
| **DoS** | Denial of Service |
| **EC** | European Commission |
| **EFTA** | European Free Trade Association |
| **ENISA** | European Union Agency for Cybersecurity |
| **ETSI** | European Telecommunications Standards Institute |
| **EU** | European Union |
| **IACS** | Industrial Automation And Control Systems |
| **ICT** | Information and Communications Technology |
| **IEC** | International Electrotechnical Commission |
| **IETF** | Internet Engineering Task Force |
| **IoT** | Internet of Things |
| **ISO** | International Organization for Standardization |
| **IT** | Information Technology |
| **JSON** | JavaScript Object Notation |
| **GDPR** | General Data Protection Regulation |
| **LDAP** | Lightweight Directory Access Protocol |
| **M2M** | Machine-to-Machine |
| **NIST** | National Institute of Standards and Technology |
| **OS** | Operative System |
| **OWASP** | Open Web Application Security Project |
| **PAP** | Policy Administration Point |
| **PEP** | Policy Enforcement Point |
| **PII** | Personally Identifiable Information |
| **PIP** | Policy Information Point |
| **PL** | Performance Level |
| **SESIP** | Security Evaluation Standard for IoT Platforms |
| **SII** | Server-Side Includes |
| **SOTA** | State Of The Art |
| **SQL** | Structured Query Language |
| **SRP** | Safety-Related Part |
| **TOE** | Target of Evaluation |

| | |
|---|---|
| **XACML** | eXtensible Access Control Markup Language |
| **XML** | eXtensible Markup Language |
| **XSS** | Cross-Site Scripting |
| **XXE** | XML External Entity |

## Executive Summary

This deliverable reports the work done in T7.1, whose purpose is the identification of a series of suitable security and privacy metrics to evaluate the security of an ICT system. The metrics have been obtained taking into account current standards, best practices, regulation and initiatives, and they have been defined in an objective and measurable way, avoiding metrics difficult to calculate and that could be misunderstood by different analysers. To provide measurable metrics, they are evidence based, capable of being measured with testing strategies. The set of metrics and security claims will set up a common basis for measuring security, providing harmonization and mutual recognition between different certification schemes. This task has been closely related with the other WPs (WP2, WP3, WP4, WP5 and WP6), taking into account the vulnerabilities and threats identified, as well as the standards and initiatives related with them. For privacy, current regulations and laws has been considered to define such metrics and claims. To this aim, compliance approaches to data protection key EU Directives and Regulations have been investigated. This task is going to serve as input for the definition and implementation of the methodology in T7.2 and T7.3, as well as for other WPs such as WP3, WP4, WP5 and WP6.

## Project Summary

Nowadays most of the ICT solutions developed by companies require the integration or collaboration with other ICT components, which are typically developed by third parties. Even though this kind of procedures are key in order to maintain productivity and competitiveness, the fragmentation of the supply chain can pose a high risk regarding security, as in most of the cases there is no way to verify if these other solutions have vulnerabilities or if they have been built taking into account the best security practices.

In order to deal with these issues, it is important that companies make a change on their mindset, assuming an “untrusted by default” position. According to a recent study only 29% of IT business know that their ecosystem partners are compliant and resilient with regard to security. However, cybersecurity attacks have a high economic impact and it is not enough to rely only on trust. ICT components need to be able to provide verifiable guarantees regarding their security and privacy properties. It is also imperative to detect more accurately vulnerabilities from ICT components and understand how they can propagate over the supply chain and impact on ICT ecosystems. However, it is well known that most of the vulnerabilities can remain undetected for years, so it is necessary to provide advanced tools for guaranteeing resilience and also better mitigation strategies, as cybersecurity incidents will happen. Finally, it is necessary to expand the horizons of the current risk assessment and auditing processes, taking into account a much wider threat landscape. BIECO is a holistic framework that will provide these mechanisms in order to help companies to understand and manage the cybersecurity risks and threats they are subject to when they become part of the ICT supply chain. The framework, composed by a set of tools and methodologies, will address the challenges related to vulnerability management, resilience, and auditing of complex systems.

## Partners

## Disclaimer

The publication reflects only the author´s view and the European Commission is not responsible for any use that may be made of the information it contains.

## Table of Contents

## List of Figures

## List of Tables

# 1. Introduction

Nowadays most of the Information and communications technology (ICT) solutions developed by companies require the integration or collaboration with other ICT components, which are typically developed by third parties. Even though this kind of procedures are key in the process of maintaining productivity and business competitiveness, the fragmentation of the supply chain can pose a high risk regarding security. In most of the cases within ICT supply chains, there are no standardised and suitable procedures to verify if third party solutions have vulnerabilities or if they have been built taking into account the best security practices. The BIECO project builds on this assumption and aims to develop a holistic framework that will provide these mechanisms in order to help companies to understand and manage the cybersecurity risks associated threats. These aspects are of interest for businesses that aim at becoming part of the ICT supply chain and therefore join a digital ecosystem.

One of the main mechanisms to manage security is the design of a security evaluation and certification methodology to measure the security achieved by the ICT system. Although the definition of such a methodology presents a lot of different challenges that will be analysed in T7.2, the first problem we encounter is the definition of *what* we should evaluate. A security evaluation approach takes as starting point a set of claims against which the Target of Evaluation (TOE) will be assessed [1]. The TOE can be a system or a system component such as software application or hardware resource.

In general, the broad range of existing security certification approaches, security standards, best practices, regulations, etc. [2], leads to a disharmonized landscape of solutions, thereby making security requirements difficult to understand. Further on, this heterogeneity makes the security comparison unfeasible because each approach uses different claims and metrics to evaluate the security of the TOE. Additionally, one of the major flaws is the lack of consistent security metrics [3]. The security level of a certain system must be quantitatively measured by certain metrics to obtain a more accurate security view. However, some of these metrics, such as likelihood, are difficult to measure because of their complexities, and some of them are subjective, as they depend on the security expert's opinion [4] [5].

This deliverable is intended to serve as a baseline for the definition of such evaluation methodology, providing a set of objective and testable security claims obtained from current literature, standards and regulations. These objectives can be used by a security evaluator as a starting point for security assessment (certification, self-assessment, security by design, etc.) with the possibility of complementing the current goals with more specific ones. In this way, the security evaluation process is streamlined, as it has a generic starting point applicable to any domain, making the work of the evaluators easier.

## 1.1. Structure of the document

The document is organised as follows: Section 0 describes the methodology followed for the claims collection, Section 0 lists the sources (standards, regulation and other initiatives) that have been considered for the collection of the claims and metrics. Section 4 describes the main taxonomies for classifying security properties and threats, as well as the approach followed to classify the claims collected, which are presented in Section 5, and detailed in Annex 1. Section 6 presents an overview of different groups of collected claims collects the artefacts produced in the deliverable, Section 0 summarises the conclusions obtained from the deliverable and Section 0 lists the references.

## 2. Methodology

In this section, we describe the methodology followed in T7.1 to gather the claims. The methodology is composed of five main steps, as shown in Figure 1, and it has been performed iteratively, after selecting a taxonomy for the claims:

- **Select Security and Privacy Sources:** This step aims at selecting the most promising sources for gathering Security and Privacy claims, taking into account that they have to be objective and testable, as well as general enough to be applied in any kind of scenario. The aim is that, based on the experience and knowledge, each partner involved in Task 7.1 can select sources taking into account the BIECO's primary mission of assuring trust in case of malicious intrusions and the needs of the use cases considered within the project. The selected sources are then grouped in:
    - Standards
    - Legal Frameworks
    - Other sources (State-of-the-Art Documents)
- **For each source S:** A specific source S is selected.
    - **Analyse S and extract Claims:** Each selected source S is then described and motivated for its inclusion in the list of relevant sources. From the source S, we then extract a set of security and privacy claims ensuring that they are objective, testable and general.
    - **For each claim C**: A specific claim C is then selected.
        - **Analyse and classify C:** The claim C is analysed, providing tests to verify its compliance in a system and classifying it according to the taxonomy selected (STRIDE) in Section 4.
    - **End for**
- **End for**

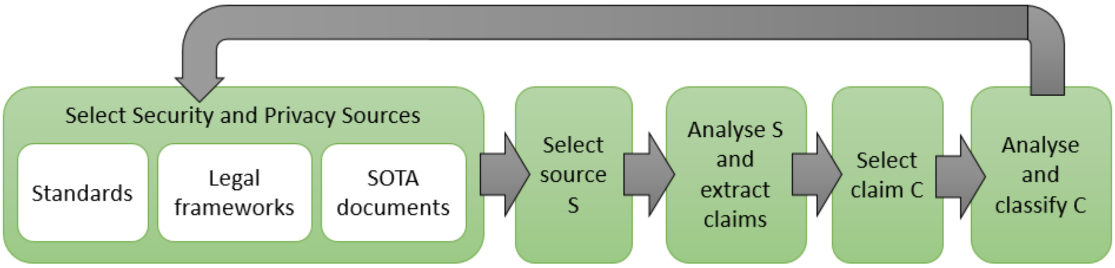

**Figure 1 Methodology followed in T7.1 to gather the claims**

During the application of our iterative methodology, we have identified and collected claims from:

- 10 Standards, which are listed in Section 3.1,
- 2 Legal Frameworks (one Regulation, the GDPR, and one Directive, the ePrivacy), which are listed in Section 3.2, and
- 11 Other Sources (State-of-the-Art Documents), which are listed in Section 3.3.

By applying the defined methodology, we have identified, analysed and selected more than 123 claims classified following the STRIDE classification [6]. In particular, and as it will be discussed in Section 4, we classified the selected claims in six different categories, which are the ones from STRIDE but in a positive way, in terms of desirable security objectives: Authentication, Integrity, Non-Repudiation, Confidentiality, Availability, and finally Authorization.

Table 1 reports for each category the number of the selected claims. It is worth noting that some claims apply for more than one category, so it may be repeated claims. More details about the selected Security and Privacy claims are reported in Section 5.

**Table 1 Number of collected claims**

| STRIDE Category | Number of Claims |
|---|---|
| Authentication | 23 |
| Integrity | 25 |
| Non repudiation | 9 |
| Confidentiality | 27 |
| Availability | 20 |
| Authorization | 19 |
| **Total Number of Claims** | **123** |

**Table 2 Collected claims per source**

| Source | Number of Claims |
|---|---|
| Standards | 51 |
| Legal frameworks | 7 |
| Other | 54 |

# 3. Sources for the collection of the security and privacy claims

This section describes the main sources (standards, regulations, state of the art documents) that were used for the collection of the security and privacy claims. The objective of this section is not to reach completeness, but rather set a valid establishment of a base that can be used to evaluate the security of a system. This establishment is complementary to more specific metrics and claims, since the generality of the proposed set does not allow comprehensively addressing all the security aspects of any type of system.

The sources have been selected based on the experience and knowledge of the different partners involved in this task, arguing for each source why it has been decided to take into account and why each source is important in the BIECO project. We gave special importance to European regulations and standards, and to those sources related with the IoT, which is usually the weakest point of the system. Given the overlap in scope between different standards, multiple claims have been grouped in order to provide a unified view of the general claims.

## 3.1. Standards

In this section are reported the set of standards that have been considered to obtain security and privacy claims. Each standard includes a description and the motivation for being chosen.

### 3.1.1. ISA/IEC 62443

The ISA/IEC 62443 [7] standard is an international standard from the International Electrotechnical Commission (IEC), which defines terminology, concepts and models for the *security of industrial automation and control systems* (IACS). In particular, it describes the *Security Life Cycle of the IACS* and *Security risk assessment for system design* for addressing the cybersecurity risks in an IACS, including the use of Zones and Conduits, and Security Levels. The *Security Life Cycle of the IACS* is composed of three phases: 1) *Assessment*, that includes activities to identify high-level risks, to carry out vulnerability and low-level risk analyses, to allocate the minimum IT security requirements for each component of System; 2) *Implementation*, which represents the set of activities needed to identify IT risks and define the related mitigations that make up the security strategy, to protect industrial systems; 3) *Maintenance*, that includes maintenance actions that constitute a process of constant monitoring of the security level of components, which allows the transmission of data to be shared safely to the outside. The *Security Life Cycle of the IACS*, also includes *threat modelling* to identify data flows, trust boundaries, attack vectors, and potential threats to the control system.

The standard is arranged in four groups: 1) General, 2) Policies and Procedures, 3) System, and 4) Component. Group three, which includes system security requirements, and group four, encompassing technical security requirements and secure product development lifecycle requirements, are the parts of the standard which are more relevant for the definition of security claims.

IACS are often integrating Commercial off-the-shelf (COTS) technologies and are always increasingly connected. These two aspects expose IACS to similar vulnerabilities as information systems. ISA/IEC 62443 series of standards can be used by a product supplier to implement a security development lifecycle, and to develop IACS systems and components that are secure by design and offer security by default. Therefore, this standard is selected as a source for the identification of security issues and for the subsequent derivation of security claims to improve the security of a system based on the security recommendations of the standard.

### 3.1.2. ISO 26262

ISO 26262 mentions simulation of systems as a way of testing the system's safety against attacks. For the particular testing of the behaviour against faults and failures, the degree of simulation details for the virtual evaluation is not fixed. This enables freedom of the usage of simulation models that are evaluated under a fault injection treatment. Namely, reaction of systems in general and ICT systems or safety critical systems in particular under fault injection testing in a simulated environment can be analysed by executing abstract simulation models or more concrete ones. The simulation models can start from a very abstract behaviour that express a correlation between input and output values and become more concrete by integrating more details of the behaviour. ISO 26262-1 [8] applies to all activities during the system lifecycle of safety critical systems, including development of software components and for this reason it is relevant for investigating the use of simulation for software testing and extracting claims that can support the usage of simulation for testing of software systems.

Model-based development that is "development that uses models to describe the functional behaviour of the elements to be developed", states that depending on the level of abstraction used, the model can be used for simulation, code generation or both. Overall, simulation is a part of the verification activities that is "determination whether an examined object meets functional requirements". Performing verification is an example indicative of a good safety culture which supports the ultimate trust. Within the ISO 26262 series, Simulation is an activity that supports system and software verification. This standard can guide the definition of safety claims that support security attributes of systems through interplay of simulation activities in the testing phase. The covered attributes are: availability, while at the same time determine claims which impact security such as linked to redundancy aspects of safe architecture.

### 3.1.3. IEC 61508

In IEC 61508 [9], Simulation is a recommended technique for assuring the quality of design and development of systems standardized by the IEC. Simulation is used for avoiding the introduction of faults within a system and for avoiding faults during safety validation. Within IEC 61508 Simulation is listed as a technique with a variable degree of effectiveness used in the avoidance of systematic failures. A low effectiveness is achieved when the modules are modelled and a high effectiveness is achieved when the components are modelled. Generally, functional and black box testing of safety-related software components can be used to verify against models of simulated processes. In this sense, simulation approaches can be coupled with automated testing tools. Review of this standard facilitates the collection of claims that address the simulation aspects involved in product development and testing.

### 3.1.4. ISO 13849

ISO 13849 [10] provides guidelines for assuring safety of mechatronic systems. More specifically, ISO 13849-1 provides guidelines for safety-related part of the control system (SRP/CS) design, while ISO 13849-2 provides guidelines for the validation of functional safety. Overall, the reliability of a safety function execution is evaluated by the performance level (PL) measure. Computation of the PL of a safety function is based on system behaviour analysis when one or more component the SRP/CS fail.

The failures that need to be considered for the analysis are standardized. The PL is then used to verify that a mechatronic system is functional safe, by checking that the PL of the SRP/CS is greater or equal to the required performance level of the overall system. The required performance level is derived a priori by performing a risk assessment. The review of this standard facilitates the collection of claims that support the risk mitigation.

### 3.1.5. ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701

ETSI EN 303 645 [11] describes a standard for cybersecurity in the Internet of Things. This document specifies 13 cybersecurity provisions for IoT devices and services, establishing a security baseline for this kind of products and providing a basis for future IoT certification schemes. Inside we will find guides and examples for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. This standard is designed to prevent attacks against smart devices, also includes data protection for consumers and will be complemented by the European Telecommunications Standards Institute (ETSI)1 with the development of a test specification and an implementation guide.

Recently, in December 2020, the ETSI TS 103 701 was released, which specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI TS 103 645 / ETSI EN 303 645, addressing the mandatory and recommended provisions as well as conditions and complements these two ETSI standards.

