ETSI TS 103 701 V1.1.1 (2021-08)

CYBER;
Cyber Security for Consumer Internet of Things:
Conformance Assessment of Baseline Requirements

Reference
DTS/CYBER-0050

Keywords
cybersecurity, IoT, privacy

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

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

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

Introduction

ETSI TS 103 645 [1]/ETSI EN 303 645 [2] specifies provisions for secure Internet of Things (IoT) products which are widely considered as good practice in IoT security. There is a broad variety of consumer IoT products: some hold sensitive personal data or fulfil safety-relevant functions, while others provide basic functionality such as play music or monitor the weather. ETSI TS 103 645 [1]/ETSI EN 303 645 [2] is applicable to this entire spectrum and as such its provisions are necessarily high-level and outcome-focused.

Multiple public and private sector organizations are operating and developing assurance schemes for consumer IoT security. The present document is independent from an assurance scheme and seeks to contribute to a harmonised approach to assessing the conformance of consumer IoT products against ETSI TS 103 645 [1]/ETSI EN 303 645 [2].

1 Scope

The present document specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI TS 103 645 [1]/ETSI EN 303 645 [2], addressing the mandatory and recommended provisions as well as conditions and complements of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] by defining test cases and assessment criteria for each provision.

The present document intends to support suppliers or implementers of consumer IoT products in first-party assessment (self-assessment), user organizations in second party assessment, independent testing organizations in third party assessment and certification and conformance declaration scheme owners in operating harmonized schemes. Defining a certification or conformance declaration scheme is out of scope of the present document.

The present document intends to contribute to the protection of consumer IoT products against the most common cybersecurity threats. Multi-medium or highly targeted/sophisticated attacks and thus the invasive analysis of hard- and software modules is out of scope of the present document. The Test Scenarios (TSOs) are targeting basic effort regarding test depth and test circumference in accordance to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] which addresses a baseline security level.

Due to the heterogeneity of consumer IoT devices, ETSI TS 103 645 [1]/ETSI EN 303 645 [2] and therefore the associated test groups in the present document are formulated in a generic manner. Thus, the present document does not describe specific tools or detailed step-by-step instructions. The test cases are intended to be performed by competent bodies that have the expertise to derive a suitable test plan.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

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

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 645 (V2.1.2) (2020-06): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[2] ETSI EN 303 645 (V2.1.1) (2020-06): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

NOTE: ETSI EN 303 645 is intended to be regularly synchronized with ETSI TS 103 645 [1].

2.2 Informative references

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

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] EN ISO/IEC 17025: "General requirements for the competence of testing and calibration laboratories".

[i.2] NIST Cryptographic Algorithm Validation Program (CAVP).

NOTE: Available at https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program.

[i.3] Mozilla®, Security/Server Side TLS.

NOTE: Available at https://wiki.mozilla.org/Security/Server_Side_TLS.

[i.4] Overview of cryptographic key length recommendations.

NOTE: Available at https://www.keylength.com/.

[i.5] ISO/IEC 15408 (all parts): "Information technology - Security techniques - Evaluation criteria for IT security".

[i.6] ETSI TS 102 165-1 (V5.2.3) (2017-10): "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.7] ETSI TR 103 621 (V0.0.6) (2021-06): "CYBER; Guide to Cyber Security for Consumer Internet of Things".

NOTE: Not published yet.

[i.8] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[i.9] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 645 [1], ETSI EN 303 645 [2] and the following apply:

assess: generate a result by analysis using evaluator expertise

NOTE: The statement that uses this verb identifies what is analysed and the properties for which it is analysed. The combination with the term "functionally" indicates, that the analysis needs to be performed practically (e.g. using the DUT).

check: generate a result by a simple comparison

NOTE: Evaluator expertise is not required. The statement that uses this verb describes what is mapped. The combination with the term "functionally" indicates, that the comparison needs to be performed practically on the DUT.

Device Under Test (DUT): consumer IoT device (as defined in ETSI TS 103 645 [1]/ETSI EN 303 645 [2]) that is the target of the conformance assessment

Implementation Conformance Statement (ICS): statement, made by the SO, of the capabilities implemented in or supported by the DUT

Implementation Conformance Statement (ICS) pro forma: document, in the form of a questionnaire, which when completed for a DUT becomes the ICS

Implementation eXtra Information for Testing (IXIT): record which contains or references all of the information (in addition to that given in the ICS) related to the DUT and its assessment environment, which will enable the TL to perform appropriate test activities

Implementation eXtra Information for Testing (IXIT) pro forma: document, in the form of a questionnaire, which when completed for a DUT becomes the IXIT

indication: documented finding by the TL used inside the assessment to assign a verdict

security guarantee: statement of the addressed security objectives

NOTE: In the present document security guarantees are used in an IXIT to describe the security objectives (e.g. confidentiality) which are realized by an implementation or process.

Supplier Organization (SO): entity that is responsible for a significant part of the supply chain of a DUT

test case: complete and independent specification of the test units required to achieve a specific test purpose

NOTE: The specification is considered to be complete if it is sufficient to enable a test case verdict to be assigned unambiguously to each potentially observable test outcome. The specification is considered to be independent if it is sufficient to execute the test units in isolation from other test cases.

test group: named set of related test cases that describe how to assess the conformance of the DUT to a single provision as specified in ETSI TS 103 645 [1]/ETSI EN 303 645 [2]

NOTE: The naming of test groups and their corresponding provisions coincide.

test group objective: prose description of the common objective which the test purposes within a specific test group are designed to achieve

Test Laboratory (TL): entity such as an independent testing organization, a user organization, or an identifiable part of a SO that carries out conformance assessment of a DUT

test purpose: prose description of a well-defined purpose of assessment, focusing on a single conformance requirement or a set of related conformance requirements

Test Scenario (TSO): named set of related test groups that describe how to assess the conformance of the DUT to a corresponding set of provisions as specified in ETSI TS 103 645 [1]/ETSI EN 303 645 [2]

NOTE: The naming of TSOs (sets of tests groups) and their corresponding sets of provisions coincide.

test unit: indivisible unit of a specification of test activities

User Organization: person or organization that represents user' interest with respect to DUT

NOTE 1: This includes, for example, purchasers or users of products, or potential customers seeking to rely on a supplier's management system, or organizations representing those interests.

NOTE 2: A user organization typically carries out a second party assessment.

3.2 Symbols

Void.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
API	Application Programming Interface
ARM	Advanced RISC Machines
BL	Boot Loader
BSI	Federal Office for Information Security (Germany)
CC	Common Criteria
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DUT	Device Under Test
ECDSA	Elliptic Curve Digital Signature Algorithm
GDB	GNU Debugger
GPS	Global Positioning System
HSM	Hardware Security Module
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICS	Implementation Conformance Statement
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
IXIT	Implementation eXtra Information for Testing
JTAG	Joint Test Action Group
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control

NOTE: In context of addressing.

MAC	Message Authentication Code

NOTE: In context of cryptography.

N/A	Not Applicable
NIST	National Institute of Standards and Technology
NX	No eXecute
OAEP	Optimal Asymmetric Encryption Padding
OS	Operating System
PC	Personal Computer
PHP	Hypertext Preprocessor
PKCS	Public-Key Cryptography Standards
PSA	Platform Security Architecture
QR	Quick Response
RAM	Random Access Memory
RFC	Request for Comments
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
SO	Supplier Organization
SOAP	Simple Object Access Protocol
SOG-IS	Senior Officials Group Information Systems Security
SSH	Secure Shell
TBB	Trusted Board Boot
TEE	Trusted Execution Environment
TL	Test Laboratory
TLS	Transport Layer Security (Protocol)
TOE	Target of Evaluation
TS	Technical Specification
TSO	Test Scenario
TVRA	Threat Vulnerability and Risk Analysis

UBIFS	Unsorted Block Image File System
UNIX	Uniplexed Information and Computing Service
URL	Uniform Resource Locator
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

4 Conformance assessment methodology

4.1 Overview and document structure

Clause 4.2 describes the relevant roles and objects for the conformance assessment procedure.

Clause 4.3 describes the assessment procedure.

Clause 4.4 describes how to declare the conformity of the consumer IoT device to the provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] in the Implementation Conformance Statement (ICS).

NOTE 1: ETSI TS 103 645 can be updated before ETSI EN 303 645. The scope of the present document lists the compatible versions of ETSI TS 103 645/ETSI EN 303 645.

Clause 4.5 describes how to declare the corresponding security measures in the Implementation eXtra Information for Testing (IXIT) using IXIT pro forma.

Clause 4.6 describes the details for how to assign verdicts for test cases, test groups and finally, how to assign an overall verdict.

Clause 4.7 describes how to use external evidences instead of performing test groups to determine the conformance to a provision.

Clause 4.8 highlights different aspects that assessment schemes typically address in addition of the content provided in the present document.

Clause 5 contains the TSOs, where each TSO addresses a set of provisions from ETSI TS 103 645 [1]/ETSI EN 303 645 [2] and is composed of a set of test groups that describe the assessment for a single provision. Each test group is composed of a description of its objective and a set of test cases, where each test case describes how to assess a specific aspect of the corresponding provision. The number of the test case is appended to the test group number (e.g. Test case 5.1-3-2 for the second test case in Test group 5.1-3). Typically, the test cases distinguish two aspects:

- Conceptual: Assessing conformity of the IXIT against the requirements of the provision (conformity of design); and
- Functional: Assessing conformity of the DUT functionality, their relation to associated services or development/management processes against the requirements of the provision (conformity of implementation).

Each test case is composed of a description of its purpose, a set of indivisible test units and criteria for generating a test case verdict. The TSOs and test groups mirror the structure and naming of the provisions.

Figure 1 illustrates the relation between ETSI TS 103 645 [1]/ETSI EN 303 645 [2] and the present document with respect to a conformance assessment process. ETSI TS 103 645 [1]/ETSI EN 303 645 [2] contain provisions concerning cyber security for consumer IoT.

NOTE 2: Terms, examples, notes, definitions and explanations from ETSI TS 103 645/ETSI EN 303 645 are also valid and therefore not redundantly specified in the present document.

The present document is the basis for conformance assessment against ETSI TS 103 645 [1]/ETSI EN 303 645 [2] and defines the ICS and IXIT pro forma. ICS and IXIT are provided by the SO based on the ICS and IXIT pro forma to the TL. The TL uses these documents to derive a test plan.

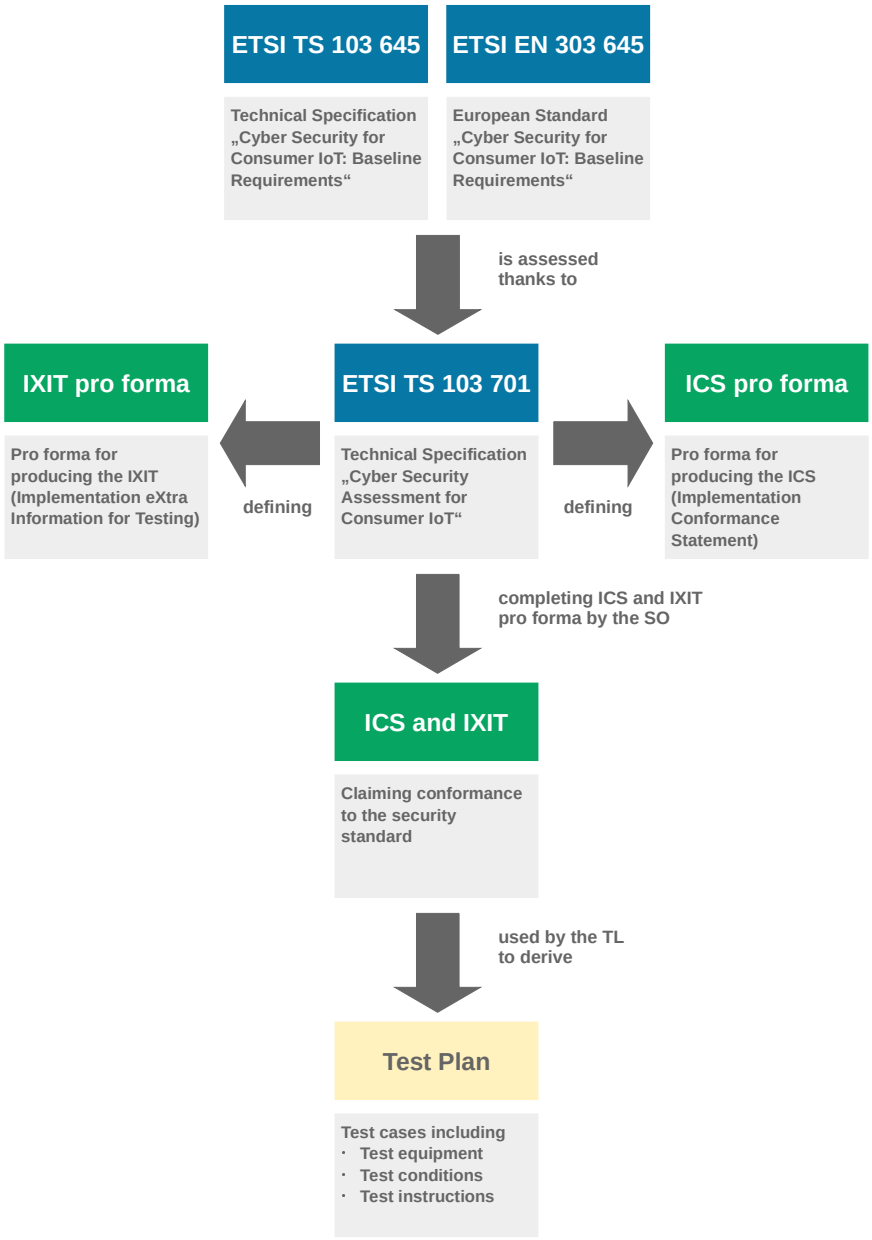

Figure 1: Relations of the present document with respect to a conformance assessment process

4.2 Roles and objects

4.2.1 Device Under Test (DUT)

The Device Under Test (DUT) is a specific consumer IoT device (as defined in ETSI TS 103 645 [1]/ETSI EN 303 645 [2]), which is subject to assessment against the provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2]. TSOs address the DUT functionality, its relation to associated services and development/management processes. For the assessment the most up-to-date software version of the DUT **should** be used. The TL is able to control the DUT via its offered interfaces and has partially knowledge about its design by the provided information in the IXIT (grey-box testing). It is assumed that the DUT is in live operation and the TL is not in control of the associated services which belong to the DUT.

NOTE: The methodology of the present document does not distinguish between different development stages within the life cycle. However, for an effective assessment and to support secure product development considering a separation between design and implementation phase is useful. Ultimately, a mature implementation allowing live operation is necessary to finalize the assessment in particular regarding the assessment of the relation to associated services and the publication of (user) information.

As illustrated in Figure 2, the present document intends to provide TSOs for a wide variety of consumer IoT devices with different interfaces. Thus, the formulation of TSOs provides a certain level of abstraction as it is not feasible to describe a specific testing procedure for every kind of consumer IoT device.

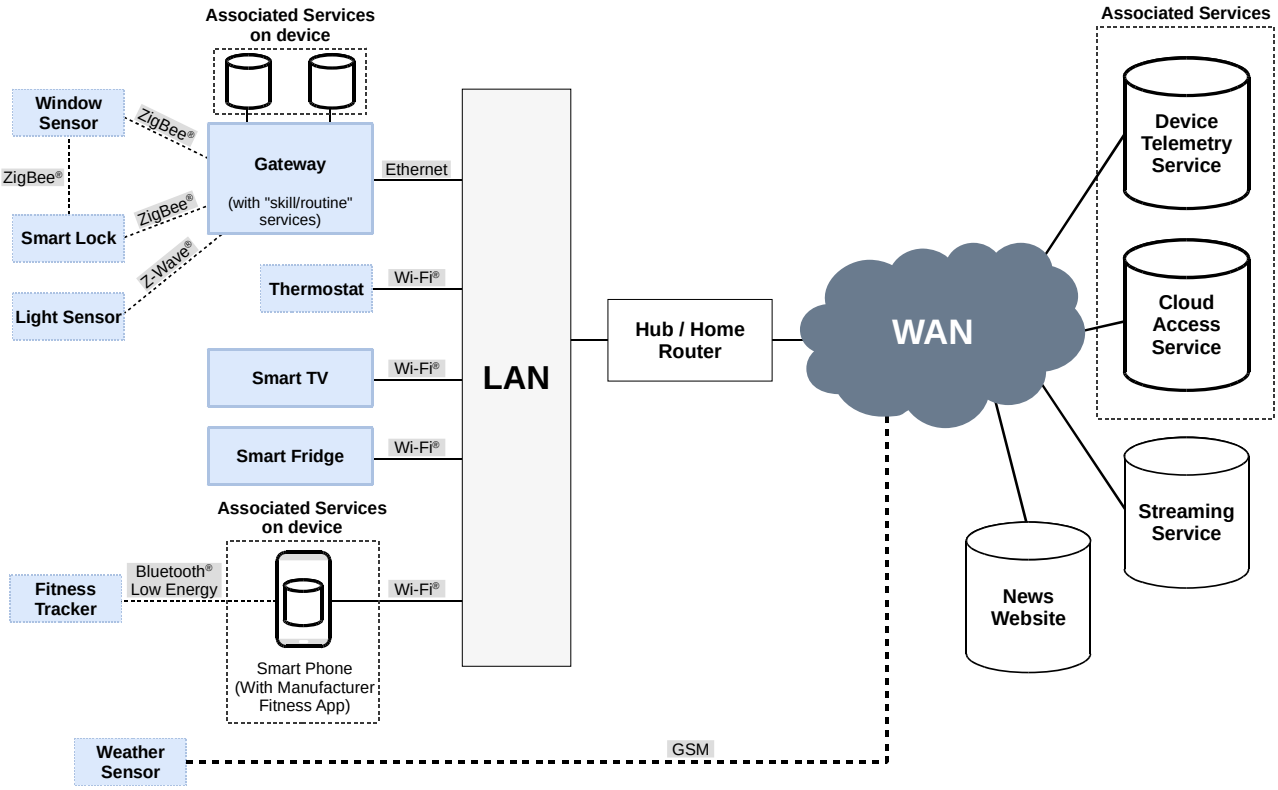

Figure 2: Examples for the heterogeneity of IoT implementations

4.2.2 Supplier Organization (SO)

The Supplier Organization (SO) requests a specific DUT to be tested against the provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2]. The SO can be the developer, manufacturer, vendor or distributor of the DUT. The SO usually serves as single point of contact to the TL, and is expected to coordinate with parties across the product's supply chain and ecosystem, such as component manufacturers, service providers and application developers.

The SO is supposed to have all necessary knowledge about the security measures of the DUT in order to provide the ICS and IXIT. The SO is the applicant for the assessment and is expected to support the TL by providing all necessary information for the assessment.

NOTE: The assessment process is designed for a cooperation between the TL and the SO. Accordingly, the SO provides reliable ICS and IXIT for the assessment. Otherwise, an assessment using parts of the present document is generally possible, but limits the validity of assessment results.

4.2.3 Test Laboratory (TL)

The Test Laboratory (TL) is (a defined part of) an entity that carries out the conformance assessment of a DUT. The relation to associated services and development/management processes of the DUT are partially also considered in the assessment (see ETSI TS 103 645 [1]/ETSI EN 303 645 [2]).

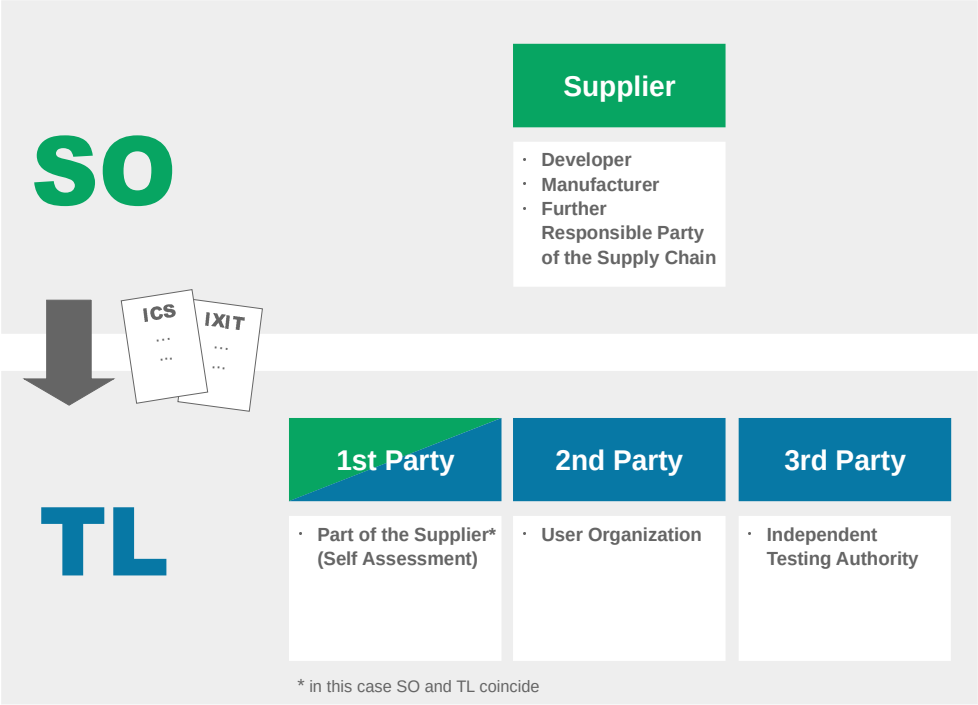

Figure 3: Test laboratory scenarios

The TL can be an identifiable part of a SO (1st party), a user organization (2nd party), or an independent testing authority (3rd party) as illustrated in Figure 3. It is assumed that the TL operates competently and is able to generate valid results.

NOTE: The competence of the TL has a strong influence on the validity of the assessment results. Requirements on the competence of the TL, as e.g. specified in EN ISO/IEC 17025 [i.1], are out of the scope of the present document.

4.3 Assessment procedure

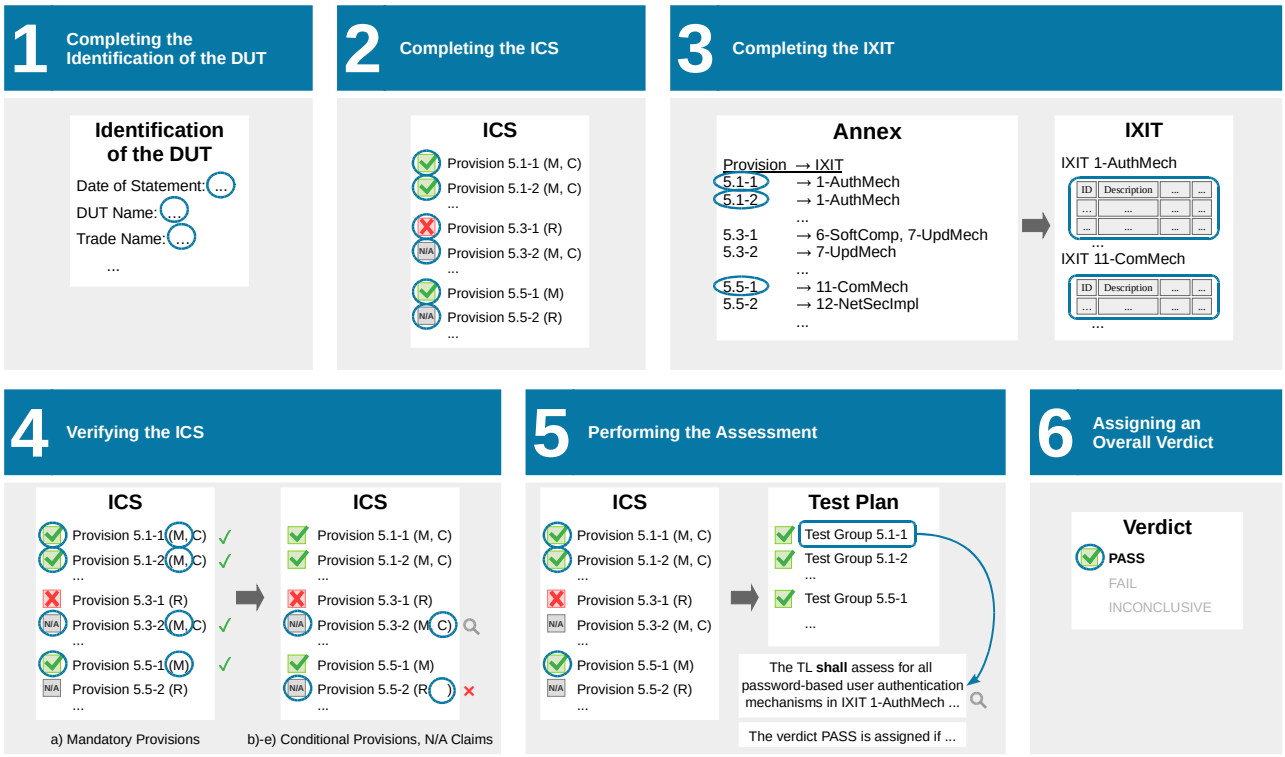

Figure 4: Phases of the assessment procedure (informative example)

The present clause provides an abstract procedure for performing the conformance assessment against the provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2]. The assessment procedure is performed by applying the following phases, which are illustrated in Figure 4.

Phase 1: Completing the Identification of the DUT

The SO **shall** complete the Identification of the DUT. The pro forma to be filled and submitted by the SO is found in clause A.2 of the present document.

Phase 2: Completing the ICS

The SO **shall** complete the ICS (see clause 4.4) in a correct manner. The pro forma to be filled and submitted by the SO (referred to as user of the present document) is found in clause A.3 of the present document.

NOTE 1: Correct manner means for example claiming conditional provision as "N/A" in accordance with the implemented functionality of the DUT. However, this does not oblige claiming recommended provisions as "Yes" if a corresponding functionality exists.

Phase 3: Completing the IXIT

The SO **shall** complete the necessary IXIT information (see clause 4.5) for all provisions claimed as "Yes" in the ICS. The pro forma to be filled and submitted by the SO is found in clause A.4 of the present document. Table B.1 gives an overview which IXIT information is necessary for each provision.

The verification of the completeness, consistency and soundness of the IXIT **shall** be done by the TL in coordination with the SO (contact person according to the Identification of the DUT). Annex C provides a sample IXIT to demonstrate the scope and the level of detail on completing the IXIT.

Phase 4: Verifying the ICS

The TL **shall** validate the ICS by:

a) verifying, that no mandatory provision (according to the status column in clause A.3) is claimed as "No"; and

b) verifying, that if a "N/A" is claimed on the base of condition 4 or 5 (according to clause A.3), the Identification of the DUT provides a valid "Justification" for the declaration of "Constrained Device" with respect to the definitions in ETSI TS 103 645 [1]/ETSI EN 303 645 [2]; and

c) verifying, that for all conditional provisions (according to the status column in clause A.3) claimed as "N/A" there are no indications that the condition is contrary to the ICS fulfilled by the DUT; and

NOTE 2: The consideration of the user documentation, IXIT and the Identification of the DUT are helpful for the plausibility verification of the "N/A" claims.

NOTE 3: The TL is not able to consider the assessment experience and results for the verification before performing the assessment (Phase 5). Therefore, the result of the plausibility verification can be revised if there are corresponding indications during the assessment. The final confirmation of the ICS verification is proceeded when assigning the overall verdict at the end of the assessment (Phase 6) including the assessment experience.

EXAMPLE 1: Provision 5.3-3 is marked as conditional regarding "an update mechanism is implemented" (condition 12) in clause A.3 and claimed as "N/A" in the ICS. If any update mechanism is implemented, the claim "N/A" is not correct.

d) verifying, that for all conditional provisions (according to the status column in clause A.3) claimed as "Yes" there are no indications that the condition is contrary to the ICS not fulfilled by the DUT, except for condition 4 and 5 (according to clause A.3); and

NOTE 4: The conditions 4 and 5 address the performance of the DUT (constrained device) and are not a technical prerequisite for applying the test cases. Therefore, these represent an exception and are not required to be verified herein.

EXAMPLE 2: Provision 5.1-1 is marked as conditional regarding "passwords are used" (condition 1) in clause A.3 and claimed as "Yes" in the ICS. If there are no passwords used by the DUT, the claim "Yes" is not correct.

e) verifying, that there are no non-conditional provisions (according to the status column in clause A.3) claimed as "N/A".

NOTE 5: The verification whether justifications for all not claimed recommended provisions exist is part of Phase 5 (see Test group 4-1).

Phase 5: Performing the assessment

The TL **shall** perform for each provision claimed as "Yes" in the ICS the corresponding test groups by devising a test plan for the DUT under consideration of the IXIT information. The deviation of the test plan **may** include restructuring and merging testing activities e.g. for optimization purposes where the same testing activity address multiple provisions.

NOTE 6: Some test cases require the verification of public documents (e.g. vulnerability disclosure policy) and the publication itself. The concept of the test plan provides flexibility e.g. concerning the assessment in development phase. Therefore pre-release documentations can be assessed in this phase such that only a final verification of the corresponding publication in live operation is necessary.

The TL **shall** choose a specific test method including test equipment, test conditions and test instructions for performing each test group. When assessment of the DUT functionality is required to perform a test group, the TL **shall** use tools that are appropriate for the test execution under consideration of the IXIT information. No specific test tools and test steps are prescribed by the test groups.

Each TSO defines test groups, test cases and test units. The TL **should** perform all test units on its own. However, the present document does not preclude any alternative entity to perform the defined test units.

Some test groups refer to examples of best practices. The references provided are neither exclusive nor exhaustive.

