IoT Security Standards Gap Analysis

Mapping of existing standards against requirements on security and privacy in the area of IoT

V1.0

DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Authors

Elżbieta Andrukiewicz
Scott Cadzow

Sławomir Górniak

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-275-2, DOI: 10.2824/713380

Table of Contents

Executive Summary 4
1. General information 5
1.1 Background and objectives of the study 5
1.2 Scope of the study 5
1.3 Related documents 5
1.4 Applied methodology 6
2. Analysis of standards gap 7
3. The certification opportunity 8
Annex A: Mapping of requirements to standards 10
A.1 Role of standardisation 10
A.2 Gaps in standardisation 11
Annex B: Proposal for security standards evolution in IoT realm 23
B.1 Introduction 23
B.2 Conventional development of ST or PP 23
B.3 Direct rationale approach for creating simpler and faster specifications 24
B.4 Composite evaluations suitable for IoT devices 26

Executive Summary

ENISA conducts a preliminary analysis of the IoT-related landscape of standards, which indicates that there is no significant gap in standards to bring secure IoT to the market. This does not mean that the security of the IoT ecosystem as a whole has been addressed by means of standards. Elements of a holistic approach towards IoT security can be found in a series of standards, however to achieve an overarching approach that protects the entire IoT ecosystem further work is needed. Accordingly, given the particularity of the IoT ecosystem (e.g. very high scalability, context of use, short time to market and cost drivers), this study does not intend to promote a specific solution for the entire IoT. Conversely, by identifying and mapping the existing standards landscape for IoT security, the study aims at pinpointing potential areas of improvement and additional efforts in securing the IoT.

In general, there is an identifiable gap in process by which a vendor can assert that their IoT product or service is secure. On the assertion that standards enable interoperability, the lack of cohesion on the use and application of standards for secure IoT mean that interoperability is not guaranteed even if all devices were to be placed on the market with security features enabled.

The primary argument of the present document is that standards are essential but not sufficient to ensure open access to markets. In the particular case of security a large number of processes as well as technical standards have to be in place to ensure that any device placed on the market is assuredly secure. In this case the present document proposes, in Annex B, a theoretical approach towards a certification and assurance and validation scheme to identify what is sufficient, as a precursor to allow for market access through device, service and process certification. It should be noted that this approach is inherently theoretical, since it does not take into account relevant concerns such as economic considerations that might affect the viability of applying standards.

The process recommended in this document is intended in part to engender a change in attitude towards device security by making secure IoT the only form of IoT that reaches the market and to give confidence to the market through a mélange of certification, assurance testing & validation, and market surveillance.

The bulk of the material in the present report is contained in Annex A, the mapping of requirements to available standards, and in Annex B, a proposal for the technical basis of market certification.

1. General information

1.1 Background and objectives of the study

In 2017, ENISA defined a set of Baseline Security Recommendations for IoT. The aim of this work was to provide insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems.

Section 4 of this report – "Security measures and good practices" and Annex A – "Detailed Security measures / Good practices" provide requirements on security and privacy. These requirements were grouped and analysed in the context of standards available in each area, providing a mapping as the result.

In 2017 ENISA published a report "Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy", available at https://www.enisa.europa.eu/publications/gaps-eu-standardisation The structure of that report has been considered as basis for this project.

The overall goal of the study is to map requirements on security and privacy in the area of IoT to existing standards, identifying the gaps.

1.2 Scope of the study

This study analyses the gaps and provides guidelines for, in particular, the development or repositioning of standards, facilitating the adoption of standards and governance of EU standardisation in the area of NIS. ENISA brings in this relationship its technical and organisational know-how in NIS which can be further leveraged into standards in terms of extending or assessing them to render them more appropriate to stakeholders and more compliant with the prevailing regulatory framework.

Special attention is given to the EU needs related to emerging cybersecurity certification schemes which will operate under the European cybersecurity certification framework. The framework is currently not adopted[1] but is expected to be finished at the end of this year. Standards or other widely adopted technical specifications containing requirements form the basis for any certification activity. European standards for security evaluation models, methods, techniques and tools adopted to the IoT world are urgently needed to complement existing initiatives, good practices and industry guidelines on IoT security.

1.3 Related documents

The study is based on the following documents:

[1] ROLLING PLAN FOR ICT STANDARDISATION 2018, https://ec.europa.eu/growth/content/2018-rolling-plan-ict-standardisation-released_en
[2] Baseline Security Recommendations for IoT, Nov 20, 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

1.4 Applied methodology

Several widely recognized standardization organizations have been surveyed to create a matrix which combines subsequent requirements from Annex A of [2] and relevant standards.

Based on the analysis of leading standardization activities in the field of IoT given in [1], the matrix contains inputs from:

- Three European Standardization Organizations (ESO) ie. CEN, CENELEC and in particular ETSI TC Cyber
- ISO/IEC JTC1 subcommittees including SC27 (IT Security Techniques) and SC41 (Internet of Things and related technologies)
- ITU-T SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORK.

The outcome is given in Annex A2.

2. Analysis of standards gap

The requirements listed in the ENISA report “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures” have been mapped to an existing identifiable standard that if followed would allow the requirement to be satisfied. The detailed, requirement by requirement, mapping is given in Annex A.

The simplified analysis yields that there is no significant standards gap - every requirement can be met by an existing standard. The problem is that this is neither the correct nor the expected answer. Standards exist for many different elements of making a device or service secure. However, when referring to IoT, one refers to an ecosystem of not only devices and services. Moreover, the context of use of IoT, its high scalability and other particularities further complicate the field and require more generic and flexible approaches. Therefore, for example the gap in IoT device standards for security is that the standards are not treated holistically so it is possible to deliver a device to the market that can authenticate its user, that can encrypt data it transmits, that can decrypt data it receives, that can deliver or verify the proof of integrity, but which will still be insecure. Similarly, the organisation developing the IoT product or service may have the development processes defined in management guidelines such as those of ISO-27000 but still delivers an insecure product.