This recent standard, which is based on the predecessor ETSI TS 103 645, represents a strong baseline in security and privacy in a context (IoT) where the lack of standards and security requirements is evident. Whereas this standard primarily helps to protect consumers, identifying IoT devices that are sufficiently secure, other users of the IoT environment benefit from the implementation of those provisions. In this sense, this source will provide some key inputs for the definition of security and privacy claims for such vulnerable devices that currently represent the most unprotected point of a system.

### 3.1.6. ISO 29100: Information technology — Security techniques — Privacy framework

The objective of this standard is to support organizations in defining the requirements to safeguard privacy in any system in which personally identifiable information is processed and to serve as a complement in the event that there are related legal considerations. Data considered in this standard includes the information that is linked

[1] Non-profit enterprise whose mission is to produce the telecommunications standards that will be used throughout Europe

to a real identity and therefore, can be used to distinguish one person from another (e.g., national identity number, bank accounts, biometric data, etc.).

ISO / IEC 29100: 2011 [12] provides a high-level framework for the protection of Personally Identifiable Information (PII) that enables organizations to define their privacy protection requirements by specifying common terminology, the definition of actors and their roles in data processing, the privacy requirements and the reference of a series of principles oriented to the management of the organizational, technical and procedural aspects of this strategy: Consent and choice, Purpose legitimacy and specification, Collection limitation, Data minimization, Use, retention and disclosure limitation, Accuracy and quality, Openness, transparency and notice, Individual participation and access, Accountability, Information security and Privacy compliance.

It is worth noting that this standard does not replace or conflict with local or international legislation aimed at protecting privacy (e.g., GDPR). On the contrary, it complements these actions and consolidates them through the establishment of transversal and strategic global actions that allow the organization not only to cover current legal requirements but also other types of contractual, business variables and other factors related to private data that should be detected within the corporate risk management process. In this sense, the standard provides some guidelines regarding data protection that BIECO should take into account to enhance the privacy aspects of the system.

### 3.1.7. GlobalPlatform - Security Evaluation Standard for IoT Platforms (SESIP)

The SESIP standard [13] specifies requirements for the security evaluation of IoT platforms and parts thereof, including in particular a set of Security Functional Requirements, and the definition of Security Assurance Requirements packages that define five assurance levels. These requirements are based on the Common Criteria standard (ISO154080, v3.1), which it refines for the specific purpose of the evaluation of IoT platforms and parts thereof. Given the usefulness of common criteria, as well as its international recognition, BIECO should take these requirements into account to guarantee the security of the weakest points of the system, the IoT devices.

The set of documents also includes the definition of a scheme based on these requirements, which defines management rules such as the management of certificates and the accreditation of certification bodies and laboratories.

### 3.1.8. The digital standard

The Digital Standard [14] is a technical standard that provides a framework to measure consumer values like privacy, security, and ownership. In particular, it offers product testing criteria for software and smart devices, providing a source of testable and objective claims useful to BIECO. Consumers or manufacturers can use the standards to evaluate the extent to which a product protects various digital rights including consumer privacy, information security, freedom of speech, and product ownership.

Since the standard is a list of questions, anyone can answer the questions for any product to generate an evaluation. Supporters of the standard argue that the answers to the questions should either be obvious or the manufacturers should voluntarily disclose the answers. Goals of the standard include setting consumer expectations for how products should protect them, communicating acceptable practices to manufacturers, and encouraging conversations about what sorts of product behaviour are either beneficial or harmful to the consumers who use them. However, some of the security objectives considered in the standard, such as data security or user safety are still in progress to be defined.

### 3.1.9. OASIS eXtensible Access Control Markup Language (XACML)

The XACML standard [15] defines an attribute-based access control policy language as well as a reference architecture for the evaluation of the access requests according to the rules defined in the policy. An XACML policy encodes a specific statement of what is and is not allowed on the basis of a set of rules, defined in terms of conditions on attributes of subjects, resources, actions, and environment. It also contains specific combining algorithms for establish the precedence among the rules. Whereas, the XACML reference architecture is then composed of the following main components: i) Policy Enforcement Point (PEP) that receives the access request in its native format, constructs an XACML request and sends it to the Policy Decision Point (PDP); ii) Policy Decision Point (PDP) that evaluates the request against the XACML policy and returns the access response; iii) Policy Information Point (PIP) that represents a source of attribute values and iv) Policy Administration Point (PAP) that is the system entity in charge of managing the policies.

Within BIECO, XACML standard could be used as a reference Access Control (AC) System so as to have a reference AC system useful for managing authorization concerns. Consequently, in BIECO, we refer to the XACML standard as a good example of an authorization system. Indeed, the XACML architecture is considered as a reference architecture that most of the current authorization systems refer to or can be mapped to. Therefore, the claims gathered from this standard can be easily applicable and adaptable to the other authorization systems, with the objective of ensuring the correct implementation of the authorization mechanisms.

### 3.1.10. ISO 27001 - Information security management

ISO/IEC 27001:2013 [16] is the international standard that establishes the specification for an information security management system (ISMS). Its best-practice approach helps organisations manage their information security by addressing people and processes as well as technology.

The standard comprises 114 controls in 14 groups and 35 control categories: Information security policies, Organization of information security, Human resource security, Asset management, Access control, Cryptography, Physical and environmental security, Operations security, Communications security, System acquisition, development and maintenance, Supplier relationships, Information security incident management, Information security aspects of business continuity management and Compliance with internal requirements, such as policies, and with external requirements, such as laws. Therefore, this standard provides a very wide source of claims, covering very diverse aspects of security management that are necessary to guarantee the security of a system.

## 3.2. Regulation

In this section are reported the set of European regulations that have been considered to obtain security and privacy claims. Each regulation includes a description and the motivation for being chosen.

### 3.2.1. General Data Protection Regulation (GDPR)

Digitization has increased the volume of data collection and accelerated the flow of information about individuals. As this information can be used for various purposes, the European Union has adopted the General Data Protection Regulation (GDPR) [17] as a new framework superseding Data Protection Directive 95/46/EC. As the GDPR is a regulation, not a directive, it is directly binding and applicable, though it provides flexibility for certain aspects to be adjusted by individual EU Member States. This also implies that the requirements are sometimes vague or too open and therefore subject to interpretation.

The GDPR radically changed the regulation of private data protection; it conferred more rights to individuals and imposed more obligations on companies collecting and processing private data. The regulation is applicable not only to information service providers established in the EU but also to those who have their place of business outside the EU and process information about individuals located in the EU. Private data has to be processed lawfully and in a fair and transparent way. Collecting private data can be done only for a particular, explicit and lawful purpose. The data has to be appropriate, relevant and limited to the purposes for which it is being processed. Furthermore, it has to coincide with the facts and has to be up-to-date. Moreover, it can be stored no longer than the purpose allows it. Finally, the data must be protected with appropriate measures against unauthorized and unlawful processing as well as accidental loss, destruction and damage.

As one of the aspects that BIECO is addressing in this deliverable is the privacy, the GDPR represents the European basis of the privacy claims that should be considered for this aspect.

### 3.2.2. ePrivacy

ePrivacy [18] [19] regulates the Machine-to-Machine (M2M) communication especially in reference to the Exchange of Data (i.e., Confidentiality of the communication). It is referring to any data and not only to Private data. In the regulatory context, pairing the GDPR and the ePrivacy is becoming pivotal for promoting trustworthiness in services and products managing and exchanging (personal) data, and for guaranteeing both data subject’s rights and private life.

Therefore, by having a unique view of the currently applicable (and the upcoming) legal frameworks could make BIECO aligned with the currently ongoing discussions in Europe, about privacy and security of both individuals and communications. Indeed, both the GDPR and the new upcoming ePrivacy Regulation are part of the reform of the EU data protection framework, which include specific security obligations such as the “integrity and confidentiality” principle (Art. of the GDPR), and the “Confidentiality of the communications” (Art. 5 of the ePrivacy).

## 3.3. Other sources

In this section are reported the set of additional sources that have been considered to obtain security and privacy claims, with a special emphasis on the IoT context. Each source includes a description and the motivation for being chosen.

### 3.3.1. ENISA- Indispensable baseline security requirements for the procurement of secure ICT products and services

In this document [20] we find practical, technologically neutral information with clear, simple and sector-agnostic minimum necessary indispensable requirements for secure ICT products and services. Any ICT product or service that does not comply with one or more of the minimum requirements of this document should be considered insecure, as reported by ENISA. It focusses on a few indispensable conditions, based on standards and expert consensus. However, it is not intended to substitute existing secure certifications schemes and standards, but a complementary security baseline.

Based on these requirements, the European Cyber Security Organisation (ECSO) has created the *cybersecurity made in Europe* label [21], whose aim is to promote European cybersecurity companies and increase their visibility in the European and global market, serving as a global differentiator. It is granted only to European cybersecurity companies from the European Union (EU), European Free Trade Association and European Economic Area countries, as well as from the United Kingdom. These companies must demonstrate, among other requirements, that they are conformity with ENISA's 'Indispensable baseline security requirements for the procurement of secure ICT products and services'. Therefore, this source of security claims for ICT products will be highly considered due not only to the involvement of well-known organizations and regulation entities such as ECSO or ENISA, but also due to the close relationship with this European cybersecurity label.

### 3.3.2. Japanese Cyber/Physical Security Framework

This framework [22] was created by the Working Group 1 (Systems, Technologies and Standardization) of the Japanese Ministry of Economy, Trade and Industry. This group is focused on the cyber/physical security in the new supply chains under the Society 5.0 policy and the Connected Industries policy. The security framework contains some guidelines for assuring security in supply chains from three different perspectives: Connections between organizations, Mutual connections between cyberspace and physical space and Connections in cyberspace. The document describes the three-layer model structure followed by the framework, a list of risk sources and security requirements to address these risks and some examples of the application of the security measures.

This framework represents a high Japanese government effort to improve the security of its products, quite in line with the European initiatives derived from the Cybersecurity Act[2]. This framework not only focuses on one of the crucial aspects in BIECO, such as

[2] This European regulation strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services

the supply chain, but also presents a point of view external to Europe and the United States (which are the typically considered ones) related to definition of security claims.

### 3.3.3. Carnegie Mellon University - Security and privacy label

Researchers from the University of Carnegie Mellon developed a security and privacy label [23] to share with consumers some general information regarding security and privacy of IoT devices, in an easy and understandable way. For more expert consumers, they include a second layer with more detailed information. Whereas the first layer (non-experts) is intended to be stuck on the product, the second layer can be accessible via a QR code.

The information reflected in the label includes security and best practices of smart devices and it was obtained not only from standard and guidelines, but also from studies and interviews with security and privacy experts from industry, academia, government and public policy organizations. The blocks considered comprises security mechanisms (updates, access control, security oversight, ports and protocols, hardware safety, personal safety, vulnerability disclosure and management, software and hardware composition and encryption and key management), data practices (data collection, type of sensor, frequency of collection, purpose, data stored, retention time, data sold and shared with external entities, data linkage, anonymity and privacy), as well as general information (manufacturer contact, functionality with no internet and no data processing and compatibility). Therefore, the information collected in this document is quite complete and although some aspects are quite difficult to measure in an objective way, and therefore, it should be considered to define the security and privacy claims for the security evaluation of a system.

### 3.3.4. ENISA: Guidelines for Securing the Internet of Things. Secure supply chain for IoT

This document [24] from ENISA[3] contains a series of recommendations and guidelines to help IoT manufacturers, developers, integrators and in general, to all stakeholders involved in the IoT supply chain, to build and deploy secure IoT technologies. The objective is to serve as a reference point for a secure IoT supply chain. The guidelines are complementary to other documents created by ENISA, such as the baseline IoT security recommendations (Section 3.3.5) and the secure software development lifecycle for IoT. It is structured in several chapters, identifying the threats (software and hardware) that could affect the IoT supply chain, enumerating a series of good practices and security measures to secure the supply chain and a set of guidelines in the format of good practices.

As the context of BIECO is the protection of the software supply chain, from the design to the runtime, this document should be highly considered for the security evaluation of a system, gathering the best practices and claims that ensures the correct functioning

[3] The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe

of the supply chain. Indeed, it was already considered in WP2, when defining the BIECO security requirements.

### 3.3.5. ENISA: Baseline Security Recommendations for IoT in the context of critical information infrastructures

This document [25] from ENISA focuses on critical information infrastructure, understood as those including facilities, networks, services and physical information technology equipment, which in case of disruption could bring major health, safety and economic consequences. It covers very sensitive vertical domains such as smart homes, smart cities and transport, smart grids, smart cars, smart airports and eHealth. In this regard, the document analyses the main critical assets associated with these domains, identifying possible threats and vulnerabilities and proposing a set of good practices and measures to avoid them and protect IoT systems.

The most interesting point of this document is the mapping that is carried out at the threat level with the critical assets that may be affected by it, which helps to infer security claims that have to be fulfilled to avoid these kind of attacks. In addition, it describes several attack scenarios detailing the steps taken by the attacker, the stakeholders involved and some very interesting metrics for the analysis of the associated risk, such as the impact or the ease of detection or the risk of cascading effect on other components, which is a very valuable information for the development of the security evaluation methodology that is going to be carried out within the WP7.

### 3.3.6. IETF: Best Current Practices for Securing Internet of Things Devices

In order to reduce frequency and severity of security incidents in embedded computing devices with Internet interfaces, this document [26] from the Internet Engineering Task Force (IETF)[4] includes a list of minimum requirements to take into account during the development of such devices and their firmware updates.

The measures described in this source focus on network-based attacks and are not intended to impede other kinds of attacks (e.g., physical access to the device). However, these are minimum requirements, that is, they are not sufficient by themselves. Therefore, vendors should analyse particular threats of each device to complement these measures.

Broadly speaking, the document includes considerations about device architecture, hardware and firmware component choices, operating system features, design and choice of protocols used to communicate, documentation and labelling. It is expected that this list of requirements will be revised from time to time, adding new threats identified and new security techniques. Nevertheless, this list represents for BIECO a list of best practices for one of the entry points of a system with less security (IoT devices) that is being maintained by the community of the IETF, which can be directly mapped to security claims.

[4] Open standards organization, which develops and promotes voluntary Internet standards

### 3.3.7. NIST SP 800-63B: Digital Identity Guidelines, authentication and lifecycle management

In the online services or transactions environment, the main representation of a subject is the digital identity. It is always unique in the context of a digital service, but does not mean that the subject's real-life representation is known. Regarding this, therefore, there are different opportunities for impersonation attacks and fraudulent claims of a digital identity.

This publication [27] focuses on providing guidelines and technical requirements related to implementation of digital identity services used by USA federal agencies and government systems. In particular, NIST SP 800-63B includes useful claims focused on authentication and lifecycle management, providing recommendations on the lifecycle of authenticators such as the expiration time of the authentication session that WP7 can use to build the basis of the certification methodology.

### 3.3.8. NIST SP800-30

The NIST SP 800-30 provides guidelines for conducting risk assessment in the Information Technology (IT) domain. It describes the process for conducting a risk assessment and provides in the appendices useful examples as a taxonomy of threat sources, threat events, vulnerabilities and predisposing conditions, and also how to establish the likelihood of threat event occurrence and risk determination. The risk assessment methodology of NIST 800-30 includes:

1. *a risk model* that defines key terms and risk factors;
2. *an assessment approach* which evaluates risk and its factors with quantitative, qualitative or semi-qualitative approaches;
3. *a risk assessment process* which is composed of four stages: **Prepare** for Risk Assessment, to identify the purpose and scope, assumptions and constraints; **Conduct** Risk Assessment, to identify the threat sources and events, vulnerabilities and related predisposing conditions, to determine the likelihood that the identified threat and the threat events would be successful; **Communicate and Share** Risk Assessment Results and **Maintain** Risk Assessment to monitor the risk factors and update the risk assessment;
4. *an analysis approach* that it is a description to identify and analyse risk factors in order to increase the coverage of the "problematic" space and it can be vulnerability-oriented, threat-oriented or asset/impact-oriented.

This document is a good reference for designing and developing a risk assessment process for BIECO and deriving security claims accordingly.

### 3.3.9. NISTIR 7628

NIST.IR 7628 *Guidelines for Smart Grid Cybersecurity* [28] provides guidelines for addressing cyber security for Smart Grid systems and their constituent hardware/software systems and components. It presents an analytical framework to help developing effective cybersecurity strategies: it describes methods and supporting information for risk identification and assessment, and application of appropriate security requirements. The risk assessment process for identifying high-level security requirements in this domain, is implemented in two different approaches: bottom-up and top-down. The document also addresses privacy issues and provides privacy-based recommendations for entities participating in the Smart Grid, and it also gives an overview of some existing privacy risk mitigation standards and frameworks. Finally, it presents an inventory of analysis and supporting references used to develop high-level security requirements, including classes of potential vulnerabilities which are classified by category, and describes specific security problems in this system architecture. It should be considered for the claims collection since it is a reference standard for the smart grid and its guidelines will be fundamental for the evaluation of BIECO solution over the use case pertaining to this domain.