The TL **shall** assign a verdict for each test case and test group as described in clause 4.6. For the assignment of verdicts based on indications the TL **shall** document the used indications to achieve a reproducible result.

Phase 6: Assigning an overall verdict

The TL **shall** assign an overall verdict according to Table 1 in clause 4.6.

NOTE 7: According to Table 1 a verdict *PASS* means that all selected test groups on the base of the claimed provisions in a valid ICS, at least all mandatory provisions (see clause 4.5), are fulfilled. When the assessment ends with the assigned verdict *FAIL*, at least one claimed provision is not fulfilled or the verification of the ICS according to Phase 4 was not successful.

NOTE 8: The aim of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] is to apply as many provisions as possible to realize a secure DUT. If the assignment of an overall verdict pass is prevented due to a test group verdict *FAIL* or *INCONCLUSIVE* of a recommended provision, all assessment results can be reused for assigning an overall verdict *PASS* for an ICS that does not claim conformance to these recommended provision when a corresponding justification is provided.

NOTE 9: The details concerning the publication of the assessment results (e.g. definition of the specific content of an assessment report) are out of scope of the current document and usually determined in an assessment scheme. However, the publication of the ICS together with the overall verdict provides transparency, especially concerning the implementation of recommended provisions and therefore incentives for the SO to claim these provisions.

4.4 Implementation Conformance Statement (ICS)

The Implementation Conformance Statement (ICS) is made by the SO, of the capabilities implemented in or supported by the DUT on the base of the provisions from ETSI TS 103 645 [1]/ETSI EN 303 645 [2]. In the ICS the SO **shall** claim all provisions which are planned for the assessment. This is done by a written "Yes" in the "Support" column.

NOTE 1: The ICS pro forma required for an assessment based on the present document is located in clause A.3. It is expected that a future version of the present document uses an ICS pro forma from ETSI TS 103 645/ETSI EN 303 645.

The mandatory provisions **shall** be claimed by the SO to achieve an overall *PASS* verdict. If a conditional provision (mandatory or recommendation) cannot be fulfilled by the DUT a "N/A" (not applicable) **shall** be written in the "Support" column. For every "N/A" a justification **shall** be given in the "Detail" column by the SO. For all provisions not fulfilled but applicable by the DUT a "No" **shall** be written in the "Support" column. In this case also a justification **shall** be given in the "Detail" column.

NOTE 2: In terms of a conditional provision a constrained device (defined in ETSI TS 103 645/ETSI EN 303 645) represents a special case. It is possible to claim conformance against a conditional provision even it is not necessary for a constrained device to fulfil the provision.

NOTE 3: Further guidance to fill in the ICS is given in clause A.3.

4.5 Implementation eXtra Information for Testing (IXIT)

The Implementation eXtra Information for Testing (IXIT) contains additional necessary information to perform the assessment. It is the basis for grey-box testing methodology which is used for the assessment and provides some design details for the TL.

The IXIT pro forma is provided in clause A.4. This pro forma describes necessary information on the implementation of security measures addressing the corresponding provisions. In conjunction with the ICS (see clause 4.4) this information is necessary for preparing and performing assessment activities.

Typically, test groups in the whole document can refer to entries in the IXIT pro forma. The order of the IXIT tables and lists is oriented on the first use in the document. The SO is not required to complete all IXIT entries. Only entries necessary for the provisions claimed as "Yes" have to be completed by the SO. Therefore Table B.1 provides a mapping between provisions/test groups and IXIT entries.

The SO **shall** provide exhaustive and correct information on completing the IXIT. Annex C provides a sample IXIT the SO can orient on concerning scope and the level of detail of the necessary information. An *INCONCLUSIVE* verdict (see clause 4.6) **may** be assigned, if incomplete or insufficient IXIT information do not allow a proper test execution. Alternatively to filling the IXIT the SO **may** add references to existing documentation there. In this case the referenced documentation **shall** be provided by the SO to the TL. The identifiers inside the IXIT **shall** be used to enable a distinct reference to any entry in a table, e.g. sequential numbering.

4.6 Assignment of verdicts

In general there are three kinds of verdicts: an overall verdict, test group verdicts and test case verdicts. The overall verdict is i.a. composed of the results of the applied test groups (the test group verdicts). The test group verdicts are in turn i.a. composed of the results of the contained test cases (the test case verdicts). For the test case verdicts there are i.a. dedicated criteria in each test case for *PASS* and *FAIL* in the present clause.

The TL assigns the overall verdict according to the instructions of Table 1.

Table 1: Instructions for the assignment of the overall verdict

Overall verdict	Instruction
PASS	This verdict is assigned when no criterion for an overall verdict *FAIL* is fulfilled and: • the ICS is valid according to Phase 4 in clause 4.3; and • for each provision claimed as "Yes" in the ICS the corresponding test group is assigned a *PASS* verdict.
FAIL	This verdict is assigned when: • the ICS is not valid according to Phase 4 in clause 4.3; or • for at least one provision claimed as "Yes" in the ICS the corresponding test group is assigned a *FAIL* verdict.
INCONCLUSIVE	This verdict is assigned when no criterion for an overall verdict *FAIL* is fulfilled and: • for at least one provision claimed as "Yes" in the ICS the corresponding test group is assigned an *INCONCLUSIVE* verdict.

The test group verdicts are achieved by applying the test groups claimed as "Yes" in the ICS. The test group verdict is assigned according to the instructions of Table 2.

Table 2: Instructions for the assignment of a test group verdict

Test group verdict	Instruction
PASS	This verdict is assigned when no criterion for a test group verdict *FAIL* is fulfilled and: • each test case of the test group is assigned a *PASS* verdict; or • an external evidence is provided which fulfils the requirements described in clause 4.7.
FAIL	This verdict is assigned when: • at least one test case of the test group is assigned a *FAIL* verdict.
INCONCLUSIVE	This verdict is assigned when no criterion for a test group verdict *FAIL* is fulfilled and: • at least one test case of the test group is assigned an *INCONCLUSIVE* verdict.

The performance of each test case results in a test case verdict based on the criteria specified at the end of each test case ("Assignment of verdict"). The test case verdict is assigned according to the instructions of Table 3.

Table 3: Instructions for the assignment of a test case verdict

Test case verdict	Instruction
PASS	This verdict is assigned when: • the required elements for the test case performance are present; and • the criteria for *PASS* defined for each test case in the "Assignment of Verdict" are fulfilled.
FAIL	This verdict is assigned when: • the required elements for the test case performance are present; and • the criteria for *FAIL* defined for each test case in the "Assignment of Verdict" are fulfilled.

Test case verdict	Instruction
INCONCLUSIVE	This verdict is assigned when: • the required elements (e.g. evaluation tools and IXIT information) for the test case performance are not present or are not sufficient to allow a proper execution of the test case and therefore no meaningful *PASS* or *FAIL* verdict can be assigned.

4.7 Usage of external evidences

Existing security certifications or third party evaluations of parts of the DUT **may** be used partially as evidence for the conformance to reduce the effort of the assessment. In this case the SO **shall** announce in the "Detail" column of the addressed provision in the ICS that conformance is already assessed combined with a reference to the according evidence. Moreover the SO **shall** provide all necessary information (e.g. certification, certification details, test reports) for the verification of the evidence to the TL. The TL **shall** verify in the assessment whether the evidence is adequate to fulfil the corresponding test group. The following aspects **shall** be examined by the TL to assign a *PASS* verdict for the corresponding test group without applying the test cases:

- the scope of the evidence **shall** be appropriate to the corresponding test group objective; and
- the description of the test activities being part of the evidence **shall** meet each test purpose inside the corresponding test group; and
- the test depth respectively the evaluation assurance level of the evidence **shall** be appropriate to the corresponding level addressed by the test group.

4.8 Assessment scheme amendments

An assessment scheme typically provides a frame for the performance of an assessment. ETSI TS 103 645 [1]/ETSI EN 303 645 [2] and the present document can be used by an assessment scheme, such as a manufacturer scheme, a self assessment scheme or a certification scheme. Figure 5 illustrates the role of an assessment scheme and the possible integration of amendments regarding ETSI TS 103 645 [1]/ETSI EN 303 645 [2] and the present document.

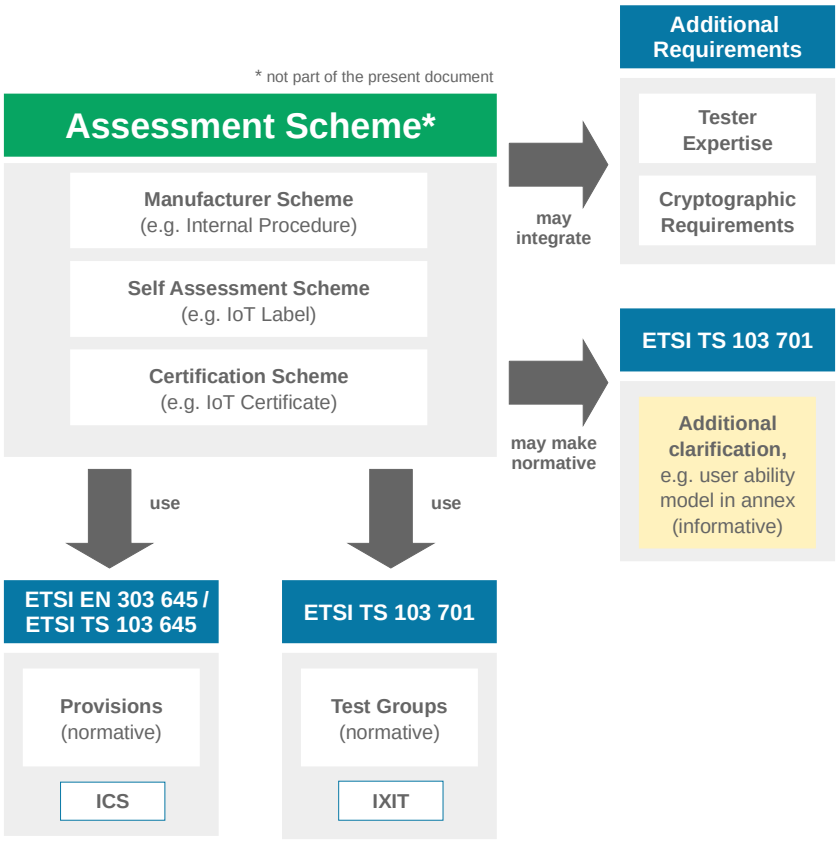

Figure 5: Role of an assessment scheme

On the base of the generic provisions from to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] it is not possible to derive specific criteria for every kind of implementation for each test case. Therefore the experience of the TL is needed to adapt the given criteria in the test cases if necessary. The requirements on the experience and equipment of the TL are typically part of an assessment scheme.

The present document contains informative content concerning best practice security. In particular cryptographic requirements are typically defined by the assessment scheme considering the corresponding information in the present document and the properties of the technology, risk and usage. This allows comparability of the assessment results under a specific scheme.

NOTE: In the cases of a certification scheme this type of specification is typically done by the party which is responsible for the scheme. Otherwise in an internal assessment scheme this is normally done by a part of the SO (e.g. testing division).

The assessment scheme typically specifies requirements for third party evidence (e.g. certificate from another certification scheme) that is accepted within an assessment (see clause 4.7).

5 Test scenarios for consumer IoT

5.0 TSO 4: Reporting implementation

5.0.1 Test group 4-1

5.0.1.0 Test group objective

The test group addresses the provision 4-1.

5.0.1.1 Test case 4-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the justifications for recommendations that are considered to be not applicable for or not fulfilled by the DUT.

Test units

a) The TL **shall** check whether a justification is given in the ICS for each recommendation that is considered to be not applicable for or not fulfilled by the DUT.

Assignment of verdict

The verdict PASS is assigned if:

- a justification is given for every recommendation that is considered to be not applicable for the DUT; and
- a justification is given for every recommendation that is considered to be not fulfilled by the DUT.

The verdict FAIL is assigned otherwise.

5.1 TSO 5.1: No universal default passwords

5.1.1 Test group 5.1-1

5.1.1.0 Test group objective

The test group addresses the provision 5.1-1.

This test group addresses all states of the DUT with the exception of factory default.

5.1.1.1 Test case 5.1-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the password-based authentication mechanisms.

Test units

a) The TL **shall** assess for all password-based user authentication mechanisms in IXIT 1-AuthMech where passwords are not defined by the user according to "Authentication Factor" and used in any state other than the factory default whether the "Password Generation Mechanism" ensures that passwords are unique per device.

Assignment of verdict

The verdict PASS is assigned if:

- each password of a password-based authentication mechanism being used in any state other than the factory default, that is not defined by the user, is unique per device.

The verdict FAIL is assigned otherwise.

5.1.1.2 Test case 5.1-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the password-based authentication mechanisms concerning the completeness of the IXIT documentation a), the passwords defined by the user b) and the generation mechanisms c).

Test units

a) The TL **shall** functionally assess whether password-based authentication mechanisms that are not documented in IXIT 1-AuthMech are available via a network interface on the DUT or described in the user manual.

EXAMPLE: Network scanning tools allow for discovery of network-based authentication mechanisms.

b) For each password-based user authentication mechanism in IXIT 1-AuthMech, the TL **shall** functionally check whether the user is required to define all passwords that are user-defined according to "Authentication Factor" before being used.

c) The TL **shall** functionally assess whether all passwords of the DUT, that are not defined by the user according to "Authentication Factor" in IXIT 1-AuthMech and used in any state other than the factory default, do not violate the description of the "Password Generation Mechanism".

Assignment of verdict

The verdict PASS is assigned if:

- every discovered password-based authentication mechanism is documented in the IXIT; and
- the user is required to define all passwords before being used, that are stated as defined by the user in the IXIT; and
- there is no indication that the generation of a not user-defined password of the DUT used in any state other than the factory default differs from the generation mechanism described in the IXIT.

The verdict FAIL is assigned otherwise.

5.1.2 Test group 5.1-2

5.1.2.0 Test group objective

The test group addresses the provision 5.1-2.

5.1.2.1 Test case 5.1-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the generation mechanisms of pre-installed passwords.

Test units

a) The TL **shall** assess for each authentication mechanism in IXIT 1-AuthMech using pre-installed passwords according to "Authentication Factor", whether the generation mechanism in "Password Generation Mechanism" induces obvious regularities in the resulting passwords.

NOTE 1: Incremental counters (such as "password1", "password2" and so on) can be obvious regularities.

b) The TL **shall** assess whether the generation mechanism induces common strings or other common patterns in the resulting passwords.

NOTE 2: Common strings can be those contained in password dictionaries, such as for example: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt.

c) The TL **shall** assess whether the generation mechanism induces passwords, that are related in an obvious way to public information.

NOTE 3: Public information can be MAC addresses, Wi-Fi® SSIDs, name, type and description of the device.

d) The TL **shall** assess whether the generation mechanism induces passwords, that are considered appropriate in terms of complexity.

NOTE 4: In this context complexity is linked to the probability of guessing the password while applying the information an attacker has. The length of a password is one important aspect to consider for a password's complexity.

Assignment of verdict

The verdict PASS is assigned if:

- no obvious regularities in pre-installed passwords are found; and
- no common strings or other common patterns in pre-installed passwords are found; and
- the generation mechanisms for pre-installed passwords do not induce passwords, that are related in an obvious way to public information; and
- the generation mechanisms for pre-installed passwords are considered appropriate in terms of complexity.

The verdict FAIL is assigned otherwise.

5.1.2.2 Test case 5.1-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the generation mechanisms of pre-installed passwords.

Test units

a) For each authentication mechanism in IXIT 1-AuthMech using pre-installed passwords according to "Authentication Factor", the TL **shall** functionally assess whether the generation mechanism is plausibly implemented in accordance to the description in "Password Generation Mechanism".

EXAMPLE: The description of the "Password Generation Mechanism" states, that passwords consist of 8 digits containing at least one character of each group uppercase letters, lowercase letters and numbers. The verification that the corresponding passwords of the DUT match the given length of 8 digits, containing at least one character of the stated groups and do not contain special characters can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if:

- for each pre-installed password there is no indication, that its generation differs from the generation mechanism described in the IXIT.

The verdict FAIL is assigned otherwise.

5.1.3 Test group 5.1-3

5.1.3.0 Test group objective

The test group addresses the provision 5.1-3.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] best practice cryptography is defined as cryptography that is suitable for the corresponding use case and has no indication of a feasible attack with current readily available techniques.

The objective of this test group is to assess, firstly, whether the cryptographic methods provide the security guarantees that are necessary for the authentication mechanisms and, secondly, whether the cryptographic methods are not known to be vulnerable to a feasible attack.

5.1.3.1 Test case 5.1-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for the authentication mechanisms concerning the use of best practice cryptography (a-c) and the vulnerability to a feasible attack d).

Test units

a) For each authentication mechanism in IXIT 1-AuthMech used to authenticate users against the DUT, the TL **shall** assess whether the "Security Guarantees" are appropriate for the use case of user authentication, at least integrity and authenticity are required to be fulfilled.

b) For each authentication mechanism in IXIT 1-AuthMech used to authenticate users against the DUT, the TL **shall** assess whether the mechanism according to "Description" is appropriate to achieve the "Security Guarantees".

NOTE 1: A holistic approach is required to assess the security of the mechanism.

c) For each authentication mechanism in IXIT 1-AuthMech used to authenticate users against the DUT, the TL **shall** assess whether the "Cryptographic Details" are considered as best practice cryptography for the use case of user authentication based on a reference catalogue. If "Cryptographic Details" are not included in a reference catalogue for the corresponding use case (e.g. novel cryptography), the SO **shall** provide evidences, e.g. a risk analysis, to justify the cryptography is appropriate as best practice for the use case. In such case the TL **shall** assess whether the evidence is appropriate and reliable for the use case.

NOTE 2: A use case based list of examples for best practice cryptography is given in ETSI TR 103 621 [i.7]. Moreover general reference catalogues of best practice cryptography are available, for example:

- SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu).

NOTE 3: A cryptographic algorithm or primitive that is deprecated with regard to its desired security property (e.g. SHA1 for collision resistance) or that relies on a cryptographic parameter (e.g. key-size) that is not appropriate, taking into account the intended lifetime of the DUT and cryptoagility, cannot be considered as best practice cryptography.

d) For each authentication mechanism in IXIT 1-AuthMech used to authenticate users against the DUT, the TL **shall** assess whether the "Cryptographic Details" are not known to be vulnerable to a feasible attack for the desired security property on the base of the "Security Guarantees" by reference to competent cryptanalytic reports.

NOTE 4: Competent cryptanalytic reports are typically published in the scientific literature or, alternatively, are to be provided by the SO. Further, clause D.2 provides information about the expected attack potential for level basic.

Assignment of verdict

The verdict PASS is assigned if for all user authentication mechanisms:

- the security guarantees are appropriate for the use case of user authentication; and
- the mechanism is appropriate to achieve the security guarantees with respect to the use case; and
- all used cryptographic details are considered as best practice for the use case; and
- all used cryptographic details are not known to be vulnerable to a feasible attack for the desired security property.

The verdict FAIL is assigned otherwise.

5.1.3.2 Test case 5.1-3-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the cryptography used for the authentication mechanisms.

Test units

a) For each authentication mechanism in IXIT 1-AuthMech used to authenticate users against the DUT, the TL **shall** functionally assess whether the described "Cryptographic Details" are used by the DUT.

EXAMPLE 1: Using a protocol analyser or packet sniffer tool for network-based mechanisms.

EXAMPLE 2: If a PKI certificate based authentication is used, sniffing the used certificates and comparing the properties with the described cryptography in the IXIT can be helpful to collect an indication.

EXAMPLE 3: If the underlying communication protocol of the authentication mechanism enables different security modes for the communication, trying to downgrade the security mode can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any used cryptographic setting differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.1.4 Test group 5.1-4

5.1.4.0 Test group objective

The test group addresses the provision 5.1-4.

5.1.4.1 Test case 5.1-4-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the mechanisms to change authentication values.

Test units

a) The TL **shall** assess whether for every authentication mechanism in IXIT 1-AuthMech where "Description" indicates that the mechanism is used for user authentication, the resource of "Documentation of Change Mechanisms" in IXIT 2-UserInfo considers the mechanism and describes how to change the authentication value for the mechanism in a manner that is understandable for a user with limited technical knowledge (see clause D.3).

Assignment of verdict

The verdict PASS is assigned if:

- for all user based authentication mechanisms the published resource describes how to change the authentication value with a simple mechanism.

The verdict FAIL is assigned otherwise.

5.1.4.2 Test case 5.1-4-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the mechanisms to change authentication values.

Test units

a) The TL **shall** perform a change of the authentication values for all user authentication mechanisms in IXIT 1-AuthMech as documented in the resource from "Documentation of Change Mechanisms" in IXIT 2-UserInfo.

b) The TL **shall** functionally assess whether all changes of user authentication values are successful.

EXAMPLE: The old authentication value is no longer valid and the new authentication value is valid after a change.

Assignment of verdict

The verdict PASS is assigned if:

- all mechanisms for the user to change authentication values for user authentication mechanisms work as described.

The verdict FAIL is assigned otherwise.

5.1.5 Test group 5.1-5

5.1.5.0 Test group objective

The test group addresses the provision 5.1-5.

5.1.5.1 Test case 5.1-5-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the mechanisms to make brute force attacks via network interfaces impracticable.

Test units

a) The TL **shall** assess whether for each authentication mechanism in IXIT 1-AuthMech, where "Description" indicates that the mechanism is directly addressable via a network interface, the mechanism in "Brute Force Prevention" makes brute force attacks via network interfaces impracticable.

NOTE 1: Methods to mitigate brute force attacks are, among others:

- Time delays between consecutive failed attempts to authenticate.
- A limited number of authentication attempts, followed by a suspension period where no login is allowed.
- A limited number of authentication attempts, followed by locking the authentication mechanism.
- Appropriate entropy for authentication values based on best practice cryptography.
- Two-factor authentication.

NOTE 2: There are best practices for brute force protection available, e.g. https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks.

Assignment of verdict

The verdict PASS is assigned if:

- the documented mechanisms make brute force attacks via network interfaces impracticable.

The verdict FAIL is assigned otherwise.

5.1.5.2 Test case 5.1-5-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the mechanisms to make brute force attacks via network interfaces impracticable concerning the completeness of the IXIT documentation a) and the corresponding mechanisms b).

Test units

a) The TL **shall** functionally assess whether there exist further network-based authentication mechanisms, that are not listed in IXIT 1-AuthMech.

NOTE: Methods for functionally checking for network-based authentication methods include network scanners such as "nmap", or wireless sniffers such as a BLE dongle.

b) The TL **shall** attempt to brute force every network-based authentication mechanisms described in IXIT 1-AuthMech.

Assignment of verdict

The verdict PASS is assigned if:

- ever discovered network-based authentication mechanism is documented in the IXIT; and
- for all authentication mechanism via network interfaces there is no indication that the implementation of brute force prevention differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.2 TSO 5.2: Implement a means to manage reports of vulnerabilities

5.2.1 Test group 5.2-1

5.2.1.0 Test group objective

The test group addresses the provision 5.2-1.

5.2.1.1 Test case 5.2-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the publication of the vulnerability disclosure policy.

Test units

a) The TL **shall** assess whether access to the publication as described in "Publication of Vulnerability Disclosure Policy" in IXIT 2-UserInfo is possible without meeting criteria such as user account, i.e. whether anybody can access the documentation.

NOTE: A website of the manufacturer is considered as appropriate.

Assignment of verdict

The verdict PASS is assigned if:

- the publication of the vulnerability disclosure policy is available for anybody.

The verdict FAIL is assigned otherwise.

5.2.1.2 Test case 5.2-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the publication of the vulnerability disclosure policy.

Test units

a) The TL **shall** functionally check whether the vulnerability disclosure policy is publicly accessible as described in "Publication of Vulnerability Disclosure Policy" in IXIT 2-UserInfo.

b) The TL **shall** functionally check whether the policy contains:

- contact information; and
- information on timelines regarding acknowledgement of receipt and status updates.

NOTE: Information on timelines provides flexibility to describe time values (e.g. "7 days", "quickly", etc.). Further, it also allows to describe whether or how a timeline is created in the case of a reported vulnerability.

Assignment of verdict

The verdict PASS is assigned if:

- the vulnerability disclosure policy is publicly accessible; and
- the vulnerability disclosure policy contains contact information and information on timelines regarding acknowledgement of receipt and status updates.

The verdict FAIL is assigned otherwise.

5.2.2 Test group 5.2-2

5.2.2.0 Test group objective

The test group addresses the provision 5.2-2.

5.2.2.1 Test case 5.2-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the manner in which vulnerabilities are acted on a) and the confirmation that the preconditions for the implementation are ensured b).

Test units

a) The TL **shall** assess whether the "Action" and the "Time Frame" of each disclosed vulnerability in IXIT 3-VulnTypes facilitate that vulnerabilities are acted on in a timely manner under consideration of the vulnerability disclosure policy according to "Publication of Vulnerability Disclosure Policy" in IXIT 2-UserInfo.

NOTE 1: The consideration of severity and criticality of the addressed vulnerabilities and the kind of vulnerability (e.g. firmware, hardware or software) is helpful.

NOTE 2: The amount of collaboration between the involved entities, the number of process steps and clearly defined responsibilities are important indicators for a timely deployment.

NOTE 3: In the case that a third party is involved (e.g. a software library vendor) the documentation of the point of contacts and defined procedures for the collaboration are indicators for a timely deployment.

NOTE 4: The comparison with the time frame for acting on vulnerabilities of similar types of IoT products is helpful.

b) The TL **shall** check whether "Confirmation of Vulnerability Actions" in IXIT 4-Conf states a confirmation.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any described kind of vulnerability is not acted on timely; and

- a confirmation for the implementation is given.

The verdict FAIL is assigned otherwise.

5.2.3 Test group 5.2-3

5.2.3.0 Test group objective

The test group addresses the provision 5.2-3.

5.2.3.1 Test case 5.2-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of continuous monitoring, identifying and rectifying security vulnerabilities concerning the described procedures (a-c) and the confirmation that the preconditions for the implementation are ensured d).

Test units

a) The TL **shall** assess whether the way of continuously monitoring for security vulnerabilities documented in IXIT 5-VulnMon is suited to systematically gather information about security vulnerabilities that potentially can affect the DUT.

b) The TL **shall** assess whether the way of identifying security vulnerabilities documented in IXIT 5-VulnMon is suited to determine if and how a security vulnerability can affect the DUT.

c) The TL **shall** assess whether the way of rectifying security vulnerabilities documented in IXIT 5-VulnMon is suited to address and mitigate the susceptibility of a DUT against a security vulnerability.

d) The TL **shall** check whether "Confirmation of Vulnerability Monitoring" in IXIT 4-Conf states a confirmation.

Assignment of verdict

The verdict PASS is assigned if:

- the described way is suited for continuously monitoring for security vulnerabilities; and
- the described way is suited for identifying security vulnerabilities; and
- the described way is suited for rectifying security vulnerabilities; and
- a confirmation for the implementation is given.

The verdict FAIL is assigned otherwise.

5.3 TSO 5.3: Keep software updated

5.3.1 Test group 5.3-1

5.3.1.0 Test group objective

The test group addresses the provision 5.3-1.

This test group handles the updatability of each software components except software updates are beyond practicability or absent for a security reason. According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] "securely updateable" means that there are adequate measures to prevent an attacker misusing the update mechanism.

NOTE: Any discovery of software components in the DUT is out of scope of this test group.

5.3.1.1 Test case 5.3-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the updatability of software components concerning the absence of software updates a) and the update mechanisms b).

Test units

a) For each software component in IXIT 6-SoftComp with an empty list in "Update Mechanism", the TL **shall** assess whether the implementation of software updates is beyond practicability or for a security reason as described in the justification for the absence of software updates.

EXAMPLE 1: An IoT device can contain separate microcontrollers from the main system which are only internally addressable. Those microcontrollers typically act as an internal service provider (e.g. temperature controller of a smart wine rack) sometimes without update functionality. A software update for those components can be beyond practicability for the DUT.

EXAMPLE 2: For some implementations, the security concept for the DUT can require that a component is not changeable (e.g. software which is part of the trust chain of the bootloader). Therefore the component is not updateable for superordinate security reasons.

b) The TL **shall** apply all test units as specified in the Test case 5.3-2-1 to every referenced "Update Mechanism" in IXIT 6-SoftComp.

Assignment of verdict

The verdict PASS is assigned if:

- for all software components without the ability for software updates, a software update is not possible for practicability reasons or security reasons; and
- no update mechanism can be misused by an attacker.

The verdict FAIL is assigned otherwise.

5.3.1.2 Test case 5.3-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the effectiveness of the update mechanisms to avoid misuse.

Test units

a) The TL **shall** apply all test units as specified in the Test case 5.3-2-2 to every referenced "Update Mechanism" in IXIT 6-SoftComp.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that a misuse of any update mechanism is possible.

The verdict FAIL is assigned otherwise.

5.3.2 Test group 5.3-2

5.3.2.0 Test group objective

The test group addresses the provision 5.3-2.

This test group examines that at least one update mechanism for the secure installation of software updates exists.

5.3.2.1 Test case 5.3-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the update installation mechanism concerning adequate measures to prevent an attacker misusing the update installation on the DUT.

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the design of the update mechanism prevents misuse from an attacker according to the "Security Guarantees", the corresponding "Description", "Cryptographic Details" and "Initiation and Interaction".

NOTE: The consideration of the baseline attacker model described in clause D.2 is helpful for the examination.

EXAMPLE: A misuse can be the installation of an old software update to downgrade the security capabilities of the DUT or the injection of malware by manipulating a valid update.