The challenge for regulators and suppliers alike is to bring only secure IoT devices to the market and this requires a different approach, which will have to be flexible enough to accommodate for the nature of the dynamic IoT ecosystem. Accepting that it is often speculation, there is a necessary challenge to imagine how society will be in a few years from now and to consider the threats to society at that time. In order to frame this, the broad assumption is that ICT will reach further into society with more connectivity, further augmentation of everyday life through ICT, and this will demand an ICT and cybersecurity response. The concerns of the next few years however stretch far beyond the remit of only security technology and many of the recommendations in the present document extend to gaining better understanding of the societal understanding of how ICT, and in particular, ICT incorporating cybersecurity impacts daily life.

Whereas this checklist of security requirements for IoT security and its mapping to specific standards can serve as a springboard towards holistic and effective IoT security, it should be noted that the intricacies of the IoT ecosystem call for more flexible approaches. Not only are the underlying technological challenges calling for adaptive, context- and risk-based solutions, but also the IoT market constraints have to be taken into account, so as not to hamper competitiveness and innovation.

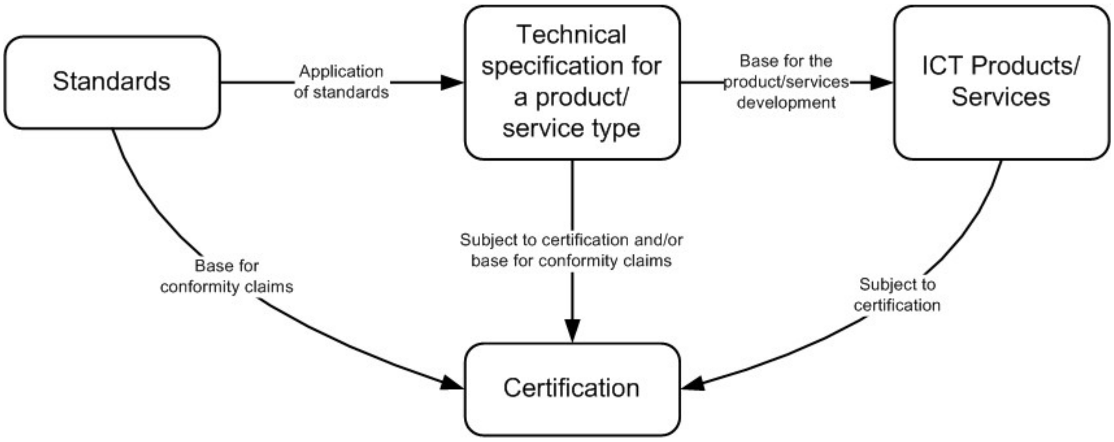
3. The certification opportunity

The overall purpose of standards from the perspective of the market is twofold in defining what a standard is intended to achieve: (1) interoperability, and (2) confidence.

The conventional role of standards in achieving interoperability is discussed in some length in Annex A and is not repeated here.

The role of standards in the domain of trust is less well defined and in a security context is difficult to state in simple terms. When referring to the IoT, one should not only consider individual devices. The inherent connectivity and interdependencies of devices, services, people, process and data call for holistic approaches. Accordingly, this implies a much more holistic view of the role of the device as opposed to a relatively closed view of what standard does it comply to for say encryption.

Standards can be used for developing technical specifications in a specific context of a product type, and provide a framework for security evaluation of products. Such general concept is presented in the figure below.


Standards
Application of standards
Technical specification for a product/ service type
Base for the product/services development
ICT Products/ Services
Subject to certification and/or base for conformity claims
Base for conformity claims
Subject to certification
Certification

As a representative use case example, we discuss here the case of the international standard ISO/IEC 15408 Evaluation criteria for IT security, widely recognized as ‘Common Criteria’ (CC)[2]. CC consists of 3 parts including:

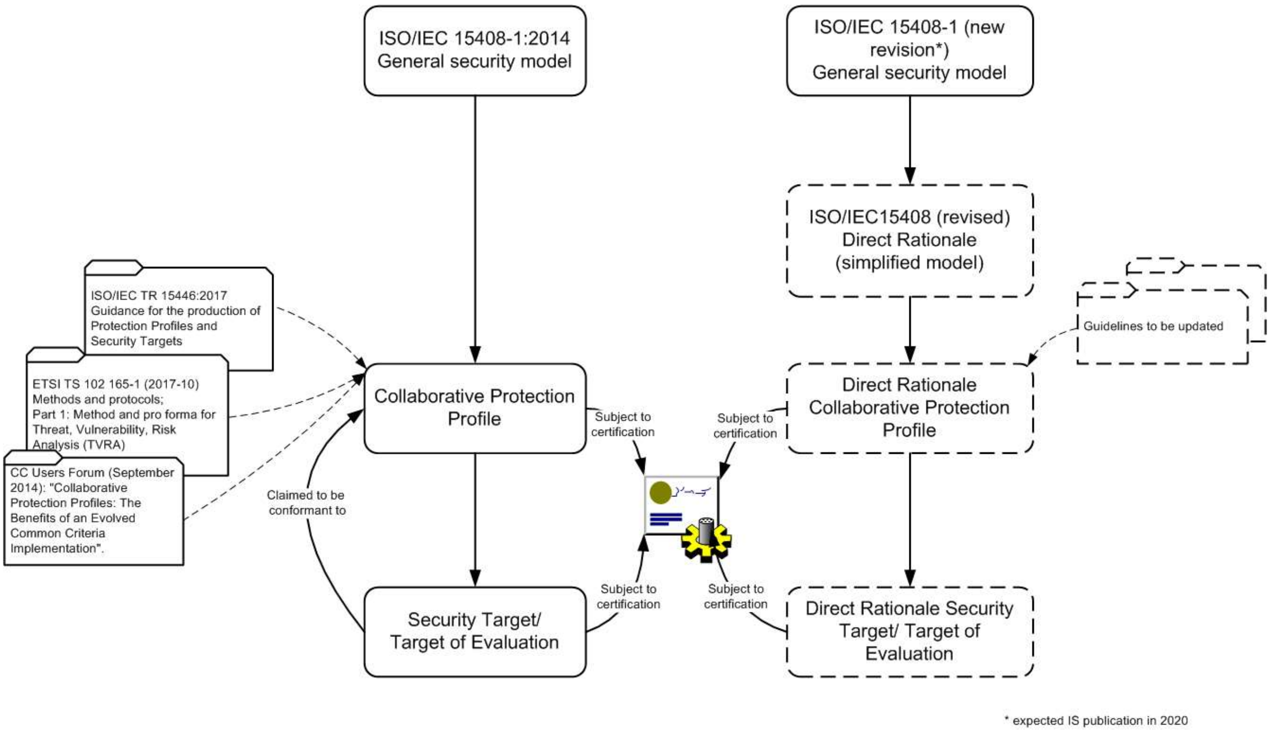
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components