### 3.3.10. OWASP

The Open Web Application Security Project (OWASP) [29] is a non-profit organization which provides publications and resources for developers about web application security field. Mainly, its popularity is based on the publication of TOP 10 security risks in web applications, named as OWASP TOP 10 list, which collects and defines the most common vulnerabilities considered as critical. Those ones are as follows[5]:

1. **Injection** occurs when untrusted data is sent to an interpreter as part of a query.
2. **Broken Authentication** refers to incorrect implementation of application functions related to authentication and session management.
3. **Sensitive Data Exposure,** due to not properly or weakly protection, could allow attackers to steal of modify the data.
4. **XML External Entities (XEE),** occurs when weakly configured XML parser process a XML input which containing a reference to an external entity and it could lead to the disclosure of confidential data or DoS.
5. **Broken Access Control**: improper application of the restrictions on what authenticated users are allowed to do.
6. **Security Misconfiguration**: it is the most common issue. It occurs when there are configurations that may impact the security of the application itself.
7. **Cross-Site Scripting (XSS):** Internet attack technique in which malicious code is executed either on the server or client side, in order to acquire sensitive data or digital identities.
8. **Insecure Deserialization**: User-controllable data is deserialized by a website provoking to remote code execution attacks.
9. **Using Components with Known Vulnerabilities** may undermine application defences and enable various attacks and impacts.
10. **Insufficient Logging and Monitoring** allows attackers to extract or destroy data, among other.

The list provided by OWASP, will allow us to prioritise security vulnerabilities as well as their relevance which facilitates their subsequent analysis for the developing of vulnerability management tools. Indeed, in BIECO (WP3) we already identify vulnerabilities taking into account the OWASP platform, as the most significant vulnerabilities are indicated. This list of vulnerabilities allow to define protection mechanisms and therefore security claims to protect a system against them.

[5] https://owasp.org/www-project-top-ten/2017/

### 3.3.11. Kantara - Information security management

Providing the data subjects means for managing personal and consent data is not only a strict adherence to the GDPR requirements: it is one of the cornerstones for building trusted business relationships. Thus, in BIECO, we exploit Consent Management Systems (CMS) to obey the EU regulation because it represents a justification for the processing of private data.

Consequently, among the best practices adopted in the CMS development, there is the definition of the consent according to specific formats, such as the one proposed by Kantara initiative[6]. Indeed, the initial “Consent Receipt Specification” [30] is currently being extended for satisfying the GDPR's obligations. In this draft version, named “GDPR Explicit Consent Record & Receipt Extension for Kantara CISWG: Consent Receipt”, the consent specification allows controllers to clearly specify, in a human-readable format, the requirements for: linking the consent to existing privacy notices and policies; describing which “information has been or will be collected, the purposes for that collection as well as relevant information about how that information will be used or disclosed.'” The peculiarity of this format is the possibility to be represented in a standard JSON format.

The initial proposal of the consent receipt specification is based on ISO 29100: Information technology — Security techniques — Privacy framework. Therefore, we can use both consent specifications (ISO 29100-based and the GDPR-based) as reference data format standard in BIECO for dealing with the Standard and EU Regulation, e.g., for encoding/testing the privacy and security claims.

[6] “Kantara Initiative operates conformity assessment, assurance and grant of Trust Marks against de-jure standards.” More information can be find at: https://kantarainitiative.org/

# 4. Classification of the security and privacy claims

The first step in building a secure and trusted system is to understand and identify the threats (if we think in negative) or the security and privacy objectives (if, on the contrary we think in positive). In fact, threats represent events that cause a system to respond in an unexpected or damaging way, and the security objectives represent the countermeasures established to avoid these threats [31]. An understanding of threats or security and privacy objectives can best be achieved by grouping them into categories [32]. The selection of an adequate classification for the identified security and privacy claims is the main purpose of this section. Furthermore, this classification is intended to serve as the basis of the security evaluation and certification methodology that will be developed in T7.2 and reported in D7.2.

It is important to mention that not all the claims and best practices included in the sources have been taken into account, since the base that we seek should be made up of objective claims, which do not depend on the personal opinion of a security expert (e.g., the usability of a graphical interface), and that can be evaluated through a test.

## 4.1. State of the art

Security threats can be observed and classified in different ways by considering different criteria like source, agents, and motivations. Threat classification helps identifying and organizing security threats into classes to assess and evaluate their impacts, and to develop strategies in order to prevent, or mitigate the impacts of threats on systems. Furthermore, threats classification allows evaluation and estimation of threats risks. It allows classifying threats into categories in order to group them by characteristics and suggest appropriate counter measures.

According to [32], a threat classification should meet the following requirements:

- Mutually Exclusive: Every threat is classified in one category excludes all others categories because categories do not overlap. Every specimen of threat should fit in at most one category.
- Exhaustive: The categories in a classification must include all the possibilities. Every specimen should fit in at least one category.
- Unambiguous: All categories must be clear and precise in scope and description so that the classification is certain. Every category should be accompanied by clear and unambiguous classification criteria defining what specimens to be put in that category.
- Repeatable: Repeated applications of the taxonomy result in the same classification, regardless of who is classifying.
- Accepted: All categories are logical, intuitive and practices (easy to apply), so they can be accepted by the majority.
- Useful: It can be used to gain insights of the field in which you are applying it, and it can be adapted to different application requirements.

In this sense, there are a wide variety of classification schemes of threats and security objectives. We review and analyse here some of the most well-known approaches in current literature, and also the ones mentioned in D2.1 [33].

### 4.1.1. The CIA triad

The CIA triad (Confidentiality, Integrity, and Availability) represents the basic classification of security objectives, possibly mentioned first by the NIST in 1977 [34]. However, it is still debated whether it is sufficient to handle rapidly changing technology and business requirements, with recommendations to consider expanding on the intersections between availability and confidentiality, as well as the relationship between security and privacy. In this sense, many experts usually add other principles [35] such as non-repudiation, privacy, authenticity and trustworthiness, accountability and auditability.

### 4.1.2. Network Security Threat Classification

Focusing on threats, more than in security objectives, the Network Security Threat Classification proposed in [36] considers four different types of threats:

- Unstructured Threats, caused by inexperienced individuals that uses hacking tools such as shell scripts and password crackers.
- Structured Threats, caused by highly motivated and competent hackers. In this case, the techniques and tools used are more sophisticated and complex.
- External Threats, caused by unauthorized individuals or organizations working outside of a company.
- Internal Threats, caused by an authorized individual (e.g., an account on a server or physical access to the network).

This classification is highly intuitive, allowing to identify and classify network threats and vulnerabilities. However, some of the categories overlap; for example, a threat caused by an inexperienced user can be either external or internal. Moreover, this classification did not cover all threats, as they just present network security threats.

### 4.1.3. ISO 7498-2

The ISO 7498-2 [37] standard has listed five major security threats and services as a reference model:

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal or loss of information and/or other resources
- Disclosure of information
- Interruption of services

This classification is mutually exclusive, but it is highly focused on information threats, and it does not cover all threats consequences.

### 4.1.4. STRIDE

STRIDE [38] is a model of threats developed by Praerit Garg and Loren Kohnfelder at Microsoft for identifying computer security threats. It provides a mnemonic for security threats in six categories, which can be understood in a positive way with its associated security property (Table 3).

The STRIDE model is a simple and a very popular threat model, and highlights many top threats. Besides, this classification allows organizing a security strategy to reduce risks. On the other hand, the STRIDE model includes a non-exhaustive list of threats.

**Table 3 STRIDE categories**

| Threat | Security objective |
|---|---|
| Spoofing | Authenticity |
| Tampering | Integrity |
| Repudiation | Non-repudiability |
| Information disclosure | Confidentiality (and privacy) |
| Denial of Service | Availability (and fault tolerance and robustness) |
| Elevation of Privilege | Authorization |

### 4.1.5. Web Application Security Consortium Threat Classification

Web Application Security Consortium Threat Classification [39] classifies threats in six categories:

- Authentication category covering attacks that target a web site's method of validating the identity of a user, service or application (e.g., Brute Force, Insufficient Authentication, Weak Password Recovery Validation).
- Authorization category covering attacks that target a web site's method of determining if a user, service, or application has the necessary permissions to perform a requested action (e.g., Credential/Session Prediction, Insufficient Authorization, Insufficient Session Expiration, Session Fixation).
- Client-Side Attacks category focused on the abuse or exploitation of a web site's users (e.g., Spoofing, Cross site Scripting).
- Command Execution category covering attacks designed to execute remote commands on the web site (e.g., Buffer Overflow, Format String Attack, LDAP Injection, OS Commanding, SQL Injection, SSI Injection, XPath Injection).
- Information Disclosure category covering attacks designed to acquire system specific information about a web site (e.g., Directory Indexing, Information Leakage, Path Traversal, Predictable Resource Location).
- Logical Attacks category focused on the abuse or exploitation of a web application's logic flow (e.g., Abuse of Functionality, Denial of Service, Insufficient Anti-automation).

This model is quite flexible and shows the direct impact on security requirements if a threat happens, which help to make appropriate countermeasures. However, the list is not exhaustive, as it is focused on web site threats.

### 4.1.6. NIST Threat Classification

NIST Threat Classification [40] focuses on threats significance criteria and considers the following types of security threats:

- Errors and Omissions, caused by intentional human mistakes.

- Fraud and Theft, which can be performed by simply automating traditional forms of fraud and theft (e.g., small transactions that will not be checked as suspicious).
- Employee Sabotage, e.g., destroying hardware of facilities, planting logic bombs that destroy programs or data, entering data incorrectly, changing data.
- Loss of Physical and Infrastructure Support, including power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes.
- Malicious Hackers, that is, people who break into computers without authorization. This threat comes either from outsiders or insiders.
- Industrial Espionage which involves gathering of proprietary data from private companies or the government for the purpose of aiding another company.
- Malicious Code, e.g., viruses, worms, Trojan horses and logic bombs.
- Foreign Government Espionage, including threats posed by foreign government intelligence services.
- Threats to Personal Privacy, which can arise from many sources (e.g., the accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies).

However, this list is not exhaustive, and some threats may combine elements from more than one area.

## 4.2. Classification approach for the BIECO claims

Based on the limitations and advantages of current taxonomies, analysed in the previous section, we decided to adopt the STRIDE classification. On the one hand, STRIDE is a simple and popular threat model that has the flexibility to classify the identified claims both in a positive (desired security property) or negative (threat) way. Furthermore, D2.1, which establishes the basis of the BIECO project requirements and objectives, also uses STRIDE as a basis to classify the supply chain threats, so this way, we can align the D7.1 claims and the methodology that will be developed in T7.2 with the BIECO requirements and identified threats.

As the claims are intended to be a set of security best practices that the system should implement, the STRIDE taxonomy has been adopted in a positive way. Therefore, we consider the following categories:

- **Authentication:** means that the claim of identify is verified.
- **Integrity:** means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.
- **Non repudiation**: implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.
- **Confidentiality:** information is not made available or disclosed to unauthorized individuals, entities, or processes. While similar to privacy, the two words aren't interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers.

- **Availability:** This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.
- **Authorization:** means that there are security mechanisms to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features.

In order to enhance the definition of the claims, we also consider the *impact* dimension that can happen as a consequence of not fulfilling a specific security claim, such as privacy leakage or safety issue with human life losses. Moreover, impact is usually considered when evaluating the risk of a vulnerability and therefore, it would be useful for the security evaluation methodology that will be developed in T7.2.

The impact cannot be considered in a single dimension, as a security failure can have different impacts over the system. In particular, and following approaches such as MoRA [41], OWASP (Section 3.3.10) or EVITA [42] and HEAVENS [43] projects, we consider the following categorisation for impact:

- **Safety:** unwanted/unauthorized interference with system or communications that may impact on the safe operation of the system.
- **Financial:** unwanted/unauthorized commercial transactions, or access to the system that may imply theft of the system, intellectual property infringement, damage to manufacturer reputation or warranty fraud, among others.
- **Operational:** unwanted/unauthorized interference with the system or communications that may impact on the operational performance of the system (without affecting physical safety).
- **Privacy and legislation:** unwanted/unauthorized acquisition of data relating to system activity, user identity data, or system design and implementation, and non-compliance with the relevant legislations.

## 5. Overview of the security and privacy claims

This section groups all the security and privacy claims collected from the selected sources reported in Section 2. Towards this end, we propose a template for collecting all the valuable information for each claim. In particular the collected information was:

- ID: a unique identifier to facilitate the identification and referral of the claims and dependencies within this deliverable.
- Claim: the name of the claim.
- Metrics: the data collected to measure the compliance of the claim.
- Dependencies: if the compliance of the claim depends on another claim.
- Possible test(s): proposed test(s) to validate if a system is compliant with the claim and obtain the metrics.
- Conditions to fail: observable issues to decide if the test fails.
- Conditions to pass: observable issues to decide if the test passes (or collected information if not applicable).
- Keywords: related words to facilitate the classification of the claim.
- Classification: STRIDE category to which the claim belongs to.
- Impact: type of impact that the non-fulfilment of the claim would cause on the system.
- Sources: sources in which this claim is considered.

A more detailed description of the claims can be found in Annex 1, whereas a brief overview is provided here.

### 5.1. Authentication claims

This claim's group is focused on the verification of the necessary access control mechanism to protect the access to the TOE, its updates, interfaces and services. Moreover, this group also checks the strength of the authentication mechanisms used and its resistance against well-known attacks such as brute force or side channel attacks. Table 4 collects the claims associated with the authentication group.

We included also general claims that could affect to authentication, such as the presence of vulnerabilities in the used libraries or the strength of dependent mechanisms (e.g., random bit generators).

**Table 4 Authentication claims**

| ID | Description | Type of source[7] |
|---|---|---|
| **C3** | Update software files should be authenticated. | S/O |
| **C5** | The exchanged messages in the communication should be integrity protected | S/O |
| **C6** | Automatically generated passwords should be unique. | S/O |
| **C7** | Passwords should avoid common patterns. | S |
| **C8** | Passwords are not obviously linked to public information. | S/O |

[7] S=Standard, R=Regulation, O=Other

| | | |
|---|---|---|
| **C9** | Passwords should be strong in terms of complexity. | S/O |
| **C10** | The changes of the authentication values for user authentication are successful. | S |
| **C15** | Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface. | S/O |
| **C16** | The system should have a mechanism available which makes brute-force attacks on authorization mechanisms via network interfaces impracticable. | S/O |
| **C20** | Authentication mechanisms must use strong passwords. | S/O |
| **C42** | Connections to remote services, interfaces, and end-points should be cryptographically authenticated. | O |
| **C43** | The software should not use unsafe libraries that contain vulnerabilities. | O |
| **C45** | Protocols and libraries used by the system are updated. | S |
| **C46** | Authentication protocols should be secure, using recommended algorithms. | S/O |
| **C47** | Authenticated sessions should expire, and a new re-authentication required. | O |
| **C48** | Random bit generators should be strong enough. | O |
| **C49** | Authentication algorithms should avoid channel side attack. | O |
| **C58** | The system shall enforce a limit of consecutive invalid login attempts during a time period. | S/O |
| **C59** | The system shall notify, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon. | O |
| **C61** | The system shall uniquely identify and authenticate users. | O |
| **C62** | The system shall uniquely identify and authenticate a defined list of devices before establishing a connection. | O |
| **C66** | The system shall lock the session after a configurable time period of inactivity. | S |
| **C71** | The system shall terminate a remote session at the end of the session or after a period of inactivity. | O |

## 5.2. Authorization claims

This claim's group is focused on the verification of the necessary mechanism to ensure that only authorized users/entities can access to the services and data of the TOE. Moreover, this group also checks the strength of the authorization mechanisms used, as well as the compliance with the XACML standard.

One important aspect covered in this group are he metrics related with the authorized access to the private data stored and shared with the TOE, following the GDPR regulation.

As before, we also included general claims that could affect to authorization, such as the presence of vulnerabilities in the used libraries or the strength of dependent mechanisms (e.g., random bit generators). Table 5 collects the claims associated with the authorization group.