Assignment of verdict

The verdict PASS is assigned if:

- one update mechanism of the DUT cannot be misused by an attacker.

The verdict FAIL is assigned otherwise.

5.3.2.2 Test case 5.3-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the effectiveness of the update mechanism to avoid misuse.

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** devise functional attacks to misuse the update mechanism based on the "Description".

EXAMPLE 1: If applicable try a Man-In-The-Middle attack (MITM) between the DUT and the update server.

NOTE 1: An attack can be trying to resume the sequence of update steps after some failure of a specific update step, installing an older firmware version that contains security vulnerabilities, or changing one byte in a signed firmware to check that it is rejected.

NOTE 2: There are multiple ways to perform an indication based security analysis even if no update is available during the assessment, e.g. verify a file based update mechanism on the base of old update packages.

b) The TL **shall** attempt to misuse each update mechanism on the base of the devised adverse actions and assess whether the design of the mechanism (see "Description", the "Cryptographic Details" and "Initiation and Interaction") effectively prevents the misuse of software updates as described in the "Security Guarantees".

EXAMPLE 2: If a file based update mechanism uses signature verifications, providing a manipulated update package to the DUT can be helpful to collect indications.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that a misuse of one update mechanism of the DUT is possible.

The verdict FAIL is assigned otherwise.

5.3.3 Test group 5.3-3

5.3.3.0 Test group objective

The test group addresses the provision 5.3-3.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] in terms of this test group an update that is simple to apply will be automatically applied, or initiated using an associated service (such as a mobile application) or via a web interface on the device. However, this does not exclude alternative solutions.

The focus of the provision is on triggering the update from the user perspective and verifying whether the user is provided with the ability to update all software components in a simple manner. This case is given if each software component is updatable with at least one simple update mechanism.

5.3.3.1 Test case 5.3-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the update mechanisms concerning simplicity for the user to apply an update.

Test units

a) For each software component in IXIT 6-SoftComp, the TL **shall** assess whether at least one "Update Mechanism" is described, which is simple for the user to apply according to "Initiation and Interaction" in IXIT 7-UpdMech based on the following factors:

- the software update is automatically applied without requiring any user interaction; or
- the software update is initiated via an associated service; or
- the software update is initiated via a web interface on the device; or
- the software update uses a comparable approach which is applicable for the user with limited technical knowledge (see clause D.3).

Assignment of verdict

The verdict PASS is assigned if:

- each software component is covered by at least one update mechanism, which is simple for the user to apply.

The verdict FAIL is assigned otherwise.

5.3.4 Test group 5.3-4

5.3.4.0 Test group objective

The test group addresses the provision 5.3-4.

Automatic mechanisms for software updates consider the checking for update availability and performing the update.

The focus of the provision is on triggering the update from the user perspective and verifying whether the user is provided with the ability to update all software components automatically. This case is given if each software component is updatable with at least one automatic update mechanism.

5.3.4.1 Test case 5.3-4-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the update mechanisms concerning automatic mechanisms.

Test units

a) For each software component in IXIT 6-SoftComp, the TL **shall** assess whether at least one "Update Mechanism" is described in IXIT 7-UpdMech, that allows:

   - the performance of updates without requiring any user interaction according to "Initiation and Interaction"; and

   - the "Update Checking" without requiring any user interaction.

b) For each software component in IXIT 6-SoftComp covered by an "Update Mechanism" in IXIT 7-UpdMech with the capability to configure the automation according to "Configuration", the TL **shall** check whether at least one of the automatic mechanisms is enabled by default.

Assignment of verdict

The verdict PASS is assigned if:

- each software component is covered by at least one update mechanism that does not require any user interaction for performing an update and for checking the availability of an update; and

- for each software component covered by a configurable update mechanism at least one of the automatic mechanisms is enabled by default.

The verdict FAIL is assigned otherwise.

5.3.5 Test group 5.3-5

5.3.5.0 Test group objective

The test group addresses the provision 5.3-5.

The focus of the provision is on the ability to check for security updates for the software of the DUT. This case is given if each software component is updatable with at least one update mechanism checking for security updates after initialization and periodically.

5.3.5.1 Test case 5.3-5-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the update mechanisms concerning the checks for available security updates.

Test units

a) For each software component in IXIT 6-SoftComp, the TL **shall** assess whether at least one "Update Mechanism" is described in IXIT 7-UpdMech, that checks the availability of security updates according to the schedule for querying for security updates in "Update Checking":

   - after initialization of the DUT; and

   - periodically.

NOTE: A daily security update check at a randomized time can be appropriate depending on the type of device.

Assignment of verdict

The verdict PASS is assigned if every software component is covered by at least one update mechanism, where:

- the checking of the availability of software updates is triggered by the DUT itself; and

- the availability of software updates is checked after initialization of the DUT; and

- the availability of software updates is checked periodically.

The verdict FAIL is assigned otherwise.

5.3.6 Test group 5.3-6

5.3.6.0 Test group objective

The test group addresses the provision 5.3-6.

NOTE 1: The entry "Initiation and Interaction" in IXIT 7-UpdMech indicates whether it is an automatic update mechanism in combination with the test units in Test group 5.3-4.

NOTE 2: The entry "User Notification" in IXIT 7-UpdMech indicates whether it supports update notifications.

NOTE 3: The provision addresses two different functionalities ("automatic updates" und "update notification") of an update mechanism. Furthermore, the provision is fulfilled for an update mechanism if one of these functionalities or both cover the requirements of the provision.

5.3.6.1 Test case 5.3-6-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the configuration of automatic updates (a-c) and update notifications (d-e).

Test units

a) The TL **shall** identify all automatic update mechanisms in IXIT 7-UpdMech by assessing whether the mechanism allows the performance of updates without requiring any user interaction according to "Initiation and Interaction".

b) For each update mechanism in IXIT 7-UpdMech that provides automatic software updates, the TL **shall** check whether it provides the user with the ability to:

- enable; or
- disable; or
- postpone

the automatic installation of security updates according to "Configuration" in IXIT 7-UpdMech.

c) For each update mechanism in IXIT 7-UpdMech that provides automatic software updates, the TL **shall** check whether automatic software updates are enabled in the initialized state according to "Configuration".

d) For each update mechanism in IXIT 7-UpdMech that provides update notifications according to "User Notification" the TL **shall** check whether it provides the user with the ability to:

- enable; or
- disable; or
- postpone

update notifications according to "Configuration" in IXIT 7-UpdMech.

e) For each update mechanism in IXIT 7-UpdMech that provides update notifications according to "User Notification", the TL **shall** check whether update notifications are enabled in the initialized state according to "Configuration".

Assignment of verdict

The verdict PASS is assigned if:

- the DUT supports automatic updates and for all update mechanisms the user is provided with the ability to enable, disable or postpone automatic installation of security updates and automatic updates are enabled in the initialized state; or the DUT does not support automatic updates; and
- the DUT supports update notifications and for all update mechanisms the user is provided with the ability to enable, disable or postpone update notifications and update notifications are enabled in the initialized state; or the DUT does not support update notifications.

The verdict FAIL is assigned otherwise.

5.3.6.2 Test case 5.3-6-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the configuration of automatic updates (a-b) and update notifications (c-d).

Test units

a) For each update mechanism in IXIT 7-UpdMech that provides automatic software updates (compare identification in Test case 5.3-6-1 (conceptual)) the TL **shall** functionally assess whether automatic updates are configured to be enabled in the initialized state of the DUT.

b) For each update mechanism in IXIT 7-UpdMech that provides automatic software updates (compare identification in Test case 5.3-6-1 (conceptual)) the TL **shall** perform a modification of the configuration of automatic update as described in "Configuration" and assess whether the user is provided with the ability to:

   - enable; or
   - disable; or
   - postpone

   automatic installation of security updates.

c) For each update mechanism in IXIT 7-UpdMech that provides update notifications according to "User Notification" the TL **shall** functionally assess whether update notifications are configured to be enabled in the initialized state of the DUT.

d) For each update mechanism in IXIT 7-UpdMech that provides update notifications according to "User Notification" the TL **shall** perform a modification of the configuration of update notifications as described in "Configuration" and assess whether the user is provided with the ability to:

   - enable; or
   - disable; or
   - postpone

   update notifications.

Assignment of verdict

The verdict PASS is assigned if:

- the DUT supports automatic updates and the configuration of automatic updates is enabled in the initialized state and can be modified by the user as described; or the DUT does not support automatic updates; and
- the DUT supports update notifications and the configuration of update notifications is enabled in the initialized state and can be modified by the user as described; or the DUT does not support update notifications.

The verdict FAIL is assigned otherwise.

5.3.7 Test group 5.3-7

5.3.7.0 Test group objective

The test group addresses the provision 5.3-7.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] best practice cryptography is defined as cryptography that is suitable for the corresponding use case and has no indication of a feasible attack with current readily available techniques.

The objective of this test group is to assess, firstly, whether the cryptographic methods provide the security guarantees that are necessary for the secure update mechanisms and, secondly, whether the cryptographic methods are not known to be vulnerable to a feasible attack.

5.3.7.1 Test case 5.3-7-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for the update mechanisms concerning the use of best practice cryptography (a-c) and the vulnerability to a feasible attack d).

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the "Security Guarantees" are appropriate for the use case of secure updates, at least integrity and authenticity are required to be fulfilled.

b) For each update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the mechanism according to "Description" is appropriate to achieve the "Security Guarantees".

NOTE 1: A holistic approach is required to assess the security of the mechanism.

c) For each update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the "Cryptographic Details" are considered as best practice cryptography for the use case of secure updates based on a reference catalogue. If "Cryptographic Details" are not included in a reference catalogue for the corresponding use case (e.g. novel cryptography), the SO **shall** provide evidences, e.g. a risk analysis, to justify the cryptography is appropriate as best practice for the use case. In such case the TL **shall** assess whether the evidence is appropriate and reliable for the use case.

NOTE 2: A use case based list of examples for best practice cryptography is given in ETSI TR 103 621 [i.7]. Moreover general reference catalogues of best practice cryptography are available, for example:

- SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu).

NOTE 3: A cryptographic algorithm or primitive that is deprecated with regard to its desired security property (e.g. SHA1 for collision resistance) or that relies on a cryptographic parameter (e.g. key-size) that is not appropriate, taking into account the intended lifetime of the DUT and cryptoagility, cannot be considered as best practice cryptography.

d) For each update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the "Cryptographic Details" are not known to be vulnerable to a feasible attack for the desired security property on the base of the "Security Guarantees" by reference to competent cryptanalytic reports.

NOTE 4: Competent cryptanalytic reports are typically published in the scientific literature or, alternatively, are to be provided by the SO. Further, clause D.2 provides information about the expected attack potential for level basic.

Assignment of verdict

The verdict PASS is assigned if for all update mechanisms:

- the security guarantees are appropriate for the use case of secure updates; and
- the mechanism is appropriate to achieve the security guarantees with respect to the use case; and

- all used cryptographic details are considered as best practice for the use case; and
- all used cryptographic details are not known to be vulnerable to a feasible attack for the desired security property.

The verdict FAIL is assigned otherwise.

5.3.8 Test group 5.3-8

5.3.8.0 Test group objective

The test group addresses the provision 5.3-8.

The assessment focuses on the management procedures that are necessary for deploying security updates timely.

5.3.8.1 Test case 5.3-8-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the manner in which security updates are deployed a) and the confirmation that the preconditions for the implementation are ensured b).

Test units

a) The TL **shall** assess whether the "Description" and the "Time Frame" of each security update procedure in IXIT 8-UpdProc facilitate that security updates are deployed in a timely manner.

NOTE 1: The consideration of severity and criticality of the addressed security vulnerabilities and the kind of vulnerability (e.g. firmware, hardware or software) is helpful.

NOTE 2: The amount of collaboration between the involved entities, the number of process steps and clearly defined responsibilities are important indicators for a timely deployment.

NOTE 3: In the case that a third party is involved (e.g. a software library vendor) the documentation of the point of contacts and defined procedures for the collaboration are indicators for a timely deployment.

NOTE 4: The comparison with the time frame for security updates of similar types of IoT products is helpful.

b) The TL **shall** check whether "Confirmation of Update Procedures" in IXIT 4-Conf states a confirmation.

Assignment of verdict

The verdict PASS is assigned if:

- there is an indication that the described management procedure allows a timely deployment of security updates; and
- a confirmation for the implementation is given.

The verdict FAIL is assigned otherwise.

5.3.9 Test group 5.3-9

5.3.9.0 Test group objective

The test group addresses the provision 5.3-9.

Verification of authenticity means the demonstration that the software update is not forged, including, in particular, the originality of the software update in regard to its source (manufacturer) and target (DUT).

Verification of integrity means the demonstration that the software update is not tampered.

The assessment focuses on the verification of authenticity and integrity that is performed by the DUT itself prior to the installation of the software update.

5.3.9.1 Test case 5.3-9-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the verification of software updates concerning authenticity a), integrity b) and the performing entity (c-d).

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the authenticity of software updates is suitably verified according to "Security Guarantees" and the corresponding "Cryptographic Details", including, in particular, the originality of the software update in regard to its source (manufacturer) and target (DUT) prior to the installation.

NOTE 1: There are different ways of verifying the originality of a software update in regard to its source and target.

NOTE 2: The validation of authenticity by the DUT serves primary for the rejection of untrustworthy software updates.

b) For each update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the integrity of software updates is suitably verified according to "Security Guarantees" and the corresponding "Cryptographic Details".

NOTE 3: The validation of integrity by the DUT serves primary for the detection injected malicious code in a valid software update.

c) For each update mechanism in IXIT 7-UpdMech, the TL **shall** check whether the authenticity verification is performed by the DUT itself according to "Security Guarantees".

d) For each update mechanism in IXIT 7-UpdMech, the TL **shall** check whether the integrity verification is performed by the DUT itself according to "Security Guarantees".

Assignment of verdict

The verdict PASS is assigned if:

- each update mechanism is effective for the verification of authenticity of software updates; and
- each update mechanism is effective for the verification of integrity of software updates; and
- the verification of authenticity and integrity of software updates is performed by the DUT itself.

The verdict FAIL is assigned otherwise.

5.3.10 Test group 5.3-10

5.3.10.0 Test group objective

The test group addresses the provision 5.3-10.

NOTE: The entry "Description" in IXIT 7-UpdMech indicates whether it is a network based update mechanism.

The validation of the trust relationship is essential to ensure that a non-authorized entity (e.g. device management platform or device) cannot install malicious code.

The essential difference between this test group and Test group 5.3-9 is that the verification of authenticity and integrity has to be performed via a trust relationship, i.e. the verification is based on actions involving an authorized entity (e.g. confirmation by an authorized user).

5.3.10.1 Test case 5.3-10-1 (conceptual/functional)

Test purpose

The purpose of this test case is the conceptual assessment of the verification of software updates via a trust relationship concerning authenticity and integrity a) and the performing entity b), and the functional assessment of the completeness of the IXIT documentation c).

Test units

a) The TL **shall** apply the test units a-b as specified in the Test case 5.3-9-1.

b) For each network based update mechanism in IXIT 7-UpdMech, the TL **shall** assess whether the verification of integrity and authenticity relies on a valid trust relationship according to "Description" and "Security Guarantees". A valid trust relationship includes:

- authenticated communication channels; or
- presence on a network that requires the device to possess a critical security parameter or password to join; or
- digital signature based verification of the update; or
- confirmation by the user; or
- a comparable secure functionality.

c) The TL **shall** functionally assess whether update mechanisms that are not documented in IXIT 7-UpdMech are available via a network interface on the DUT.

EXAMPLE: Network scanning tools allow for discovery of network-based update mechanisms.

Assignment of verdict

The verdict PASS is assigned if:

- each update mechanism is effective for the verification of authenticity of software updates; and
- each update mechanism is effective for the verification of integrity of software updates; and
- the verification of authenticity and integrity of software updates is based on a valid trust relationship; and
- every discovered network-based update mechanism is documented in the IXIT.

The verdict FAIL is assigned otherwise.

5.3.11 Test group 5.3-11

5.3.11.0 Test group objective

The test group addresses the provision 5.3-11.

5.3.11.1 Test case 5.3-11-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the method and content of information for the user about required security updates.

Test units

a) For each update mechanism in IXIT 7-UpdMech the TL **shall** assess whether the method to inform the user about the availability of required security updates is recognizable and apparent according to "User Notification".

EXAMPLE 1: A notification via user interface, push message, e-mail is recognizable.

EXAMPLE 2: A sufficiently sized pop-up using short and concise language is apparent.

b) For each update mechanism in IXIT 7-UpdMech the TL **shall** assess whether the user notification on required security updates includes information about the risks mitigated by the update according to "User Notification".

Assignment of verdict

The verdict PASS is assigned if for all update mechanisms:

- the method to inform the user about required security updates is recognizable and apparent; and
- the notification on required security updates includes information about the risks mitigated by the update.

The verdict FAIL is assigned otherwise.

5.3.12 Test group 5.3-12

5.3.12.0 Test group objective

The test group addresses the provision 5.3-12.

NOTE: When the basic functioning of the DUT is never disrupted by a software update, no user notification is necessary. In such a situation the test cases of this test group are fulfilled.

5.3.12.1 Test case 5.3-12-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of user notifications in case of disruptive software updates.

Test units

a) The TL **shall** check whether each update mechanism in IXIT 7-UpdMech supports user notification in case of disruptive software updates according to "User Notification" and it is indicated as realized on the DUT itself.

Assignment of verdict

The verdict PASS is assigned if for each update mechanism:

- the user is appropriately notified about the disruption of basic functioning during the software update; and
- the user notification is realized on the DUT itself.

The verdict FAIL is assigned otherwise.

5.3.13 Test group 5.3-13

5.3.13.0 Test group objective

The test group addresses the provision 5.3-13.

The defined support period describes the time span during which the manufacturer provides support regarding software updates. The defined software update support period is expected to be published even when no software updates are supported, in which case it indicates the absence of software updates.

5.3.13.1 Test case 5.3-13-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the publication of the defined support period.

Test units

a) The TL **shall** assess whether access to the "Publication of Support Period" in IXIT 2-UserInfo is understandable and comprehensible for a user with limited technical knowledge (see clause D.3).

EXAMPLE: With help of the model designation of the DUT the user finds the support period over a search engine on website of the manufacturer.

Assignment of verdict

The verdict PASS is assigned if:

- the publication of software update support period is understandable and comprehensible for a user with limited technical knowledge.

The verdict FAIL is assigned otherwise.

5.3.13.2 Test case 5.3-13-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the publication of the defined support period.

Test units

a) The TL **shall** functionally check whether the user information on accessing the resource for publishing the defined support period according to "Publication of Support Period" in IXIT 2-UserInfo is provided as described.

b) The TL **shall** functionally check whether the resource for publishing the defined support period according to "Publication of Support Period" in IXIT 2-UserInfo is accessible without restrictions (like e.g. a registration prior to the access).

c) The TL **shall** functionally check whether the published support period according to "Publication of Support Period" in IXIT 2-UserInfo actually defines the support period with respect to the updateable software components as described in "Support Period" in IXIT 2-UserInfo.

Assignment of verdict

The verdict PASS is assigned if:

- the access to the resource for publishing the defined support period to the user is provided as described in the IXIT; and
- the access to the resource for publishing the defined support period is unrestricted; and
- the defined support period is published.

The verdict FAIL is assigned otherwise.

5.3.14 Test group 5.3-14

5.3.14.0 Test group objective

The test group addresses the provision 5.3-14.

5.3.14.1 Test case 5.3-14-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the publication of the rationale for absence of updates and hardware replacement support.

Test units

a) The TL **shall** assess whether the access to the "Publication of Non-Updatable" and "Documentation of Replacement" in IXIT 2-UserInfo is understandable for a user with limited technical knowledge (see clause D.3).

Assignment of verdict

The verdict PASS is assigned if:

- the publication of the rationale for absence of updates and hardware replacement support is understandable for a user with limited technical knowledge.

The verdict FAIL is assigned otherwise.

5.3.14.2 Test case 5.3-14-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the publication of the rationale for absence of updates and hardware replacement support.

Test units

a) The TL **shall** functionally check whether the user information on accessing the resource for the rationale for absence of updates and publishing the hardware replacement support according to "Publication of Non-Updatable" and "Documentation of Replacement" in IXIT 2-UserInfo is provided as described.

b) The TL **shall** functionally check whether the resource for publishing the rationale for absence of updates and hardware replacement support according to "Publication of Non-Updatable" and "Documentation of Replacement" in IXIT 2-UserInfo is accessible without restrictions (like e.g. a registration prior to the access).

c) The TL **shall** functionally check whether the published rationale for absence of updates according to "Publication of Non-Updatable" in IXIT 2-UserInfo contains the rationale for the absence of software updates.

d) The TL **shall** functionally check whether the published hardware replacement support according to "Documentation of Replacement" in IXIT 2-UserInfo contains the hardware replacement plan in terms of the period and method of hardware replacement support.

NOTE: This plan would typically detail a schedule for when technologies will need to be replaced.

e) The TL **shall** functionally check whether the published rationale for absence of updates according to "Publication of Non-Updatable" in IXIT 2-UserInfo contains a defined support period.

Assignment of verdict

The verdict PASS is assigned if:

- the access to the resource for publishing the rationale for absence of updates and hardware replacement support to the user is provided as described in the IXIT; and
- the access to the resource for publishing the rationale for absence of updates and hardware replacement support is unrestricted; and
- the rationale for the absence of software updates is published; and
- the period and method of hardware replacement support is published; and
- a support period is published.

The verdict FAIL is assigned otherwise.

5.3.15 Test group 5.3-15

5.3.15.0 Test group objective

The test group addresses the provision 5.3-15.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] the IoT product, i.e. the DUT and its associated services, is isolable if it is able:

- to be removed from the network it is connected to, where any functionality loss caused is related only to that connectivity and not to its main function; or
- to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured.

5.3.15.1 Test case 5.3-15-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the isolation capabilities a) and hardware replacement support b) of the DUT.

Test units

a) The TL **shall** assess whether the described method in "Isolation" in IXIT 9-ReplSup is suitable to isolate the IoT product, i.e. to remove the IoT product from the network it is connected to, or to place the IoT product in a self-contained environment.

b) The TL **shall** assess whether the described method in "Hardware Replacement" in IXIT 9-ReplSup is suitable to be able to replace the hardware.

Assignment of verdict

The verdict PASS is assigned if:

- the described method is suited for the isolation of the IoT product; and
- the described method is suited for the replacement of the hardware.

The verdict FAIL is assigned otherwise.

5.3.15.2 Test case 5.3-15-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the isolation capabilities (a-c) and hardware replacement support (d-e) of the DUT.

Test units

a) The TL **shall** set up the IoT product in the intended environment.

b) The TL **shall** perform the method described in "Isolation" in IXIT 9-ReplSup in order to isolate the IoT product, i.e. to remove the IoT product from the network it is connected to, or to place the IoT product in a self-contained environment, as appropriate.

c) The TL **shall** functionally assess whether on the isolated IoT product:

- in case of removing the IoT product from the network connection: any functionality loss caused is related only to that connectivity and not to the main function of the DUT; or
- in case of placing the IoT product in a self-contained environment with other devices: the integrity of devices within that environment is ensured.

d) The TL **shall** perform the method described in "Hardware Replacement" in IXIT 9-ReplSup in order to replace the hardware in the intended environment.

e) The TL **shall** functionally assess whether the connectivity and associated functionality can be regained on the replaced DUT.

Assignment of verdict

The verdict PASS is assigned if:

- the IoT product can be isolated successfully according to the described method for isolation; and
- the hardware can be replaced successfully according to the described method for hardware replacement.

The verdict FAIL is assigned otherwise.

5.3.16 Test group 5.3-16

5.3.16.0 Test group objective

The test group addresses the provision 5.3-16.

5.3.16.1 Test case 5.3-16-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the model designation.

Test units

a) The TL **shall** assess whether the model designation of the DUT can be obtained in a clearly recognizable way, either by labelling on the DUT or via a physical interface according to "Model Designation" in IXIT 2-UserInfo.

Assignment of verdict

The verdict PASS is assigned if:

- the model designation of the DUT can be obtained clearly recognizable by labelling on the DUT or via a physical interface.

The verdict FAIL is assigned otherwise.

5.3.16.2 Test case 5.3-16-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the model designation.

Test units

a) The TL **shall** functionally check whether the model designation of the DUT can be obtained applying the described way of recognition in "Model Designation" in IXIT 2-UserInfo.

b) The TL **shall** functionally assess whether the obtained model designation is available in simple text and corresponds with the expected model designation described in "Model Designation" in IXIT 2-UserInfo.

Assignment of verdict

The verdict PASS is assigned if:

- the model designation of the DUT can be extracted according to the described way of recognition; and
- the model designation is available in simple text; and

- the model designation is corresponding with the expected model designation according to the IXIT.

The verdict FAIL is assigned otherwise.

5.4 TSO 5.4: Securely store sensitive security parameters

5.4.1 Test group 5.4-1

5.4.1.0 Test group objective

The test group addresses the provision 5.4-1.

This test group assesses whether sensitive security parameters are securely stored according to their type using the claimed protection schemes. However the assessment does not give assurance for the completeness of the documented sensitive security parameters apart from consistency with respect to other IXIT.

NOTE: Threat modelling e.g. provided by the SO and the baseline attacker model described in clause D.2 is helpful to derive appropriate security guarantees, conceptually evaluate the corresponding protection schemes and functionally evaluate the correct implementation on a basic level.

5.4.1.1 Test case 5.4-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the secure storage of sensitive security parameters concerning the security claims (a-c) and the completeness of the IXIT documentation d).

Test units

a) The TL **shall** assess whether the declaration in "Type" of each sensitive security parameter provided in IXIT 10-SecParam is consistent with the "Description".

b) The TL **shall** assess whether the "Security Guarantees" of each sensitive security parameter provided in IXIT 10-SecParam matches at least the protection needs indicated by "Type".

NOTE 1: Critical security parameter require integrity and confidentiality protection while public security parameter require integrity protection only.

c) The TL **shall** assess whether the "Protection Scheme" of each sensitive security parameter provided in IXIT 10-SecParam provides the claimed "Security Guarantees".

NOTE 2: Consider the usage of external evidences (see clause 4.7) to (partially) cover the provision if a secure element is used.

d) The TL **shall** assess the completeness of the sensitive security parameters in IXIT 10-SecParam by considering indications for sensitive security parameters in the provided information in all other IXITs.

EXAMPLE: If there are authentication mechanisms described in IXIT 1-AuthMech, the verification whether the corresponding cryptographic parameters are listed in IXIT 10-SecParam can be helpful to collect indications.

Assignment of verdict

The verdict PASS is assigned if:

- for every sensitive security parameter the declaration is consistent with its description; and
- for every sensitive security parameter the claimed security guarantees match their minimal protection needs; and
- every sensitive security parameter has a suitable protection mechanism for the claimed security guarantees; and

- there is no indication, that the listed sensitive security parameters are incomplete.

The verdict FAIL is assigned otherwise.

5.4.1.2 Test case 5.4-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the secure storage of sensitive security parameters.

Test units

a) The TL **shall** functionally assess whether for all sensitive security parameters provided in IXIT 10-SecParam "Protection Scheme" is implemented according to the IXIT documentation.

NOTE: Typically, while examine the DUT for indicating evidences for the existence and enforcement of the documented protection scheme for a sensitive security parameter, an indication for non-conformity of the implementation can be found, if existing on a basic level.

EXAMPLE: If the "Protection Scheme" states that a sensitive security parameter is only accessible for a privileged user and is protected by the OS access control, attempting to gain access to the parameter over unprivileged processes (e.g. path manipulation via remote interfaces) can be helpful to collect indications.

Assignment of verdict

The verdict PASS is assigned if:

- for every sensitive security parameter there is no indication that the implementation of the corresponding protection scheme differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.4.2 Test group 5.4-2

5.4.2.0 Test group objective

The test group addresses the provision 5.4-2.

In this case hard-coded unique per device identity is an individual and static value, that represents the DUT and potential hard-coded information the value is derived from.

The test group addresses the identification of hard-coded device identities and whether adequate protection needs are identified. A functional evaluation for tamper proof storage by any means is not in focus of this TSO.

NOTE 1: The conceptual evaluation of protection schemes for tamper-resistance of hard-coded identities and an inspection for indication for the correct implementation of the corresponding schemes is part of Test group 5.4-1 by construction. However, the corresponding test units are referenced here and are optimizable when deriving a test plan.

NOTE 2: A communicated device identity can be derived from a - potentially secret - piece of information that persists in hardware (e.g. a seed value for a randomization algorithm). This information can be considered as part of a device identity.

5.4.2.1 Test case 5.4-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of tamper-resistant storage of hard-coded identities.

Test units

a) The TL **shall** check whether for each sensitive security parameter in IXIT 10-SecParam where the "Description" indicates that it is used as an hard-coded identity, a corresponding explicit statement is provided.

b) The TL **shall** assess whether for each hard-coded identity as indicated in "Description" in IXIT 10-SecParam the corresponding "Security Guarantees" provide tamper-resistance.

NOTE 1: Tamper-resistance addresses protection against means such as physical, electrical and software means.

NOTE 2: Consider the usage of external evidences (see clause 4.7) to (partially) cover the provision if a secure element is used.

c) The TL **shall** assess whether the "Protection Scheme" of each hard-coded identity as indicated in "Description" in IXIT 10-SecParam provides the claimed "Security Guarantees" with respect to tamper-resistance.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any hard-coded identity is not documented as such; and
- for all hard-coded identities the security guarantee includes tamper-resistance; and
- every hard-coded identity has a suitable protection mechanism for tamper-resistance.