Based on the security model discussed in part 1 one can develop technical specifications, called – in CC language – ‘protection profiles’ (PP) for the product type, or ‘security target’ (ST) for a given product. Such specifications contain security requirements according to the formal taxonomy given in part 2 of CC, and

[2] It should be underlined that this discussion is indicative and serve as an example, thus in no way implying any preference towards the use of CC or any other standard in the IoT domain. This would require a far more thorough analysis taking into account all related aspects and particularities, including the ones related to economics.

simultaneously create the evaluation requirements by using security assurance components given in part 3 of CC.

The evolution of CC from PP/ST through cPPs (collaborative Protection Profiles) and into the proposed “Direct Rationale” approach from the Common Criteria group does provide a framework for a wider, holistic view of security and therefore of confidence. The “Direct Rationale” approach provides a way of producing comprehensive security specifications for products, which is simpler than a traditional one hence it could be potentially applied in the IoT for preparing good technical specifications, giving simultaneously the ground for providing requiring solid and proven confidence the product meets security requirements.


ISO/IEC 15408-1:2014
General security model
ISO/IEC 15408-1 (new revision*)
General security model
ISO/IEC15408 (revised)
Direct Rationale
(simplified model)
Guidelines to be updated
ISO/IEC TR 15446:2017
Guidance for the production of Protection Profiles and Security Targets
ETSI TS 102 165-1 (2017-10)
Methods and protocols;
Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)
CC Users Forum (September 2014): "Collaborative Protection Profiles: The Benefits of an Evolved Common Criteria Implementation".
Collaborative Protection Profile
Subject to certification
Subject to certification
Direct Rationale Collaborative Protection Profile
Claimed to be conformant to
Subject to certification
Subject to certification
Security Target/ Target of Evaluation
Direct Rationale Security Target/ Target of Evaluation
* expected IS publication in 2020

The opportunity to drive market confidence in security of IoT may be developed from the work outlined in evolution of the Common Criteria (see also a detail examination in Annex B) to propose to all ICT security developing SDOs, to work towards cPPs and from there to work in the Direct Rationale cPP development.

Evidently, the example use case of CC can be considered for other standards when it comes to IoT. As mentioned, there is a growing call for flexible and adaptive solutions in this environment and therefore a complete analysis is beyond the scope of this report.

There is an opportunity to develop standards that have to be testable and that will be cited in the certification chain as proof of assurance. A subtle assertion is that if you comply with a standard, and that standard is properly maintained, then conformance is sufficient. Less obvious is that the proof of security assurance will require many standards to be conformed to.

Annex A: Mapping of requirements to standards

A.1 Role of standardisation

A.1.1 General overview

In the context of IoT devices, a broad generalisation of the role of standards is that their role is to provide interoperability of "things". It is also a broad generalisation that standards provide requirements to be met and do not provide instructions on how to implement a requirement. For security standards these statements apply as a broad interpretation but with the slight modification that many security standards, or more likely the security functions defined in standards, give assurance of the interoperability of "things" when subject to attack by hostile parties. Thus standards may address functionality (e.g. an encryption algorithm), application of that functionality (e.g. use of specific encryption mode (say counter mode)), and contextual use of that functionality (e.g. application of encryption to provision of confidentiality protection services).

Entities involved in cryptographic security that are required to interoperate will also require sharing knowledge and functionality that will include the identification of keys and algorithms. Thus security standards have to address simple mechanical interconnection, semantic and syntactic shared meaning, and management of attributes and organisations to react to security transgressions in an appropriate manner.

A.1.2 Organisational interoperability

There is a class of organisational management standards in security that defines roles within organisations that seek to enforce a "need to know". From a security perspective when two organisations share data they may transfer data securely by having a common Communications Security (ComSec) framework, but the ComSec exchange cannot make any inference on how data is treated prior to, or after, transfer. Thus the local IT security policy of the sending and receiving organisations is trusted to be equivalent and this trust may be reinforced by external measures.

A.1.3 Syntactic interoperability

Syntax derives from the Greek word meaning ordering and arrangement. The English language sentence structure of subject-verb-object is a simple example of syntax, and generally in formal language syntax is the set of rules that allows a well formed expression to be formed from a fundamental set of symbols. In computing science syntax refers to the normative structure of data. In order to achieve syntactic interoperability there has to be a shared understanding of the symbol set and of the ordering of symbols. In any language the dictionary of symbols is restricted, thus in general a verb should not be misconstrued as a noun for example (although there are particularly glaring examples of misuse that have become normal use, e.g. the use of "medal" as a verb wherein the conventional text "He won a medal" has now been abused as "He medalled").

A.1.4 Semantic interoperability

Syntax cannot convey meaning and this is where semantics is introduced. Semantics derives meaning from syntactically correct statements. Semantic understanding itself is dependent on both pragmatics and context. There are a number of ways of exchanging semantic information although the success is dependent on structuring data to optimise the availability of semantic content and the transfer of contextual knowledge (although the transfer of pragmatics is less clear). The most obvious examples of semantic containers for syntactically correct information are protocols whereby the protocol (e.g. an authentication protocol) gives context to message sets. This may be further extended using the concept of shared state as a means of identifying context and this is often embedded in protocol (e.g. an authentication protocol may go through states that include "Identified", "Challenge issued", "Response pending" prior to finalising on the state "Authenticated").