**Table 5 Authorization claims**

| ID | Description | Type of source |
|---|---|---|
| **C18** | All unused network interfaces shall be disabled. | S/O |
| **C25** | Lawfulness of processing of personal data. | S/R |
| **C26** | Personal data must be processed for a specific purpose. | S/R/O |
| **C27** | The system should allow data subject to access its personal data | S/R/O |
| **C33** | The adopted XACML-based authorization mechanism (PDP) must implement the mandatory functionalities of the XACML standard specification language. | S |
| **C34** | The access control mechanism (PDP) that evaluates the authorization requests against a policy must correctly implement the policy. | S |
| **C35** | The adopted XACML access control policy must be correct with respect to a specification (model) of the access control rights. | S |
| **C40** | Endpoints should only run applications or services whose TCP or UDP ports are described in the MUD profile. Unnecessary interfaces, and services should be disabled. | S/O |
| **C41** | A MUD file should be provided in accordance with MUD RFC. | S/O |
| **C43** | The software should not use unsafe libraries that contain vulnerabilities. | O |
| **C45** | Protocols and libraries used by the system are updated. | S |
| **C48** | Random bit generators should be strong enough. | O |
| **C51** | The system should allow data subject to modify its personal data. | R |
| **C52** | The system should allow data subject to delete permanently personal data concerning it. | R |
| **C53** | The system should allow data subject to withdraw its given consent | R |
| **C57** | The system shall enforce assigned authorizations for controlling the flow of information within the system and from interconnected systems. | O |
| **C65** | The system shall monitor events to detect attacks, unauthorized activities or conditions, and non-malicious errors. | S/O |
| **C71** | The system shall terminate a remote session at the end of the session or after a period of inactivity. | O |

| | | |
|---|---|---|
| **C73** | The system shall provide a proof of notice requirements for an explicit consent receipt for demonstrating compliance with the GDPR. | R/O |

## 5.3. Integrity claims

This claim's group is focused on the verification of the necessary mechanisms to ensure that all the data stored and exchanged in any communications with the TOE is protected against modifications.

As before, we also included general claims that could affect to integrity, such as the presence of vulnerabilities in the used libraries or the strength of dependent mechanisms (e.g., random bit generators). Table 6 collects the claims associated with the integrity group.

**Table 6 Integrity claims**

| ID | Description | Type of source |
|---|---|---|
| **C2** | Update software files should be integrity protected. | S/O |
| **C5** | The exchanged messages in the communication should be integrity protected. | S/O |
| **C11** | Sensitive security parameters exchanged during the communication for the establishment of a secure association should be integrity protected. | S/O |
| **C12** | Stored sensitive security parameters should be integrity protected. | S/O |
| **C21** | Integrity mechanisms must be strong. | S/O |
| **C28** | The source code must not contain SQL injection vulnerabilities. | S/O |
| **C29** | The source code must not contain command injection vulnerabilities. | S/O |
| **C30** | The source code must not contain code injection vulnerabilities. | O |
| **C31** | The source code must not contain path traversal vulnerabilities. | O |
| **C32** | The source code must not use components with known vulnerabilities. | S/O |
| **C39** | Automatic updates should not change the network protocol interfaces in any way that is incompatible with previous versions. | O |
| **C43** | The software should not use unsafe libraries that contain vulnerabilities. | O |
| **C45** | Protocols and libraries used by the system are updated. | S |
| **C48** | Random bit generators should be strong enough | O |
| **C54** | The system shall implement mechanisms of protection from malicious code manipulation. | O |
| **C55** | The system shall update protection mechanisms whenever new releases are available. | O |

| | | |
|---|---|---|
| **C56** | The system shall prevent anyone from circumventing malicious code protection mechanisms. | O |
| **C60** | The system shall execute a fail-safe procedure upon the loss of communications with other systems. | O |
| **C61** | The system shall uniquely identify and authenticate users. | O |
| **C63** | The system shall isolate security functions from non-security functions. | O |
| **C64** | The system shall separate user functionalities from management functionalities. | O |
| **C65** | The system shall monitor events to detect attacks, unauthorized activities or conditions, and non-malicious errors. | S/O |
| **C68** | The system shall prevent messages from being received from external users or systems. | S |
| **C69** | The system shall operate in a degraded mode during a DoS event. | S |
| **C70** | The system shall limit the use of resources by security functions to prevent resource exhaustion. | S |

## 5.4. Availability claims

This claim's group is focused on the verification of the necessary mechanisms to ensure that the system is permanently in operation and no external faults can alter its normal functionality. A failure in the availability of the system can lead to significant monetary and operational losses.

As before, we also included general claims that could affect to availability, such as the presence of vulnerabilities in the used libraries or the strength of dependent mechanisms (e.g., random bit generators). Table 7 collects the claims associated with the availability group.

**Table 7 Availability claims**

| ID | Description | Type of source |
|---|---|---|
| **C4** | The update mechanism shall prevent downgrade. | S |
| **C22** | Resistance to DoS attacks. | S/O |
| **C23** | Data input validation. | S/O |
| **C28** | The source code must not contain SQL injection vulnerabilities. | S/O |
| **C29** | The source code must not contain command injection vulnerabilities | S/O |
| **C30** | The source code must not contain code injection vulnerabilities. | O |
| **C31** | The source code must not contain path traversal vulnerabilities. | O |
| **C32** | The source code must not use components with known vulnerabilities. | S/O |

| | | |
|---|---|---|
| **C39** | Automatic updates should not change the network protocol interfaces in any way that is incompatible with previous versions. | O |
| **C43** | The software should not use unsafe libraries that contain vulnerabilities. | O |
| **C44** | Device should remain operating and locally functional in the case of a lost network connection. | S/O |
| **C45** | Protocols and libraries used by the system are updated. | S |
| **C48** | Random bit generators should be strong enough. | O |
| **C50** | System should work in case of power outage. | S |
| **C55** | The system shall update protection mechanisms whenever new releases are available. | O |
| **C56** | The system shall prevent anyone from circumventing malicious code protection mechanisms. | O |
| **C60** | The system shall execute a fail-safe procedure upon the loss of communications with other systems. | O |
| **C67** | The system shall set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. | S |
| **C69** | The system shall operate in a degraded mode during a DoS event. | S |
| **C70** | The system shall limit the use of resources by security functions to prevent resource exhaustion. | S |

## 5.5. Confidentiality claims

This claim's group is focused on verifying that any data or message exchanged or stored in the TOE is protected against prying attackers and sniffers. This not only guarantees data privacy, but also prevents an attacker from obtaining additional information useful to plan a future attack.

As before, we also included general claims that could affect to confidentiality, such as the presence of vulnerabilities in the used libraries or the strength of dependent mechanisms (e.g., random bit generators). We also include claims derived from the currently applicable EU legal framework (i.e., the GDPR) so as to guarantee lawfulness processing of personal data. Table 8 collects the claims associated with the confidentiality group.

**Table 8 Confidentiality claims**

| ID | Description | Type of source |
|---|---|---|
| C0 | Update software files should be encrypted and be transmitted using encryption. | S/O |
| C2 | Update software files should be encrypted using strong keys and algorithms. | S/O |
| C6 | Automatically generated passwords should be unique. | S/O |
| C7 | Passwords should avoid common patterns. | S |

| | | |
|---|---|---|
| C8 | Passwords are not obviously linked to public information. | S/O |
| C9 | Passwords should be strong in terms of complexity. | S/O |
| C13 | Stored critical security parameters should be ciphered. | S/O |
| C14 | Ciphered communications should use strong algorithms. | S/O |
| C17 | Critical security parameters should be encrypted in transit, with such encryption appropriate. | S/O |
| C19 | The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography. | S/O |
| C24 | Data Communications should be ciphered. | S/O |
| C25 | Lawfulness of processing of personal data. | S/O |
| C26 | Personal data must be processed for a specific purpose. | S/R/O |
| C27 | The system should allow data subject to access its personal data. | S/R/O |
| C28 | The source code must not contain SQL injection vulnerabilities. | S/O |
| C29 | The source code must not contain command injection vulnerabilities | S/O |
| C30 | The source code must not contain code injection vulnerabilities. | O |
| C31 | The source code must not contain path traversal vulnerabilities. | O |
| C32 | The source code must not use components with known vulnerabilities. | S/O |
| C43 | The software should not use unsafe libraries that could derive on vulnerabilities. | O |
| C45 | Protocols and libraries used by the system are updated. | S |
| C48 | Random bit generators should be strong enough. | O |
| C51 | The system should allow data subject to modify its personal data. | R |
| C52 | The system should allow data subject to delete permanently personal data concerning it. | R |
| C53 | The system should allow data subject to withdraw its given consent | R |
| C57 | The system shall enforce assigned authorizations for controlling the flow of information within the system and from interconnected systems. | O |
| C68 | The system shall prevent messages from being received from external users or systems. | S |

## 5.6. Non repudiation claims

This claim's group is focused on in verifying that the transactions are registered and it is not possible to attempt against this registry to erase traces of malicious activities. It also involves aspects related to explicit consent (as defined in the GDPR), so that both parties are aware (and thus be recorded) of the conditions.

As before, we also included general claims that could affect to confidentiality, such as the presence of vulnerabilities in the used libraries or the strength of dependent mechanisms (e.g., random bit generators). Table 9 collects the claims associated with the non-repudiation group.

**Table 9 Non repudiation claims**

| ID | Description | Type of source |
|---|---|---|
| C43 | The software should not use unsafe libraries that contain vulnerabilities. | O |
| C45 | Protocols and libraries used by the system are updated. | S |
| C48 | Random bit generators should be strong enough. | O |
| C61 | The system shall uniquely identify and authenticate users. | O |
| C62 | The system shall uniquely identify and authenticate a defined list of devices before establishing a connection. | O |
| C65 | The system shall monitor events to detect attacks, unauthorized activities or conditions, and non-malicious errors. | S/O |
| C66 | The system shall lock the session after a configurable time period of inactivity. | S |
| C72 | Logs should be protected against removal. | O |
| C73 | The system shall provide a proof of notice requirements for an explicit consent receipt for demonstrating compliance with the GDPR. | R/O |

## 6. Artefacts

Table 10 shows the artefacts produced in this deliverable.

**Table 10 Artefacts**

| Name | Description |
|---|---|
| Sources | List of standards, regulation and best practices useful to create a basic set of objective security claims to evaluate the security of a system. |
| Security claims | List of basic security claims obtained from the previous sources covering different aspects such as confidentiality, integrity, authentication, authorization and non-repudiation. The selected claims are intended to be objective enough to be evaluated empirically. |

# 7. Conclusions

This deliverable reports the collection of an objective, measurable, testable and general set of security and privacy claims. For this, diverse sources have been considered, such as standards, regulations or state-of-the-art documents (best practices, recommendations, etc.). Each of the sources has been analysed in detail to extract valid claims from it.

While the set obtained is designed so that a security evaluator has a starting point, thereby streamlining said process, it should be understood as something complementary to more specific claims of the system, since the generality of the proposed set does not allow comprehensively addressing all the security aspects of any type of system.

This deliverable, as well as the selected set of claims, will serve as input for task 7.2, focused on the design of a security assessment methodology. It will also provide a basic set of possible vulnerabilities to other WPs such as WP3, WP4, WP5 and WP6.

## 8. References

[1] ECSO, "European Cyber Security Certification A Meta-Scheme Approach v1.0." 2017.

[2] ECSO, "State of the Art Syllabus V2." 2017.

[3] AIOTI, *Report on Workshop on Security and Privacy in the Hyper-Connected World*. 2016.

[4] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, "A Survey of Cybersecurity Certification for the Internet of Things," *ACM Computing Surveys*, vol. 53, no. 6. Association for Computing Machinery, p. 115, Feb. 01, 2021, doi: 10.1145/3410160.

[5] ECSO, "European Cyber Security Certification - Assessment Options," 2019. Accessed: Jul. 01, 2021. [Online]. Available: https://ecs-org.eu/documents/publications/5ea49d3a940a3.pdf.

[6] MICROSOFT, *The {STRIDE} {Threat} {Model}*. .

[7] International Society of Automation, "New ISA/IEC 62443 standard specifies security capabilities for control system components," 2018, [Online]. Available: https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c.

[8] Virtual Open Systems, "ISO 26262:2011 Certification." http://www.virtualopensystems.com/en/company/vosysmonitor-iso26262-asilc/.

[9] IEC, "IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems," 2010. https://webstore.iec.ch/publication/22273 (accessed Jul. 01, 2021).

[10] ISO, "ISO 13849 - Safety of machinery — Safety-related parts of control systems," 2015. https://www.iso.org/standard/69883.html (accessed Jul. 01, 2021).

[11] E. T. C. on Cybersecurity, "ETSI EN 303 645 - ETSI releases world-leading Consumer IoT Security standard," 2020. https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard (accessed Jul. 01, 2021).

[12] ISO, "ISO/IEC 29100 - Information technology — Security techniques — Privacy framework," 2011. https://www.iso.org/standard/45123.html (accessed Jul. 01, 2021).

[13] GlobalPlatform, "Security Evaluation Standard for IoT Platforms (SESIP) v1.1," 2021. https://globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip-v1-0-gp_fst_070/#collapse- (accessed Jul. 01, 2021).

[14] The Digital Standard, "The Digital Standard | Raising the standard for connected products, services and systems," 2020. https://thedigitalstandard.org/ (accessed Jul. 01, 2021).

[15] OASIS, "{eXtensible Access Control Markup Language Version} 3.0." 2013.

[16] ISO, "ISO/IEC 27001 — Information security management," 2013. https://www.iso.org/isoiec-27001-information-security.html (accessed Jul. 01, 2021).

[17] European Parliament, "Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR)," 2016. https://gdpr-info.eu/ (accessed Jul. 01, 2021).

[18] European Commission, “The ePrivacy Directive | Shaping Europe’s digital future,” 2002. https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive (accessed Jul. 01, 2021).

[19] “The EU ePR (ePrivacy Regulation) | What You Need to Know.” https://www.itgovernance.co.uk/eprivacy-regulation-epr (accessed Jul. 01, 2021).

[20] European Union Agency for Network and Information Security (ENISA), “Indispensable baseline security requirements for the procurement of secure ICT products and services,” 2017. https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services (accessed Jul. 01, 2021).

[21] European Cyber Security Organisation (ECSO), “Cybersecurity made in Europe - The label,” 2020. https://ecs-org.eu/initiatives/cybersecurity-made-in-europe (accessed Jul. 01, 2021).

[22] T. and I. (METI) Ministry of Economy, “Cyber/Physical Security Framework (CPSF),” 2019. https://www.meti.go.jp/english/press/2019/0418_001.html (accessed Jul. 01, 2021).

[23] Carnegie Mellon University, “IoT Security & Privacy Label,” 2020. https://www.iotsecurityprivacy.org/ (accessed Jul. 01, 2021).

[24] European Union Agency for Network and Information Security (ENISA), “Guidelines for Securing the Internet of Things,” 2020. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things (accessed Jul. 01, 2021).

[25] European Union Agency for Network and Information Security (ENISA), “Baseline Security Recommendations for IoT,” 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (accessed Jul. 01, 2021).

[26] K. Moore, R. Barnes, and H. Tschofenig, “Best {{Current Practices}} for {{Securing Internet}} of {{Things}} ({{IoT}}) {{Devices}}.” 2016.

[27] NIST, “Digital Identity Guidelines: Authentication and Lifecycle Management,” *Spec. Publ. (NIST SP) - 800-63B*, 2017, doi: 10.6028/nist.sp.800-63b.

[28] NIST, “NISTIR 7628 Rev. 1, Guidelines for Smart Grid Cybersecurity,” 2014. https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final (accessed Jul. 01, 2021).

[29] OWASP, *OWASP Application Security Verification Standard (ASVS) Project*. .

[30] M. Lizar and D. Turner, “Consent Receipt Specification – Kantara Initiative,” 2018. https://kantarainitiative.org/download/7902/ (accessed Jul. 01, 2021).

[31] B. Gupta, D. P. Agrawal, and S. Yamaguchi, Eds., *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. IGI Global, 2016.

[32] M. Jouini and L. B. A. Rabai, “Threats Classification,” 2016, pp. 368–392.

[33] “D2.1 Definition of Project Requirements and Success Criteria.” BIECO project, 2021.

[34] A. J. Neumann, N. Statland, and R. D. Webb, “Post-processing audit tools and techniques,” *US Dep. Commer. Natl. Bur. Stand.*, pp. 11–3 – 11–4, 1977.

[35] J. Hughes and G. Cybenko, “Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity,” *Technol. Innov. Manag. Rev.*, vol. 3, no. 8, pp. 15–24, Aug. 2013, doi: 10.22215/timreview/712.