The verdict FAIL is assigned otherwise.

5.4.2.2 Test case 5.4-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of tamper-resistant storage of hard-coded identities.

Test units

a) The TL **shall** functionally assess whether each hard-coded identity as indicated in "Description" in IXIT 10-SecParam the "Protection Scheme" with respect to tamper-resistance is implemented according to the IXIT documentation.

NOTE: Typically, while examine the DUT for indicating evidences for the existence and enforcement of the documented protection scheme for a sensitive security parameter, indication for non-conformity of the implementation can be found, if existing on a basic level.

EXAMPLE: If the "Protection Scheme" states that a hard-coded identity is protected against tampering by a secure element, verifying the existence and the correct integration of a secure element can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if:

- for every hard-coded identity, there is no indication that the implementation of any protection scheme with respect to tamper-resistance differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.4.3 Test group 5.4-3

5.4.3.0 Test group objective

The test group addresses the provision 5.4-3.

In this case a hard-coded parameter in device software source code is a static value, that is common in every device where the same code as for the DUT is implemented.

This test group assesses whether there is an indication for not documented hard-coded critical security parameters in device software source code in the provided provisioning mechanisms for critical security parameters. Wherever critical security parameters are hard-coded in device software source code the assessment focuses on conformity of design and functional evaluation of the provisioning mechanism that makes sure that these are not used during the operation of the DUT. This approach cannot provide strong assurance for completeness of the IXIT documentation concerning the identification of hard-coded critical security parameters in device software source code.

It is noted that this approach does not preclude supplementary approaches, e.g. active approaches based on scanning the software of the DUT for embedded patterns that match critical security parameters. Supplementary approaches are at the discretion of the TL.

NOTE: Public security parameters can be embedded in the object code of the software of the DUT.

5.4.3.1 Test case 5.4-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of hard-coded critical security parameters.

Test units

a) The TL **shall** check whether for all critical security parameters provided in IXIT 10-SecParam where "Provisioning Mechanism" indicates that it is hard coded in device software source code, the fact is reflected in "Description".

b) The TL **shall** assess whether for all critical security parameters in IXIT 10-SecParam, which are hard coded in device software source code according to "Description", the corresponding "Provisioning Mechanism" ensures that it is not used during the operation of the DUT.

NOTE: According to the definition of critical security parameter in ETSI TS 103 645 [1]/ETSI EN 303 645 [2] the disclosure or modification of such a parameter can compromise the security of the DUT. Parameters where disclosure or modification compromises solely other assets (e.g. intellectual properties) are not covered by the definition.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any critical security parameter hard-coded in device software source code is not documented as such; and
- for all critical security parameter hard-coded in device software source code, the "Provisioning Mechanism" ensures that it is not used during the operation of the DUT.

The verdict FAIL is assigned otherwise.

5.4.3.2 Test case 5.4-3-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of hard-coded critical security parameters.

Test units

a) The TL **shall** functionally assess whether for all critical security parameters hard-coded in device software source code documented in "Description" of IXIT 10-SecParam, the "Provisioning Mechanism" is indeed applied during the operation of the DUT.

EXAMPLE: If a provisioning mechanism states that a hard-coded critical security parameter is intended to be replaced by the user using individual data (e.g. based on a QR code), the verification that the user is requested to input this data can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if:

- for all critical security parameter hard-coded in device software source code there is no indication that the application of the provisioning mechanism differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.4.4 Test group 5.4-4

5.4.4.0 Test group objective

The test group addresses the provision 5.4-4.

This test group assesses by documentation whether all critical security parameter addressed by the underlying provision are identified and that their generation mechanisms meet the corresponding requirement.

5.4.4.1 Test case 5.4-4-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services concerning the generation mechanisms.

Test units

a) The TL **shall** check whether all critical security parameter provided in IXIT 10-SecParam, where "Description" indicates that the critical security parameters are used for integrity and authenticity checks of software updates or for protection of communication with associated services are documented as such in "Generation Mechanism".

b) The TL **shall** assess for all critical security parameters provided in IXIT 10-SecParam, whether the "Generation Mechanism" ensures that the critical security parameter is unique per device and produced with a mechanism that reduces the risk of automated attacks against classes of devices.

NOTE 1: A random number generator used for the generation of the critical security parameter that has been certified (e.g. against a scheme applicable under the European Cybersecurity Act) can be seen as a source of sufficient entropy.

NOTE 2: It is also possible that custom solutions (that are e.g. not certified) provide sufficient entropy for the use case of the DUT.

NOTE 3: The degree to which a generation mechanism is widely accepted as appropriate for a given use case is a function of the consensus among the subject matter community. Generation mechanisms that are standardized rank highest in such consensus, due to the high degree of scrutiny to which they are subjected in their development. Standardization bodies offer publicly available sources of information on suitable generation mechanisms, e.g. National Institute of Standards and Technology (NIST) runs the Cryptographic Algorithm Validation Program [i.2] for random bit generators, key derivation, secure hashing, etc. In regard to end-to-end security and communities to which SME IoT manufacturers are possibly keener with, Mozilla® publicly lists configuration profiles for Transport Layer Security (TLS) [i.3]. Finally, there are publicly available catalogues of references to relevant standards, e.g. the KeyLength catalogue [i.4] that indexes standards published by NIST, ANSSI, BSI, etc. on the matter of cryptographic key length.

Assignment of verdict

The verdict PASS is assigned if:

- all critical security parameter where the purpose in "Description" indicates that the critical security parameters are used for integrity and authenticity checks of software updates or for protection of communication with associated services are documented as such in "Generation Mechanism"; and

- for all critical security parameters the "Generation Mechanism" ensures that the critical security parameters are unique per device and produced with a mechanism that reduces the risk of automated attacks against classes of devices.

The verdict FAIL is assigned otherwise.

5.5 TSO 5.5: Communicate securely

5.5.1 Test group 5.5-1

5.5.1.0 Test group objective

The test group addresses the provision 5.5-1.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2] best practice cryptography is defined as cryptography that is suitable for the corresponding use case and has no indication of a feasible attack with current readily available techniques.

The objective of this test group is to assess, firstly, whether the cryptographic methods provide the security guarantees that are necessary for the use case of the communication and, secondly, whether the cryptographic methods are not known to be vulnerable to a feasible attack.

5.5.1.1 Test case 5.5-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for the communication mechanisms concerning the use of best practice cryptography (a-c) and the vulnerability to a feasible attack d).

Test units

a) For each communication mechanism in IXIT 11-ComMech, the TL **shall** assess whether the "Security Guarantees" are appropriate for the use case of the communication.

b) For each communication mechanism in IXIT 11-ComMech, the TL **shall** assess whether the mechanism according to "Description" is appropriate to achieve the "Security Guarantees".

NOTE 1: A holistic approach is required to assess the security of the communication mechanism.

c) For each communication mechanism in IXIT 11-ComMech, the TL **shall** assess whether the "Cryptographic Details" are considered as best practice cryptography for the use case of secure communication based on a reference catalogue. If "Cryptographic Details" are not included in a reference catalogue for the corresponding use case (e.g. novel cryptography), the SO **shall** provide evidences, e.g. a risk analysis, to justify the cryptography is appropriate as best practice for the use case. In such case the TL **shall** assess whether the evidence is appropriate and reliable for the use case.

NOTE 2: A use case based list of examples for best practice cryptography is given in ETSI TR 103 621 [i.7]. Moreover general reference catalogues of best practice cryptography are available, for example:

- SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu).

NOTE 3: A cryptographic algorithm or primitive that is deprecated with regard to its desired security property (e.g. SHA1 for collision resistance) or that relies on a cryptographic parameter (e.g. key-size) that is not appropriate, taking into account the intended lifetime of the DUT and cryptoagility, cannot be considered as best practice cryptography.

d) For each communication mechanism in IXIT 11-ComMech, the TL **shall** assess whether the "Cryptographic Details" are not known to be vulnerable to a feasible attack for the desired security property on the base of the "Security Guarantees" by reference to competent cryptanalytic reports.

NOTE 4: Competent cryptanalytic reports are typically published in the scientific literature or, alternatively, are to be provided by the SO. Further, clause D.2 provides information about the expected attack potential for level basic.

Assignment of verdict

The verdict PASS is assigned if for all communication mechanisms:

- the security guarantees are appropriate for the use case of secure communication; and
- the mechanism is appropriate to achieve the security guarantees with respect to the use case; and
- all used cryptographic details are considered as best practice for the use case; and
- all used cryptographic details are not known to be vulnerable to a feasible attack for the desired security property.

The verdict FAIL is assigned otherwise.

5.5.1.2 Test case 5.5-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the cryptography used for the communication mechanisms.

Test units

a) For each communication mechanism in IXIT 11-ComMech, the TL **shall** functionally assess whether the described "Cryptographic Details" are used by the DUT.

EXAMPLE 1: Using a protocol analyser or packet sniffer tool.

EXAMPLE 2: If a TLS secured communication is used, sniffing the TLS handshake and comparing the used cipher suites with the described cryptography in the IXIT can be helpful to collect an indication.

EXAMPLE 3: If the protocol enables different security modes for the communication, trying to downgrade the security mode can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any used cryptographic setting differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.5.2 Test group 5.5-2

5.5.2.0 Test group objective

The test group addresses the provision 5.5-2.

The terms "reviewed" and "evaluated" allow for a range of way to fulfil this provision. The term "reviewed" hints at actions undertaken for finding and correcting defects, e.g. an independent security audit or a continuous process allowing review and disclosure of vulnerabilities (a bug tracking system or automated code analysis). The term "evaluated" hints at a formal comparison against a set of objectives, e.g. a recognized certification scheme.

The objective of this test group is to assess, firstly, whether the network and security functionalities are reviewed or evaluated on the base of the corresponding scope and secondly, whether the report matches the identification (version and name) of the DUT implementation.

5.5.2.1 Test case 5.5-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the implementations of network and security functionalities concerning reviews and evaluations.

Test units

a) For each implementation in IXIT 12-NetSecImpl, the TL **shall** check whether it has been reviewed or evaluated according to "Review/Evaluation Method".

b) For each review or evaluation method associated to an implementation in IXIT 12-NetSecImpl, the TL **shall** assess whether the "Review/Evaluation Method" and its "Report" covers the related implementation scope as described in "Description".

Assignment of verdict

The verdict PASS is assigned if:

- all implementations of network and security functionalities are reviewed or evaluated; and
- all review and evaluation methods cover the scope of the related implementation.

The verdict FAIL is assigned otherwise.

5.5.2.2 Test case 5.5-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the implementations of network and security functionalities concerning reviews and evaluations.

Test units

a) For each implementation associated with a review or evaluation method in IXIT 12-NetSecImpl, the TL **shall** functionally check whether the identification of the implementation (name and version) on the DUT matches the identification of the implementation provided in the "Report".

Assignment of verdict

The verdict PASS is assigned if:

- the name and version of every provided implementation matches the name and version provided in the related report; or
- the necessary information is not obtainable, because the DUT does not provide any information on the implementation name and version.

The verdict FAIL is assigned otherwise.

5.5.3 Test group 5.5-3

5.5.3.0 Test group objective

The test group addresses the provision 5.5-3.

The ability to update cryptographic algorithms and primitive does not only rely on the existence of an update mechanism. It requires that the implementation can be replaced on the device, and that software that rely on cryptographic algorithms and primitives can support such replacement.

The objective of this test group is to assess, firstly, whether there is an update mechanism for each software component indicating such implementation and, secondly, whether the implementations providing cryptographic algorithms and primitives can be replaced and side effects of updating are considered by the manufacturer.

5.5.3.1 Test case 5.5-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of implementations providing cryptographic algorithms and primitives concerning the updatability.

Test units

a) For each software component in IXIT 6-SoftComp indicating "Cryptographic Usage", the TL **shall** check whether an "Update Mechanism" to update the software component is referenced.

b) For each software component in IXIT 6-SoftComp indicating "Cryptographic Usage", the TL **shall** check whether side effects of updating those algorithms and primitives are considered by the manufacturer.

NOTE: Typical side effects are that the existing data structures or hardware are incompatible regarding the new cryptography.

Assignment of verdict

The verdict PASS is assigned if:

- for every software component indicating cryptographic usage an update mechanism is referenced; and
- side effects of updating those algorithms and primitives are considered by the manufacturer.

The verdict FAIL is assigned otherwise.

5.5.4 Test group 5.5-4

5.5.4.0 Test group objective

The test group addresses the provision 5.5-4.

There exist many authentication methods based on a variety of authentication factors and applying to different subjects (such as persons, devices, or functions). Three important characteristics to look for is whether the authentication method can discriminate between multiple subjects, whether it can reject authentication attempts based on invalid credentials or no proper access rights (effectiveness), and whether it is resistant to an adversary by providing its own security guarantees or rely on the security guarantees provided by an underlying protocol (e.g. TLS).

The objective of this test group is to assess, firstly, whether the device functionalities are accessible only after authentication, secondly, whether the authentication method can discriminate between different subjects, thirdly, whether it is effective and resistant to adversaries and, finally, whether the authorization step is effective.

5.5.4.1 Test case 5.5-4-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of device functionality via a network interface in the initialized state concerning authentication and authorization.

Test units

a) For each device functionality in IXIT 13-SoftServ indicated as accessible via network interface in the initialized state according to "Description", the TL **shall** check whether there is at least one "Authentication Mechanism" referenced.

b) For each "Authentication Mechanism" referenced in IXIT 13-SoftServ, the TL **shall** assess whether the authentication mechanism described in IXIT 1-AuthMech allows to discriminate between multiple authentication subjects and can reject authentication attempts based on invalid identities and/or authentication factors.

NOTE: Discriminating is typically done based on unique identities and/or authentication factors.

c) For each "Authentication Mechanism" referenced in IXIT 13-SoftServ, the TL **shall** assess whether the means protecting the authentication mechanism in "Cryptographic Details" in IXIT 1-AuthMech provide the "Security Guarantees" identified for the mechanism and are resistant to attempts at compromising the mechanism.

d) For each "Authentication Mechanism" referenced in IXIT 13-SoftServ, the TL **shall** assess whether the authorization process described in "Description" in IXIT 1-AuthMech allows authenticated subjects with proper access rights to be granted access and denies authenticated subjects with inadequate access rights or unauthenticated subjects to be granted access.

Assignment of verdict

The verdict PASS is assigned if:

- at least one authentication mechanism is referenced for every device functionality accessible via network interface in the initialized state; and
- every authentication mechanism allows to discriminate between multiple authentication subjects and to reject authentication attempts based on invalid identities and/or authentication factors; and
- the means used to protect an authentication mechanism provide the expected security guarantees and are resistant at attempts to compromise the mechanism; and
- every authorization mechanism allows access to authenticated subjects with proper access rights; and
- every authorization mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects.

The verdict FAIL is assigned otherwise.

5.5.4.2 Test case 5.5-4-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of device functionality via a network interface in the initialized state concerning authentication and authorization.

Test units

a) For each "Authentication Mechanism" referenced in IXIT 13-SoftServ, the TL **shall** functionally assess whether an unauthenticated subject and a subject with invalid identity or credentials and an authenticated subject without appropriate access rights cannot access the device functionality in the initialized state.

NOTE: This test unit cannot in principle distinguish between the authentication and the authorization step - implementation aiming at reducing information leak will not disclose which step would fail to the subject.

b) For each "Authentication Mechanism" referenced in IXIT 13-SoftServ, the TL **shall** functionally assess whether an authenticated subject with appropriate access rights can access the device functionality in the initialized state.

c) For each "Authentication Mechanism" referenced in IXIT 13-SoftServ, the TL **shall** functionally assess whether the protection of the authentication mechanism conforms to the description in "Security Guarantees" and "Cryptographic Details" in IXIT 1-AuthMech.

EXAMPLE: If a PKI certificate based authentication is used, sniffing the used certificates and comparing the properties with the described cryptography in the IXIT can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if for every device functionality accessible via network interface in the initialized state:

- an unauthenticated subject, a subject with invalid identity or invalid credentials and an authenticated subject without appropriate access rights cannot access the functionality in the initialized state; and

- an authenticated subject with appropriate access rights can access the device functionality in the initialized state; and
- there is no indication that the mechanism to secure the authentication differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.5.5 Test group 5.5-5

5.5.5.0 Test group objective

The test group addresses the provision 5.5-5.

The considerations given for Test group 5.5-4 apply to this test group as well. Compared to Test group 5.5-4, there is an expectation that authentication and authorization will be active in the factory default and the initialized state if the functionality allows security-relevant changes in the configuration.

The objective of this test group is to assess, firstly, whether the device functionality allowing security-relevant changes is accessible only after authentication, secondly, whether the authentication method can discriminate between different subjects, thirdly, whether it is effective and resistant to adversaries and, finally, whether the authorization step is effective.

5.5.5.1 Test case 5.5-5-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of device functionality allowing security-relevant changes via a network interface concerning the authentication and authorization.

Test units

a) The TL **shall** apply all test units as specified in the Test case 5.5-4-1 for all states of the DUT with restriction to the functionalities that allow security-relevant changes according to "Allows Configuration" in IXIT 13-SoftServ. Network service protocols that are relied upon by the DUT and where the manufacturer cannot guarantee what configuration will be required for the DUT to operate are excluded.

NOTE: Network service protocols that are designed to enable external configuration without authentication, e.g. DHCP, are excluded in context of this provision.

Assignment of verdict

The verdict PASS is assigned if:

- at least one authentication mechanism is referenced for every device functionality accessible via network interface that allows security-relevant changes; and
- every authentication mechanism allows to discriminate between multiple authentication subjects and to reject authentication attempts based on invalid identities and/or authentication factors; and
- the means used to protect an authentication mechanism provide the expected security guarantees and are resistant at attempts to compromise the mechanism; and
- every authorization mechanism allows access to authenticated subjects with proper access rights; and
- every authorization mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects.

The verdict FAIL is assigned otherwise.

5.5.5.2 Test case 5.5-5-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of device functionality allowing security-relevant changes via a network interface concerning the authentication and authorization a) and the completeness of the IXIT documentation b).

Test units

a) The TL **shall** apply all test units as specified in the Test case 5.5-4-2 for all states of the DUT with restriction to the functionalities that allow security-relevant changes according to "Allows Configuration" in IXIT 13-SoftServ. Network service protocols that are relied upon by the DUT and where the manufacturer cannot guarantee what configuration will be required for the DUT to operate are excluded.

NOTE: Network service protocols that are designed to enable external configuration without authentication, e.g. DHCP, are excluded in context of this provision.

b) The TL **shall** functionally assess whether communication mechanisms that are not documented in IXIT 11-ComMech are available via a network interface on the DUT.

EXAMPLE: Network scanning tools allow for discovery of network-based communication mechanisms

Assignment of verdict

The verdict PASS is assigned if:

- an unauthenticated subject, a subject with invalid identity or invalid credentials and an authenticated subject without appropriate access rights cannot access the functionality; and
- an authenticated subject with appropriate access rights can access the device functionality; and
- there is no indication that the mechanism to secure the authentication differs from its IXIT documentation; and
- every discovered network-based communication mechanism is documented in the IXIT.

The verdict FAIL is assigned otherwise.

5.5.6 Test group 5.5-6

5.5.6.0 Test group objective

The test group addresses the provision 5.5-6.

The difference compared to Test group 5.5-1 is, that the use case in the underlying provision is concretised on the communication of critical security parameters, which requires at least an encryption in transit.

The objective of this test group is to assess, firstly, whether the cryptographic methods provide the security guarantees that are necessary for the use case of the communication of critical security parameters and, secondly, whether the cryptographic methods are not known to be vulnerable to a feasible attack.

5.5.6.1 Test case 5.5-6-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for communicating critical security parameters.

Test units

a) For all "Communication Mechanisms" in IXIT 11-ComMech referenced in any critical security parameter in IXIT 10-SecParam, the TL **shall** apply all test units as specified in the Test case 5.5-1-1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.

Assignment of verdict

The verdict PASS is assigned if for all communication mechanisms used for communicating critical security parameters:

- the security guarantees are appropriate for the use case of secure communication; and
- the mechanism is appropriate to achieve the security guarantees with respect to the use case; and
- all used cryptographic details are considered as best practice for the use case; and
- all used cryptographic details are not known to be vulnerable to a feasible attack.

The verdict FAIL is assigned otherwise.

5.5.6.2 Test case 5.5-6-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the cryptography used for communicating critical security parameters.

Test units

a) For all "Communication Mechanisms" in IXIT 11-ComMech referenced in any critical security parameter in IXIT 10-SecParam, the TL **shall** apply all test units as specified in the Test case 5.5-1-2.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any used cryptographic setting differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.5.7 Test group 5.5-7

5.5.7.0 Test group objective

The test group addresses the provision 5.5-7.

The difference compared to Test group 5.5-1 and Test group 5.5-6 is, that the use case in the underlying provision is concretised on the communication of critical security parameters via remotely accessible network interfaces, which requires at least the security guarantee of confidentiality.

The objective of this test group is to assess, firstly, whether the cryptographic methods provide the security guarantees that are necessary for the use case of the communication of critical security parameters and, secondly, whether the cryptographic methods are not known to be vulnerable to a feasible attack.

5.5.7.1 Test case 5.5-7-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for communicating critical security parameters via remotely accessible network interfaces.

Test units

a) For all "Communication Mechanisms", that are remotely accessible according to their "Description" in IXIT 11-ComMech referenced in any critical security parameter in IXIT 10-SecParam, the TL **shall** apply all test units as specified in the Test case 5.5-1-1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.

Assignment of verdict

The verdict PASS is assigned if for all communication mechanisms used for communicating critical security parameters via remotely accessible network interfaces:

- the security guarantees are appropriate for the use case of secure communication; and
- the mechanism is appropriate to achieve the security guarantees with respect to the use case; and
- all used cryptographic details are considered as best practice for the use case; and
- all used cryptographic details are not known to be vulnerable to a feasible attack.

The verdict FAIL is assigned otherwise.

5.5.7.2 Test case 5.5-7-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the cryptography used for communicating critical security parameters via remotely accessible network interfaces.

Test units

a) For all "Communication Mechanisms", that are remotely accessible according to their "Description" in IXIT 11-ComMech referenced in any critical security parameter in IXIT 10-SecParam, the TL **shall** apply all test units as specified in the Test case 5.5-1-2.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any used cryptographic setting differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.5.8 Test group 5.5-8

5.5.8.0 Test group objective

The test group addresses the provision 5.5-8.

5.5.8.1 Test case 5.5-8-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the secure management processes concerning the coverage of the parameter life cycles a) and the confirmation that the preconditions for the implementation are ensured b).

Test units

a) The TL **shall** assess whether the secure management of critical security parameters covers the whole life cycle of a critical security parameter considering its:

   - generation; and
   - provisioning; and
   - storage; and
   - updates; and
   - decommissioning, archival, and destruction; and
   - processes to handle the expiration and compromise;

according to the processes in IXIT 14-SecMgmt.

b) The TL **shall** check whether "Confirmation of Secure Management" in IXIT 4-Conf states a confirmation.

Assignment of verdict

The verdict PASS is assigned if:

- the secure management covers the whole life cycle of a critical security parameter according to its processes; and
- a confirmation for the implementation is given.

The verdict FAIL is assigned otherwise.

5.6 TSO 5.6: Minimize exposed attack surfaces

5.6.1 Test group 5.6-1

5.6.1.0 Test group objective

The test group addresses the provision 5.6-1.

In principle a logical interface can be accessible via a plurality of network interface: the manufacturer therefore ensures that all access paths to a logical interface are identified. The manufacturer disables those network and logical interfaces that are not required to provide the device functionality, depending on the interface purpose. This requires having knowledge of their platform and understand which components provide network or logical interfaces, and how. This is critical when hardware platforms and components from third-parties are reused.

5.6.1.1 Test case 5.6-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the network and logical interfaces of the DUT.

Test units

a) For each network and logical interface in IXIT 15-Intf that is described as enabled according to "Status", the TL **shall** assess whether the purpose of the interface in "Description" provides a valid justification for being enabled.

Assignment of verdict

The verdict PASS is assigned if:

- for every network or logical interface that is marked as enabled in the IXIT documentation, there is a purpose that provides a valid justification for the interface to be enabled.

The verdict FAIL is assigned otherwise.

5.6.1.2 Test case 5.6-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the network and logical interfaces of the DUT a) and the completeness of the IXIT documentation b).

Test units

a) For each network and logical interface in IXIT 15-Intf, the TL **shall** functionally check whether the status of the interface matches the "Status" in the IXIT documentation.

NOTE: A possible method to analyse an interface is to use protocol testing tools in a black-box setting and to infer from the obtained information whether the interface is enabled or disabled on the DUT. For cases where the DUT provides an indication (e.g. a visual indication of connectors, antennas and components) whether the interface is enabled or disabled, the accessibility test allows to confirm or disprove the indication.

b) The TL **shall** functionally assess whether network or logical interfaces that are not documented in IXIT 15-Intf are available via a network interface on the DUT.

EXAMPLE: Network scanning tools allow for discovery of network or logical interfaces.

Assignment of verdict

The verdict PASS is assigned if:

- every documented network or logical interface that is marked as disabled in the IXIT documentation is found to be disabled or not accessible on the DUT; and
- every discovered network and logical interface is documented in the IXIT.

The verdict FAIL is assigned otherwise.

5.6.2 Test group 5.6-2

5.6.2.0 Test group objective

The test group addresses the provision 5.6-2.

The principle of minimization applied to security-relevant information in unauthenticated context dictates that only such information that is necessary for device or service operations in unauthenticated context are disclosed. It is to be noted that the manufacturer might not be able to minimize disclosed information if requirements exist to conform to standardized protocols which, by design, disclose more information than necessary.

EXAMPLE: MAC address in Ethernet, Bluetooth® and Wi-Fi®, ARP, DNS.

5.6.2.1 Test case 5.6-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the information disclosed by network interfaces without authentication in the initialized state.

Test units

a) For each network interface in IXIT 15-Intf, the TL **shall** assess whether the "Disclosed Information" disclosed by the interface without authentication in the initialized state and indicated as not security-relevant, is however security-relevant.

b) For each network interface in IXIT 15-Intf, the TL **shall** assess whether the "Disclosed Information" disclosed by the interface without authentication in the initialized state and indicated as security-relevant, is necessary for the operation of the DUT.

Assignment of verdict

The verdict PASS is assigned if for every network interface:

- every security-relevant information disclosed by the interface without authentication in the initialized state is documented as such; and
- all security-relevant information disclosed by the interface without authentication in the initialized state is necessary for the operation of the DUT.

The verdict FAIL is assigned otherwise.

5.6.2.2 Test case 5.6-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the information disclosed by the network interfaces without authentication in the initialized state.

Test units

a) For each network interface in IXIT 15-Intf, the TL **shall** functionally assess whether security-relevant information can be observed from the interface without authentication in the initialized state, that is not described in "Disclosed Information".

Assignment of verdict

The verdict PASS is assigned if:

- for every network interface, only security-relevant information can be observed that is described in the IXIT documentation.

The verdict FAIL is assigned otherwise.

5.6.3 Test group 5.6-3

5.6.3.0 Test group objective

The test group addresses the provision 5.6-3.

Some physical interfaces require exposure in order to allow normal operations. The remaining interfaces are to be protected in exposure. In order to identify the appropriate level of protection, the introduction of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] is considered, which indicates a protection "against elementary attacks on fundamental design weaknesses". Taking this in consideration, protection from exposure for physical interfaces is relative to the device casing, i.e. the protection is sufficient when accessing the physical interface requires opening or breaking the device casing (this does not preclude stronger measures when necessary) or similar measures.

It is to be noted that protection through the casing is not effective for air interfaces. Such air interfaces that do not require exposure are to be disabled. Interfaces that are not permanently necessary require a form of trusted enabling mechanism (with a default of disabled).

The objective of this test group is to assess on the one hand, whether physical port interfaces that never require exposure are protected by the device casing. On the other hand it is assessed, whether air interfaces that never require exposure are disabled.

5.6.3.1 Test case 5.6-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the physical interfaces of the DUT concerning interfaces that do not require exposure in general (a-b) and interfaces that do not require permanent exposure c).

Test units

a) For each physical interface in IXIT 15-Intf that does not require exposure according to "Description", the TL **shall** assess whether the protection means of the interface in "Protection" include protection by the device casing or similar measures.

NOTE: For air interfaces it is acceptable that the antenna part remains outside of the device casing.

b) For each air interface in IXIT 15-Intf that does not require exposure according to "Description", the TL **shall** check whether the interface is disabled according to "Status".

c) For each physical interface in IXIT 15-Intf that does not require permanent exposure according to "Description", the TL **shall** check whether the interface is disabled according to "Status" for all periods in which the use of the interface is not required.

Assignment of verdict

The verdict PASS is assigned if:

- for every physical interface that does not require exposure, the protection means of the interface includes protection by the device casing or similar measures; and
- for every air interface that does not require exposure, the interface is disabled; and
- for every physical interface that does not require permanent exposure, the interface is disabled for all periods in which the use of the interface is not required.

The verdict FAIL is assigned otherwise.

5.6.3.2 Test case 5.6-3-2 (functional)

Test purpose

The purpose of this test case is the completeness of the IXIT documentation a) and the functional assessment of the physical interfaces of the DUT (b-d).

Test units

a) For each physical interface identified on the DUT the TL **shall** functionally check whether exposed physical interfaces on the DUT are contained in IXIT 15-Intf and described as required or intermittently required in "Description".

b) For each physical interface identified on the DUT that does not require exposure according to "Description" the TL **shall** functionally assess whether physical interfaces on the DUT are protected by device casing or similar measures.