A.1.5 Electrical and mechanical interoperability

Quite simply a device with a power connector using, for example, a Type IEC 60906-2 connection cannot accept power from anything other than a Type IEC 60906-2 connector. Similarly, for example, a serial port complying to USB-Type-A will not be able to connect with a USB-Type-C lead. In addition to simple mechanical compatibility there is a requirement to ensure electrical interoperability covering amongst others the voltage level, amperage level, DC or AC, frequency if AC, variation levels and so forth.

A.1.6 Radio communication interoperability

Radio (wireless) communication requires shared knowledge of frequency band, modulation technique, symbol rate, power, and so forth. In general radio communication can be characterised as broadcast and unreliable. The nature of the physical media requires that radio protocols make provisions to maximise link reliability, most often achieved using various forms of Forward Error Correction in the Link Layer (layer 2 of the OSI stack).

A.2 Gaps in standardisation

It is recognised that whilst there are a very large number of bodies that develop standards it is also recognised that most service providers, manufacturers and governments are involved in a significant number of them. This unfortunately also means that as each standards body is in competition with each other, that there is overlap in capability and of itself this constitutes a risk to security.

ASSERTION: Gaps in standards present risk that additional standardisation effort may mitigate, but overlaps in standardisation effort present risk that may not be mitigated by additional standardisation effort but rather by agreed reduction, or redaction of existing standards.

TABLE A.1: MAPPING OF REQUIREMENTS TO AVAILABLE STANDARDS

Req. ID	Statement of requirement	Standards in support of requirement
	Security by Design	
GP-PS-01	Consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacture, and deployment.	ISO 30141 clause 11.3.3, ITU Y.4806 Security capabilities supporting safety of the Internet of things
GP-PS-02	Ensure the ability to integrate different security policies and techniques.	ISO 30141 clause 11.3.2
GP-PS-03	Security must consider the risk posed to human safety.	ISO 30141 clause 11.2
GP-PS-04	Designing for power conservation should not compromise security.	n/a
GP-PS-05	Design architecture by compartments to encapsulate elements in case of attacks.	ISO 30141 clause 11.3.2
GP-PS-06	For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.	ISO/IEC 15408-3 (ATE and AVA Classes description) May be addressed in part by independent assurance testing against documented security claims. The role of penetration testing is often prohibited, or restricted, by legislation (e.g. the Computer Misuse Act).
GP-PS-07	For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.	ISO/IEC 15408-3 (ATE Class description) Whilst this is not directly mappable to standards there are quality practices that may impose code review. In addition many coding practice guidelines will explicitly address means to perform code reviews, and many frameworks will explicitly identify when a code-review should be performed.

		Apple secure development guidelines, from https://developer.apple.com/library/content/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html Microsoft Security Development Lifecycle (SDL) from https://www.microsoft.com/en-us/sdl Open Software Assurance Maturity Model (SAMM) from http://www.opensamm.org Building Security in Maturity Model (BSIMM), incorporating the SSDL method, from https://www.bsimm.com
NOTE: For each of the above, particularly GP-PS-05 and GP-PS-07. there exist some best practice guidelines for specific developer environments.		
Privacy by Design		
GP-PS-08	Make privacy an integral part of the system	ISO 29550
NOTE: It is noted that a breach of privacy requires at least one actor to perform the breach. The GDPR recommendation to undertake a DPIA when applied would restrict breaches to explicit breaking of any measures applied or to specific actions by actors at the edge of the system.		
GP-PS-09	Perform privacy impact assessments before any new applications are launched	ISO/IEC 27005, ISO/IEC 29134. ISO 27005 defines a method of conducting a PIA. It is noted that GDPR requires that a DPIA/PIA is performed
GP-PS-10	Establish and maintain asset management procedures and configuration controls for key network and information systems	ETSI TS 103 305 (from controls from CIS). ISO/IEC 27002 clause 8.1 may apply in selection of controls with other parts of the ISO 27002 ISO 55000 Asset management
GP-PS-11	Identify significant risks using a defence-in-depth approach	Military standards such as below may apply. In general there are no standards that define the defence in

		depth approach although it is an accepted best practice of most security professionals
https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/archive/assets/public/upload/Defense-in-Depth.pdf&WpKes=aF6woL7fQp3dJiLgJBSABf7qwgxHD5mzFWdTgW		
GP-PS-12	Identify the intended use and environment of a given IoT device	Required in development of a risk analysis in defining the scope of security evaluation (the ToE in ISO/IEC 15408-1 and -2)). Addressed in some IoT best practices including the (soon to be published) ETSI TS 103 645.
Organisational, People and Process measures		
GP-OP-01	Develop an end-of-life strategy for IoT products	ISO 30141 clause 11.3.3 (IoT system & product Security Life Cycle Reference Model)Addressed in TS 103 645 and in ETSI TR 103 533.
GP-OP-02	Disclose the duration and end-of-life security and patch support (beyond product warranty)	ISO 30141 clause 11.3.3 (IoT system & product Security Life Cycle Reference Model)Addressed in TS 103 645 and in ETSI TR 103 533.
GP-OP-03	Monitor the performance and patch known vulnerabilities up until the “end-of-support|” period of a product’s lifecycle	ISO 30141 clause 11.3.3 (IoT system & product Security Life Cycle Reference Model)Addressed in TS 103 645 and in ETSI TR 103 533.
GP-OP-04	Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided	ISO 27002 clause 10 ISO 11770 (key management) Series of standards ISO/IEC 29192 (Lightweight cryptography – 7 parts, covering algorithms and protocols) Not specifically addressed in standards. The reason is that standards by design are built on proven solutions and conforming to standards addresses this.
GP-OP-05	Establish procedures for analysing and handling security incidents	ISO 27002 16Addressed in TS 103 645 and in ETSI TR 103 533.