[36] A. W. Rufi, “Vulnerabilities, Threats, and Attacks,” *Netw. Secur. 1 2 Companion Guid. Cisco Netw. Acad.*, 2008.

[37] ISO, “ISO 7498 - Information processing systems — Open Systems Interconnection — Basic Reference Model,” 1989. https://www.iso.org/standard/14256.html (accessed Jul. 01, 2021).

[38] Microsoft, “STRIDE chart | Microsoft Security Blog,” 2007. https://www.microsoft.com/security/blog/2007/09/11/stride-chart/ (accessed Jul. 01, 2021).

[39] Web Application Security Consortium WASC, “WASC threat classification,” 2010.

[40] M. Nieles, K. Dempsey, and V. Y. Pillitteri, “An introduction to information security: the NIST Handbook,” Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-12r1.

[41] J. Eichler and D. Angermeier, “Modular Risk Assessment for the Development of Secure Automotive Systems,” *31. VDI/VW-Gemeinschaftstagung Automot. Secur.*, vol. VDI-Berich, no. January 2015, p. 11, 2015, Accessed: Feb. 17, 2021. [Online]. Available: https://www.researchgate.net/publication/283087728_Modular_risk_assessment_for_the_development_of_secure_automotive_systems.

[42] EVITA, *E-{Safety} {Vehicle} {Intrusion} {Protected} {Applications}*. 2008.

[43] HEAVENS, *HAVENS: HEAling Vulnerabilities to ENhance Software Security and Safety – Project Proposal*. 2012.

[44] “Keylength - Cryptographic Key Length Recommendation.” https://www.keylength.com/ (accessed Jul. 01, 2021).

[45] E. Lear, D. Romascanu, and R. Droms, “Manufacturer Usage Description Specification (RFC 8520).” 2019.

# 9. Annex: Detailed security claims

## 9.1. C0: Update software files should be encrypted and be transmitted using encryption

This claim is related with the process of software update of the TOE, ensuring that the update is ciphered to prevent code analysis.

| | |
|---|---|
| **STRIDE category** | Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Cryptography, updates, confidentiality |

**Requirements to apply the claim**: The TOE has a software update process.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. The manufacturer server sends a software update for the TOE (or one of its components). A sniffer is listening the communications.
2. The TOE receives the update.

PASS: The sniffer is not able to see the content of the update because it is ciphered.

FAIL: The sniffer is able to read the content of the update, which is in clear.

**Sources:** OWASP/ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, Carnegie Mellon label, SESIP, ISO 27001, IEC 62443.

## 9.2. C1: Update software files should be integrity protected

This claim is related with the process of software update of the TOE, ensuring that the update is integrity protected against any type of manipulation. A non-compliance with this claim would derive on a wide variety of attacks, e.g., the malfunctioning of the device or the compromising of the component to access to other parts of the system.

| | |
|---|---|
| **STRIDE category** | Integrity |
| **Impact** | Operational, financial |
| **Keywords** | Cryptography, updates, integrity |

**Requirements to apply the claim**: The TOE has a software update process.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. The manufacturer server sends a software update for the TOE (or one of its components).
2. An attacker is on the middle of the communication and modifies the content of the update.
3. The TOE receives the update.

PASS: The TOE detects that the update has suffered a modification.

FAIL: The TOE installs the modified update.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA: Baseline Recommendations for IoT critical infrastructures, SESIP, ISO 27001, IEC 62443.

## 9.3. C2: Update software files should be encrypted using strong keys and algorithms

This claim is related with the process of software update of the TOE, ensuring that the update is ciphered using an adequate key length and cryptographic algorithm to prevent code analysis.

| | |
|---|---|
| **STRIDE category** | Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Cryptography, updates, confidentiality |

**Requirements to apply the claim**: The TOE has a software update process and the update is sent encrypted.

**Dependencies:** C0

**Metrics:** PASS/FAIL the tests, algorithm and key length used for encryption

**Proposed test:**

1. The manufacturer server sends a software update for the TOE (or one of its components). A sniffer is listening the communications.
2. The TOE receives the update.

PASS: The sniffer obtains the key length and algorithms used to cipher the update and they are secure enough, following the recommendations of the NIST or other entities [44].

FAIL: The sniffer obtains the key length and algorithms used to cipher the update and they are weak, not following the recommendations of the NIST or other entities.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, SESIP, ISO 27001, IEC 62443.

## 9.4. C3: Update software files should be authenticated

This claim is related with the process of software update of the TOE, ensuring that the update has been sent by the manufacturer and not by a malicious entity.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Operational, financial |
| **Keywords** | Cryptography, updates, authentication |

**Requirements to apply the claim**: The TOE has a software update process.

**Dependencies:** None.

**Metrics:** PASS or FAIL the test

**Proposed test 1:**

1. The attacker send a software update for the TOE (or one of its components). The update has been authenticated by the attacker, using a non-valid key/certificate.
2. The TOE receives the update.

PASS: The TOE cannot validate the authenticity of the update so it discards it.

FAIL: The TOE installs the update.

**Proposed test 2:**

1. The attacker send a software update for the TOE (or one of its components). The update has not been authenticated.
2. The TOE receives the update.

PASS: The TOE cannot validate the authenticity of the update so it discards it.

FAIL: The TOE installs the update.

**Proposed test 3:**

1. The attacker send a software update for the TOE (or one of its components). The attacker has access to the public certificate/key of the manufacturer and tries to authenticate the update using it.
2. The TOE receives the update.

PASS: The TOE cannot validate the authenticity of the update so it discards it (the attacker is not able to authenticate the update using the public information of the manufacturer).

FAIL: The TOE installs the update.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, The digital standard, SESIP, ISO 27001, IEC 62443.

## 9.5. C4: The update mechanism shall prevent downgrade

This claim is related with the process of software update of the TOE, ensuring that the TOE is protected against attacks aiming to install previous version that could have vulnerabilities.

| **STRIDE category** | Availability |
|---|---|
| **Impact** | Operational |
| **Keywords** | Updates |

**Requirements to apply the claim**: The TOE has a software update process.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. The manufacturer server sends a software update for the TOE with a release date before the one that has currently installed.
2. The TOE receives the update.

PASS: The TOE discards the update as it is a previous version.

FAIL: The TOE installs the update and downgrades to a previous version.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701.

## 9.6. C5: The exchanged messages in the communication should be integrity protected

This claim is related with the protection of the integrity of the exchanged messages, guaranteeing that any alteration in the content or message fields is detected. This could derive on attacks not only against the integrity of the transmitted data, but also attacks willing to downgrade the communication protocol version or attacks to weaken the cryptographic parameters.

| | |
|---|---|
| **STRIDE category** | Integrity |
| **Impact** | Operational |
| **Keywords** | Integrity, protocol, message, field |

**Requirements to apply the claim**: None.

**Dependencies:** None

**Metrics:** PASS/FAIL the test, percentage of integrity protection (number of PASS tests/total number of tests).

**Proposed tests (one test per each field and message $X_M$):**

1. The sender sends message M.
2. An attacker modifies the field x of the message M ($X_M$).
3. The receiver (TOE) receives the altered message .

PASS: The TOE detects that the message has been modified and discards it.

FAIL: The TOE continues the communication without detecting the modification.

**Sources:** IETF Best Current Practices for IoT, The Digital Standard, SESIP, ISO 27001, IEC 62443.

## 9.7. C6: Automatically generated passwords should be unique

This claim is related with the strength of the automatically generated passwords/keys. In particular, the claim focuses on the uniqueness of the password, so attackers cannot use this knowledge to access to the system/information.

| | |
|---|---|
| **STRIDE category** | Confidentiality, Authentication |
| **Impact** | Privacy, Financial |
| **Keywords** | Confidentiality, authentication, cryptography |

**Requirements to apply the claim**: The TOE uses automatically generated passwords/keys (by default or after a key derivation process).

**Dependencies:** None.

**Metrics:** PASS/FAIL the test

**Proposed test:**

1. Two different entities generate a password/key.

PASS: The generated passwords/keys are different.

FAIL: The generated passwords/keys are the same.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, The Digital Standard, SESIP.

## 9.8. C7: Passwords should avoid common patterns

This claim is related with the strength of the passwords/keys. In particular, the claim focuses on the resistance against brute force attacks using a dictionary of commonly used passwords.

| | |
|---|---|
| **STRIDE category** | Confidentiality, Authentication |
| **Impact** | Privacy, Financial |
| **Keywords** | Confidentiality, authentication, cryptography |

**Requirements to apply the claim**: The TOE uses passwords established by a human or it uses automatically generated passwords.

**Dependencies:** None.

**Metrics:** PASS/FAIL the test, time after the key is broken, number of attempts.

**Proposed test:**

1. Attacker tries to access to the system performing a dictionary attack to obtain the password.

PASS: The attack is not successful.

FAIL: The attack is successful after a certain time and attempts.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, SP 800-63b.

## 9.9. C8: Passwords are not obviously linked to public information

This claim is related with the strength of the passwords/keys. In particular, the claim focuses on the resistance against brute force attacks based on social engineering, using public information.

| | |
|---|---|
| **STRIDE category** | Confidentiality, Authentication |
| **Impact** | Privacy, Financial |
| **Keywords** | Confidentiality, authentication, cryptography |

**Requirements to apply the claim**: The TOE uses passwords established by a human or it uses automatically generated passwords.

**Dependencies:** None.

**Metrics:** PASS/FAIL the test, number of matches with public information.

**Proposed test:**

1. Gather the public information available about the TOE (name, email, ID, IP, role, age, etc.).
2. Compare the password of the TOE with the public information.

PASS: There are no matches between the public information and the password of the TOE.

FAIL: There is at least one match between the public information and the password of the TOE.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701/ENISA Secure supply chain for IoT, sp800-63b.

## 9.10. C9: Passwords should be strong in terms of complexity

This claim is related with the strength of the passwords/keys that could be used for authentication and ciphering. In particular, the claim focuses on the compliance with best practices and recommendations from cybersecurity entities such as the NIST.

| | |
|---|---|
| **STRIDE category** | Confidentiality, Authentication |
| **Impact** | Privacy |
| **Keywords** | Cryptography, confidentiality, authentication |

**Requirements to apply the claim**: The TOE uses passwords or keys.

**Dependencies:** None

**Metrics:** PASS/FAIL the tests, algorithm and key length used.

**Proposed test:**

1. Generate the password/key of the TOE.
2. A sniffer is on the middle of the communication (if the keys are generated as a consequence of a message exchanging the security parameters)

PASS: The key length and algorithms used are secure enough, following the recommendations of the NIST or other entities [44].

FAIL: The key length and algorithms used are weak, not following the recommendations of the NIST or other entities.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701/ENISA Secure supply chain for IoT, ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, The Digital Standard, SP 800-63b.

## 9.11. C10 The changes of the authentication values for user authentication are successful

This claim is related with the process of changing authentication keys/passwords. The process should be secure, making the necessary changes and removing the old authentication values to avoid attacks based on leaked passwords.

| **STRIDE category** | Authentication |
|---|---|
| **Impact** | Privacy, Operational |
| **Keywords** | Cryptography, authentication |

**Requirements to apply the claim**: The TOE uses passwords or keys.

**Dependencies:** None

**Metrics:** PASS/FAIL the tests, algorithm and key length used.

**Proposed test 1:**

1. The TOE changes the password/Initiates the process of refreshing the authentication keys.
2. The process ends.
3. The TOE authenticates itself with the old authentication password/key.

PASS: The authentication fails.

FAIL: The TOE is authenticated with the old key.

**Proposed test 2:**

1. The TOE changes the password/Initiates the process of refreshing the authentication keys.
2. The process ends.
3. The TOE authenticates itself with the new authentication password/key.

PASS: The TOE is authenticated.

FAIL: The authentication fails.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701

## 9.12. C11: Sensitive security parameters exchanged during the communication for the establishment of a secure association should be integrity protected

This claim is related with the protection of the security parameters that are used to establish a security association among two entities (e.g., to authenticate both sides, to derive keys, etc.). A non-compliance of this claim can allow an attacker to weaken the cryptography used.

| **STRIDE category** | Integrity |
|---|---|
| **Impact** | Operational |
| **Keywords** | Integrity, protocol, message, field, cryptography |

**Requirements to apply the claim**: A security association is established between the TOE and another entity through a certain protocol (e.g., EAP, DTLS, TLS, EDHOC, etc.)

**Dependencies:** None

**Metrics:** PASS/FAIL the test, percentage of integrity protection (number of PASS tests/total number of tests), algorithm, hash length

**Proposed tests (one test per each field and message $X_N$):**

1. The sender sends message N.
2. An attacker modifies the field X of the message M ($X_N$).
3. The receiver (TOE) receives the altered message .

PASS: The TOE detects that the message has been modified and discards it.

FAIL: The TOE continues the communication and establishes the security association without detecting the modification or the TOE crashes.

**Proposed test 2:**

1. The TOE establishes the security association.
2. A sniffer is on the middle of the communication and obtains the algorithm used for the integrity check and the length.

PASS: The length and algorithms used are secure enough, following the recommendations of the NIST or other entities [44].

FAIL: The length and algorithms used are weak, not following the recommendations of the NIST or other entities.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, SESIP, sp800-63b, Japanese METI, ISO 27001, IEC 62443.

## 9.13. C12: Stored sensitive security parameters should be integrity protected

This claim is related with the protection of the security parameters that are stored in a specific device or database. A non-compliance of this claim can allow an attacker to modify the value of such parameters and weaken the cryptography used.

| | |
|---|---|
| **STRIDE category** | Integrity |
| **Impact** | Privacy |
| **Keywords** | Integrity, cryptography |

**Requirements to apply the claim**: The SUT uses cryptographic mechanisms and some of their parameters are stored inside or in a specific database.

**Dependencies:** None

**Metrics:** PASS/FAIL the test

**Proposed tests (one test per each security parameter stored S):**

1. Modify the stored parameter S (scripts can be used to modify it if it is stored in a file).

PASS: It is not possible to modify the parameter S or the TOE detects that the parameter has been modified.

FAIL: The parameter S is successfully changed without the TOE notifying it.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, SESIP, Japanese METI, ISO 27001, IEC 62443.

## 9.14. C13: Stored sensitive security parameters should be integrity protected

This claim is related with the protection of the security parameters that are stored in a specific device or database. A non-compliance of this claim can allow an attacker to reveal the value of such parameters and break the cryptography used.

| | |
|---|---|
| **STRIDE category** | Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Confidentiality, cryptography |

**Requirements to apply the claim**: The SUT uses cryptographic mechanisms and some of their parameters are stored inside or in a specific database.

**Dependencies:** None

**Metrics:** PASS/FAIL the test

**Proposed tests (one test per each security parameter stored S):**

1. Access to the storage of the sensitive parameter S (e.g., a file with the keys).

PASS: It is not possible to access go the sensitive parameter S or the parameter is ciphered or hashed and salted using a strong one-way key derivation function.

FAIL: It is possible to access to the parameter S and it is not ciphered or hashed or the functions are weak.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, SESIP, sp800-63b, Japanese METI, ISO 27001, IEC 62443.

## 9.15. C14: Ciphered communications should use strong algorithms

This claim is related with the protection of the confidentiality of the exchanged messages, ensuring that the update is ciphered using an adequate key length and cryptographic algorithm to prevent code analysis.

| | |
|---|---|
| **STRIDE category** | Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Confidentiality, cryptography, channel protection |

**Requirements to apply the claim**: The TOE uses encrypted communications.

**Dependencies:** C24

**Metrics:** PASS/FAIL the tests, algorithm and key length used for encryption

**Proposed tests (one per each other entity communicating with the TOE):**

1. The TOE exchanges a message with the other entity. A sniffer is listening the communications.

PASS: The sniffer obtains the key length and algorithms used to cipher the messages and they are secure enough, following the recommendations of the NIST or other entities [44].

FAIL: The sniffer obtains the key length and algorithms used to cipher the messages and they are weak, not following the recommendations of the NIST or other entities.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA baseline security requirements for the procurement of secure ICT products and services/ENISA Secure supply chain for IoT, GlobalPlatform - Security Evaluation Standard for IoT Platforms, Carnegie Mellon label, SESIP, SP 800-63b, Japanese METI, ISO 27001, IEC 62443.

## 9.16. C15: Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface

This claim is related with the protection of the access to the device functionality, ensuring that the access is allowed using authentication mechanisms.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Operational, financial |
| **Keywords** | Authorization, authentication, communication |

**Requirements to apply the claim**: The TOE offers functionality via a network interface to other entities.

**Dependencies:** None

**Metrics:** PASS/FAIL the test

**Proposed tests 1 (one per each offered functionality F):**

1. The attacker tries to access to the functionality F. The attacker is using a non-valid key/certificate.
2. The TOE receives the access request.