NOTE: For air interfaces it is acceptable that the antenna part remains outside of the device casing.

c) For each air interface identified on the DUT the TL **shall** functionally check whether it is enabled or disabled as indicated in "Status" in IXIT 15-Intf.

d) For each physical interface identified on the DUT the TL **shall** functionally assess whether the physical interfaces that are not permanently required are disabled for all periods in which the use of the interface is not required.

Assignment of verdict

The verdict PASS is assigned if:

- all exposed physical interfaces on the DUT are described as "required" or "intermittently required" in the IXIT documentation; and
- all physical interfaces that are identified as never requiring exposure in the IXIT documentation, the interface is protected by the device casing or similar measures; and
- all air interfaces that are enabled on the DUT are marked as "required" or "intermittently required" in the IXIT documentation; and
- for all physical interfaces that are marked as "intermittently required" in the IXIT documentation, the interface is disabled for all periods in which the use of the interface is not required.

The verdict FAIL is assigned otherwise.

5.6.4 Test group 5.6-4

5.6.4.0 Test group objective

The test group addresses the provision 5.6-4.

Similar considerations to those of Test group 5.6-3 apply, with the exception that a software mechanism to disable the debug interface is mandatory. Here, the debug interface might be permanently disabled in software or, if it is foreseen that it can be useful in specific cases of the device lifecycle, be under the control of a trusted software mechanism.

Considering the level of security intended by ETSI TS 103 645 [1]/ETSI EN 303 645 [2], physically accessible is defined as being readily usable with a standard interface cable. Using specific tooling to physically access the interface (such as testing probes) is not in scope of the assessment.

5.6.4.1 Test case 5.6-4-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of physically accessible debug interfaces of the DUT.

Test units

a) For each physical interface in IXIT 15-Intf that is described as an accessible debug interface according to "Debug Interface", the TL **shall** assess whether the protection means for the interface in "Protection" include a software mechanism to disable the interface.

b) For each physical interface in IXIT 15-Intf that is described as an accessible debug interface, that is not indicated as intermittently required according to "Description", the TL **shall** check whether the interface is disabled permanently according to "Status".

c) For each physical interface in IXIT 15-Intf that is described as an accessible debug interface, that is indicated as intermittently required according to "Description", the TL **shall** check whether the interface is disabled by default according to "Status".

Assignment of verdict

The verdict PASS is assigned if:

- for every accessible physical debug interface, there is a software mechanism described to disable the interface; and
- for every accessible physical debug interface that is not indicated as intermittently required, the interface is permanently disabled; and
- for every accessible physical debug interface that is indicated as intermittently required, the interface is disabled by default.

The verdict FAIL is assigned otherwise.

5.6.4.2 Test case 5.6-4-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of physically accessible debug interfaces of the DUT a) and the completeness of the IXIT documentation b).

Test units

a) For each accessible physical interface on the DUT indicated as "Debug Interface" in IXIT 15-Intf, the TL **shall** functionally check whether the interface is disabled.

NOTE 1: For this test unit the TL is to ensure that the interface is in its default state.

b) For each accessible physical interface on the DUT the TL **shall** functionally assess whether the interface can be used for debugging purposes although it is not indicated as "Debug Interface" in IXIT 15-Intf.

NOTE 2: For this test unit the TL can attempt to use the interface as a debug interface using standard methods and tools.

Assignment of verdict

The verdict PASS is assigned if:

- every accessible physical debug interface is disabled; and
- every physical debug interface is indicated as such in the IXIT.

The verdict FAIL is assigned otherwise.

5.6.5 Test group 5.6-5

5.6.5.0 Test group objective

The test group addresses the provision 5.6-5.

There exist primarily three approaches to fulfil this provision, firstly, a service management framework is configured to only launch and manage those software services that are required for the operation of the consumer IoT device. Secondly, access to these software services is prevented through a filtering mechanism such as a packet filter (firewall), even if such service is active. Finally, software services that are not required for the operation of the device are not installed - this is the hardest approach and it goes beyond the requirements of the provision.

It is to be noted that it is difficult to achieve full minimization, for example there can be services that are enabled by default by an IoT platform provider.

5.6.5.1 Test case 5.6-5-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the enabled services concerning the intended use or operation of the DUT.

Test units

a) For each software service in IXIT 13-SoftServ that is enabled by default according to "Status", the TL **shall** assess whether the service is necessary for the intended use or operation of the DUT according to the purpose in "Description" and the "Justification" for enabling the service.

Assignment of verdict

The verdict PASS is assigned if:

- for every enabled by default software service, the service is necessary for the intended use or operation of the DUT.

The verdict FAIL is assigned otherwise.

5.6.6 Test group 5.6-6

5.6.6.0 Test group objective

The test group addresses the provision 5.6-6.

There exist many options to minimize code. Within large software projects, automated tools can be used to identify and remove dead code. Dependency and package managers allow to install only the components needed for the operations of service software, some have the ability to prune unused software out of the codebase once an option is disabled or a package removed. Third-party software providers possibly give options to what is included in the packaging, compilation or installation of their software.

Code minimization is assessed in terms of whether the selected method actually helps in minimizing code, to which extend, and whether the code minimization effort is proportionate to the reduction of the security risk. In assessing this latter dimension the introduction of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] can be referred to.

5.6.6.1 Test case 5.6-6-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the code minimization techniques.

Test units

a) The TL **shall** assess whether the code minimization techniques in IXIT 16-CodeMin are appropriate for reducing code to the necessary functionality.

Assignment of verdict

The verdict PASS is assigned if:

- the described code minimization techniques are appropriate for reducing code to the necessary functionality.

The verdict FAIL is assigned otherwise.

5.6.7 Test group 5.6-7

5.6.7.0 Test group objective

The test group addresses the provision 5.6-7.

Many operating systems for the IoT allow to reduce the privileges necessary for a given piece of software to run. This approach relies on three principles: separation of duty, need to know, and minimization of privileges. The ability to minimize privileges depends both on the application of the first two principles and on the functionalities provided by the hardware and software platform (for example mechanisms such as No eXecute (NX) bit, system calls, accounts, capabilities, pledge). The principle of need to know goes together with minimization of privilege.

5.6.7.1 Test case 5.6-7-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the privilege control mechanisms of the DUT.

Test units

a) The TL **shall** assess whether all mechanisms to control privileges of software on the DUT in IXIT 17-PrivlCtrl together facilitate the principles of separation of duty, need to know and minimization of privilege.

Assignment of verdict

The verdict PASS is assigned if:

- the described privilege control mechanisms are adequate to facilitate the principles of separation of duty, need to know and minimization of privilege.

The verdict FAIL is assigned otherwise.

5.6.8 Test group 5.6-8

5.6.8.0 Test group objective

The test group addresses the provision 5.6-8.

Many options exist that can be combined to provide hardware-level access control mechanisms for memory. At the level of grey-box testing this can be evaluation based on documentation provided by the manufacturer (e.g. schematics, bill of material, documentation resulting from certification of hardware components) or upon visual inspection of the board (visual identification of components) and documentation provided by hardware components suppliers.

The objective of this test group is to assess whether the identified hardware-level mechanisms do provide for access control to memory.

5.6.8.1 Test case 5.6-8-1 (conceptual)

Test purpose

The purpose of this test case is the conceptional assessment of the hardware-level mechanisms for access control to memory of the DUT.

Test units

a) For each hardware-level access control mechanism for memory in IXIT 18-AccCtrl, the TL **shall** assess whether the mechanism is implemented at the level of the hardware.

NOTE: Implementation at the level of the hardware can include software embedded in the hardware.

b) For each hardware-level access control mechanism for memory in IXIT 18-AccCtrl, the TL **shall** assess whether the mechanism allows to control access to memory.

Assignment of verdict

The verdict PASS is assigned if:

- for every hardware-level access control mechanism for memory, the mechanism is implemented at the level of the hardware; and
- for every hardware-level access control mechanism for memory, the mechanism allows to control access to memory.

The verdict FAIL is assigned otherwise.

5.6.9 Test group 5.6-9

5.6.9.0 Test group objective

The test group addresses the provision 5.6-9.

5.6.9.1 Test case 5.6-9-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the secure development processes a) and the confirmation that the preconditions for the implementation are ensured b).

Test units

a) The TL **shall** assess whether the secure development of software covers:

- security training of developers; and
- the requirement and design phases of the software; and
- secure coding techniques; and
- security tooling for the implementation phase; and
- security testing; and
- security review; and
- archival of assets and information relevant to maintaining security of the software; and
- secure deployment; and

- handling of third-party software providers.

according to the processes in IXIT 19-SecDev.

NOTE: Handling of third-party software providers is relevant only if these are part of the development process.

b) The TL **shall** check whether "Confirmation of Secure Development" in IXIT 4-Conf states a confirmation.

Assignment of verdict

The verdict PASS is assigned if the secure development covers:

- security training of developers; and
- the requirement and design phases of the software; and
- secure coding techniques; and
- security tolling for the implementation phase; and
- security testing; and
- security reviews; and
- archival of assets and information relevant to maintaining security of the software; and
- secure deployment; and
- if applicable, handling of third-party software providers; and
- a confirmation for the implementation is given.

The verdict FAIL is assigned otherwise.

5.7 TSO 5.7: Ensure software integrity

5.7.1 Test group 5.7-1

5.7.1.0 Test group objective

The test group addresses the provision 5.7-1.

This test group assesses whether the verification mechanism is suitable to verify the software based on the provided security guarantees and provides evidence about their implementation. To enable tamper resistance, at least integrity and authenticity are necessary secure guarantees in context of this test group.

NOTE: Threat modelling and the baseline attacker model described in clauses D.1 and D.2 are helpful to derive appropriate security guarantees, conceptually evaluate the corresponding mechanisms and functionally evaluate the correct implementation on a basic level.

5.7.1.1 Test case 5.7-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the secure boot mechanisms of the DUT.

Test units

a) The TL **shall** assess whether the "Security Guarantees" of each secure boot mechanism in IXIT 20-SecBoot provide at least verification of integrity and authenticity of device software.

b) The TL **shall** assess whether for each secure boot mechanism in IXIT 20-SecBoot the "Description" and corresponding "Detection Mechanisms" are suitable to provide the "Security Guarantees" it is used.

Assignment of verdict

The verdict PASS is assigned if:

- every secure boot mechanism provides the security guarantees of integrity and authenticity of the device software; and
- every secure boot mechanism and its detection mechanisms is suitable to provide the described security guarantee.

The verdict FAIL is assigned otherwise.

5.7.1.2 Test case 5.7-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the secure boot mechanisms of the DUT.

Test units

a) The TL **shall** functionally assess whether the verification of the device software is implemented according to the information in IXIT 20-SecBoot.

NOTE: Such inspection can include the simple manipulation of the firmware (e.g. bit manipulation), if the TL can get access to the firmware with basic resources (compare to clause D.2).

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication, that the implementation of any secure boot mechanism differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.7.2 Test group 5.7-2

5.7.2.0 Test group objective

The test group addresses the provision 5.7-2.

This test group assesses whether in the case that unauthorized changes in software are detected, the designated entity is alerted and communication of the DUT is restricted to that which is absolutely necessary for the alerting function (in the following referred to as "restricting mechanism").

5.7.2.1 Test case 5.7-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the alerting mechanisms a) and mechanisms for restricting the communication b) in case of detecting an unauthorized software change.

Test units

a) The TL **shall** assess whether the method for "User Notification" including its contained information is sufficient to inform the user and/or administrator about unauthorized changes in device software.

b) The TL **shall** assess whether every "Notification Functionality" in IXIT 20-SecBoot is necessary for the described method of "User Notification".

Assignment of verdict

The verdict PASS is assigned if:

- the described way of user notification is sufficient to inform the user and/or administrator about unauthorized changes in device software; and
- every described notification functionality is necessary for the user notification in case of detecting unauthorized software changes.

The verdict FAIL is assigned otherwise.

5.7.2.2 Test case 5.7-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the alerting mechanisms a) and mechanisms for restricting the communication b) in case of detecting an unauthorized software change.

Test units

a) The TL **shall** functionally assess whether alerting takes place as described in "User Notification" in IXIT 20-SecBoot after the detection of an unauthorized change in device software.

b) The TL **shall** functionally assess whether the communication capabilities of the DUT to wider networks are restricted to the ones described in "Notification Functionality" in IXIT 20-SecBoot after the detection of an unauthorized change in device software.

NOTE: Methods for functional evaluation of the communication capacities can include passive traffic inspection (e.g. by means of a protocol analyser) or traffic manipulation (e.g. redirection of traffic to a log facility).

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that the implementation of any alerting mechanism of the DUT differs from its IXIT documentation; and
- only communication to wider networks is detected after detection of unauthorized changes, that is described as necessary.

The verdict FAIL is assigned otherwise.

5.8 TSO 5.8: Ensure that personal data is secure

5.8.1 Test group 5.8-1

5.8.1.0 Test group objective

The test group addresses the provision 5.8-1.

The difference compared to Test group 5.5-1 is, that the use case in the underlying provision is concretised on the communication of personal data, which requires at least confidentiality.

The objective of this test group is to assess, firstly, whether the cryptographic methods provide the security guarantees that are necessary for the use case of the communication of personal data and, secondly, whether the cryptographic methods are not known to be vulnerable to a feasible attack.

5.8.1.1 Test case 5.8-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for communicating personal data between a device and a service.

Test units

a) For all "Communication Mechanisms" in IXIT 11-ComMech referenced in any personal data in IXIT 21-PersData, the TL **shall** apply all test units as specified in the Test case 5.5-1-1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.

NOTE: In this case the security guarantee "confidentiality" means confidentiality protection against unauthorized parties. This can include authenticity verification of a communication partner.

Assignment of verdict

The verdict PASS is assigned if for all communication mechanisms used for communicating personal data:

- the security guarantees are appropriate for the use case of communicating personal data; and
- the mechanism is appropriate to achieve the security guarantees with respect to the use case; and
- all used cryptographic details are considered as best practice for the use case; and
- all used cryptographic details are not known to be vulnerable to a feasible attack.

The verdict FAIL is assigned otherwise.

5.8.1.2 Test case 5.8-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the cryptography used for communicating personal data between a device and a service.

Test units

a) For all "Communication Mechanisms" in IXIT 11-ComMech referenced in any personal data in IXIT 21-PersData, the TL **shall** apply all test units as specified in the Test case 5.5-1-2.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any used cryptographic setting differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.8.2 Test group 5.8-2

5.8.2.0 Test group objective

The test group addresses the provision 5.8-2.

The difference compared to Test group 5.5-1 and Test group 5.8-1 is, that the use case in the underlying provision is concretised on the communication of sensitive personal data between the device and associated services, which requires at least confidentiality.

The objective of this test group is to assess, firstly, whether the cryptographic methods provide the security guarantees that are necessary for the use case of the communication of personal data and, secondly, whether the cryptographic methods are not known to be vulnerable to a feasible attack.

5.8.2.1 Test case 5.8-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for communicating sensitive personal data between the device and associated services.

Test units

a) For all "Communication Mechanisms" in IXIT 11-ComMech referenced in any sensitive personal data in IXIT 21-PersData according to "Sensitive", where the communication partner is an associated service, the TL **shall** apply all test units as specified in the Test case 5.5-1-1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.

NOTE: In this case the security guarantee "confidentiality" means confidentiality protection against unauthorized parties. This can include authenticity verification of a communication partner.

Assignment of verdict

The verdict PASS is assigned if for all communication mechanisms used for communicating sensitive personal data between the device and an associated service:

- the security guarantees are appropriate for the use case of communicating sensitive personal data between the device and an associated service; and
- the mechanism is appropriate to achieve the security guarantees with respect to the use case; and
- all used cryptographic details are considered as best practice for the use case; and
- all used cryptographic details are not known to be vulnerable to a feasible attack.

The verdict FAIL is assigned otherwise.

5.8.2.2 Test case 5.8-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the cryptography used for communicating sensitive personal data between the device and associated services.

Test units

a) For all "Communication Mechanisms" in IXIT 11-ComMech referenced in any sensitive personal data in IXIT 21-PersData according to "Sensitive", where the communication partner is an associated service, the TL **shall** apply all test units as specified in the Test case 5.5-1-2.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any used cryptographic setting differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.8.3 Test group 5.8-3

5.8.3.0 Test group objective

The test group addresses the provision 5.8-3.

This test group aims at revealing any capabilities of a DUT to sense information about its surroundings, such as optic, acoustic, biometric or location sensors. It is to be documented in a way that the user is knowledgeable about information that is obtained by the DUT.

NOTE 1: The aim is to ensure that no functional sensing capabilities exist in the DUT that are undocumented. Inactive sensing capabilities could be activated by an attacker e.g. using compromised firmware. In general, not all sensing capabilities of the DUT are necessarily active. Still, all capabilities have to be documented.

NOTE 2: Clearness and transparency of documentation refer to an understandable description in the documentation, as well as an explanation for the presence of sensing capabilities in the DUT.

5.8.3.1 Test case 5.8-3-1 (functional)

Test purpose

The purpose of this test case is the functional assessment of the documentation of external sensing capabilities (a-b) and the completeness of the IXIT documentation c).

Test units

a) The TL **shall** functionally check whether the documentation of external sensing capabilities is accessible as documented in "Documentation of Sensors" in IXIT 2-UserInfo.

b) The TL **shall** functionally assess whether the documentation of external sensing capabilities as documented in "Documentation of Sensors" in IXIT 2-UserInfo is understandable for a user with limited technical knowledge (see clause D.3).

c) The TL **shall** functionally assess whether all obvious sensing capabilities of the DUT are documented in IXIT 22-ExtSens.

NOTE: Such assessment can include a visual inspection of the DUT's casing with regard to indications for undocumented sensoring capabilities. If indications are found, opening the casing can provide clarity.

Assignment of verdict

The verdict PASS is assigned if:

- the documentation is accessible according to the IXIT; and
- the documentation is understandable for a user with limited technical knowledge; and
- each obvious sensing capability of the DUT is documented for the user.

The verdict FAIL is assigned otherwise.

5.9 TSO 5.9: Make systems resilient to outages

5.9.1 Test Group 5.9-1

5.9.1.0 Test group objective

The test group addresses the provision 5.9-1.

5.9.1.1 Test case 5.9-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the resilience mechanisms concerning outages of network and power.

Test units

a) The TL **shall** assess whether the combination of the resilience mechanisms in IXIT 23-ResMech are appropriate to protect against network connectivity and power outages according to the "Security Guarantees".

b) For each resilience mechanism in IXIT 23-ResMech the TL **shall** assess whether the mechanism according to the "Description" is appropriate to achieve the "Security Guarantees".

Assignment of verdict

The verdict PASS is assigned if:

- the resilience mechanisms are appropriate to protect against network connectivity and power outages; and
- every resilience mechanism is appropriate to achieve its security guarantees.

The verdict FAIL is assigned otherwise.

5.9.1.2 Test case 5.9-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the resilience mechanisms concerning outages of network and power.

Test units

a) The TL **shall** interrupt the DUT's connection to the network and functionally assess whether the resilience mechanisms operate as described in IXIT 23-ResMech.

b) The TL **shall** interrupt the DUT's power supply and functionally assess whether the resilience mechanisms operate as described in IXIT 23-ResMech.

EXAMPLE: If the DUT monitors local events and to report them to an associated service via network, disrupting the network connection while triggering a local event and verifying that after reconnection to the network the event is visible on the interface of the associated service can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that the operation of the resilience mechanisms during network connectivity and power outages differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.9.2 Test Group 5.9-2

5.9.2.0 Test group objective

The test group addresses the provision 5.9-2.

5.9.2.1 Test case 5.9-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the resilience mechanisms concerning outages of network and power a) and the operation during network outages b) and restoration after power outages c).

Test units

a) The TL **shall** apply all test units as specified in the Test case 5.9-1-1 for the resilience mechanisms in IXIT 23-ResMech.

b) The TL **shall** assess whether the resilience mechanisms in IXIT 23-ResMech protecting against network connectivity outages according to "Type" are appropriate to ensure, that the DUT remains operating and locally functional in the case of a loss of network connectivity.

c) The TL **shall** assess whether the resilience mechanisms in IXIT 23-ResMech protecting against power outages according to "Type" are appropriate to ensure, that the DUT resumes the connectivity and functionality after a loss of power in the same or improved state as before.

Assignment of verdict

The verdict PASS is assigned if:

- the resilience mechanisms are appropriate to protect against network connectivity and power outages; and
- every resilience mechanism is appropriate to achieve its security guarantees; and
- the resilience mechanisms are appropriate to ensure that the DUT remains operating and locally functional in the case of a loss of network connectivity; and
- the resilience mechanisms are appropriate to ensure that the DUT recovers cleanly after a loss of power.

The verdict FAIL is assigned otherwise.

5.9.2.2 Test case 5.9-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the resilience mechanisms concerning outages of network and power, the operation during network outages and restoration after power outages.

Test units

a) The TL **shall** interrupt the DUT's connection to the network and functionally assess whether the resilience mechanisms operate as described in IXIT 23-ResMech and the DUT remains operating and locally functional after the loss of network connectivity.

EXAMPLE 1: If the DUT monitors local events and to report them to an associated service via network, disrupting the network connection while triggering a local event and verifying that after reconnection to the network the event is visible on the interface of the associated service can be helpful to collect an indication.

b) The TL **shall** interrupt the DUT's power supply and functionally assess whether the resilience mechanisms operate as described in IXIT 23-ResMech and the DUT resumes the connectivity and functionality after a loss of power in the same or improved state as before.

EXAMPLE 2: If the DUT monitors local events and to report them to an associated service via network, triggering a local event after power resumption and verifying that the event is visible on the interface of the associated service can be helpful to collect an indication.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that the operation of the resilience mechanisms during network connectivity or power outages differs from its IXIT documentation; and
- there is no indication that the DUT does not remain operating and locally functional after the loss of network connectivity; and
- there is no indication that the DUT does not resume the connectivity and functionality after a loss of power in the same or improved state as before.

The verdict FAIL is assigned otherwise.

5.9.3 Test Group 5.9-3

5.9.3.0 Test group objective

The test group addresses the provision 5.9-3.

This test group considers the capabilities:

- to perform a standardized connection establishment, and
- to protect against mass-reconnections.

5.9.3.1 Test case 5.9-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the resilience measures for the communication mechanisms.

Test units

a) For each communication mechanism in IXIT 11-ComMech the TL **shall** assess whether the "Resilience Measures" are appropriate to achieve a connection to a network in an orderly fashion taking the capability of the infrastructure into consideration.

NOTE 1: An appropriate measure to achieve a connection in an orderly fashion is to follow suitable standards for initialization and termination.

b) For each communication mechanism in IXIT 11-ComMech the TL **shall** assess whether the "Resilience Measures" are appropriate to support the operation of a stable network taking the capability of the infrastructure into consideration.

NOTE 2: An appropriate measure to support a stable network is to prevent simultaneous mass-reconnections. This can be done by connecting to a random server from a given list (load balancing) or a random delay when reconnecting.

Assignment of verdict

The verdict PASS is assigned if:

- every communication mechanism provides appropriate measures to achieve a connection to a network in an orderly fashion; and
- every communication mechanism provides appropriate measures to support the operation of a stable network.

The verdict FAIL is assigned otherwise.

5.9.3.2 Test case 5.9-3-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the resilience measures for the communication mechanisms.

Test units

a) The TL **shall** functionally assess whether the implemented "Resilience Measures" for each communication method in IXIT 11-ComMech are implemented as described, especially considering the protection against simultaneous mass-reconnections.

EXAMPLE: If the DUT uses the TCP/IP protocol, a network sniffer to verify the initialization and termination concerning the connection establishment follows the corresponding standards can be helpful to collect indications.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that the operation of any implemented resilience measure differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.10 TSO 5.10: Examine system telemetry data

5.10.1 Test Group 5.10-1

5.10.1.0 Test group objective

The test group addresses the provision 5.10-1.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2], telemetry data can provide information to help the manufacturer identify issues or information related to DUT usage.

5.10.1.1 Test case 5.10-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the security anomaly examination.

Test units

a) The TL **shall** check whether at least one "Security Examination" is provided in IXIT 24-TelData for examining for security anomalies.

b) For each "Security Examination" of telemetry data in IXIT 24-TelData, the TL **shall** assess whether the associated telemetry data in "Description" are suited for the described security examination and for examining the data for security anomalies.

Assignment of verdict

The verdict PASS is assigned if:

- at least one security anomaly examination is provided; and
- each security anomaly examination is suited for examining the associated telemetry data for a security anomaly.

The verdict FAIL is assigned otherwise.

5.11 TSO 5.11: Make it easy for users to delete user data

5.11.1 Test group 5.11-1

5.11.1.0 Test group objective

The test group addresses the provision 5.11-1.

5.11.1.1 Test case 5.11-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the user data erasure functionalities of the DUT.

Test units

a) The TL **shall** assess whether at least one functionality is provided according to IXIT 25-DelFunc, which can be performed by the user with limited technical knowledge (see clause D.3) according to "Description" and "Initiation and Interaction" to erase user data from the device according to "Target Type".

b) The TL **shall** assess whether each functionality in IXIT 25-DelFunc is adequate to erase the targeted user data from the device.

NOTE 1: Erasure can be realized by overwriting with a pre-defined value or by internal irreversible blocking of all access to the data on the device.

c) The TL **shall** assess whether the functionalities to erase user data in IXIT 25-DelFunc cover personal data, user configuration and user-related cryptographic material.

NOTE 2: The information in IXIT 10-SecParam, IXIT 21-PersData and other IXITs is helpful to identify user data.

NOTE 3: Cryptographic material can be user passwords or keys.

Assignment of verdict

The verdict PASS is assigned if no user data is stored on the device; or:

- at least one simple functionality to erase user data from the device is provided to the user; and
- the described functionality is adequate to erase the targeted user data from the device; and
- personal data, user configuration and cryptographic material is covered by the functionalities to erase user data from the device.

The verdict FAIL is assigned otherwise.

5.11.1.2 Test case 5.11-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the user data erasure functionalities of the DUT.

Test units

a) The TL **shall** create typical user data on the DUT with regard to the usage of the device.

NOTE: Such data can be personal data, user configuration or cryptographic material such as user passwords or keys, which differ from the standard configuration.

b) The TL **shall** perform each functionality to erase user data from the device according to "Target Type" in IXIT 25-DelFunc and functionally assess whether the "Initiation and Interaction" is consistent with the IXIT.

c) The TL **shall** perform each functionality to erase user data from the device according to "Target Type" in IXIT 25-DelFunc and functionally assess whether the corresponding user data still exists after completing the operation.

EXAMPLE: The comparison between the configuration before and after the erasure can be helpful to collect an indication concerning not erased user data.

Assignment of verdict

The verdict PASS is assigned if for any functionality to erase user data from the device:

- the initiation and interaction of the user is consistent with the IXIT; and
- there is no indication that the corresponding user data is not erased successfully.

The verdict FAIL is assigned otherwise.

5.11.2 Test group 5.11-2

5.11.2.0 Test group objective

The test group addresses the provision 5.11-2.

The provision implies that a functionality for removal of personal data can be clearly identified (possibly in relation to a specific associated service that can be used from the device) and can be easily performed.

5.11.2.1 Test case 5.11-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the personal data removal functionalities of the DUT.

Test units

a) For all deletion functionalities in IXIT 25-DelFunc the TL **shall** assess whether at least one functionality is provided, which can be performed by the user with limited technical knowledge (see clause D.3) according to "Description" and "Initiation and Interaction" to remove all personal data stored on the associated services according to "Target Type".

b) The TL **shall** assess whether all associated services storing personal data according to "Processing Activities" in IXIT 21-PersData are covered by the combination of all deletion functionalities in IXIT 25-DelFunc.

Assignment of verdict

The verdict PASS is assigned if:

- at least one simple functionality to remove personal data from associated services is provided to the user; and
- every associated service storing personal data is covered by a simple deletion functionality.

The verdict FAIL is assigned otherwise.

5.11.2.2 Test case 5.11-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the personal data removal functionalities of the DUT.

Test units

a) The TL **shall** create typical personal data on associated services with regard to the usage of the DUT.

NOTE 1: The information from "Processing Activities" IXIT 21-PersData can be helpful to create personal data which are stored on associated services.

b) The TL **shall** perform each functionality to remove personal data according to "Target Type" in IXIT 25-DelFunc and functionally assess whether the "Initiation and Interaction" is consistent with in the IXIT.

c) The TL **shall** perform each functionality to remove personal data according to "Target Type" in IXIT 25-DelFunc and functionally assess whether the corresponding personal data still exists on the associated services after completing the operation.

EXAMPLE: The comparison between the stored personal data before and after the removal and verifying that user accounts are not accessible anymore can be helpful to collect an indication concerning not removed personal data from associated services.

NOTE 2: Although it is assumed, that the TL is not in control of the associated services (see clause 4.2.1), there can be an indication for completing the operation by the associated services, e.g. notification about completion or log files.

Assignment of verdict

The verdict PASS is assigned if for every functionality to remove personal data on associated services:

- the initiation and interaction of the user is consistent with the IXIT; and
- there is no indication that the corresponding personal data stored on the associated service is not removed successfully.

The verdict FAIL is assigned otherwise.

5.11.3 Test group 5.11-3

5.11.3.0 Test group objective

The test group addresses the provision 5.11-3.

Characteristics of clear instructions as expected by a user include conciseness and accuracy.

5.11.3.1 Test case 5.11-3-1 (functional)

Test purpose

The purpose of this test case is the functional assessment of the user documentation for the personal data deletion functionalities of the DUT.