GP-OP-06	Coordinated disclosure of vulnerabilities	ISO/IEC 301111 (Addressed in TS 103 645 and in ETSI TR 103 533. In addition the use of Common Vulnerability handling processes) and Disclosure (ISO/IEC 29147 (Vulnerability disclosure)) applies.
GP-OP-07	Participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners	ISO 27002 6.1.3 ISO 27002 6.1.4 Addressed in TS 103 645 and in ETSI TR 103 533. In addition the use of Common Vulnerability Disclosure (ISO/IEC 29147) applies. It is also noted in a number of regulatory instruments (GDPR, NIS, …) that common use of the CERT framework is expected.
GP-OP-08	Create a publicly disclosed mechanism for vulnerability reports, e.g. Bug Bounty <tba>programs	ISO/IEC 301111 (Vulnerability handling processes) and 29147 (Vulnerability disclosure)Addressed in TS 103 645 and in ETSI TR 103 533. Some vendors provide financial incentives and this has to be considered (it may be argued that if a financial incentive is offered then bug hunters may be more incentivised than if no such incentive applies).
GP-OP-09	Ensure the personnel practices promote privacy and security – train employees in good privacy and security practices	ISO 27002 clause 7.2
GP-OP-10	Document and monitor the privacy and security training activities	ISO 27002 clause 7.2.2
GP-OP-11	Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs	ISO 27002 clause 7.2.1
GP-OP-12	Data processed by a third-party must be protected by a data processing agreement	ISO 27002 clause 13.2.4, clause 15

GP-OP-13	Only share consumers' personal data with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations	ISO 27002 clause 18.1.4 This is a key constraint of the GDPR and is specifically addressed in Article 6 for the lawful processing of data.
GP-OP-14	For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners	ISO 27002 clause 15
Technical measures		
GP-TM-01	Employ a hardware-based immutable root of trust	TPM from TCG (published as ISO/IEC 11889) SIM from ETSI SCP
GP-TM-02	Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security	TPM from TCG (published as ISO/IEC 11889)
GP-TM-03	Trust must be established in the boot environment before any trust in any other software or executable program can be claimed	Secure boot, Defined by TCG (published as ISO/IEC 11889)
GP-TM-04	Sign code cryptographically to ensure it has not been tampered with after signing it as safe for the device, and implement run-time protection and secure execution monitoring to make sure malicious attacks do not overwrite code after it is loaded	Series of standards ISO/IEC 29192-5 and 6 (Lightweight cryptography – Part 5: Hash-functions, Part 6: Message authentication codes (MACs), ITU X.1362 Simple ecryption procedure for IoT environments
GP-TM-05	Control the installation of software in operating systems, to prevent unauthenticated software and files from being loaded onto it	ISO 27002 clause 12.6.2. This is covered by techniques including load time attestation, boot time attestation and run time attestation. Many of these techniques are built on TPMs (published as ISO/IEC 11889). In

		addition the ETSI GR NFV-SEC-007 gives broad guidance to this topic.
GP-TM-06	Enable a system to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful	ISO 27002 clause 12.3
GP-TM-07	Use protocols and mechanisms able to represent and manage trust and trust relationships	In general for cryptographic trust the mechanisms inherent in X.509 apply, with additional protocol mechanisms to transfer X.509 certificates such as those in TLS apply.
GP-TM-08	Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default	ISO/IEC 15408-1 and -2Addressed in TS 103 645 and in ETSI TR 103 533. It is noted that if the secure by default approach is selected there will be no requirement to disable insecure functionalities as they will not exist.
GP-TM-09	Establish hard to crack, device-individual default passwords	ISO 27002 clause 9.2.4. This is not a recommended approach as the use of default passwords should be avoided. Addressed in TS 103 645 and in ETSI TR 103 533
GP-TM-10	Personal data must be collected and processed fairly and lawfully, it should never be collected and processed without the data subject's consent	ISO 27002 18.1.4 ISO 29100 ISO/IEC 29184 Online privacy notice and consent ISO 30141 clause 11.4 (Privacy and PII Protection). This is a pre-requisite in GDPR (Article 6 applies). Regarding consent not all parts of Article 6 apply (consent is not the only path to allow for lawful processing).
GP-TM-11	Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed	This is a pre-requisite in GDPR ISO 29100.

GP-TM-12	Minimise the data collected and retained	This is a pre-requisite in GDPR ISO 29100.
GP-TM-13	IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR)	No standardisation applies.
GP-TM-14	Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing	GDPR ISO 29100 ISO 30141 11.4 (ea: other PII standards to be identified)No specific standards apply. There are obligations from GDPR that address this and some ETSI best practices are being developed.
GP-TM-15	Design with system and operational disruption in mind, preventing the system from causing an unacceptable risk of injury or physical damage	ISO 27002 17.1.1
GP-TM-16	Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state	ISO 27031 (guidelines for information and communication technology readiness for business continuity)
GP-TM-17	Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems	ISO 27031 (guidelines for information and communication technology readiness for business continuity)By default an IoT device cannot operate in stand-alone mode, it is designed to be tethered to the Internet. This introduces a new mode to the IoT device.
GP-TM-18	Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins	Addressed in TS 103 645 and in ETSI TR 103 533.

GP-TM-19	Offer an automatic firmware update mechanism	Addressed in best practice guidance from ETSI and others
GP-TM-20	Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification	Addressed in best practice guidance from ETSI and others
GP-TM-21	Design the authentication and authorisation schemes (unique per device) based on the system-level threat models	29192 CD Lightweight cryptography --Part 7: Broadcast Requires a system wide threat analysis. Approaches to such threat analysis include ETSI TS 102 165-1, ISO27000 series, ISO15408 series and others for specific sectors. Frameworks for authentication protocol and authorisation schemes are defined in ETSI TS 102 165-2 and in ISO/IEC 29115.
GP-TM-22	Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed	ISO 27002 9.2.4, ISO 27002 9.4.2 ISO 27002 9.4.3 Addressed in TS 103 645 and in ETSI TR 103 533.
GP-TM-23	Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates	ISO/IEC 19790 Security requirements for cryptographic modules
GP-TM-24	Authentication credentials shall be salted, hashed and/or encrypted	ISO/IEC 19790 Security requirements for cryptographic modules
GP-TM-25	Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices	ISO/IEC 19790 Security requirements for cryptographic modules
GP-TM-26	Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms	ISO/IEC 19790 Security requirements for cryptographic modules