PASS: The TOE cannot authenticate the attacker, so access to the functionality is denied.

FAIL: The attacker can access to the functionality.

**Proposed test 2 (one per each offered functionality F):**

1. The attacker tries to access to the functionality F. The attacker does not have any authentication key.
2. The TOE receives the access request.

PASS: The TOE cannot authenticate the attacker, so access to the functionality is denied.

FAIL: The attacker can access to the functionality.

**Proposed test 3 (one per each offered functionality F):**

1. The attacker tries to access to the functionality F. The attacker has access to the public certificate/key of an allowed entity and tries to authenticate itself using it.
2. The TOE receives the request.

PASS: The TOE cannot authenticate the attacker, so access to the functionality is denied.

FAIL: The attacker can access to the functionality.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA baseline security requirements for the procurement of secure ICT products and services, The Digital Standard, SESIP, JAPANESE METI, ISO 27001, IEC 62443.

## 9.17. C16: The system should have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable

This claim is related with the protection against brute force attacks of network-based authentication mechanisms.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Privacy, operational, financial |
| **Keywords** | Authentication |

**Requirements to apply the claim**: The authentication mechanism used by the TOE is directly addressable from a network interface.

**Dependencies:** None

**Metrics:** PASS/FAIL the tests, number of possible attempts, and delay between attempts.

**Proposed test:**

1. The attacker attempts to authenticate itself to access to the TOE using non valid password/key, via the network interface.
2. Authentication fails.
3. Repeat step 1 several times.

PASS: The authentication is blocked, and the attacker is not allowed to access any more, at least for a certain time.

FAIL: The attacker can keep trying to authenticate with a non-valid password/key.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA: Baseline Recommendations for IoT critical infrastructures, ENISA: Baseline Recommendations for IoT critical infrastructures, Japanese METI, ISO 27001, IEC 62443.

## 9.18. C17: Sensitive security parameters should be encrypted in transit, with such encryption appropriate

This claim is related with the protection of the confidentiality of the exchanged security parameters, ensuring that the parameters are ciphered using an adequate key length and cryptographic algorithm to prevent an attacker from breaking the cryptography.

| | |
|---|---|
| **STRIDE category** | Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Confidentiality, cryptography, channel protection |

**Requirements to apply the claim**: The TOE exchanges sensitive security parameters with other entities.

**Dependencies:** C48

**Metrics:** PASS/FAIL the tests, algorithm and key length used for encryption.

**Proposed tests (one per each sensitive parameter P):**

1. The TOE and the other entity exchanges the sensitive parameter P. A sniffer is listening the communications.

PASS: The sniffer obtains the key length and algorithms used to cipher the sensitive parameter and they are secure enough, following the recommendations of the NIST or other entities [44].

FAIL: The sniffer obtains the key length and algorithms used to cipher the messages and they are not used or they are weak, not following the recommendations of the NIST or other entities.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ENISA baseline security requirements for the procurement of secure ICT products and services, ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, sp800-63b, Japanese METI.

## 9.19. C18: All unused network interfaces shall be disabled

This claim is related with the reduction of the network attack surface, enabling only those interfaces that the TOE uses. Fuzzing techniques and port scanning tools could be used to automate the validation of this claim.

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational |
| **Keywords** | Authorization, communication |

**Requirements to apply the claim**: It is necessary to know the interfaces that should be enabled for the normal functioning of the TOE, for example though the usage of a Manufacturer Usage Description (MUD) [45] file.

**Dependencies:** None

**Metrics:** PASS/FAIL the test, number of exposed interfaces.

**Proposed test (for each interface N not considered in the MUD or in the description of the TOE):**

1. The attacker tries to communicate with the TOE using the interface N (IP, port).

PASS: The TOE receives the request but it discards it or the request is filtered before reaching the TOE.

FAIL: The attacker can communicate with the TOE though the interface N.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701/ENISA Secure supply chain for IoT, ENISA: Baseline Recommendations for IoT critical infrastructures, Japanese METI.

### 9.20. C19: The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography

This claim is related with the protection of the personal data privacy, ensuring that it is ciphered using an adequate key length and cryptographic algorithm.

| | |
|---|---|
| **STRIDE category** | Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Confidentiality, cryptography, data protection |

**Requirements to apply the claim**: The TOE uses encrypted communications and the TOE exchanges personal data with other entities.

**Dependencies:** C48

**Metrics:** PASS/FAIL the tests, algorithm and key length used for encryption

**Proposed tests (one per each personal data exchange with another entity):**

1. The TOE send personal data to another entity. A sniffer is in the middle of the communication.
2. The other entity receives the data.

PASS: The sniffer is not able to see the content of the personal data because it is ciphered.  The sniffer obtains the key length and algorithms used to cipher the data and they are secure enough, following the recommendations of the NIST or other entities [44].

FAIL: The sniffer is able to read the personal data, which is in clear or the sniffer obtains the key length and algorithms used to cipher the messages and they are weak, not following the recommendations of the NIST or other entities.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, SESIP, Japanese METI, ISO 27001, IEC 62443.

## 9.21. C20: Authentication mechanisms must use strong passwords

This claim is related with the strength of the authentication keys used in the communications with/from the TOE, ensuring the compliance with best practices and recommendations from cybersecurity entities such as the NIST.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Privacy |
| **Keywords** | Cryptography, authentication |

**Requirements to apply the claim**: The TOE has authentication mechanisms for authenticate itself/for authenticate other entities.

**Dependencies:** C46

**Metrics:** PASS/FAIL the tests, authentication mechanism (PSK/certificate/Personal ID/User Password/other), if authentication is bidirectional or unidirectional, key/certificate length used.

**Proposed test (for each authentication process in the TOE):**

1. The TOE and the other entity initiate the authentication process.
2. A sniffer is on the middle of the communication .
3. The TOE and the other entity finish the authentication process.

PASS: The key/certificate length and algorithms used are secure enough, following the recommendations of the NIST or other entities [44]. The authentication is bidirectional.

FAIL: The key/certificate length and algorithms used are weak, not following the recommendations of the NIST or other entities. The authentication is unidirectional.

**Sources:** ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701/ENISA Secure supply chain for IoT, ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, SP 800-63b, Japanese METI.

## 9.22. C21: Integrity mechanisms must be strong

This claim is related with the strength of the integrity mechanisms used within the TOE, ensuring the compliance with best practices and recommendations from cybersecurity entities such as the NIST.

| | |
|---|---|
| **STRIDE category** | Integrity |
| **Impact** | Privacy, operational |
| **Keywords** | Cryptography, Integrity |

**Requirements to apply the claim**: The TOE uses integrity mechanisms for the messages/data sent/received.

**Dependencies:** C5

**Metrics:** PASS/FAIL the tests, integrity mechanism (MAC/HASH/Other), length of the integrity check.

**Proposed test (for each integrity mechanism in the TOE):**

1. The TOE and the other entity exchanges integrity protected messages.
2. A sniffer is on the middle of the communication

PASS: The length and algorithms used are secure enough, following the recommendations of the NIST or other entities [44].

FAIL: The length and algorithms used are weak, not following the recommendations of the NIST or other entities.

**Sources:** ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, SESIP, SP 800-63b, Japanese METI, ISO 27001, IEC 62443.

## 9.23. C22: Resistance to DoS attacks

This claim is related with the resistance of the TOE against DoS attacks.

| | |
|---|---|
| **STRIDE category** | Availability |
| **Impact** | Financial, Operational |
| **Keywords** | Availability, DoS |

**Requirements to apply the claim**: The TOE is able to receive messages from other entities/user.

**Dependencies:** None

**Metrics:** Maximum number of simultaneous connections, Number of successful connections at the end of the experiment.

**Proposed tests (increasing N):**

1. N entities send a request/message to the TOE at the same time.
2. The TOE receives and process the messages/requests.

PASS: The TOE is still available and it is able to process the requests properly.

FAIL: The TOE crashes due to the number of simultaneous requests or it is not able to attend all the requests properly.

**Sources:** ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, ISO 27001, IEC 62443.

## 9.24. C23: Data input validation

This claim is related with the resistance of the TOE against invalid data inputs that may cause buffer overflows or DoS attacks. This set of tests can be automated with fuzzing testing techniques, varying the length and format of the data.

| | |
|---|---|
| **STRIDE category** | Availability |
| **Impact** | Financial, Operational |
| **Keywords** | Availability |

**Requirements to apply the claim**: None

**Dependencies:** None

**Metrics:** PASS/FAIL the test.

**Proposed tests (one test per input needed by the TOE):**

1. Send an invalid input to the TOE
2. The TOE receives the input and processes it.

PASS: The TOE detects that the input is invalid and sends an alert.

FAIL: The TOE crashes due to the invalid input or processes it as it was a valid input.

**Sources:** ENISA: Baseline Recommendations for IoT critical infrastructures, IETF Best Current Practices for IoT, ISO 27001, IEC 62443.

## 9.25. C24: Data Communications should be ciphered

This claim is related with the protection of the data confidentiality exchanged between the TOE and other entities.

| | |
|---|---|
| **STRIDE category** | Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Confidentiality, communication |

**Requirements to apply the claim**: The TOE uses encrypted communications.

**Dependencies:** None

**Metrics:** PASS/FAIL the tests, percentage of ciphered data.

**Proposed tests (one per each message exchange with another entity):**

1. The TOE and the other entity exchanges information.
2. There is a sniffer in the middle on the communication to inspect the traffic

PASS: The sniffer is not able to see the content or only part of the exchanges messages. Determine the percentage of ciphered data.

FAIL: The sniffer is able to see the whole content of all the exchanges messages.

**Sources:** IETF Best Current Practices for IoT, The Digital Standard. The standard, ENISA: Baseline Recommendations for IoT critical infrastructures, The Digital Standard, SESIP, Japanese METI, ISO 27001, IEC 62443.

## 9.26. C25: Lawfulness of processing of personal data

This claim is related with the processing of personal data and in particular with the lawfulness of such a processing. In this claim we refer to consent as legal basis.

| | |
|---|---|
| **STRIDE category** | Authorization, Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Privacy, Data Protection, Lawfulness of Processing |

**Requirements to apply the claim**: The Controller is processing personal data concerning a data subject

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test**

1. Perform access to personal data collected without the consent of data subject.

PASS: The access to personal data is denied

FAIL: Personal data is processed without legal basis

**Sources:** GDPR (Art. 6 GDPR), ISO 29100.

## 9.27. C26: Personal data must be processed for a specific purpose

This claim is related with processing personal data for a specific purpose as defined in the GDPR (Art. 5).

| | |
|---|---|
| **STRIDE category** | Authorization, Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Privacy, Data Protection, Purpose Limitation Principle |

**Requirements to apply the claim**: The Controller is processing personal data concerning a data subject for a specific purpose.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Perform Access to the collected personal data for a different Purpose or for a Generic Purpose.

PASS: The access to the collected personal data is denied.

FAIL: Personal data is processed for a different purpose or for a generic purpose.

**Sources:** GDPR (Art. 5 GDPR), Open Web Application Security Project. IoT security guidance, Carnegie Mellon label, ETSI TS 103 702, ISO 29100.

## 9.28. C27: The system should allow data subject to access its personal data

This claim is related with the right of access by the data subject as defined in the GDPR.

| | |
|---|---|
| **STRIDE category** | Authorization, Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Privacy, Data Protection, Right of access by the data subject |

**Requirements to apply the claim**: The controller is processing personal data for a given purpose based, for instance, on the consent given by data subject.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Perform an access request by the data subject.

PASS: Obtain a list of personal data (Categories of) and the Purpose of processing; OR, if the system does not collect any information regarding the requester (data subject): a message stating that no data are stored in the system.

FAIL: The collected personal data are not given to data subject. Or there is no answer from Controller within the period time defined in the GDPR.

**Sources:** GDPR (Art. 15.1 Letters (a) and (b)), The Digital Standard - The standard, Carnegie Mellon label, ISO 29100.

## 9.29. C28: The source code must not contain SQL injection vulnerabilities

This claim is related with having a source code that must not contain SQL injection vulnerabilities.

| | |
|---|---|
| **STRIDE category** | Availability, Confidentiality, Integrity |
| **Impact** | Operational, Privacy |
| **Keywords** | Tampering, elevation of privilege, Information disclosure, Denial of Service |

**Requirements to apply the claim**: The system uses SQL Databases.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Scan the source code using the vulnerability detections tool looking for SQL injections vulnerabilities.

PASS: The tool does not detect SQL injection vulnerabilities.

FAIL: The tool detects SQL injection vulnerabilities.

**Sources:** OWASP, ISO 27001, IEC 62443.

## 9.30. C29: The source code must not contain command injection vulnerabilities

This claim is related with having a source code that must not contain command injection vulnerabilities.

| | |
|---|---|
| **STRIDE category** | Availability, Confidentiality, Integrity |
| **Impact** | Operational, Privacy |
| **Keywords** | Tampering, elevation of privilege, Information disclosure, Denial of Service |

**Requirements to apply the claim**: Always

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Scan the source code using the vulnerability detection tool looking for command injections vulnerabilities.

PASS: The tool does not detect Command injection vulnerabilities.

FAIL: The tool detects command injection vulnerabilities.

**Sources:** OWASP, ISO 27001, IEC 62443.

## 9.31. C30: The source code must not contain code injection vulnerabilities

This claim is related with having a source code that must not contain code injection vulnerabilities.

| | |
|---|---|
| **STRIDE category** | Availability, Confidentiality, Integrity |
| **Impact** | Operational, Privacy |
| **Keywords** | Tampering, Denial of Service |

**Requirements to apply the claim**: Always

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Scan the source code using the vulnerability detection tool looking for code injections vulnerabilities.

PASS: The tool does not detect code injection vulnerabilities.

FAIL: The tool detects code injection vulnerabilities.

**Sources:** OWASP

## 9.32. C31: The source code must not contain path traversal vulnerabilities

This claim is related with having a source code that it must not contain path traversal vulnerabilities

| | |
|---|---|
| **STRIDE category** | Availability, Confidentiality, Integrity |
| **Impact** | Operational, Privacy |
| **Keywords** | Tampering, elevation of privilege, Information disclosure, Denial of Service |

**Requirements to apply the claim**: The system uses local resources (images and other files).

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Scan the source code using the using the vulnerability detection tool looking for path traversal vulnerabilities.

PASS: The tool does not detect path traversal vulnerabilities.

FAIL: The tool detects path traversal vulnerabilities.

**Sources:** OWASP

## 9.33. C32: The source code must not use components with known vulnerabilities

This claim is related with having a source code that must not use components with known vulnerabilities

| | |
|---|---|
| **STRIDE category** | Availability, Confidentiality, Integrity |
| **Impact** | Operational, Privacy |
| **Keywords** | Tampering, elevation of privilege, Information disclosure, deny of service, CVSS, Exploitation, |

**Requirements to apply the claim**: The system uses third party components.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Scan the source code using the vulnerability detection tool looking for vulnerabilities of third-party components.

PASS: The tool does not detect components with known vulnerabilities.

FAIL: The tool detects components with known vulnerabilities.

**Sources:** OWASP, The Digital Standard, Carnegie Mellon label, Japanese METI, ISO 27001.

## 9.34. C33: The adopted XACML-based authorization mechanism (PDP) must implement the mandatory functionalities of the XACML standard specification language

This claim is related with systems that use an authorization system for ruling access to protected resources. We refer to the XACML standard as good example of authorization system. In particular, we illustrate how the most vulnerable component of the authorization system, i.e., the Policy Decision Point (PDP).

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational, Financial |
| **Keywords** | Authorization, Access Control, PDP Conformance Testing |

**Requirements to apply the claim**: The system uses an authorization system based on the XACML standard for ruling access to protected resources.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Execute on the PDP all the tests of the OASIS XACML 2.0 Conformance Tests suite v0.4[8].

PASS: For each authorization request belonging to the conformance test suite, the access decision in the PDP authorization response is equal to that specified in the conformance test suite.

FAIL: For an authorization request belonging to the XACML conformance test suite, the PDP response is different from the authorization response associated to that request in the conformance test suite.

**Sources:** OASIS XACML[9]

### 9.35. C34: The access control mechanism (PDP) that evaluates the authorization requests against a policy must correctly implement the policy

This claim is related with the assessment of the correctness of the PDP in reference to a specific access control policy.