Test units

a) The TL **shall** create typical personal data with regard to the usage of the DUT.

NOTE 1: The information from "Processing Activities" IXIT 21-PersData can be helpful to create personal data which are stored on the DUT and on associated services.

b) The TL **shall** functionally assess whether all deletion functionalities in IXIT 25-DelFunc are covered by the "Documentation of Deletion" in IXIT 2-UserInfo.

c) For each deletion functionality in IXIT 25-DelFunc the TL **shall** perform the functionality according to the "Documentation of Deletion" in IXIT 2-UserInfo and functionally assess whether it is described in a concise manner and includes all necessary steps to delete the personal data from the device or associated service according to "Target Type" in IXIT 25-DelFunc.

Assignment of verdict

The verdict PASS is assigned if every deletion functionality:

- is covered by the documentation; and
- is documented in a concise manner and includes the necessary steps to be taken to delete personal data.

The verdict FAIL is assigned otherwise.

5.11.4 Test group 5.11-4

5.11.4.0 Test group objective

The test group addresses the provision 5.11-4.

A clear confirmation entails a transparent message that carries a positive statement in the case that the requested operation was successfully completed. The aim of the test group is to assess the design of the confirmation. The functionality of the mechanism is verified in Test group 5.11-1 and Test group 5.11-2.

5.11.4.1 Test case 5.11-4-1 (functional)

Test purpose

The purpose of this test case is the functional assessment of the confirmation for the user concerning the deletion functionalities.

Test units

a) The TL **shall** perform each deletion functionality in IXIT 25-DelFunc according to "Documentation of Deletion" in IXIT 2-UserInfo.

b) For each deletion functionality in IXIT 25-DelFunc the TL **shall** functionally assess whether the user is provided with a clear "Confirmation", that the corresponding data is deleted.

Assignment of verdict

The verdict PASS is assigned if:

- for every deletion functionality a clear confirmation is provided, that the corresponding data is deleted.

The verdict FAIL is assigned otherwise.

5.12 TSO 5.12: Make installation and maintenance of devices easy

5.12.1 Test group 5.12-1

5.12.1.0 Test group objective

The test group addresses the provision 5.12-1.

Involving minimal decisions by the user entails that some decision steps are automated by the DUT. Security best practices on usability entail that decision steps are prominently displayed to the use (not hidden) and that the configuration parameters have secure defaults.

NOTE: Considering the level of assurance aimed by ETSI TS 103 645 [1]/ETSI EN 303 645 [2], physical installation and physical security are not in scope of this test group.

5.12.1.1 Test case 5.12-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the installation and maintenance decisions to be taken by the user.

Test units

a) For each decision in IXIT 26-UserDec the TL **shall** assess whether it is necessary regarding the usage in the operational environment.

NOTE 1: The operational environment can vary. An indicator for minimal decisions is that only decisions with impact on the operation environment are taken by the user, e.g. to avoid incompatibilities, otherwise default values are used.

b) For each decision in IXIT 26-UserDec the TL **shall** assess whether the default value for the decision according to "Options" follows security best practice.

NOTE 2: It is helpful to use the provisions from ETSI TS 103 645 [1]/ETSI EN 303 645 [2] as guidance for security best practice.

Assignment of verdict

The verdict PASS is assigned if:

- every decision taken by the user is necessary regarding the usage in the operational environment; and
- every default value for a decision taken by the user follows security best practice.

The verdict FAIL is assigned otherwise.

5.12.1.2 Test case 5.12-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the installation and maintenance decisions to be taken by the user.

Test units

a) The TL **shall** trigger all user-based decisions in IXIT 26-UserDec according to "Triggered By".

b) For each decision in IXIT 26-UserDec the TL **shall** functionally assess whether it is prominently requested from the user during the installation and maintenance flows.

c) For each decision in IXIT 26-UserDec the TL **shall** functionally assess whether the decision and its "Options" are understandable for a user with limited technical knowledge (see clause D.3).

d) The TL **shall** functionally assess whether the decisions to be taken by the user during installation and maintenance on the DUT are conformant to their "Description" and "Options" in IXIT 26-UserDec.

Assignment of verdict

The verdict PASS is assigned if:

- every decision taken by the user is prominently requested during the installation and maintenance flows; and
- every decision taken by the user is understandable for a user with limited technical knowledge; and
- every decision taken by the user during installation or maintenance on the DUT is as described in the IXIT.

The verdict FAIL is assigned otherwise.

5.12.2 Test group 5.12-2

5.12.2.0 Test group objective

The test group addresses the provision 5.12-2.

Guidance entails describing what the setup parameters are that have an impact on security, issuing a recommendation on how to configure the parameters to achieve a secure setup.

5.12.2.1 Test case 5.12-2-1 (functional)

Test purpose

The purpose of this test case is the functional assessment of the user guidance on securely setting up the DUT.

Test units

a) The TL **shall** set up the DUT using the "Documentation of Secure Setup" described in IXIT 2-UserInfo.

b) The TL **shall** functionally assess whether in the "Documentation of Secure Setup" described in IXIT 2-UserInfo each security-relevant user decision in IXIT 26-UserDec is covered by the documentation.

c) The TL **shall** functionally assess whether the "Documentation of Secure Setup" described in IXIT 2-UserInfo includes recommendations on how to take the security-relevant user decisions to achieve a secure setup.

Assignment of verdict

The verdict PASS is assigned if:

- every security-relevant user decision is covered by the documentation; and
- for every security-relevant user decision a recommendation on how to achieve a secure setup is given.

The verdict FAIL is assigned otherwise.

5.12.3 Test group 5.12-3

5.12.3.0 Test group objective

The test group addresses the provision 5.12-3.

Because the methods available to check whether a device is securely set up vary from product to product, the test group focuses on verifying the existence of guidance documentation and its key characteristics: accessible, on topic, concise, accurate, with clear verification criteria, and reproducible by the user.

5.12.3.1 Test case 5.12-3-1 (functional)

Test purpose

The purpose of this test case is the functional assessment of the user guidance on checking whether the DUT is securely set up.

Test units

a) The TL **shall** set up the DUT using an example configuration.

NOTE: It can be helpful to use an insecure configuration on purpose to comprehend the criteria for the security check.

b) The TL **shall** functionally assess whether in the "Documentation of Setup Check" described in IXIT 2-UserInfo each step for checking whether the DUT is securely set up is covered by the documentation.

c) The TL **shall** functionally assess whether the check applied to the example configuration results in a reasonable outcome.

EXAMPLE: Verifying that the result of checking a secure and an insecure configuration states that the DUT is securely and not securely set up respectively is helpful to collect an indication for a reasonable result.

Assignment of verdict

The verdict PASS is assigned if:

- every step for checking the securely set up is covered by the documentation; and
- the application of the check for securely set up according to the documentation results in an outcome and there is an indication that the result is reasonable.

The verdict FAIL is assigned otherwise.

5.13 TSO 5.13: Validate input data

5.13.1 Test group 5.13-1

5.13.1.0 Test group objective

The test group addresses the provision 5.13-1.

Input data validation ensures that the receiving end can process the data without causing unexpected behaviour. This entails verifying that the provided data is of the correct type (allowed data format and data structures), of allowed value, and of allowed cardinalities and ordering. This can be done against a list of acceptable values when such list is short.

5.13.1.1 Test case 5.13-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the data input validation methods of the DUT.

Test units

a) The TL **shall** assess whether the combination of data input validation methods in IXIT 29-InpVal covers all sources for data input including

- the user interfaces, which enable data input from the user in IXIT 27-UserIntf; and
- the application programming interfaces (APIs), which enable data input from external sources in IXIT 28-ExtAPI; and
- the network communications, which enable data input according to the corresponding remotely accessible communication methods in IXIT 11-ComMech.

b) For each data input validation method in IXIT 29-InpVal, the TL **shall** assess whether it is effective for validating the corresponding data input.

NOTE: Validation typically includes checks that data input is of an allowed format and structure, of an allowed value, of an allowed cardinality and of an allowed ordering with the aim to prevent misuse.

Assignment of verdict

The verdict PASS is assigned if:

- the data input validation methods cover data input via user interfaces, transmitted via APIs and between networks in services and devices; and
- every described data input validation method is effective for validating the corresponding data input.

The verdict FAIL is assigned otherwise.

5.13.1.2 Test case 5.13-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the data input validation methods of the DUT a) and the completeness of the IXIT documentation (b-c).

Test units

a) The TL **shall** functionally assess whether each data input validation method in IXIT 29-InpVal prevents the processing of unexpected data input.

NOTE 1: The TL is free to choose a source of data input for each data input validation method.

NOTE 2: The TL possesses all credentials of a user to attempt the misuses.

NOTE 3: Automated tools can be used to generate unexpected data which does not suit to the expected input, e.g. in format and structure, value, cardinality or ordering.

EXAMPLE 1: If the DUT uses an interface with a stateless protocol, usage of a fuzzer with random input to verify the described input validation method can be helpful to collect indications.

EXAMPLE 2: If the DUT presents a web interface, usage of a web application scanner to verify there are no typical web-related issues like XSS, SQL injections, or CSRF can be helpful to collect indications.

b) The TL **shall** functionally assess whether all user interfaces of the DUT are described in IXIT 27-UserIntf according to the documentation for the user, e.g. user manual.

c) The TL **shall** functionally assess whether all remotely accessible APIs of the DUT are described in IXIT 28-ExtAPI.

EXAMPLE: Network scanning tools allow for discovery of remotely accessible APIs.

Assignment of verdict

The verdict PASS is assigned if:

- there is no indication that any data input validation does not protect against the processing of unexpected data input; and
- every discovered user interface is documented in the IXIT; and
- every discovered remotely accessible API is documented in the IXIT.

The verdict FAIL is assigned otherwise.

5.14 TSO 6: Data protection for consumer IoT

5.14.1 Test group 6-1

5.14.1.0 Test group objective

The test group addresses the provision 6-1.

5.14.1.1 Test case 6-1-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the user information about the processing of personal data.

Test units

a) The TL **shall** assess whether the "Documentation of Personal Data" in IXIT 2-UserInfo is suitable for the consumer to obtain the information about processing personal data.

Assignment of verdict

The verdict PASS is assigned if:

- the information about processing personal data is suitably provided to the consumer.

The verdict FAIL is assigned otherwise.

5.14.1.2 Test case 6-1-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the user information about the processing of personal data.

Test units

a) The TL **shall** functionally assess whether the provided information about processing personal data (obtained information) is consistent to the description in "Documentation of Personal Data" in IXIT 2-UserInfo.

b) The TL **shall** functionally assess whether the obtained information about processing personal data accessing the "Documentation of Personal Data" in IXIT 2-UserInfo match their description in "Processing Activities" in IXIT 21-PersData.

c) The TL **shall** functionally assess whether the obtained information describes what personal data is processed in a way understandable for a user with limited technical knowledge (see clause D.3).

d) The TL **shall** functionally assess whether the obtained information describe how personal data is being used, by whom, and for what purposes in a way understandable for a user with limited technical knowledge (see clause D.3).

Assignment of verdict

The verdict PASS is assigned if:

- the information about processing personal data can be obtained as described; and
- the obtained information about processing personal data match their description; and
- the personal data being processed is clearly and transparently described; and
- it is clearly and transparently described how personal data is being used, by whom, and for what purposes.

The verdict FAIL is assigned otherwise.

5.14.2 Test group 6-2

5.14.2.0 Test group objective

The test group addresses the provision 6-2.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2], obtaining consent "in a valid way" normally involves giving consumers a free, obvious and explicit opt-in choice of whether their personal data is used for a specified purpose.

5.14.2.1 Test case 6-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** assess whether the opt-in choice:

   - is given freely; and
   - is given obviously; and
   - is given explicitly

according to the description of "Obtaining Consent".

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- it is described how to express consent (opt-in choice) to the processing of personal data for specific purposes; and

- the opt-in choice is given freely, obviously and explicitly.

The verdict FAIL is assigned otherwise.

5.14.2.2 Test case 6-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** functionally assess whether consumers' consent to processing personal data is obtained as described in the IXIT.

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- the way of obtaining consumers' consent matches the description.

The verdict FAIL is assigned otherwise.

5.14.3 Test group 6-3

5.14.3.0 Test group objective

The test group addresses the provision 6-3.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2], withdrawing consent at any time normally involves configuring IoT device and service functionality appropriately.

5.14.3.1 Test case 6-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of withdrawing consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** assess whether the information on "Withdrawing Consent" describes how to withdraw consent to the processing of personal data at any time by configuring IoT device and service functionality appropriately.

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- it is described how to withdraw consent to the processing of personal data at any time.

The verdict FAIL is assigned otherwise.

5.14.3.2 Test case 6-3-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of withdrawing consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** functionally assess whether consumers' consent to processing personal data can be withdrawn as described in "Withdrawing Consent".

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- the way of withdrawing consumers' consent matches the description.

The verdict FAIL is assigned otherwise.

5.14.4 Test group 6-4

5.14.4.0 Test group objective

The test group addresses the provision 6-4.

5.14.4.1 Test case 6-4-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the processing of telemetry data.

Test units

a) The TL **shall** assess whether the personal data in IXIT 21-PersData that are referenced in "Personal Data" in IXIT 24-TelData is necessary for the intended functionality as described in the "Purpose" of collecting the data.

NOTE: Telemetry data are considered to be necessary for the intended functionality if and only if they are needed for achieving the processing purposes.

Assignment of verdict

The verdict PASS is assigned if for each telemetry data:

- their processing is necessary for the intended functionality.

The verdict FAIL is assigned otherwise.

5.14.5 Test group 6-5

5.14.5.0 Test group objective

The test group addresses the provision 6-5.

5.14.5.1 Test case 6-5-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the user information about the processing of telemetry data.

Test units

a) The TL **shall** assess whether the "Documentation of Telemetry Data" in IXIT 2-UserInfo is suitable for the consumer to obtain the information about processing telemetry data.

Assignment of verdict

The verdict PASS is assigned if:

- the information about processing telemetry data is suitably provided to the consumer.

The verdict FAIL is assigned otherwise.

5.14.5.2 Test case 6-5-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of user the information about the processing of telemetry data.

Test units

a) The TL **shall** functionally assess whether the provided information about processing telemetry data (obtained information) is consistent with the description in "Documentation of Telemetry Data" in IXIT 2-UserInfo.

b) The TL **shall** functionally assess whether the obtained information about processing telemetry data accessing the "Documentation of Telemetry Data" in IXIT 2-UserInfo match their "Purpose" described in IXIT 24-TelData.

c) The TL **shall** functionally check whether the obtained information describes what telemetry data is collected.

d) The TL **shall** functionally check whether the obtained information describes how telemetry data is being used, by whom, and for what purposes.

Assignment of verdict

The verdict PASS is assigned if:

- the information about processing telemetry data can be obtained as described; and
- the obtained information about processing telemetry data match their description; and
- the telemetry data being collected is described; and
- it is completely described how telemetry data is being used, by whom, and for what purposes.

The verdict FAIL is assigned otherwise.

Annex A (normative): Pro formas for the SO

A.1 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the Identification of the DUT pro forma, ICS pro forma and IXIT pro forma in this annex so that they can be used for their intended purposes and may further publish the completed pro formas.

A.2 Identification of the DUT pro forma

The Identification of the DUT provides information as detailed as possible about the DUT regarding version numbers and configuration options. Further, a declaration concerning constrained devices and contact information for the TL are part of the pro forma.

Date of the statement

Date of the statement	

DUT identification

DUT name	
Brand/Trade Names: The devices with alternative brand/trade names are expected to be functionally equivalent to the DUT	
Hardware configuration (including Release Number and Serial Number)	
Runtime environment/Operating system (if applicable)	
Firmware version in factory setting	
Associated services necessary for the assessment (including e.g. Release Number, URL)	

Constrained Device

Constrained Device (according to ETSI TS 103 645 [1]/ ETSI EN 303 645 [2])	Yes/No
Justification	(detailed)

Supplier Organization (SO)

Name	
Address	
Telephone number	
E-mail address	
Additional information	

SO contact person

Name	
Telephone number	
E-mail address	
Additional information	

A.3 Implementation conformance statement (ICS) pro forma

Table A.1 provides a mechanism for the user of the present document (who is expected to be an entity involved in the development or manufacturing of consumer IoT) to give information about the implementation of the provisions within ETSI TS 103 645 [1]/ETSI EN 303 645 [2].

The provision column gives reference to the provisions in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].

The status column indicates the status of a provision. The following notations are used:

M the provision is a mandatory requirement

R the provision is a recommendation

M C the provision is a mandatory requirement and conditional

R C the provision is a recommendation and conditional

NOTE: Where the conditional notation is used, this is conditional on the text of the provision. The conditions are provided at the bottom of the table with references provided for the relevant provisions to help with clarity.

The support column can be filled in by the user of the present document. The following notations are used:

Y supported by the implementation

N not supported by the implementation

N/A the provision is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the product in question)

The detail column can be filled in by the user of the present document:

- If a provision is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.

- If a provision is not supported by the implementation, the entry in the detail column is to contain information on the reasons why implementation is not possible or not appropriate.
- If a provision is not applicable, the entry in the detail column is to contain the rationale for this determination.

Table A.1: Implementation of provisions for consumer IoT security

Clause number and title			
Provision	**Status**	**Support**	**Detail**
4 Reporting implementation			
4-1	M		
5.1 No universal default passwords			
5.1-1	M C (1)		
5.1-2	M C (2)		
5.1-3	M C (8)		
5.1-4	M C (8)		
5.1-5	M C (5)		
5.2 Implement a means to manage reports of vulnerabilities			
5.2-1	M		
5.2-2	R		
5.2-3	R		
5.3 Keep software updated			
5.3-1	R		
5.3-2	M C (5)		
5.3-3	M C (12)		
5.3-4	R C (12)		
5.3-5	R C (12)		
5.3-6	R C (9, 12)		
5.3-7	M C (12)		
5.3-8	M C (12)		
5.3-9	R C (12)		
5.3-10	M C (11, 12)		
5.3-11	R C (12)		
5.3-12	R C (12)		
5.3-13	M		
5.3-14	R C (3, 4)		
5.3-15	R C (3, 4)		
5.3-16	M		
5.4 Securely store sensitive security parameters			
5.4-1	M C (14)		
5.4-2	M C (10)		
5.4-3	M		
5.4-4	M C (15)		
5.5 Communicate securely			
5.5-1	M		
5.5-2	R		
5.5-3	R		
5.5-4	R C (16)		
5.5-5	M C (17)		
5.5-6	R C (18)		
5.5-7	M C (19)		
5.5-8	M C (20)		
5.6 Minimize exposed attack surfaces			
5.6-1	M		
5.6-2	M		
5.6-3	R		
5.6-4	M C (13)		
5.6-5	R		
5.6-6	R		
5.6-7	R		
5.6-8	R		
5.6-9	R		
5.7 Ensure software integrity			
5.7-1	R		
5.7-2	R		

Clause number and title			
Provision	**Status**	**Support**	**Detail**
5.8 Ensure that personal data is secure			
5.8-1	R C (21)		
5.8-2	M C (22)		
5.8-3	M C (23)		
5.9 Make systems resilient to outages			
5.9-1	R		
5.9-2	R		
5.9-3	R		
5.10 Examine system telemetry data			
5.10-1	R C (6)		
5.11 Make it easy for users to delete user data			
5.11-1	M C (24)		
5.11-2	R C (25)		
5.11-3	R C (26)		
5.11-4	R C (26)		
5.12 Make installation and maintenance of devices easy			
5.12-1	R		
5.12-2	R		
5.12-3	R		
5.13 Validate input data			
5.13-1	M C (27)		
6 Data protection provisions for consumer IoT			
6-1	M C (28)		
6-2	M C (7)		
6-3	M C (7)		
6-4	R C (6)		
6-5	M C (6)		

Conditions

1) passwords are used;
2) pre-installed unique per device passwords are used;
3) software components are not updateable;
4) the device is constrained;
5) the device is not constrained;
6) telemetry data being collected;
7) personal data is processed on the basis of consumers' consent;
8) the device allowing user authentication;
9) the device supports automatic updates and/or update notifications;
10) a hard-coded unique per device identity is used for security purposes;
11) updates are delivered over a network interface;
12) an update mechanism is implemented;
13) a debug interface is physically accessible;
14) sensitive security parameters are stored persistently;
15) critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist;
16) access to device functionality via a network interface in the initialized state is possible;
17) device functionality that allows security-relevant changes in configuration via a network interface exists;
18) critical security parameters are transmitted;
19) critical security parameters are transmitted via remotely accessible network interfaces;
20) critical security parameters relating to the device exist;
21) personal data is transmitted between a device and a service;
22) sensitive personal data is transmitted between a device and a service;
23) external sensing capabilities exist;
24) user data is stored on the device;
25) personal data is stored on associated services;
26) personal data is stored;
27) data input via user interfaces or transferred via APIs or between networks in services and devices is supported;
28) personal data is processed.

A.4 Implementation eXtra Information for Testing (IXIT) pro forma

IXIT 1-AuthMech: Authentication Mechanisms

The completed IXIT lists all authentication mechanisms of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 1: Sequential numbering ("AuthMech-1") or labelling scheme ("AuthMech-PswdWebIf").

- **Description:** Brief description of the authentication mechanism and its corresponding authorization process. It is indicated additionally whether the mechanism is used for user or machine-to-machine authentication and whether it is directly addressable from a network interface.

- **Authentication Factor:** The type of attribute used for authentication. For passwords it is indicated additionally whether the password is set by the user and used in the initialized state.

EXAMPLE 2: Password (set by user), password (pre-installed), biometric fingerprint.

- **Password Generation Mechanism:** If the authentication factor is a password, which is not set by the user: Description of the mechanism to generate the password. It is indicated additionally whether the password is unique per device and whether it is pre-installed.

NOTE 1: A detailed specification of the password generation mechanism is not necessary. It is considered as sufficient when the description explains the measures to ensure that the passwords are unique per device in any state other than the factory default and to reduce the risks of automated attacks based on obvious regularities, common strings, public available information or inappropriate complexity when used as pre-installed and unique per device password.

- **Security Guarantees:** Description of the realized security objectives and the threats the mechanism is protected against.

EXAMPLE 3: The mechanisms attests that the authenticated entity is in possession of a valid password. The confidentiality and integrity protection of the password during transfer is also guaranteed within the session.

- **Cryptographic Details:** Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the authentication mechanism considering key management, and to facilitate the described "Security Guarantees".

EXAMPLE 4: Authentication is performed via http authentication framework (IETF RFC 7235 [i.8]). Integrity and confidentiality of the password transfer to the DUT is realized with the TLS cipher suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA256.

- **Brute Force Prevention:** If the authentication mechanism is directly addressable from a network interface: Description of the method to prevent an attacker from brute forcing credentials via network interfaces.

EXAMPLE 5: A time delay of 5 seconds after an unsuccessful login before a new login can follow.

IXIT 2-UserInfo: User Information

The completed IXIT lists documentations, publications and information provided to users. The pro forma contains the following entries, which are independent from each other, and is typically filled out in form of a list.

- **Documentation of Change Mechanisms:** Description of the way the mechanisms to change the authentication values are documented for the user, including all information to access the documentation.

NOTE 2: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Documentation of Replacement:** If the DUT is not updatable: Description of the way the guidance to isolate the DUT and the hardware replacement plan is documented for the user, including all information to access the documentation.

NOTE 3: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Documentation of Sensors:** Description of the way the information about external sensing capabilities is documented for the user, including all information to access the documentation.

NOTE 4: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Documentation of Secure Setup:** Description of the way the method for securely setting up the DUT is documented for the user, including all information to access the documentation.

NOTE 5: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Documentation of Setup Check:** Description of the way the method for checking the secure setup of the DUT is documented for the user, including all information to access the documentation.

NOTE 6: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Documentation of Personal Data:** Description of the way the information about processing personal data is documented for the user, including all information to access the documentation.

NOTE 7: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Documentation of Telemetry Data:** Description of the way the information about collecting telemetry data is documented for the user, including all information to access the documentation.

NOTE 8: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Documentation of Deletion:** Description of the way the methods for deletion of personal data documented to the user, including all information to access the documentation.

NOTE 9: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- **Model Designation:** Model designation of the DUT and a brief description of how the user can recognize the model designation of the DUT.

NOTE 10: API call for or labelling sticker on the DUT are options to inform the user about the model designation.

- **Support Period:** Time during which the product or service is maintained by the manufacturer, e.g. in terms of updates.

- **Publication of Support Period:** Description of the way the defined "Support Period" is published and documented to the user, including all information to access the publication.

NOTE 11: Possible way of publication is the website of the manufacturer and the corresponding URL.

- **Publication of Vulnerability Disclosure Policy:** Description of the way the vulnerability disclosure policy is published, including all information to access the publication.

NOTE 12: Possible way of publication is the website of the manufacturer and the corresponding URL.

- **Publication of Non-Updatable:** If the DUT is not updatable: Description of the way the rationale for the absence of software updates is published, including all information to access the publication.

NOTE 13: Possible way of publication is the website of the manufacturer and the corresponding URL.

IXIT 3-VulnTypes: Relevant Vulnerabilities

The completed IXIT lists all types of vulnerabilities that are relevant for the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 6: Sequential numbering ("VulnTypes-1") or labelling scheme ("VulnTypes-Firmw").

- **Description:** Brief description of the kind of vulnerability that is relevant for the DUT.

NOTE 14: Hardware, software and firmware are possible kinds of vulnerabilities. If all vulnerabilities are covered by a single process a separation is not necessary.

- **Action:** Description of the way of acting on this kind of vulnerability in case of a vulnerability disclosure including all entities and responsibilities.

NOTE 15: Rolling out patches and publishing advisories are possible actions in this case.

- **Time Frame:** Targeted time frame in which the given steps of the action in case of a vulnerability are scheduled.

EXAMPLE 7: 5 days for initial response and 90 days until publication of the patch.

IXIT 4-Conf: Confirmations

The completed IXIT lists confirmations for the establishment of processes. The pro forma contains the following entries, which are independent from each other, and is typically filled out in form of a list.

- **Confirmation of Vulnerability Actions (Yes/No):** Confirmation that for every "Action" described in IXIT 3-VulnTypes the required infrastructure is in place and operators are briefed in order to achieve the targeted "Time Frame".

- **Confirmation of Vulnerability Monitoring (Yes/No):** Confirmation that for every vulnerability monitoring, identifying and rectifying described in IXIT 5-VulnMon the required infrastructure is in place and operators are briefed.

- **Confirmation of Update Procedures (Yes/No):** Confirmation that for every update procedure described in IXIT 8-UpdProc the required infrastructure is in place and operators are briefed in order to achieve the targeted "Time Frame".

- **Confirmation of Secure Management (Yes/No):** Confirmation that the secure management processes described in IXIT 14-SecMgmt are established.

- **Confirmation of Secure Development (Yes/No):** Confirmation that the secure development processes described in IXIT 19-SecDev are established.

IXIT 5-VulnMon: Vulnerability Monitoring

The completed IXIT lists all procedures for monitoring, identifying and rectifying vulnerabilities. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 8: Sequential numbering ("VulnMon-1") or labelling scheme ("VulnMon-Rectf").

- **Description:** Description of the way security vulnerabilities are monitored, identified and rectified in products and services.

NOTE 16: Procedures for identifying vulnerabilities commonly include assessments whether a potential vulnerability is relevant for a certain product, responsible persons, an approach to gather information and a workflow to perform in case a vulnerability is discovered.

IXIT 6-SoftComp: Software Components

The completed IXIT lists all software components of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

NOTE 17: The used level of detail concerning the division of the DUT software into software components serves for the fact that the TL can identify which components are updatable and which are not.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 9: Sequential numbering ("SoftComp-1") or labelling scheme ("SoftComp-Firmw").

- **Description:** Brief description of the software component.

NOTE 18: BIOS, firmware and boot loader are possible software components of the DUT.

- **Update Mechanism:** Reference to update mechanisms in IXIT 7-UpdMech that are used for updating the software component. An empty list of update mechanisms indicates the absence of updates for the software component and in this case a justification is provided.

- **Cryptographic Usage:** Indicates, if the software component makes use of cryptographic algorithms or primitives (Yes/No) and if so, it is included additionally, whether side effects of updating those algorithms and primitives are considered by the manufacturer (Yes/No).

IXIT 7-UpdMech: Update Mechanisms

The completed IXIT lists all update mechanisms of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 10: Sequential numbering ("UpdMech-1") or labelling scheme ("UpdMech-Firmw").

- **Description:** Brief description of the update mechanism including its major characteristics. It is indicated additionally whether the delivery of an update is network-based.

NOTE 19: Depending on the complexity it may be useful to divide the description into the steps in which the update is performed.

EXAMPLE 11: Update step 1) DUT queries server X to verify if an update is available, initiated by the user; 2) Server delivers the update to the DUT (network-based); 3) DUT verifies authenticity and integrity of the update; 4) After successful validation the installation of the update is performed.

- **Security Guarantees:** Description of the realized security objectives and the threats the mechanism is protected against. For authenticity and integrity is indicated additionally whether the security guarantee is given by the DUT itself.

EXAMPLE 12: The mechanism validates the integrity and authenticity before the installation of an update on the DUT itself.

- **Cryptographic Details:** Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the update mechanism considering key management, and to facilitate the described "Security Guarantees".

EXAMPLE 13: Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 3852 [i.9]. For the signature SHA-256 with RSA 2048 and PSS padding is used. The signing of the firmware package is performed with the private key of the manufacturer. The public key for the update validation is integrated during the manufacturing process of the DUT.