GP-TM-27	Limit the actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible	No standards apply. Best practice requirement
GP-TM-28	Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them. Device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code	No standards apply. Best practice requirement
GP-TM-29	Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy	ISO 27002 9
GP-TM-30	Ensure a context-based security and privacy that reflects different levels of importance	ISO 27002 8.2
GP-TM-31	Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity	ISO/IEC 19790 Security requirements for cryptographic modules
GP-TM-32	Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed	ISO/IEC 19790 Security requirements for cryptographic modules, ITU-T Y.4415 Reference architecture for IoT device capability exposure
GP-TM-33	Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections	ISO/IEC 15408-2 (to be further investigated)
GP-TM-34	Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation	ISO 27002 10
GP-TM-35	Cryptographic keys must be securely managed	See GP-Op-04

GP-TM-36	Build devices to be compatible with lightweight encryption and security techniques	See GP-Op-04
GP-TM-37	Support scalable key management schemes	No specific standards apply. Best practice requirement
GP-TM-38	Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud	ISO 27002 5 ISO 27034 (application security) ISO 27033 (network security) ISO 27040 (storage security) ISO 27017 (27002 for cloud services)
GP-TM-39	Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption	No specific standards apply. Best practice requirement
GP-TM-40	Ensure credentials are not exposed in internal or external network traffic	ISO/IEC 15408-2 (to be further investigated)
GP-TM-41	Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored	ISO/IEC 15408-2 (to be further investigated)
GP-TM-42	Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services	ISO/IEC 15408-2 (to be further investigated)
GP-TM-43	IoT devices should be restrictive rather than permissive in communicating	Best practice requirement
GP-TM-44	Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols	ISO/IEC 15408-2 (to be further investigated)
GP-TM-45	Disable specific ports and/or network connections for selective connectivity	ISO/IEC 15408-2 (to be further investigated)
GP-TM-46	Rate limiting. Controlling the traffic sent or received by a network to reduce the risk of automated attacks	No specific standards apply. Best practice requirement

GP-TM-47	Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimise the overall risk	ISO/IEC 27033 Network security (6 parts)
GP-TM-48	Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set	No specific standards apply. Best practice requirement
GP-TM-49	Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family	ISO/IEC 15408-2 (to be further investigated)
GP-TM-50	Ensure only necessary ports are exposed and available	No specific standards apply. Best practice requirement
GP-TM-51	Implement a DDoS-resistant and Load-Balancing infrastructure	No specific standards apply. Best practice requirement
GP-TM-52	Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc	No specific standards apply. Best practice requirement
GP-TM-53	Avoid security issues when designing error messages	ISO/IEC 15408-2 (to be further investigated)
GP-TM-54	Data input validation (ensuring that data is safe prior to use) and output filtering	ISO/IEC 15408-2 (to be further investigated)
GP-TM-55	Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. Logs must be preserved on durable storage and retrievable via authenticated connections	ISO/IEC 15408-2 (to be further investigated)
GP-TM-56	Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors	No specific standards apply. Best practice requirement
GP-TM-57	Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually	ISO 27002 12

Annex B: Proposal for security standards evolution in IoT realm

B.1 Introduction

As has been suggested in the main body of the present document there is a gap in standards only insofar as it is unclear what combination of standards, when applied to a product, service or system, will result in a recognizably secure IoT. The proposal presented below is to develop a processthat alongside some certification marking on IoT products and services, that gives assurance to the market that the IoT product is as secure as can be reasonably expected. As an example of how this process could work, we consider the case of Common Criteria (standardized in ISO/IEC 15408). It should be noted that this example does not imply that CC is an optimal or preferred approach in the context of IoT and serves only as an example to illustrate the generic process.

Accordingly, the overall concept is intended to build from best practice in evaluation of security claims that derive from the Common Criteria and to ensure that developers address how security claims will be evaluated both by professional evaluators and by the market. In the past (from 2010 roughly) ETSI has promoted a paradigm of “design for assurance” that has considered this form of development to ensure that developers undertake a risk analysis and provide a rationale for every security mechanism standardized for a product or service, whilst making clear the security claims of the protocol.

B.2 Conventional development of ST or PP

ISO/IEC 15408-1 contains detailed guidance on the development of technical specifications in the form of general description of the product type, called Protection Profile (PP) or dedicated one, called Security Target (ST). A product that is then characterized as a Target of Evaluation (ToE) and which has been developed according to content of either an ST or a PP could be the subject for further security evaluation. If an evaluator agrees that the ToE (the product) conforms to the claims made in the ST/PP then it is reasonable to claim the ToE (the product) is secure within the constraints described in the ST/PP. The process of developing security requirement for the ST/PP encompass several steps which are presented in Figure B.1 (numbers indicate steps in the process of producing the specification).