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational, Financial |
| **Keywords** | Authorization, Access Control, PDP Testing |

**Requirements to apply the claim**: The system uses an authorization system based on the XACML standard model for ruling access to protected resources.

**Dependencies: C33**

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Execute a set of XACML requests derived from the policy on the PDP.

PASS: For each XACML request (combination of subject, action and resource values) the obtained PDP response (Permit/Deny/Not Applicable) is equal to the access right specified in the policy.

FAIL: For a given combination of subject, action and resource values in the authorization request, the authorization response (Permit/Deny/Not Applicable) is different from that that is specified in the policy.

**Sources:** OASIS XACML

[8] https://www.oasis-open.org/committees/download.php/14877/ConformanceTests.html
[9] https://csrc.nist.gov/projects/access-control-policy-tool

## 9.36. C35: The adopted XACML access control policy must be correct with respect to a specification (model) of the access control rights

This claim is related with assessment of the PDP with respect to an independent oracle, i.e., a specification model of the access rights.

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational, Financial |
| **Keywords** | Authorization, Access Control, Policy Testing |

**Requirements to apply the claim**: The system uses an authorization system based on the XACML standard for ruling access to protected resources. Specific XACML-based access control policies must be defined.

**Dependencies:** C33, C34

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Execute all the XACML requests derived from the policy and check the results against the specification of the access control rights.

PASS: For each XACML based authorization request the access decision is equal to that of the access control rights specification.

FAIL: For a given XACML based authorization request the access decision is different from that of the access control rights specification.

**Sources:** OASIS XACML

## 9.37. C36: Warning must be issued in case of potentially reduced functionality

The claim relates to the specification of system modes of degraded operation.

| | |
|---|---|
| **STRIDE category** | Integrity, Availability |
| **Impact** | Safety |
| **Keywords** | Failure Detection |

**Requirements to apply to the claim:** The system's behaviour must specify which, if any, modes of degraded operation are anticipated. Where relevant, operator warning must be issued to alert the operators of the degraded performance.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Degrade an operation.

PASS: Warning is issued.

FAIL: No warning is issued.

**Sources:** ISO/DS 26262-1:2016(E) 3.181.

## 9.38. C37: Warning must be followed by triggering fail-over behaviour

The claim relates to bringing the system back to a safe state.

| | |
|---|---|
| **STRIDE category** | Integrity, Availability |
| **Impact** | Safety |
| **Keywords** | Fail-Over Behaviour |

**Requirements to apply to the claim:** The system specification must include associated emergency operation(s) and tolerance intervals. In case of behaviour involving operator actions, the latter must be specified in documentation and/or training.

**Dependencies:** C36

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Self-diagnostic test for confirming automatic fail-over behaviour is triggered.

PASS: Self-diagnostic test passes i.e. fail-over test behaviour is executed.

FAIL: Self-diagnostic test fails i.e. fail-over test behaviour is not executed.

**Sources:** ISO/DS 26262-1:2016(E) 3.181

## 9.39. C38: Safety Risk Management has been applied

The claim relates to applying a safety risk management process to the system. This includes:

- Specifying which operational events are considered to be critical with respect to safety.
- Specifying the preliminary risk of the system's operation after each event.
- Specifying appropriate mitigation measures to reduce the risk to an acceptable level.

| | |
|---|---|
| **STRIDE category** | Integrity, Availability |
| **Impact** | Safety |
| **Keywords** | Development Assurance |

**Requirements to apply to the claim:** Hazard assessment and risk analysis process has been performed adequately to identify relevant conditions of unacceptable safety risk and appropriate means of reducing the risk to an acceptable level.

**Dependencies:** C37

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Hazard assessment and risk analysis process has identified relevant security events and corresponding mitigating measures.

PASS: Relevant security events and mitigating measures have been specified across the identified security events.

FAIL: Relevant security events and mitigating measures have not been specified across the identified security events.

**Sources:** ISO 26262-3:2016(E) 6.4.2.5

## 9.40. C39: Automatic updates should not change the network protocol interfaces in any way that is incompatible with previous versions

This claim is related with the process of software update of the TOE, ensuring that the updates do not affect the TOE basic network functionality described in the MUD or in the TOE description.

| | |
|---|---|
| **STRIDE category** | Availability, Integrity |
| **Impact** | Operational, Financial |
| **Keywords** | Updates |

**Requirements to apply the claim**: The TOE has a software update process.

**Dependencies:** C41

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. The manufacturer server sends a software update for the TOE that removes/blocks a necessary network interface.
2. The TOE receives the update.

PASS: The TOE detects that the new update is not compliant with the MUD/TOE description of the needed network interfaces and it does not install it, raising an alert.

FAIL: The TOE installs the update and basic network interfaces necessary for the functionality of the TOE are disabled.

**Sources:** IETF Best Current Practices for IoT, ENISA: Baseline Recommendations for IoT critical infrastructures.

## 9.41. C40: Endpoints should only run applications or services whose TCP or UDP ports are described in the MUD profile

This claim is related with the reduction of the network attack surface, enabling only those interfaces that the manufacturer recommends, in a complementary way to C19. Fuzzing techniques and port scanning tools could be used to automate the validation of this claim.

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational, Financial |

| | |
|---|---|
| **Keywords** | Authorization, communication, network |

**Requirements to apply the claim**: The TOE should have a MUD file.

**Dependencies:** C41

**Metrics:** PASS/FAIL the test, number of exposed interfaces, number of necessary interfaces blocked.

**Proposed test (for each interface N not considered in the MUD):**

1. The attacker tries to communicate with the TOE using the interface N (IP, port).

PASS: The TOE receives the request but it discards it or the request is filtered before reaching the TOE.

FAIL: The attacker can communicate with the TOE though the interface N.

**Proposed test (for each interface N considered in the MUD):**

1. An authorized entity tries to communicate with the TOE using the interface N (IP, port).

PASS: The entity can communicate with the TOE though the interface N.

FAIL: The TOE receives the request but it discards it or the request is filtered before reaching the TOE.

**Sources:** Japanese METI, ISO 27001, IEC 62443.

## 9.42. C41: A MUD file should be provided in accordance with MUD RFC

This claim is related with the reduction of the network attack surface from the manufacturing phase, requesting the creation of a MUD file that describes the minimum network interfaces that should be available.

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational |
| **Keywords** | Authorization, communication, network |

**Requirements to apply the claim**: None

**Dependencies:** None

**Metrics:** PASS/FAIL the test

**Proposed test:**

1. The TOE starts the process of bootstrapping to take part of the deployment network.
2. The TOE sends during this process a MUD URL to obtain its associated MUD file.
3. The entity acting as MUD manager in the deployment network gathers the MUD files using the URL and validates it.

PASS: The TOE sends the MUD URL, the MUD manager is able to obtain the MUD file and the MUD file is signed and follows the structure of the MUD RFC.

FAIL: The TOE does not send the MUD URL or the MUD manager is not able to obtain the MUD file or the MUD file is not signed or it do not follow the structure of the MUD RFC.

**Sources:** GlobalPlatform - Security Evaluation Standard for IoT Platforms, Carnegie Mellon label.

## 9.43. C42: Connections to remote services, interfaces, and end-points should be cryptographically authenticated

This claim is related with the protection of the TOE services when it is possible to access to them remotely.

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational, Financial |
| **Keywords** | Authorization, communication, network |

**Requirements to apply the claim**: The TOE has remote services.

**Dependencies:** None

**Metrics:** PASS/FAIL the test

**Proposed tests 1 (one per each remote service S):**

1. The attacker tries to access to the service S. The attacker is using a non-valid key/certificate.
2. The TOE receives the access request.

PASS: The TOE cannot authenticate the attacker, so access to the service is denied.

FAIL: The attacker can access to the service.

**Proposed test 2 (one per each offered service S):**

1. The attacker tries to access to the service S. The attacker does not have any authentication key.
2. The TOE receives the access request.

PASS: The TOE cannot authenticate the attacker, so access to the service is denied.

FAIL: The attacker can access to the service.

**Proposed test 3 (one per each offered service S):**

3. The attacker tries to access to the service S. The attacker has access to the public certificate/key of an allowed entity and tries to authenticate itself using it.
4. The TOE receives the request.

PASS: The TOE cannot authenticate the attacker, so access to the service is denied.

FAIL: The attacker can access to the service.

**Sources:** Carnegie Mellon label, Japanese METI.

## 9.44. C43: The software should not use unsafe libraries that contain vulnerabilities

This claim is related with the security of the software libraries that the TOE uses internally. This set of tests could be automated using source code vulnerability scanners.

| | |
|---|---|
| **STRIDE category** | Confidentiality, Integrity, Availability, Authentication, Authorization, Non-repudiation |
| **Impact** | Operational, Financial, Privacy, Safety |
| **Keywords** | Known vulnerabilities, libraries |

**Requirements to apply the claim**: The TOE uses libraries.

**Dependencies:** None

**Metrics:** PASS/FAIL the test, Number of encountered vulnerabilities.

**Proposed test (for each library used by the TOE):**

1. Check if the library used contains vulnerabilities collected in the NVD.

PASS: No vulnerabilities were encountered

FAIL: At least one library of the TOE has vulnerabilities.

**Sources:** Carnegie Mellon label.

## 9.45. C44: Device should remain operating and locally functional in the case of a lost network connection

This claim is related with the resilience of the TOE against loss of network connection.

| | |
|---|---|
| **STRIDE category** | Availability |
| **Impact** | Operational, Financial |
| **Keywords** | Availability, resilience, internet |

**Requirements to apply the claim**: The TOE has internet connectivity.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Cut the internet connection to the TOE.
2. A client tries to interact with the TOE services.

PASS: The TOE provides the service to the Client.

FAIL: The TOE is not available, it does not answers or it does not give the service to the client.

**Sources:** Carnegie Mellon label, ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701, ISO 27001, IEC 62443.

## 9.46. C45: Protocols and libraries used by the system are updated

This claim is related with the security of the software libraries that the TOE uses internally, verifying that all of them are updated to avoid recent vulnerabilities.

| STRIDE category | Confidentiality, Integrity, Availability, Authentication, Authorization, Non-repudiation |
|---|---|
| Impact | Operational, Financial, Privacy, Safety |
| Keywords | Known vulnerabilities, libraries |

**Requirements to apply the claim**: The TOE uses libraries.

**Dependencies:** None

**Metrics:** PASS/FAIL the test, Number of out-of-date libraries.

**Proposed test (for each library used by the TOE):**

1. Check the library version.
2. Compare with the last stable release of the library

PASS: The library version is the last stable release or it is between an acceptable time threshold.

FAIL: The library of the TOE is out-of-date and out of the time threshold.

**Sources:** The digital standard.

## 9.47. C46: Authentication protocols should be secure, using recommended algorithms

This claim is related with the strength of the authentication mechanisms used to access to the different services of the TOE.

| STRIDE category | Authentication |
|---|---|
| Impact | Privacy, safety |
| Keywords | Authentication, cryptography |

**Requirements to apply the claim**: The TOE uses authentication mechanisms.

**Dependencies:** C15

**Metrics:** PASS/FAIL the tests, mechanism used for authentication.

**Proposed tests (one per each authentication mechanism):**

1. The TOE uses the authentication mechanisms with another entity.
2. A sniffer obtains the authentication mechanism used by observing the traffic

PASS: The authentication mechanism used in considered secure enough, following the recommendations of the NIST SP 800-63B or other entities [27] (e.g., Memorized Secret, Look-Up Secret, Out-of-Band Devices, Single-Factor One-Time Password (OTP) Device, Multi-Factor OTP Device, Single-Factor Cryptographic Software, Single-Factor Cryptographic Device, Multi-Factor Cryptographic Software, Multi-Factor Cryptographic Device).

FAIL: The authentication mechanism used is weak, not following the recommendations of the NIST or other entities.

**Sources:** NIST SP800-63b, Japanese METI, ISO 27001, IEC 62443.

## 9.48. C47: Authenticated sessions should expire, and a new reauthentication required

This claim is related with the freshness of the security associations established between the TOE and another entity.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Privacy, safety |
| **Keywords** | Authentication, cryptography, freshness |

**Requirements to apply the claim**: The TOE uses authentication mechanisms.

**Dependencies:** C15

**Metrics:** PASS/FAIL the tests, time of expiration

**Proposed tests (one per each authentication mechanism):**

1. The TOE and another entity authenticate themselves using the authentication mechanism.
2. A sniffer is in the middle of the communication observing the traffic

PASS: The sniffer sees how the authentication association expires and the TOE and the other entity repeat the authentication process.

FAIL: After a period of time recommended by the NIST [27], the TOE and the other entity still maintain the same security association.

**Sources:** NIST SP800-63b.

## 9.49. C48: Random bit generators should be strong enough

This claim is related with the strength of the random bit generators used in the cryptographic mechanisms of the TOE. A weak random generator may weaken also the protection mechanisms that make use of it.

| | |
|---|---|
| **STRIDE category** | Confidentiality, Integrity, Availability, Authentication, Authorization, Non-repudiation |
| **Impact** | Operational, Financial, Privacy, Safety |
| **Keywords** | Cryptography |

**Requirements to apply the claim**: The TOE uses random generators.

**Dependencies:** None

**Metrics:** PASS/FAIL the tests, mechanism used for random generation.

**Proposed tests (one per each cryptographic mechanism using random generators):**

1. The TOE uses the cryptographic mechanism.
2. The TOE uses the random bit generator as part of the previous mechanism.
3. Check the random generator mechanism used.

PASS: The random generator mechanism used in considered secure enough, following the recommendations of the NIST SP 800-90Ar1[10] or other standards and it provides at least the minimum security strength specified e.g., in the latest revision of SP 800-131A[11] or other standards.

FAIL: The random generator mechanism used is weak, not following the recommendations of the NIST or other entities.

**Sources:** NIST SP800-63b.

## 9.50. C49: Authentication algorithms should avoid channel side attacks

This claim is related with the resistance of the authentication mechanism used by the TOE against attacks focused on measuring the energy consumption, for example to extract the keys used.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Privacy, safety |
| **Keywords** | Authentication, cryptography, physical, power |

**Requirements to apply the claim**: The TOE uses authentication mechanisms.

**Dependencies:** C16

**Metrics:** PASS/FAIL the tests

**Proposed tests (one per each authentication mechanism):**

1. The TOE and another entity authenticate themselves using the authentication mechanism.
2. Measure the energy and time consumption
3. Repeat the authentication process with different secret values and measure again the energy and time.

PASS: The energy and time consumption is constant regardless of secret values.

FAIL: The energy and time consumption depends of the secret values.

**Sources:** NIST SP800-63b.

## 9.51. C50: The system should work in case of power outage

This claim is related with the resilience of the TOE against loss of power outage.

| | |
|---|---|
| **STRIDE category** | Availability |
| **Impact** | Operational, Financial |
| **Keywords** | Availability, resilience, power |

**Requirements to apply the claim**: None

[10] https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final
[11] https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Cut the power outage of the TOE.
2. A client tries to interact with the TOE services.

PASS: The TOE provides the service to the Client.

FAIL: The TOE is not available, it does not answers or it does not give the service to the client.

**Sources:** ISO 27001, IEC 62443.

## 9.52. C51: The system should allow data subject to modify its personal data

This claim is related with the rectification request from the data subject to the Controller who is processing its personal data.

| | |
|---|---|
| **STRIDE category** | Authorization, Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Privacy, Data Protection, Right to Rectification |

**Requirements to apply the claim**: The controller processes personal data concerning data subject for a specific purpose based on a legal basis (e.g., Consent given by data subject).

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

3. Perform a modification request by the data subject for a specific personal data.

PASS: The modification is performed according to the data subject Request.

FAIL: Personal data is not modified.

**Sources:** GDPR (Art. 16)

## 9.53. C52: The system should allow data subject to delete permanently personal data concerning it

This claim is related with the right to be forgotten (in the GDPR is referred as Right to erasure).

| | |
|---|---|
| **STRIDE category** | Authorization, Confidentiality |
| **Impact** | Privacy |
| **Keywords** | Privacy, Data Protection, Right to Erasure (“right to be forgotten”) |

**Requirements to apply the claim**: The controller processes personal data concerning data subject for a specific purpose based on a legal basis (e.g., Consent given by data subject).

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Perform a deletion request.

PASS: Personal data is deleted from the system.

FAIL: Personal data is not deleted and still available into the system.

**Sources:** GDPR (Art. 17).

## 9.54. C53: The system should allow data subject to withdraw its given consent

This claim is related with exercising the right to withdraw a consent given by data subject for processing its personal data.

| **STRIDE category** | Authorization, Confidentiality |
|---|---|
| **Impact** | privacy |
| **Keywords** | Privacy, Data Protection, Right to Withdraw a Given Consent |

**Requirements to apply the claim**: The controller processes personal data for a specific purpose based on the Consent (i.e., the legal basis) given by data subject.