- **Initiation and Interaction:** Brief description of the procedure how an update is initiated and a brief description of the user interaction, which is necessary to initiate and apply an update.

NOTE 20: This entry serves also for the indication whether it is an automatic update mechanism.

- **Configuration:** Brief description of how automation and notification of software updates can be configured by the user and which options the user can choose from. The default configuration is indicated additionally.

NOTE 21: Enable, disable and/or postpone automatic updates and enable, disable and/or postpone notifications are possible configurations or options to choose from.

- **Update Checking:** Brief description of the mechanism and the schedule for querying for security updates. It is indicated additionally whether the availability check is performed by the DUT itself.

EXAMPLE 14: HTTPS query for latest stable Firmware version to EXAMPLE.ORG and comparison to installed version after initialization and every day at 2 am (initiated and performed by the DUT).

- **User Notification:** Brief description of how the user is informed about an available update and about disruptions caused by the update mechanism, e.g. limited availability of certain features. It is indicated additionally which information are contained in the notification and if the notification is realized by the DUT itself.

NOTE 22: Notifications via user interfaces and push messages are possible ways to inform the user.

IXIT 8-UpdProc: Update Procedures

This completed IXIT lists procedures of the manufacturer for the management of security updates. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 15: Sequential numbering ("UpdProc-1") or labelling scheme ("UpdProc-SecUpd").

- **Description:** Brief description of the procedure for deploying security updates including all entities and responsibilities.

- **Time Frame:** Targeted time frame for completing the procedure.

IXIT 9-ReplSup: Replacement Support

The completed IXIT lists information about the isolation and hardware replacement of the DUT. The pro forma contains the following entries, which are independent from each other, and is typically filled out in form of a list.

- **Isolation:** Description of the method including the steps to isolate the DUT.

- **Hardware Replacement:** Description of the method including the steps to replace the hardware of the DUT.

IXIT 10-SecParam: Security Parameters

The completed IXIT lists all sensitive (public and critical) security parameters that are persistently stored on the DUT during intended usage. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 16: Sequential numbering ("SecParam-1") or labelling scheme ("SecParam-Pswd").

- **Description:** Brief description of the security parameter, including its purpose. It is indicated additionally whether the parameter is a hard-coded unique per device identity used in a device for security purposes (hard-coded identity) and/or hard-coded in device software source code.

- **Type:** Indication whether the security parameter is public or critical.

NOTE 23: Public and critical security parameters are defined in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].

- **Security Guarantees:** Description of the realized baseline security objectives and threats the security parameter is protected against during persistent storage.

- **Protection Scheme:** Description of the measures that are applied to achieve the Security Guarantees. This includes the principals and roles through which access to the parameter is possible, including the privileges associated to each role.

- **Provisioning Mechanism:** If the "Type" indicates that the parameter is critical: Description of the mechanism through which the parameter is assigned its value for the operation of the DUT.

NOTE 24: Such assignment can happen during initialization or in initialized state (e.g. when a device functionality relying on the parameter is activated by the user).

NOTE 25: Persistent configuration data, runtime configuration data, protocol negotiation and assignment to a default value are potentially possible provisioning mechanisms.

- **Communication Mechanisms:** Reference to communication mechanisms in IXIT 11-ComMech that are used for communicating the parameter and an indication whether the communication is done via remotely accessible interfaces.

- **Generation Mechanism:** If the "Type" indicates that the parameter is critical and used for integrity and authenticity checks of software updates or for protection of communication with associated services: Description of the mechanism used to generate the values of the parameter and it is indicated additionally that the parameter is used for integrity and authenticity checks of software updates or for protection of communication with associated services.

EXAMPLE 17: References to a standard random number generator and applicable design documents.

IXIT 11-ComMech: Communication Mechanisms

The completed IXIT lists all communication mechanisms of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 18: Sequential numbering ("ComMech-1") or labelling scheme ("ComMech-IP").

- **Description:** Brief description of the communication mechanism, including its purpose and a description of the used protocol. For standardized protocols a reference is sufficient. It is indicated additionally whether the mechanism is remotely accessible.

NOTE 26: A possible communication mechanism is the use of Bluetooth®, WiFi® or NFC for a local connection between a mobile application and the DUT.

- **Security Guarantees:** Description of the realized security objectives and the threats the mechanism is protected against.

NOTE 27: The most common security guarantees to be considered include authentication of peers, authentication of origin, integrity protection, confidentiality protection, and anti-replay.

- **Cryptographic Details:** Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the communication mechanism considering key management, and to facilitate the described "Security Guarantees".

NOTE 28: Cryptographic Details contain information such as: the protocol Z-Wave® with Security 2 Command Class v1 is used for the communication. The transferred data is authenticated encrypted with AES-128 CCM to facilitate confidentiality and integrity. The key exchange is based on an out-of-band mechanism.

- **Resilience Measures:** Description of the measures to ensure that the connection establishment is performed in an orderly fashion including an expected, operational and stable state to achieve a stable connection.

NOTE 29: Resilience measures consider the sequence of the used protocol, the capability of the infrastructure, reset and initialization of the protocol and problems caused by mass reconnections.

IXIT 12-NetSecImpl: Network and Security Implementations

The completed IXIT lists all implementations of network and security functionalities of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 19: Sequential numbering ("NetSecImpl-1") or labelling scheme ("NetSecImpl-SecLib").

- **Description:** Brief description of the implementation of the network or security functionality, including its purpose and scope.

NOTE 30: The kind of implementation (e.g. software library or separate microcontroller) is helpful to determine the relevant functionality for an evaluation or review.

- **Review/Evaluation Method:** Description of the method used to review or evaluate the implementation, including the principles it is based on (e.g. audit, peer review, automated code analysis). Additionally the implementation scope is described, that is covered by the method.

- **Report:** Outcome of the review or evaluation or a reference to the certificate or the evaluation report that proves that the implementation has been successfully evaluated.

NOTE 31: The outcome of the review or evaluation does not need to be a single document. For instance, it is also possible to use the documentation of bug tracking in a software management tool to demonstrate that the implementation is reviewed.

IXIT 13-SoftServ: Software Services

This completed IXIT lists all software services of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 20: Sequential numbering ("SoftServ-1") or labelling scheme ("SoftServ-WebServ").

- **Description:** Brief description of the service, including its purpose. It is indicated additionally whether the service is accessible via network interface and whether this is the case in the initialized state.

NOTE 32: A SSH daemon not started by default (disabled), because it was used only for development purposes, is such a service.

- **Status:** Indication whether the service is enabled or disabled in the initialized state.

- **Justification:** If the service is enabled: Justification why the service is necessary for the intended use or operation of the DUT.

- **Allows Configuration (Yes/No):** If the service is accessible via network interface: Indication whether the service allows security-relevant changes in configuration and if so, a brief description of the possible configuration.

- **Authentication Mechanism:** If the service is accessible via network interface: Reference to authentication mechanisms in IXIT 1-AuthMech that are used for authentication prior the use of the service.

IXIT 14-SecMgmt: Secure Management Processes

The completed IXIT lists all secure management processes for critical security parameters implemented by the SO for the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 21: Sequential numbering ("SecMgmt-1") or labelling scheme ("SecMgmt-Passwd").

- **Description:** Brief description of the secure management process regarding the whole life cycle for critical security parameters. If an existing standard is used, a reference to the corresponding standard is provided.

NOTE 33: The life cycle of a critical security parameters typically considers generation, provisioning, storage, updates, decommissioning, archival, destruction, processes to handle the expiration and compromise of the parameter.

IXIT 15-Intf: Interfaces

The completed IXIT lists all network, physical and logical interfaces of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 22: Sequential numbering ("Intf-1") or labelling scheme ("Intf-LanPort").

- **Description:** Brief description of the interface, including its purpose. For physical interfaces, it is described additionally whether the interface is always required, never required or required only in specific cases (e.g. intermittently usage), which are briefly described then.

- **Type:** Indication whether the interface is network, physical (includes also air interfaces), logical or several types.

NOTE 34: The provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] distinguish between network and logical interfaces, but typically both types are equivalent. Therefore, in this case both types are to be indicated.

- **Status:** Indication whether the interface is enabled or disabled in the initialized state. For enabled interfaces a justification is given.

- **Disclosed Information:** If the interface is a network interface: Description of the information disclosed without authentication in the initialized state and the reason for the disclosure. It is indicated additionally whether the information is security-relevant.

NOTE 35: Disclosed information can be used by an attacker to identify a vulnerable device, e.g. software version.

- **Debug Interface:** If the interface is a physical interface: Indication whether the interface can be used as debug interface.

- **Protection:** If the interface is a physical interface: Description of the protection methods necessary to limit exposure of the interface.

NOTE 36: For debug interfaces a description of the software mechanism used to disable the interface is expected (see Test group 5.6-4).

NOTE 37: For non-radio interfaces a device casing is a protection method.

IXIT 16-CodeMin: Code Minimization

The completed IXIT lists all methods for minimizing code. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 23: Sequential numbering ("CodeMin-1") or labelling scheme ("CodeMin-DeadCode").

- **Description:** Brief description of the method used to minimize code to the necessary functionality.

IXIT 17-PrivlCtrl: Privilege Control

The completed IXIT lists all privilege control mechanisms. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 24: Sequential numbering ("PrivlCtrl-1") or labelling scheme ("PrivlCtrl-OS").

- **Description:** Brief description of the mechanism to control privileges of software on the DUT.

IXIT 18-AccCtrl: Access Control

The completed IXIT lists all access control mechanisms for memory on hardware-level. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 25: Sequential numbering ("AccCtrl-1") or labelling scheme ("AccCtrl-TEE").

- **Description:** Brief description of the hardware-level access control mechanism. It is described additionally how it is supported by the operating system of the DUT.

IXIT 19-SecDev: Secure Development Processes

The completed IXIT lists all secure development processes implemented by the SO for the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 26: Sequential numbering ("SecDev-1") or labelling scheme ("SecDev-Testing").

- **Description:** Brief description of the secure development process. If an existing standard is used, a reference to the corresponding standard is provided.

IXIT 20-SecBoot: Secure Boot Mechanisms

The completed IXIT lists all secure boot mechanisms of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 27: Sequential numbering ("SecBoot-1") or labelling scheme ("SecBoot-TEE").

- **Description:** Brief description of the mechanism (including trust assumptions) used for the secure boot process of the DUT and the part of the software that is protected.

- **Security Guarantees:** Description of the realized security objectives of the mechanism.

EXAMPLE 28: The mechanisms realizes authenticity and integrity of the operating systems kernel.

- **Detection Mechanisms:** Description of the mechanism detecting an unauthorized change in the software of the DUT.

- **User Notification:** Brief description of how the user is informed about an unauthorized change in the software. It is indicated additionally which information are contained in the notification.

NOTE 38: Email address of a user account, communication endpoint (e.g. network address or link address) of a user device (e.g. smart phone, smart watch) or status LED are possible ways to inform the user.

- **Notification Functionality:** Brief description of the network functionalities necessary to notify a user.

EXAMPLE 29: SMTP protocol (in case of email notifications), RFCOMM protocol details (in case of Bluetooth® notifications).

IXIT 21-PersData: Personal Data

The completed IXIT lists all personal data processed by the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 30: Sequential numbering ("PersData-1") or labelling scheme ("PersData-PayInfo").

- **Description:** Brief description of the category of personal data processed by the DUT.

EXAMPLE 31: Log data on the usage of the DUT, payment information, timestamped location data, audio input stream or biometric data.

NOTE 39: According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2], personal data is any information relating to an identified or identifiable natural person. This term is used to align with well-known terminology but has no legal meaning within ETSI TS 103 645 [1]/ETSI EN 303 645 [2] and the present document.

NOTE 40: Categories of personal data need to be described at a level of detail that provides a general understanding of what kind of data is being processed. This includes a general understanding of the level of sensitivity of personal data aligned with well-known terminology.

- **Processing Activities:** Description of how the personal data is being processed, including all involved parties. It is described additionally for what purposes the processing is done.

NOTE 41: Permanent storage of personal data, also as backup, is a processing activity.

- **Communication Mechanisms:** Reference to communication mechanisms in IXIT 11-ComMech that are used for communicating the personal data and an indication whether the communication partner is an associated service (Yes/No). An empty list of communication mechanisms indicates that the personal data is not transmitted.

- **Sensitive (Yes/No):** Indication whether the personal data is sensitive according to the definition in the provision 5.8-2 in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].

- **Obtaining Consent:** If the personal data is processed on the basis of consumer's consent: Description of how the consent for the processing is obtained from the consumer.

- **Withdrawing Consent:** If the personal data is processed on the basis of consumer's consent: Description of how the consumer can withdraw the consent for processing the personal data.

IXIT 22-ExtSens: External Sensors

The completed IXIT lists all external sensing capabilities of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 32: Sequential numbering ("ExtSens-1") or labelling scheme ("ExtSens-Cam").

- **Description:** Brief description of the sensing capability.

NOTE 42: Such sensing capabilities can be a microphone or camera.

IXIT 23-ResMech: Resilience Mechanisms

The completed IXIT lists all resilience mechanisms for network connectivity and power outages of the DUT. The pro forma contains the following entries and is typically filled in the form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 33: Sequential numbering ("ResMech-1") or labelling scheme ("ResMech-Power").

- **Description:** Description of the mechanism that contributes to the DUT's resilience to network and/or power outages.

NOTE 43: Such a resilience mechanism can be a journaling mechanism on ext4 that protects the file system's integrity in case of a power outage.

NOTE 44: Such a resilience mechanism can be a small battery that enables a clean emergency device shutdown (backup battery). It protects against loss of data in case of power outage.

- **Type:** Indication whether the resilience mechanism addresses network connectivity or power outages or both.
- **Security Guarantees:** Description of the realised security objectives and the threats the mechanism protects against.

EXAMPLE 34: The mechanism protects the DUT's data integrity in case of a power outage.

IXIT 24-TelData: Telemetry Data

The completed IXIT lists all telemetry data collected by the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 35: Sequential numbering ("TelData-1") or labelling scheme ("TelData-CrashLog").

- **Description:** Brief description of the telemetry data being collected and provided to the manufacturer by the DUT.
- **Purpose:** Brief description for what purpose the data is collected.
- **Security Examination:** If the data is used for security examination: Description of how and by whom (device or associated service) the telemetry data is examined for security anomalies.

NOTE 45: The security anomaly examination can be realized outside the DUT, i.e. by associated services.

NOTE 46: A device telemetry service captures crash logs and data on usage (telemetry data) from the DUT in order to enable the developers to determine security flaws (security anomaly detection).

- **Personal Data:** Reference to personal data in IXIT 21-PersData that are processed in the telemetry data.

IXIT 25-DelFunc: Deletion Functionalities

The completed IXIT lists all deletion functionalities for data of the user. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 36: Sequential numbering ("DelFunc-1") or labelling scheme ("DelFunc-CloudServ").

- **Description:** Brief description of the functionality used to delete data of the user. If the "Target Type" indicates, that an associated service is addressed: The concerning associated service which is covered by the functionality is indicated additionally.

NOTE 47: The DUT's settings could provide a functionality to remove personal data from a cloud server.

- **Target Type:** Indicates whether the functionality addresses user data on the device or personal data on associated services or both.
- **Initiation and Interaction:** Brief description of the user interaction, which is necessary to initiate and apply the deletion functionality.
- **Confirmation:** Brief description of how the user is given indication that the addressed data has been deleted after applying the deletion functionality.

IXIT 26-UserDec: User Decisions

The completed IXIT lists all decisions to be taken by the user during installation and maintenance. The pro forma contains the following entries and is typically filled in the form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 37: Sequential numbering ("UserDec-1") or labelling scheme ("UserDec-Encrypt").

- **Description:** Description of the decision to be taken by the user within the installation and maintenance flows. Its position within the installation or maintenance flow is additionally described.
- **Options:** Description of the security-relevant options the user can take and an indication for the default value.
- **Triggered By:** Brief description how the decision is triggered. It is indicated additionally whether the decision can be triggered by the user.

IXIT 27-UserIntf: User Interfaces

The completed IXIT lists all user interfaces of the DUT, which enable input from the user. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 38: Sequential numbering ("UserIntf-1") or labelling scheme ("UserIntf-Config").

- **Description:** Brief description of the user interface enabling data input from the user. It is indicated additionally how the interface can be accessed by the user.

IXIT 28-ExtAPI: External APIs

The completed IXIT lists all APIs of the DUT, which enables data input from external sources. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 39: Sequential numbering ("ExtAPI-1") or labelling scheme ("ExtAPI-SOAP-Cloud").

- **Description:** Description of the API enabling data input from external sources of the DUT.

NOTE 48: External APIs are typically used for machine-to-machine communication.

IXIT 29-InpVal: Data Input Validation

The completed IXIT lists all data input validation methods of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 40: Sequential numbering ("InpVal-1") or labelling scheme ("InpVal-NetwCom").

Description: Description of the method for validating the data input via user interfaces, or transferred via APIs and between networks in services and devices including the handling of unexpected data. It is indicated additionally which of the sources for data input are addressed by the method.

NOTE 49: To validate the data input, it can be checked whether it is of an allowed type (format and structure), of allowed value, an allowed cardinality or an allowed ordering.

Annex B (informative): Overview of required IXIT entries per provision

As described in the assessment procedure in clause 4.3, Table B.1 describes for each provision in ETSI TS 103 645 [1]/ETSI EN 303 645 [2] which IXIT entries are required to perform the corresponding test group.

Table B.1: Required IXIT entries per provision

Provision	Required IXIT entries
4-1	(none)
5.1-1	**IXIT 1-AuthMech**: ID, Description, Authentication Factor, Password Generation Mechanism
5.1-2	**IXIT 1-AuthMech**: ID, Description, Authentication Factor, Password Generation Mechanism
5.1-3	**IXIT 1-AuthMech**: ID, Description, Security Guarantees, Cryptographic Details
5.1-4	**IXIT 1-AuthMech**: ID, Description **IXIT 2-UserInfo**: Documentation of Change Mechanisms
5.1-5	**IXIT 1-AuthMech**: ID, Description, Brute Force Prevention
5.2-1	**IXIT 2-UserInfo**: Publication of Vulnerability Disclosure Policy
5.2-2	**IXIT 2-UserInfo**: Publication of Vulnerability Disclosure Policy **IXIT 3-VulnTypes**: ID, Description, Action, Time Frame **IXIT 4-Conf**: Confirmation of Vulnerability Actions
5.2-3	**IXIT 4-Conf**: Confirmation of Vulnerability Monitoring **IXIT 5-VulnMon**: ID, Description
5.3-1	**IXIT 6-SoftComp**: ID, Description, Update Mechanism **IXIT 7-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details, Initiation and Interaction
5.3-2	**IXIT 7-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details, Initiation and Interaction
5.3-3	**IXIT 6-SoftComp**: ID, Description, Update Mechanism **IXIT 7-UpdMech**: ID, Description, Initiation and Interaction
5.3-4	**IXIT 6-SoftComp**: ID, Description, Update Mechanism **IXIT 7-UpdMech**: ID, Description, Initiation and Interaction, Configuration
5.3-5	**IXIT 6-SoftComp**: ID, Description, Update Mechanism **IXIT 7-UpdMech**: ID, Description, Update Checking
5.3-6	**IXIT 7-UpdMech**: ID, Description, Initiation and Interaction, Configuration, User Notification
5.3-7	**IXIT 7-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details
5.3-8	**IXIT 4-Conf**: Confirmation of Update Procedures **IXIT 8-UpdProc**: ID, Description, Time Frame
5.3-9	**IXIT 7-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details
5.3-10	**IXIT 7-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details
5.3-11	**IXIT 7-UpdMech**: ID, Description, User Notification
5.3-12	**IXIT 7-UpdMech**: ID, Description, User Notification
5.3-13	**IXIT 2-UserInfo**: Support Period, Publication of Support Period
5.3-14	**IXIT 2-UserInfo**: Documentation of Replacement, Publication of Non-Updatable
5.3-15	**IXIT 9-ReplSup**: Isolation, Hardware Replacement
5.3-16	**IXIT 2-UserInfo**: Model Designation
5.4-1	**IXIT 10-SecParam**: ID, Description, Type, Security Guarantees, Protection Scheme
5.4-2	**IXIT 10-SecParam**: ID, Description, Type, Security Guarantees, Protection Scheme
5.4-3	**IXIT 10-SecParam**: ID, Description, Type, Provisioning Mechanism
5.4-4	**IXIT 10-SecParam**: ID, Description, Type, Generation Mechanism
5.5-1	**IXIT 11-ComMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-2	**IXIT 12-NetSecImpl**: ID, Description, Review/Evaluation Method, Report
5.5-3	**IXIT 6-SoftComp**: ID, Description, Update Mechanism, Cryptographic Usage **IXIT 7-UpdMech**: ID, Description
5.5-4	**IXIT 1-AuthMech**: ID, Description, Security Guarantees, Cryptographic Details **IXIT 13-SoftServ**: ID, Description, Authentication Mechanism
5.5-5	**IXIT 1-AuthMech**: ID, Description, Security Guarantees, Cryptographic Details **IXIT 13-SoftServ**: ID, Description, Allows Configuration, Authentication Mechanism
5.5-6	**IXIT 10-SecParam**: ID, Description, Type, Communication Mechanisms **IXIT 11-ComMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-7	**IXIT 10-SecParam**: ID, Description, Type, Communication Mechanisms **IXIT 11-ComMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-8	**IXIT 4-Conf**: Confirmation of Secure Management **IXIT 14-SecMgmt**: ID, Description
5.6-1	**IXIT 15-Intf**: ID, Description, Type, Status
5.6-2	**IXIT 15-Intf**: ID, Description, Type, Disclosed Information
5.6-3	**IXIT 15-Intf**: ID, Description, Type, Status, Protection

Provision	Required IXIT entries
5.6-4	**IXIT 15-Intf**: ID, Description, Type, Status, Debug Interface, Protection
5.6-5	**IXIT 13-SoftServ**: ID, Description, Status, Justification
5.6-6	**IXIT 16-CodeMin**: ID, Description
5.6-7	**IXIT 17-PrivlCtrl**: ID, Description
5.6-8	**IXIT 18-AccCtrl**: ID, Description
5.6-9	**IXIT 4-Conf**: Confirmation of Secure Development **IXIT 19-SecDev**: ID, Description
5.7-1	**IXIT 20-SecBoot**: ID, Description, Security Guarantees, Detection Mechanisms
5.7-2	**IXIT 20-SecBoot**: ID, Description, User Notification, Notification Functionality
5.8-1	**IXIT 11-ComMech**: ID, Description, Security Guarantees, Cryptographic Details **IXIT 21-PersData**: ID, Description, Communication Mechanisms
5.8-2	**IXIT 11-ComMech**: ID, Description, Security Guarantees, Cryptographic Details **IXIT 21-PersData**: ID, Description, Processing Activities, Communication Mechanisms, Sensitive
5.8-3	**IXIT 2-UserInfo**: Documentation of Sensors **IXIT 22-ExtSens**: ID, Description
5.9-1	**IXIT 23-ResMech**: ID, Description, Security Guarantees
5.9-2	**IXIT 23-ResMech**: ID, Description, Type, Security Guarantees
5.9-3	**IXIT 11-ComMech**: ID, Description, Resilience Measures
5.10-1	**IXIT 24-TelData**: ID, Description, Security Examination
5.11-1	**IXIT 25-DelFunc**: ID, Description, Target Type, Initiation and Interaction
5.11-2	**IXIT 21-PersData**: ID, Description, Processing Activities **IXIT 25-DelFunc**: ID, Description, Target Type, Initiation and Interaction
5.11-3	**IXIT 2-UserInfo**: Documentation of Deletion **IXIT 21-PersData**: ID, Description, Processing Activities **IXIT 25-DelFunc**: ID, Description, Target Type
5.11-4	**IXIT 2-UserInfo**: Documentation of Deletion **IXIT 25-DelFunc**: ID, Description
5.12-1	**IXIT 26-UserDec**: ID, Description, Options, Triggered By
5.12-2	**IXIT 2-UserInfo**: Documentation of Secure Setup **IXIT 26-UserDec**: ID, Description, Options
5.12-3	**IXIT 2-UserInfo**: Documentation of Setup Check
5.13-1	**IXIT 11-ComMech**: ID, Description **IXIT 27-UserIntf**: ID, Description **IXIT 28-ExtAPI**: ID, Description **IXIT 29-InpVal**: ID, Description
6-1	**IXIT 2-UserInfo**: Documentation of Personal Data **IXIT 21-PersData**: ID, Description, Processing Activities
6-2	**IXIT 21-PersData**: ID, Description, Obtaining Consent
6-3	**IXIT 21-PersData**: ID, Description, Obtaining Consent, Withdrawing Consent
6-4	**IXIT 21-PersData**: ID, Description **IXIT 24-TelData**: ID, Description, Purpose, Personal Data
6-5	**IXIT 2-UserInfo**: Documentation of Telemetry Data **IXIT 24-TelData**: ID, Description, Purpose

Annex C (informative): Sample IXIT

C.1 Overview

To demonstrate the scope and the level of detail on completing the IXIT pro formas, clause C.3 provides a sample IXIT on the base of a fictive IoT device a SO can orient on (see Table C.1 to Table C.29).

NOTE 1: The sample IXIT does not provide a set of examples of how to fulfil the provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2], but it represents a sample for a completed IXIT. Therefore it contains the necessary elements of the IXIT pro formas to enable a feasible assessment by a TL using the present document. For example implementations fulfilling the provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] please refer to the guide document ETSI TR 103 621 [i.7]. However, the sample IXIT aims to fulfil the requirements of the provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2].

NOTE 2: The sample IXIT exemplarily describes some external documents as "attached". Those documents are not part of the present document.

C.2 Sample DUT - Fictional IP Camera

This clause provides a brief overview of the sample DUT and its main functionalities used in the sample IXIT.

The DUT for the sample IXIT is a fictional IP camera "IPC 2000" that has real-world functionalities typically and representative for an IoT device. Its purpose is the recording and playback of video and audio data, e.g. of the user's estate, which can be viewed through the corresponding app "IP camera App" or the web interface. The IP camera is connected via LAN or WLAN to the network of the user and can be configured by a local web interface or the app. Web interface and app provide also the capability of performing firmware updates or user management. To access the web interface, the user has to complete an authentication process before, using username and password. Moreover the user can connect to the camera via SSH after enabling this functionality in the configuration. This interface can be used to copy video files script based or to check log files. The IP camera also offers a SOAP interface that can be used by other devices to control the movement of the camera and receive audio and video streams via a direct connection.

Connections between IP camera and app are managed by cloud servers of the manufacturer (the cloud infrastructure represents the associated services of the DUT). There is no direct connection between the app and the IP camera itself. This infrastructure is contacted when the user decides to submit crash reports or to contact the developer's support. The cloud servers also provide the firmware updates for the IP camera. Figure C.1 illustrates the example infrastructure.

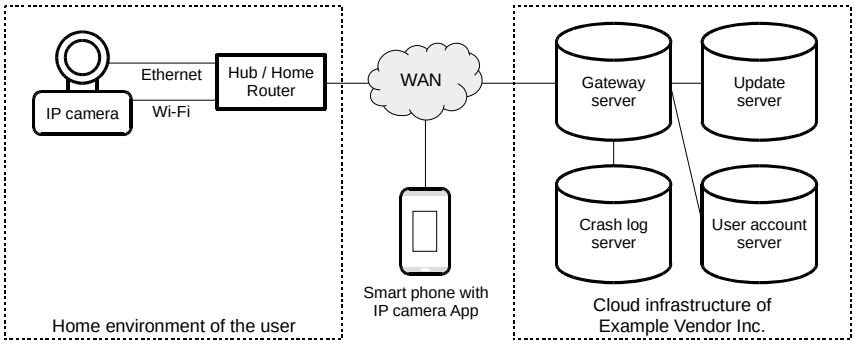

Figure C.1: Infrastructure used for sample IXIT

The IP camera provides different update mechanisms to install software updates. The default way is the user initiation via web interface or app, where the user is also informed about the availability of an update. Alternatively, the user can attach a USB drive with an update file the user downloaded from the manufacturer's website before. In both cases the update package is encrypted and the integrity and authenticity are verified before an installation.

On purchasing the camera, the user is provided with a user manual. Additionally the user can find information in the "Help" section of the app and the manufacturer provides some user information on a product specific area of its website.

C.3 Sample IXIT tables and lists

Table C.1: Sample IXIT 1-AuthMech (Authentication Mechanisms)

ID	Description	Authentication Factor	Password Generation Mechanism	Security Guarantees	Cryptographic Details	Brute Force Prevention
AuthMech-1	A user can login over HTTPS at port 443 to gain access to the web frontend. (A user can request a login over HTTP at port 80 but is forwarded automatically to HTTPS on port 443.) The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	Username and password (pre-installed and used in initialized state).	The username is fixed "admin". The password is generated randomly and is unique per device. The password has a length of 16 and consists of upper case chars, lower case chars and numbers. The password is generated by use of /dev/urandom on a UNIX configuration system during manufacturing phase.	The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Authentication is performed via a form-based HTML interface by an internal PHP script in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	After 3 invalid login attempts the login interface is inaccessible for 5 minutes.
AuthMech-2	A device can exchange data with the DUT over HTTPS/SOAP on port 8085. The authentication via Basic-Auth is confirmed before any payload data over HTTP is exchanged. No payload is readable without providing correct access credentials. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	Username and password (set by user and used in initialized state).	*N/A (Authentication mechanism is password set by the user)*	The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Authentication is performed via an HTTP authentication framework (IETF RFC 7235 [i.8]) by the internal Apache Webserver in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over TLS 1.2 with the TLS cipher suites: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	After 10 invalid login attempts user/password combination is disabled for further access.