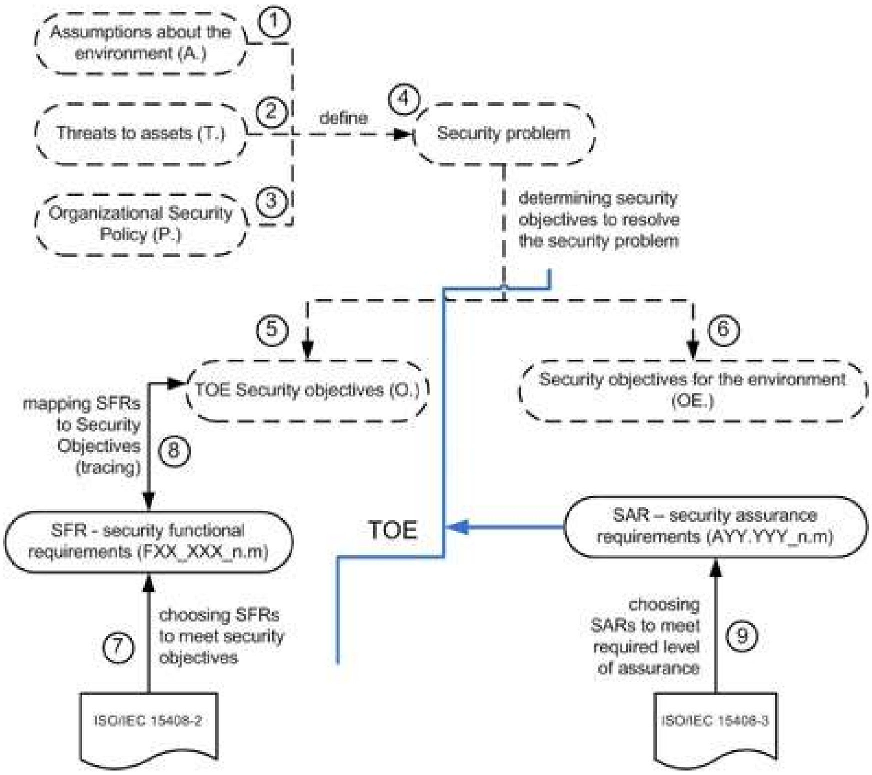

Assumptions about the environment (A.)
1
Threats to assets (T.)
2
Organizational Security Policy (P.)
3
define
4
Security problem
determining security objectives to resolve the security problem
5
6
TOE Security objectives (O.)
Security objectives for the environment (OE.)
mapping SFRs to Security Objectives (tracing)
8
SFR - security functional requirements (FXX_XXX_n.m)
TOE
SAR – security assurance requirements (AYY.YYY_n.m)
7
choosing SFRs to meet security objectives
choosing SARs to meet required level of assurance
9
ISO/IEC 15408-2
ISO/IEC 15408-3

Figure B.1: Regular approach to producing a technical specification (ST or PP)

The outcome of this process usually results in a lengthy technical specification which is difficult to understand for non-experienced users.

The idea of simplification of this time- and resource consuming process is present in the current version of ISO/IEC 15408-1 under the name of 'low assurance' ST/PP. However, its usage is restricted to the lowest level of assurance, i.e. EAL1 and only briefly discussed in the standard.

In a revised version of ISO/IEC 15408-1 the concept of 'low assurance' is replaced with a 'direct rationale' one. However, it is not only changing the name but the approach as well. The direct rationale is now one of the type of PP/ST with simplifying method of creating specifications. Moreover, it is not restricted to low assurance packages but can request a higher level of assurance.

B.3 Direct rationale approach for creating simpler and faster specifications

By definition, 'direct rationale' means a type of Protection Profile or Security Target in which the Security Problem Definition (SPD) elements (i.e. of Assumptions, Threats and Organizational Security Policies) are mapped directly to the Security Functional Requirements (SFRs) and, possibly Security Objectives for the operational environment (see Figure B.2).

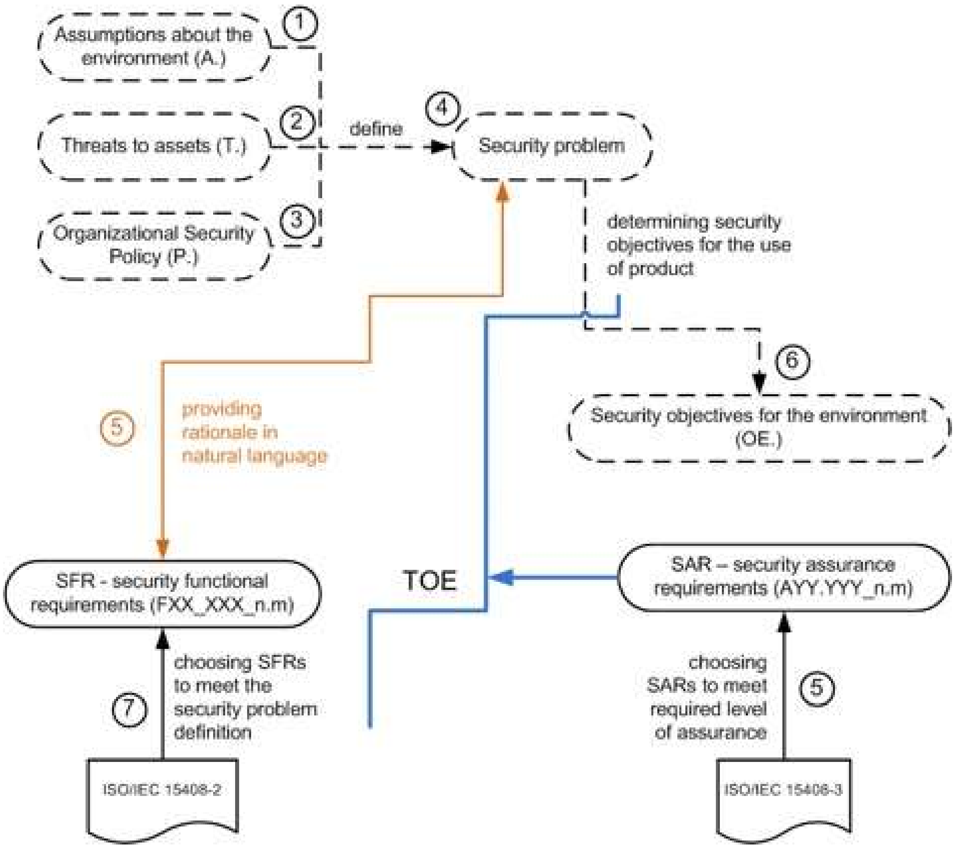

Assumptions about the environment (A.)
1
Threats to assets (T.)
2
Organizational Security Policy (P.)
3
define
4
Security problem
determining security objectives for the use of product
6
Security objectives for the environment (OE.)
5
providing rationale in natural language
SFR - security functional requirements (FXX_XXX_n.m)
TOE
SAR – security assurance requirements (AYY.YYY_n.m)
7
choosing SFRs to meet the security problem definition
choosing SARs to meet required level of assurance
5
ISO/IEC 15408-2
ISO/IEC 15408-3

Fig. 2 Using a 'Direct rationale' approach to create technical specifications

A Direct Rationale ST has all the following differences compared to a regular ST:

- no Security Objectives for the TOE are described. The Security Objectives for the operational environment must still be described;
- there is no Security Objectives rationale as there are no TOE Security Objectives in the ST;
- there is a requirement to provide natural language description of the SFRs and their relationship to security functionality regarding the architecture that is visible to Administrators and other users;
- the security requirements rationale directly maps the elements of the SPD to the SFRs and the Security Objectives for the operational environment.