**Dependencies: C27**

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. A withdrawn consent request is sent by the data subject related to a specific personal data (PD) and Purpose (P) .

PASS: The access (processing of) to PD is no longer allowed for the purpose P, i.e., the consent related to DP and P is deleted from the system.

FAIL: The processing of PD is still performed for the purpose P .

**Sources:** GDPR (Art. 17 letter b).

## 9.55. C54: The system shall implement mechanisms of protection from malicious code manipulation

This claim is related to the protection of a system (e.g., a smart grid information system) from malicious code, and spam to assure the integrity of the system itself, of its information and the protection of sensitive data from unauthorized modification or deletion.

| | |
|---|---|
| **STRIDE category** | Integrity |
| **Impact** | operational, privacy |
| **Keywords** | Tampering, malicious code |

**Requirements to apply the claim**: none.

**Dependencies:** None

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Attack injection aiming at manipulate code.

PASS: The system detects code modifications.

FAIL: The system does not detect code modifications.

**Sources:** NIST IR 7628 (SG.SI-3).

### 9.56. C55: The system shall update protection mechanisms whenever new releases are available

This claim is related to the update of the protection mechanisms of a system (e.g., a smart grid information system) from malicious code, and spam whenever new releases are available.

| | |
|---|---|
| **STRIDE category** | Integrity, availability |
| **Impact** | Operational, privacy |
| **Keywords** | Security update |

**Requirements to apply the claim**: the system already has in place protection mechanisms from malicious code and is able to receive communications about the release of new updates.

**Dependencies:** C54

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Release an update (or send a message communicating the new release availability) and check if the protection mechanisms are updated.

PASS: The system installs the updates (and it does it timely, in accordance with the update policy) .

FAIL: The system does not install the updates even if they are available.

**Sources:** NIST IR 7628 (SG.SI-3).

## 9.57. C56: The system shall prevent anyone from circumventing malicious code protection mechanisms

This claim is related to the prevention of circumvention attempts, attempted by malicious entities, and targeted to protection mechanisms of a system (e.g., a smart grid information system) from malicious code, and spam.

| | |
|---|---|
| **STRIDE category** | Integrity, availability |
| **Impact** | Operational, privacy |
| **Keywords** | Tampering |

**Requirements to apply the claim**: the system already has in place protection mechanisms from malicious code.

**Dependencies:** C54

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Injection of an attack aiming at disabling or manipulating the protection mechanism.

PASS: The system detects the attack and any code modification attempt.

FAIL: The system does not detect code modifications.

**Sources:** NIST IR 7628 (SG.SI-3).

## 9.58. C57: The system shall enforce assigned authorizations for controlling the flow of information within the system and from interconnected systems.

This claim is related to the information flow control which regulates where information is allowed to travel within a system (e.g., a smart grid information system) and between interconnected systems; in particular, the claim addresses the enforcement of assigned authorizations for controlling the flow .

| | |
|---|---|
| **STRIDE category** | Authorization, confidentiality |
| **Impact** | Operational, privacy |
| **Keywords** | Authorization, dataflow, flows |

**Requirements to apply the claim**: The system shall already have assigned authorizations for controlling the flow in order to enforce them.

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Attempt of unauthorized flow control.

PASS: The system blocks the unauthorized flow control attempt.

FAIL: The system does not block the unauthorized flow control attempt.

**Sources:** NIST IR 7628 (SG.AC-5).

## 9.59. C58: The system shall enforce a limit of consecutive invalid login attempts during a time period.

This claim is related to the detection, and logging of consecutive login attempts and to the enforcement of a limit of number of invalid attempts; when the limit is exceeded, the system (e.g., smart grid information system) should initiate an automatic lockout.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Operational, privacy |
| **Keywords** | Authentication |

**Requirements to apply the claim**: the system shall have an authentication mechanism

**Dependencies:** none

**Metrics:** PASS or FAIL the test, number of possible attempts, and delay between attempts.

**Proposed test:**

1. The TOE attempts to authenticate itself using non valid password/key.
2. Authentication fails.
3. Repeat step 1 several times.

PASS: The system detects and logs that the number of login attempts exceeded the limit, blocks any further attempt originating from the same entity as soon as the limit is exceeded.

FAIL: The system does not (timely) detect or log that the number of login attempts has exceeded the limit, and subsequent attempts are allowed.

**Sources:** NIST IR 7628-1 (SG.AC-8), ETSI EN 303 645/ ETSI TS 103 645/ETSI TS 103 701/OWASP, The Digital Standard, sp800-63b, Japanese METI, ISO 27001, IEC 62443.

## 9.60. C59: The system shall notify, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

This claim is related to the notification expected from a system (e.g., a smart grid information system) to a user which successfully logged in, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

| | |
|---|---|
| **STRIDE category** | Authentication |
| **Impact** | Operational, privacy |
| **Keywords** | Authentication |

**Requirements to apply the claim**: the system shall have an authentication mechanism.

**Dependencies:** C62

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Execute a sequence of login operations, where the first and the last are correct attempts and between them there is a number of incorrect attempts.

PASS: The system does not notify the number of unsuccessful login attempt or the information about the last successful attempt.

FAIL: The system does not notify the number of unsuccessful login attempt or the information about the last successful attempt.

**Sources:** NIST IR 7628-1 (SG.AC-10).

## 9.61. C60: The system shall execute a fail-safe procedure upon the loss of communications with other systems.

This claim is related to the event of a loss of communication between a system and the other systems or entities interconnected and foresees the execution of a procedure that provides the maximum protection (e.g., of controlled infrastructure), especially from the point of view of safety.

| **STRIDE category** | Integrity, availability |
|---|---|
| **Impact** | Operational, safety |
| **Keywords** | Fail-safe, communication |

**Requirements to apply the claim**: the system shall be able to communicate with other systems

**Dependencies:** none

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Disrupt communication channel with other systems.

PASS: Fail-safe procedures are correctly triggered by the related failure.

FAIL: Not all the fail-safe procedures are triggered by the related failure.

**Sources:** NIST IR 7628-1 (SG.CP-11).

## 9.62. C61: The system shall uniquely identify and authenticate users.

This claim is related to the unique identification and authentication of users (or, e.g., of processes acting on behalf of users) expected from a system (e.g., a smart grid information system).

| **STRIDE category** | Integrity, authentication, non-repudiation |
|---|---|
| **Impact** | Privacy |
| **Keywords** | Authentication |

**Requirements to apply the claim**: the system shall have registration and authentication mechanisms in place.

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Perform multiple attempts of user registration with the same set of credentials (e.g., identical username and authentication factor(s)).

PASS: Registration procedure terminates successfully only for the first attempt.

FAIL: Multiple users are registered with the same credentials.

**Sources:** NIST IR 7628-1 (SG.IA-4).

## 9.63. C62: The system shall uniquely identify and authenticate a defined list of devices before establishing a connection.

This claim is related to the maintenance by a system, of a whitelist of known and registered entities (e.g., defined by type, by specific device, etc.), to be used for the unique identification and authentication of devices before the establishment of a connection with them.

| | |
|---|---|
| **STRIDE category** | Authentication, non-repudiation |
| **Impact** | Operational, privacy |
| **Keywords** | Authentication |

**Requirements to apply the claim**: the system shall be able to establish connection with other entities/devices

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Perform a connection attempt from a device not authenticated and not listed.

PASS: The device connection attempt is detected and not allowed.

FAIL: The device connection attempt in authorized.

**Sources:** NIST IR 7628-1 (SG.IA-5).

## 9.64. C63: The system shall isolate security functions from non-security functions.

This claim is related to isolation of security functions (e.g., hardware, software, firmware of a system) required for enforcing a security policy, from the other system functions.

| | |
|---|---|
| **STRIDE category** | integrity |
| **Impact** | Operational, privacy |
| **Keywords** | Isolation, separation |

**Requirements to apply the claim**: the system shall have security functions and non-security functions.

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Perform a workload consisting of security functions and non-security functions. Trace the activity of the system processes.

PASS: Security functions are executed in isolation from non-critical ones.

FAIL: A security process is not isolated from non-security processes.

**Sources:** NIST IR 7628-1 (SG.SC-3).

## 9.65. C64: The system shall separate user functionalities from management functionalities.

This claim is related to the separation of user functionalities (e.g., user interface services) from management functionalities (e.g., including functions necessary to administer databases, network components, workstations, servers, or any functionality that typically requires privilege).

| **STRIDE category** | integrity |
|---|---|
| **Impact** | Operational, privacy |
| **Keywords** | Isolation, separation |

**Requirements to apply the claim**: the system shall have user functionalities and management functionalities.

**Dependencies:** none

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Perform a workload consisting of user functions and management functions. Trace the activity of the system processes.

PASS: User functionalities are separated from management functionalities.

FAIL: A management process is not isolated from non-security processes.

**Sources:** NIST IR 7628-1 (SG.SC-29).

## 9.66. C65: The system shall monitor events to detect attacks, unauthorized activities or conditions, and non-malicious errors.

This claim is related to the monitoring capability of a system (e.g., a smart grid information system) which is aimed at detect attacks, unauthorized activities or condition, and non-malicious errors and that can be achieved through a variety of tools and techniques.

| **STRIDE category** | Authorization, non-repudiation, integrity |
|---|---|
| **Impact** | Operational, privacy and legislation |
| **Keywords** | Monitoring, authorization |

**Requirements to apply the claim**: none

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Inject a sequence of faults and attacks attempt, including attempt of performing activities by unauthorized entities, together with non-malicious errors injection.

PASS: All the events are monitored and all the different attempts are correctly detected and categorized.

FAIL: Absence of monitoring system or monitoring activity unable to detect and distinguish attacks, unauthorized activities or conditions or non-malicious errors.

**Sources:** NIST IR 7628-1 (SG.SI-4), ANSI/ISA-62443-3-3-2013, requirement 6.4.3, NIST IR 7628-1 (SG.AU-3).

## 9.67. C66: The system shall lock the session after a configurable time period of inactivity.

This claim is related to the locking of a session after an idle activity period from a user or entity already successfully authenticated with a system. The threshold for the inactivity period should be configurable.

| **STRIDE category** | Authentication, non-repudiation |
|---|---|
| **Impact** | Operational, privacy |
| **Keywords** | Authentication |

**Requirements to apply the claim**: the system shall have an authentication mechanism

**Dependencies:** none

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Leave the system inactive for a period greater than the configurable time period threshold.

PASS: The system locks the session.

FAIL: The system does not lock the session.

**Sources:** ANSI/ISA-62443-3-3-2013, requirement 6.7.1.

### 9.68. C67: The system shall set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.

This claim is related to the arrangement of a fail-safe operation by a system, which involves the setting of predetermined outputs states and which should be executed in case of an attack to the system (e.g., an IACS) that caused the inability to maintain normal operation.

| | |
|---|---|
| **STRIDE category** | Availability |
| **Impact** | Operational, safety |
| **Keywords** | Availability, resilience |

**Requirements to apply the claim**: none

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Attack injection preventing the system to execute normal operation.

PASS: Default output is set as result of the attack.

FAIL: Default output is not set.

**Sources:** ANSI/ISA-62443-3-3-2013, requirement 7.8.1.

### 9.69. C68: The system shall prevent end-to-end messages from being received from external users or systems.

This claim is related to the prevention of the occurrence of interceptions (e.g., man-in-the-middle performed by external users or entities) of end-to-end communications between system components.

| | |
|---|---|
| **STRIDE category** | Confidentiality, integrity |
| **Impact** | Privacy and legislation |
| **Keywords** | Confidentiality, integrity, network, encryption |

**Requirements to apply the claim**: none

**Dependencies:** none

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Try to intercept end-to-end communications with state-of-the-art approaches (e.g., man in the middle).

PASS: No communication is intercepted.

FAIL: man in the middle attack terminates successfully.

**Sources:** ANSI/ISA-62443-3-3-2013, requirement 9.5.1

## 9.70. C69: The system shall operate in a degraded mode during a DoS event.

This claim is related to the ability of a system to operate in a degraded and fail-safe mode (e.g., with a reduction of performance) in occurrence of an attack (as Denial of Service) which makes the system unable to operate as expected during normal conditions.

| **STRIDE category** | Availability, integrity |
|---|---|
| **Impact** | Operational, safety |
| **Keywords** | Availability, resilience, network |

**Requirements to apply the claim**: none

**Dependencies:** none

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. DoS Attack injection.

PASS: The system enters the degraded mode and is still able to operate (even if with a reduction of performance).

FAIL: The system does not enter the degraded mode and is completely unavailable.

**Sources:** ANSI/ISA-62443-3-3-2013, requirement 11.3.1

## 9.71. C70: The system shall limit the use of resources by security functions to prevent resource exhaustion.

This claim is related to the security functions of a system (e.g., hardware, software, firmware or any function for enforcing a security policy) and in particular to the ability of a system to limit the resource usage needed by these functions in order to avoid exceeding thresholds and causing resource exhaustion.

| **STRIDE category** | Availability, integrity |
|---|---|
| **Impact** | Operational |
| **Keywords** | Availability, robustness |

**Requirements to apply the claim**: the system shall have security functions.

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Stress test of resources required by security functions (e.g., by injecting multiple attacks concurrently).

PASS: System resources are not exhausted and security functions.

FAIL: CPU usage or RAM usage or storage usage overcome critical thresholds during the test.

**Sources:** ANSI/ISA-62443-3-3-2013, requirement 11.4.1.

## 9.72. C71: The system shall terminate a remote session at the end of the session or after a period of inactivity.

This claim is related to the ability of a system to terminate a remote session after an idle activity period or at the conclusion of the session.

| **STRIDE category** | Authentication, authorization |
|---|---|
| **Impact** | Operational, privacy |
| **Keywords** | Network |

**Requirements to apply the claim**: the system shall have mechanisms for remote authentication.

**Dependencies:** none

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Leave the system inactive for a period greater than the threshold.

PASS: The remote session is terminated.

FAIL: The remote session is not terminated.

**Sources:** NIST IR 7628, SG.AC-13.

## 9.73. C72: Logs should be protected against removal

This claim is related to the protection of any type of system logs, avoiding the removal of the fingerprints after an attack or malicious action is performed.

| **STRIDE category** | Non-repudiation |
|---|---|
| **Impact** | Operational |
| **Keywords** | Logging, monitoring |

**Requirements to apply the claim:** The system should have an auditing mechanism

**Dependencies:** C65

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. The attack accesses to the system and tries to remove the stored logs in the system.

PASS: The logs cannot be removed or the logs are removed but there is an updated back up copy is available.

FAIL: The logs are removed successfully and no back up copy is available.

**Sources:** NIST IR 7628.

## 9.74. C73: The system shall provide a proof of notice requirements for an explicit consent receipt for demonstrating compliance with the GDPR

This claim is related with demonstrating that the data subject has given the consent before processing its personal data by the Controller, in compliance with the GDPR.

| | |
|---|---|
| **STRIDE category** | Non-Repudiation |
| **Impact** | Operational, Privacy |
| **Keywords** | Explicit Consent, Lawfulness of Processing |

**Requirements to apply the claim**: The Controller has already defined a specific purpose for processing personal data.

**Dependencies:** None

**Metrics:** PASS or FAIL the test.

**Proposed test:**

1. Give Consent for processing personal data.

PASS: A consent receipt must be delivered to the data subject, and a record entry is added to the records of processing.

FAIL: Consent receipt is not produced to the data subject; or no new entry is added to the records of processing.

**Sources:** GDPR, Kantara Initiative.

## 9.75. C74: The system should ensure that only authorised users may gain access to the information under the circumstances specified in the access control policy

This claim is related with the assessment of authorization systems. In particular, the claim aims at assessing both access control policies and access control mechanisms used for ruling access and protecting valuable resources.

| | |
|---|---|
| **STRIDE category** | Authorization |
| **Impact** | Operational, Financial |
| **Keywords** | Authorization, Access Control |

**Requirements to apply the claim**: The system uses an authorization system for ruling access to protected resources, by specifying well-defined access control policies that specify the conditions under which the access of a given information is allowed.

**Dependencies:** C33, C34, C35

**Metrics:** PASS or FAIL the test

**Proposed test:**

1. Try to access the system with permission rights not compliant to the defined access control policies.

PASS: The system blocks the access request .

FAIL: The system does not block the access request .

**Sources:** OASIS XACML.