A Direct Rationale PP has the same simplifications about a regular PP like a Direct Rationale ST to a regular ST.

Several ‘direct rationale’ PPs exist[3] and are in use as a base for Direct Rationale ST.

In the case of Direct Rationale ST/PP, Security Assurance Requirements (SARs) are usually not related to pre-defined Evaluation Assurance Levels (EALs). Instead of, there is a list of specific assurance components suitable for the specification. When the TOE is evaluated, there is no need to check every assurance

[3] See for example, collaborative Protection Profile for Full Drive 2 Encryption - Encryption Engine (https://www.commoncriteriaportal.org/files/ppfiles/CPP_FDE_EE_V2.0.pdf), collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition v2.0 (https://www.commoncriteriaportal.org/files/ppfiles/CPP_FDE_AA_V2.0.pdf)

component from the package. Such an approach could make evaluations faster and more cost-efficient than traditional ones.

In specific contexts, applicable to simple devices or products with a short Time-to-Market parameter or intended to be produced on a massive scale, the direct rationale approach could be a useful solution.

B.4 Composite evaluations suitable for IoT devices

The revised ISO/IEC 15408 series of standards also provides flexible approaches to evaluations, which could be potentially prove to be suitable for the IoT world. This approach is called a 'composite evaluation'. The composite evaluation takes place where one considers a product comprised of two or more components which can be organized in two layers: a layer of autonomous base component(s) and a layer of dependent components. The composite evaluation can be applied as many times as necessary to a multi-component/multi-layered product, in an incremental approach.

The composite product evaluation meets different types of objectives:

- independently perform one evaluation of a platform to address several applications and customers;
- create one or several applications to load on one or several certified platforms;
- install one or several applications onto one already certified platform to reduce the evaluation effort keeping a high level of confidence.

Composite evaluations have been developed for the smart card world as shown in Figure B.3 and appeared to be the most successful implementation of the CC certifications. Such an approach allows developers and evaluators to re-use results from previous evaluations thus reduce the time and cost the current one.

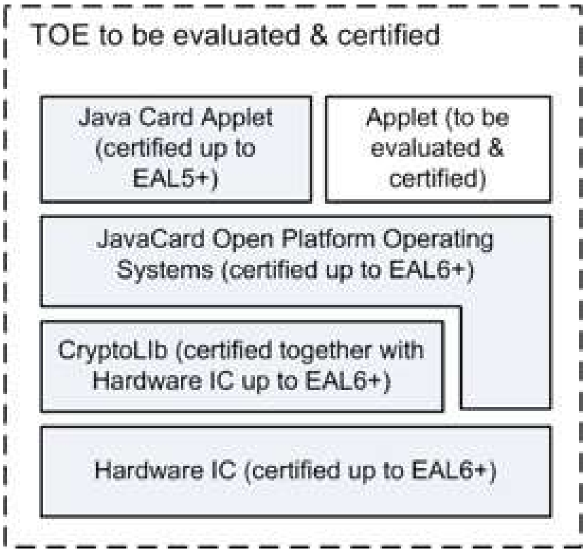

TOE to be evaluated & certified
Java Card Applet (certified up to EAL5+)
Applet (to be evaluated & certified)
JavaCard Open Platform Operating Systems (certified up to EAL6+)
CryptoLib (certified together with Hardware IC up to EAL6+)
Hardware IC (certified up to EAL6+)

Figure B. 3 Composite product evaluation in the smart card environment

Several constraints should be applied to the product development regarding conformity to take benefits from the re-use approach, but detailed discussion on this issue is outside the scope.

Considering layered architecture of certain IoT devices the composite evaluation approach introduced in the revised version of ISO/IEC 15408-1 could be under circumstances seen to be applicable to the IoT world.

A general architecture of an IoT device concerning the composite evaluation[4] is presented in Figure B.4.

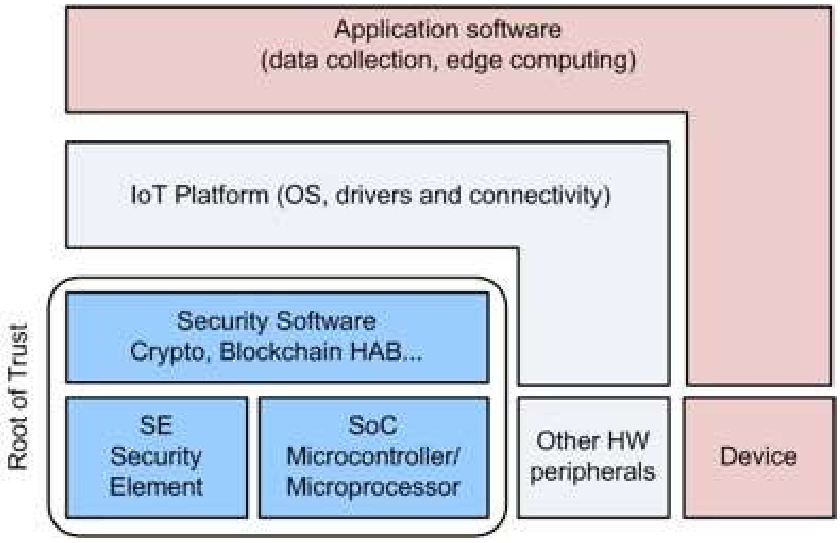


Figure B.4 Layered architecture of the IoT product with the concept of re-used evaluation results

The concept of 'root of trust' establish a base for cost-efficient security evaluations based on previously certified HW or HW-SW components and thus creates a highly controlled environment to execute higher layers of the IoT device architecture.

[44] The figure is adopted from Vetillard, E., Stütz, G., "Common Criteria as Backbone for IoT Security Certification", the 17th International Common Criteria Conference (ICCC) Amsterdam, 30 Oct – 01 Nov 2018

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number TP-07-18-076-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-275-2
DOI: 10.2824/713380