ID	Description	Authentication Factor	Password Generation Mechanism	Security Guarantees	Cryptographic Details	Brute Force Prevention
AuthMech-3	The user can login via SSH at port 22 to gain remote command line access. The authentication via SSH is confirmed before any payload data over SSH is exchanged. No payload is readable without providing correct access credentials. The SSH server authenticates a given signature against the public keys stored on the file system. (The private key is generated on the DUT the key pair can be downloaded over an HTTPS channel via the web interface.) The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	Client private and public key.	*N/A* *(Authentication mechanism is not a password)*	With the use of SSH the DUT ensures confidentiality, authenticity and integrity during the transfer.	Authentication is performed via the SSH protocol (IETF RFC 4253 [i.10]) by the internal SSH server of the DUT. The key pair is built on ECDSA 256 bit and is not protected with a password. Integrity and confidentiality of the SSH credentials to the DUT is realized over SSH2 with cipher suites conformant to the following security parameters: Key exchange: diffie-hellman-group-exchange-sha256 (2048-bit), encryption: AEAD_AES_256_GCM, MAC: hmac-sha2-256.	The DUT uses the "fail2ban" framework as unix daemon that scans the system log files for rejected login attempts and dynamically adjusts the firewall rules to drop packets from an attacker's IP address.

Table C.2: Sample IXIT 2-UserInfo (User Information)

Documentation of Change Mechanisms	The user can find information for changing the authentication values in the PDF-File user's manual IPC 2000 downloadable on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example. The printed product information contains this URL in section 3. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Menus".
Documentation of Replacement	*N/A* *(There are no non-updatable components)*
Documentation of Sensors	The microphone functionality, camera functionality (visible spectrum), and camera functionality (infrared spectrum) are explained on the product website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example. The printed product information contains this URL in section 9. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Functional Overview".
Documentation of Secure Setup	The user is guided through a setup wizard per pre-defined dialogs after the initial password is changed. By these dialogs it is ensured that no insecure configuration can be made by user during the setup. The dialogs are documented on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example. The printed product information contains this URL in section 1. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Setup".
Documentation of Setup Check	Every user input is checked against validation rules. The only option where the user can make an insecure choice is the password for new user accounts. If the entered password does not comply with the password rules, the user is notified immediately over the web interface or the App and the setup procedure cannot be continued until the user chooses a valid input. The dialogs are documented on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example. The printed product information contains this URL in section 1. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Setup".

Documentation of Personal Data	The user can find this information in PDF-File user's manual IPC 2000 downloadable on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example. The printed product information contains this URL in section 6. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Reset".
Documentation of Telemetry Data	The user can find this information in PDF-File user's manual IPC 2000 downloadable on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example.The printed product information contains this URL in section 6. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Reset".
Documentation of Deletion	The user can find this information on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example. The printed product information contains this URL in section 7. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Reset" and "Help" -> "Account deletion".
Model Designation	The model designation "IPC 2000" is provided to user on the bottom of the DUT's case in plain text. Also the designation can be read from the app under "Help" -> "About" and from the web interface under "Devices".
Support Period	This DUT is actively maintained concerning security updates for the following 6 years after placing on the market.
Publication of Support Period	The user can find this information on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example. The printed product information contains this URL in section 4. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Security Policy".
Publication of Vulnerability Disclosure Policy	The user can retrieve the vulnerability disclosure policy from the website of the Example Vendor Inc., accessible under https://example.net/security/disclosure-policy. The printed product information contains this URL in section 3. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Security Policy". On this site the user finds also the contact form to submit potential security flaws for the DUT.
Publication of Non-Updatable	*N/A* *(There are no non-updatable components)*

Table C.3: Sample IXIT 3-VulnTypes (Relevant Vulnerabilities)

ID	Description	Action	Time Frame
VulnTypes-1	Vulnerabilities on the user web frontend regarding HTTP, PHP or HTML and the integration into the related components (web server, database, OS and used libraries).	When a notification about a potential vulnerability is received via the contact form according to the Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it proposes a fix for the Software Development Department (SDD). The SDD then implements the fix and verifies the effectiveness within. After confirmation from both teams that the vulnerability is fixed, the new firmware is rolled out and the updated changelog is published with containing a description of the closed vulnerability.	7 days for initial response, 30 days for SIT to investigate and propose a fix, 30 days for SDD to integrate the fix. By no later than 90 days after receiving the vulnerability the fix will be released according to the published vulnerability disclosure policy.
VulnTypes-2	Vulnerabilities concerning the hardware or underlying OS.	When a notification about a potential vulnerability is received via the contact form according to Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it contacts the vendors of the underlying OS or hardware via a defined support email address (the responsible contact persons are known) to discuss further steps. If the vulnerability affects the hardware, the SIT will try to mitigate the issue in software in corporation with the external vendor. If the hardware affects the underlying OS, the SIT will contact the particular vendor for help on this issue. Any change of software will be handled and released by the Software Development Department (SDD). Depended on the result, a fix is rolled out or in case the vulnerability cannot be fixed by Example Vendor Inc. a warning for customers is published on the website under the following URL: https://example.net/support/devices/ip-camera-example.	7 days for initial response are defined according to the published vulnerability disclosure policy. Usually 90 days after receiving the vulnerability a fix will be released or a warning is published. The warning will be withdrawn since a fix is released.
VulnTypes-3	Vulnerabilities concerning commercially licensed third-party libraries.	When a notification about a potential vulnerability is received via the contact form according to the Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it contacts the vendor of the library via a defined support email address (the responsible contact persons are known) to discuss further steps. The SIT will contact the particular vendor for help on this issue. Any change of software will be handled and released by the Software Development Department (SDD). Depended on the result, a fix is rolled out or in case the vulnerability cannot be fixed by Example Vendor Inc. a warning for customers is published on the website under the following URL: https://example.net/support/devices/ip-camera-example.	7 days for initial response are defined according to the published vulnerability disclosure policy. By no later than 60 days after receiving the vulnerability a fix will be released or a warning is published, as it is assured by contract with the third parties.

Table C.4: Sample IXIT 4-Conf (Confirmations)

Confirmation of Vulnerability Actions	Yes
Confirmation of Vulnerability Monitoring	Yes
Confirmation of Update Procedures	Yes
Confirmation of Secure Management	Yes
Confirmation of Secure Development	Yes

Table C.5: Sample IXIT 5-VulnMon (Vulnerability Monitoring)

ID	Description
VulnMon-1	The Example Vendor Inc. monitors the CVE sites https://www.cvedetails.com/ and https://cve.mitre.org/ for vulnerabilities that affect components used for the DUT. Further, the suppliers of the used software components for the DUT have committed themselves to publishing security vulnerabilities on these CVE pages. The Security Incident Team (SIT) weekly checks both sites. Once a potential vulnerability is spotted, the SIT continues with the process described in IXIT 3-VulnTypes. If a vulnerability is listed on one or both of the mentioned websites but is not applicable for the DUT, the CVE is noted internally as "n/a" to document that the vulnerability was investigated.
VulnMon-2	The Example Vendor Inc. monitors the following sites for leaked credentials or other sensitive information that can be unambitiously traced back to the DUT: https://one.example.net, https://two.example.net. If there is a finding, the privacy officer of Example Vendor Inc. is responsible for investigating this issue further to confirm or deny that further privacy related measures are necessary. In the former case the procedure depends on the concrete issue and government regulations. If the issue affects identifiable users of the DUT, the Security Incident Team (SIT) will be involved to notify registered customers about the issue.

Table C.6: Sample IXIT 6-SoftComp (Software Components)

ID	Description	Update Mechanism	Cryptographic Usage
SoftComp-1	Firmware consisting of a Linux-based operating system, the OpenSSL cryptographic library, Apache Web-Server including PHP and SQLite, various libraries.	Firmware can be updated according to UpdMech-1, UpdMech-2, and Upd-Mech-3.	Yes, the firmware includes the cryptographic algorithms available to the DUT. Yes, side effects of updating those algorithms and primitives are considered by the manufacturer through exhaustive testing of the DUT's interfaces by the Software Development Department (SDD), both with negative and positive tests.
SoftComp-2	Boot loader 1 (BL1) according to https://github.com/ARM-software/arm-trusted-firmware/blob/master/docs/design/firmware-design.rst that is responsible for booting up the ARM processor.	The boot loader cannot be updated since this the root component for the boot process and resists in ROM.	Yes, the boot loader contains cryptographic algorithms necessary for checking the signature of the "boot loader 2" BL2. Since this component cannot be updated, the manufacturer did not consider side effects of updating these algorithms.

Table C.7: Sample IXIT 7-UpdMech (Update Mechanisms)

ID	Description	Security Guarantees	Cryptographic Details	Initiation and Interaction	Configuration	Update Checking	User Notification
UpdMech-1	User-initiated firmware update over web interface. The DUT queries the update server https://update.example.net to verify if an update is available. This is done automatically once per day. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The DUT checks automatically once a day (the time is chosen randomly for each day) for firmware updates stored at https://update.example.net. The user will be notified when an update is available. The user then can trigger the update by logging in to the web interface and manually starting the update process by pressing the button "Apply update and restart", or the DUT starts the update itself automatically, depending on its configuration. Once the update is started it proceeds without any further user interaction.	The user can configure the DUT to start an update automatically when available. The default option is that the user is only notified about an update and triggers it manually. In this case the user is asked whether the update should be installed now or on a later date ("install now" or "postpone").	The DUT contacts the update server at https://update.example.net once per day (the time is chosen randomly for each day). If the server is not reachable, the update check is postponed for 2 hours. The DUT initiates and performs the update check.	The user is notified via the app (by push messages) about a pending update. The user is also informed after login on the web interface. The notification contains: • estimated time needed to apply the update • a warning that during this period the services will be not available • brief changelog of the most important changes The notifications on the web interface are realized by the DUT itself.

ID	Description	Security Guarantees	Cryptographic Details	Initiation and Interaction	Configuration	Update Checking	User Notification
UpdMech-2	User-initiated firmware update over the app. The description is the same as in UpdMech-1, the only difference is that the update is triggered through the app.	See UpdMech-1.	See UpdMech-1.	See UpdMech-1.	See UpdMech-1.	See UpdMech-1.	See UpdMech-1.
UpdMech-3	User-initiated firmware update over USB. The user plugs in a USB drive with a firmware file to a local computer and points the DUT to the file via the web interface. This is done manually. When the user starts the update mechanism, the DUT verifies authenticity and integrity of the update file and the installation is initiated. Once the update is finished, the user is notified about the successful update.	See UpdMech-1.	See UpdMech-1.	The user then can trigger the update by logging in to the web interface and manually pointing the DUT to the update file. The update file can be downloaded from https://example.net/updates/devices/ip-camera-example and copied onto an USB stick by the user. Then the user starts the update process by pressing the button "Apply update and restart" on the web interface. Once the update is started it proceeds without any further user interaction.	No configuration options.	The user initiates the update manually.	Since the DUT does not have any meta data about the update, only a warning that during the update period the services will be not available is displayed.

Table C.8: Sample IXIT 8-UpdProc (Update Procedures)

ID	Description	Time Frame
UpdProc-1	Every release of the DUT's firmware is under responsibility of the Software Development Team (SDD). The SDD is responsible for integrating security fixes and testing the firmware with positive and negative tests. Once the change was is verified and tested, the SDD rolls out the update over the official update server. To coordinate the handling of security fixes the team uses an internal ticket system, so that no security fix will be overlooked. The changes regarding each firmware release are protocolled in a changelog by the SDD, which is published on the product website.	As mentioned in VulnTypes-1 the time for rolling out a new firmware is 30 days.

NOTE: IXIT 9-ReplSup is only applicable for constrained devices. Since the fictional IP camera is not a constrained device in the sense of ETSI TS 103 645 [1]/ETSI EN 303 645 [2], Table C.9 is filled with exemplary information that is not directly related to the IP camera. Instead, another fictional device is used as an example, namely a window sensor that can detect the opening or closing of a window and submits its state via ZigBee® to a ZigBee® hub.

Table C.9: Sample IXIT 9-ReplSup (Replacement Support)

Isolation	The window sensor can be disconnected from the ZigBee® network in the Smart Hub it is connected to. Afterwards the signals from the window sensor cannot affect the network anymore. In this case the window sensor remains its core functionality to notify a user about the opening or closing of a window by a short acoustical peep sound emitted in case of such an event.
Hardware Replacement	The window sensor can be replaced as a whole by a new window sensor device, which is then connected to the ZigBee® network instead of the old one.

Table C.10: Sample IXIT 10-SecParam (Security Parameters)

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism
SecParam-1	RSA public signature key of update server to verify authenticity and integrity of firmware updates (after decrypting with SecParam-2). The key is not a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	A trustworthy user does not have access to the key through any interfaces. A non-trustworthy user needs root access to stop the update process and change the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read and to modify the key is the software update process which is run under a different account "software-updater" than any of the accounts used for external interfaces.	*N/A* *(The security parameter is not critical)*	*N/A* *(The security parameter is not transmitted)*	*N/A* *(The security parameter is not critical)*
SecParam-2	AES key for decrypting firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key. The delivered firmware package from the update server is encrypted. Therefore the key is not extractable. The access to the file system is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify and to read the key is the software update process which is run under a different account ''software-updater'' than any of the account used for external interfaces.	The key is hard-coded in the firmware and is modified only through a verified firmware update package.	*N/A* *(Parameter is not transmitted)*	The AES key is generated before a firmware update package is released on a separate offline Linux® PC with the most recent OpenSSL version at the time of the key generation. OpenSSL uses its own random number generator, which is seeded by /dev/random of the Linux® machine. /dev/random again is seeded by an HSM connected to the machine.

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism
SecParam-3	ECDSA public key in X.509 certificate for authentication in TLS connection over web interface. This key is a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	An attacker needs access to the file system on the DUT to change the certificate. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify the key is the software update process which is run under a different account ''software-updater'' than any of the processes used for external interfaces.	*N/A (Parameter is not critical)*	ComMech-1	*N/A (Parameter is not critical)*
SecParam-4	ECDSA private key for authentication in TLS connection over web interface. The key is a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key The delivered firmware package from the update server is encrypted. Therefore the key is not extractable. The access to the file system on the DUT is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify the key is the software update process which is run under a different account ''software-updater'' than any of the account used for external interfaces. The only user role that has access rights to read the key is the web server which is run under a different account ''web'' than any of the other processes used for external interfaces.	The private key is hard-coded in the firmware and is modified only through a verified firmware update package.	ComMech-1	*N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)*
SecParam-5	Salt for the bcrypt-Hash to store user credentials in SQLite databases for web interface. The salt is not a hard-coded identity. The salt is not hard-coded in device software source code.	public	The salt is not modifiable by an attacker so that its integrity is ensured.	An attacker needs access to the file system to change the hash. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify the key is the web server which is run under a different account ''web'' than any of the other processes used for external interfaces.	*N/A (Parameter is not critical)*	*N/A (Parameter is not transmitted)*	*N/A (Parameter is not critical)*

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism
SecParam-6	ID for Identification of the DUT against the associated services (cloud infrastructure) of Example Vendor Inc. The key is a hard-coded identity. The key is hard-coded in device software source code.	critical	The ID is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to gain access to the ID. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read the key is the app connector which is run under a different account ''app-connector'' than any of the other processes used for external interfaces.	The ID is hard-coded in the hardware and cannot be modified during the operation.	ComMech-2	*N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)*
SecParam-7	ECDSA private key for authenticating a client against the SSH server of the DUT. The key is a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to gain access to the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify the key is the web server process which is run under a different account ''web'' than any of the account used for external interfaces. The only user role that has access rights to read the key is the SSH server which is run under a different account ''ssh-server'' than any of the other processes used for external interfaces.	The private key is generated on demand on the DUT. For generating the key the DUT uses the OpenSSL random number generator that is based on the DUT's /dev/urandom, which itself is seeded with noise information from its video and audio sensors.	ComMech-4	*N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)*
SecParam-8	ECDSA public key in X.509 certificate for authentication in SSH. The key is a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	An attacker needs access to the file system to change the certificate. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify the key is the web server which is run under a different account ''web'' than any of the processes used for external interfaces.	*N/A (Parameter is not critical)*	ComMech-4	*N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)*

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism
SecParam-9	Username and password combination for authentication against the web interface. The combination is no hard-coded identity and is not hard-coded in device software source code.	critical	The combination is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to change the password. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify the key is the web server which is run under a different account ''web'' than any of the other processes used for external interfaces.	The initial password for the admin account is generated and assigned in the DUT's manufacturing phase and is then stored in a pre-defined entry in an SQLite file. The password is announced to the user by a sticker in the packaging. When the password is changed by the user it needs to be in compliance with the password rules and is then stored in the SQLite file.	ComMech-1	*N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)*
SecParam-10	ECDSA public key in X.509 certificate for verifying the boot loaders involved in the ARM boot process. The key is not a hard-coded identity. The key is not hard-coded in device software source code.	critical	The key is not modifiable by an attacker so that its integrity is ensured.	An attacker needs access to the ROM of the DUT. This is not possible without attacking the chip hardware, especially an attack over DUT's interfaces is not possible. There is no user role of the OS that has access to this key.	The key is loaded into ROM during the initial manufacturing process.	*N/A (Parameter is not transmitted)*	*N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)*

Table C.11: Sample IXIT 11-ComMech (Communication Mechanisms)

ID	Description	Security Guarantees	Cryptographic Details	Resilience Measures
ComMech-1	The DUT offers a connection for its web interface in a LAN environment as server. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: The DUT acts as TLS server which offers the following cipher suites for the connection establishment: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. Mass reconnections may result in a DoS of the DUT, however the security of its services would be unaffected by this.
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no potential problems regarding mass connections.
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no potential problems regarding mass connections.
ComMech-4	The DUT offers a connection for its SSH interface in a LAN environment as server. This connection is based on IP/TCP/SSH. The mechanism is remotely accessible.	Through SSH the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over the SSH2 protocol keys with cipher suites conformant to the following security parameters: Key exchange: diffie-hellman-group-exchange-sha256 (2048-bit), encryption: AEAD_AES_256_GCM, MAC: hmac-sha2-256	The connection uses the well-defined SSH2 protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. Mass reconnections may result in a DoS of the DUT, however the security of its services would be unaffected by this.

Table C.12: Sample IXIT 12-NetSecImpl (Network and Security Implementations)

ID	Description	Review/Evaluation Method	Report
NetSecImpl-1	The network functionality is implemented by the Linux® network stack. Its purpose is to provide APIs for the application layer to be used by the DUT applications like the internal web server. It is part of the Linux® kernel, version 5.10.30.	The Linux® network stack is widely used on all type of systems all over the world. The Example Vendor Inc. itself did not review the stack. It trusts on the analysis made by security researchers not employed by Example Vendor Inc. The way defects are reported is described on the websites of the Linux® Foundation: https://www.linuxfoundation.org/en/blog/how-to-report-security-vulnerabilities-to-the-linux-foundation/.	None generated especially for this DUT.

ID	Description	Review/Evaluation Method	Report
NetSecImpl-2	The cryptographic functionality regarding the web interfaces is provided by the OpenSSL library, version 1.1.1k. Its purpose is to provide all cryptographic functions necessary for operate the web interfaces.	The Example Vendor Inc. did a code review of the OpenSSL parts used by the DUT. The review was done by two people which used an approach of both manual and automated code analysis. The team manually reviewed code responsible for the Diffie-Hellmann key exchange. If vulnerabilities had been discovered, the team would have followed the instructions published on https://www.openssl.org/community/#securityreports. The code was also analysed with a Static Code Analyzing Tool named EXAMPLE TOOL. This tool searches for potential race conditions, buffer overflows, out-of-bound errors, and format-string attacks.	The review team generated an internal code audit report which is attached to this IXIT. Neither the manual nor the automated code analysis found any vulnerabilities.
NetSecImpl-3	The cryptographic functionality regarding the update verification is provided by the Botan library, version 2.18.0. Its purpose is to provide all cryptographic functions necessary for the update verification.	The Botan code was reviewed by Rohde & Schwarz® together with the BSI, see https://www.bsi.bund.de/EN/Topics/Cryptography/CryptoLibrary/crypto_library_node.html.	The report is available under https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Projektzusammenfassung_Botan.pdf?__blob=publicationFile&v=1. The report mentions that all found potential vulnerabilities were fixed, side channel attack resistance was evaluated, missing crypto primitives were implemented according to standards and/or RFCs, and a test specification was implemented.

Table C.13: Sample IXIT 13-SoftServ (Software Services)

ID	Description	Status	Justification	Allows Configuration	Authentication Mechanism
SoftServ-1	Web service for providing the HTTP interface. The service is accessible over the network. The service is accessible in the initialized state.	Enabled	The service is necessary to provide the user the possibility to configure the DUT.	Yes. The user can • configure username/password configurations for web access, • configure SSH accounts.	AuthMech-1, AuthMech-2
SoftServ-2	SSH service for providing a remote command line access. The service is accessible over the network. The service is not accessible in the initialized state and needs to be enabled by the user.	Disabled	*N/A* *(The service is not enabled)*	Yes. The user has limited file system access which allows him/her to modify configuration files, read video and audio stream files.	AuthMech-3
SoftServ-3	Update service for downloading and applying firmware updates. The service is not accessible over the network.	Enabled	The service is responsible for checking remote for firmware updates and is enabled by default for security reasons.	No.	*N/A* *(The service is not accessible over the network)*
SoftServ-4	Video service for capturing and processing the video and audio signal and providing it as a data stream. The service is accessible over the network. The service is accessible in the initialized state.	Enabled	The service represents the core functionality and therefore is enabled by default.	No.	AuthMech-1, AuthMech-2

Table C.14: Sample IXIT 14-SecMgmt (Secure Management Processes)

ID	Description
SecMgmt-1	The Example Vendor Inc. uses ANSI/ISA-62443 to manage its security management processes. This includes all critical security parameters listed in IXIT 10-SecParam. The documentation of the implementation of the standard is attached. In conformance to the standard it covers the generation and provisioning of security parameters according to sections 5 and 8. The storage is done according to section 5. Updates are handled according to sections 9, 10 and 11. The decommissioning and expiration of the DUT is done according to section 12.

Table C.15: Sample IXIT 15-Intf (Interfaces)

ID	Description	Type	Status	Disclosed Information	Debug Interface	Protection
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is vulnerable.	*N/A (The interface is not a physical interface)*	*N/A (The interface is not a physical interface)*
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	Disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is vulnerable.	*N/A (The interface is not a physical interface)*	*N/A (The interface is not a physical interface)*
Intf-3	The board of the DUT has a JTAG interface. This interface is not required for the DUT's normal operation.	Physical, logical	Enabled, because it is used to initially flash the DUT. The interface cannot be disabled by the firmware.	The JTAG interface discloses diagnosis information. This information is security-relevant because it can give an attacker complete access to the DUT's software.	Yes, this interface is just used for debug purposes.	The interface is protected by the DUT's casing. The case is adhered, hence it requires a careful and time-consuming approach to access the interface without damaging the casing, which would be visible for the user.
Intf-4	USB interface for manual firmware updates.	Physical	Enabled, because it is used for manual firmware updates in case the DUT is not connected to a network.	None.	No, this interface cannot be used for debug purposes.	There is no need to limit exposure of the interface because its accessibility is necessary to provide its functionality.

Table C.16: Sample IXIT 16-CodeMin (Code Minimization)

ID	Description
CodeMin-1	The code is analysed with static code analysis tools during the development phase. The tools list unused functions which are removed according to section 8 of ANSI/ISA-62443.
CodeMin-2	The Example Vendor Inc. uses a code review process according to section 8 of ANSI/ISA-62443. Each code change is reviewed by at least one additional person to ensure that code published in official firmware packages does not contain any unused functions and statements.

Table C.17: Sample IXIT 17-PrivlCtrl (Privilege Control)

ID	Description
PrivlCtrl-1	The Example Vendor Inc. uses a secure code design process according to section 7 of ANSI/ISA-62443. This includes that for each component of the DUT a list of all technical user accounts and their privileges is maintained. During the design process the privileges are planned to have a minimal configuration so that the DUT's operation is not disturbed. The correct implementation of the defined privileges is then checked by tests according to section 9 of ANSI/ISA-62443 so that it is ensured that each component is operating with at least privileges as possible.

Table C.18: Sample IXIT 18-AccCtrl (Access Control)

ID	Description
AccCtrl-1	The DUT uses an ARM Cortex A8 processor which includes a memory management unit responsible for assigning memory access permissions and memory attributes to separated regions for different processes. The memory management unit controls table walk hardware that accesses translation tables in main memory by enabling a fine-grained memory system control through a set of virtual-to-physical address mappings and memory attributes held in instruction and data TLBs. The operating system Arch Linux® ARM depends heavily on use of the memory management unit, especially with its page table management.

Table C.19: Sample IXIT 19-SecDev (Secure Development Processes)

ID	Description
SecDev-1	The Example Vendor Inc. uses a secure development process according to ANSI/ISA-62443. This covers the specification of security requirements by threat models, a defined review process by at least two persons of the security design, the usage of the coding standard MISRA-C for a well-formed implementation representation, the application of pair programming so that every code change is reviewed by at least one additional person, and defined testing strategies including penetration testing and negative testing.

Table C.20: Sample IXIT 20-SecBoot (Secure Boot Mechanisms)

ID	Description	Security Guarantees	Detection Mechanisms	User Notification	Notification Functionality
SecBoot-1	The DUT implements a secure boot process. The bootloader is based on Trusted Board Boot (TBB), which prevents malicious firmware from running on the platform by authenticating all firmware images up to and including the normal world bootloader. It is done by establishing a Chain of Trust using Public-Key-Cryptography Standards (PKCS). The root of trust is a hardcoded public key that is initially loaded at the DUT's first configuration. The trust key is immutable and cannot be changed. The root of trust together with the RAM chip is certified according to PSA Level 3. A SHA256 of this key is stored into trusted root-key registers. The boot mechanism includes various boot loaders. The "boot loader 1" (BL1) resides in the ROM so it cannot be tampered with. The succeeding other boot loader images BL2, BL31 and BL33 are loaded one after another, where for each BL its integrity is verified by its preceding BL. A chain of trust for the software loaded by the ARM chip is done as described in section "Trusted Board Boot Sequence" at https://github.com/ARM-software/arm-trusted-firmware/blob/master/docs/design/trusted-board-boot.rst.	By establishing a consistent chain of trust, the complete software image including the OS kernel is protected, so that both integrity and authenticity are ensured. The software image is protected against manipulation before booting up.	If an arbitrary part of the boot loader chain including the software image cannot be verified, the DUT's verification of its boot loaders will fail because the signature check fails. In this case the DUT panics and stops its boot process completely.	The user will be notified through a red blinking LED at the left side of the DUT when an unauthorized change appears.	There are no network functionalities involved.

Table C.21: Sample IXIT 21-PersData (Personal Data)

ID	Description	Processing Activities	Communication Mechanisms	Sensitive	Obtaining Consent	Withdrawing Consent
PersData-1	Full name of the user	The user's name is entered on the app or the web interface and is used for displaying an individualized welcome message. Also the user's name will be used for sending failure reports solely to the Example Vendor Inc.	ComMech-2, ComMech-1. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user can withdraw his/her consent by resetting the DUT to factory defaults.
PersData-2	Email address of the user	The user's email address is entered on the app and the DUT and used for identifying a user against the backend servers. Also the user's email address will be used for sending failure reports solely to the Example Vendor Inc. and for advertisement emails regarding products of the Example Vendor Inc.	ComMech-2, ComMech-1. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user can withdraw his/her consent for receiving advertisement emails by sending an email to privacy@example.net opting out.
PersData-3	GPS data of the DUT's location	The GPS data is transmitted to the associated services (cloud infrastructure) of Example Vendor Inc. for a statistical evaluation to find out where its products are being used.	ComMech-2. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user can withdraw his/her consent by disabling the checkbox "Help improving this product" on the configuration page on the web interface or in the app.
PersData-4	Audio input/output stream	The audio stream of the DUT's main functionality is transmitted to the associated services (cloud infrastructure) of Example Vendor Inc. so that a user can listen to the DUT's environment over the app and web interface. Also the user can speak to the app and this audio is transmitted the DUT, which plays the audio.	ComMech-2, ComMech-1. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user can withdraw his/her consent by resetting the DUT to factory defaults.
PersData-5	Video input stream	The video stream of the DUT's main functionality is transmitted to the associated services (cloud infrastructure) of Example Vendor Inc. so that a user can see the DUT's environment over the app and web interface.	ComMech-2, ComMech-1. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user cannot withdraw his/her consent.

ID	Description	Processing Activities	Communication Mechanisms	Sensitive	Obtaining Consent	Withdrawing Consent
PersData-6	Age of the user	The user's age is transmitted to the associated services (cloud infrastructure) of Example Vendor Inc. for a statistical evaluation to find out what customers use this product.	ComMech-2, ComMech-1. The communication partner is an associated service.	No	The user nees to confirm the general terms and conditions prior to installing the DUT and the app and enter this optional value on the web interface or app.	The user can withdraw his/her consent by just deleting this value in the web interface or app.

Table C.22: Sample IXIT 22-ExtSens (External Sensors)

ID	Description
ExtSens-1	Microphone to record the sound of the DUT's environment located on the front of the DUT.
ExtSens-2	Camera (visible spectrum) to record the DUT's environment located on the front of the DUT.
ExtSens-3	Camera (infrared spectrum) for the DUT's motion sensor functionality located on the front of the DUT.

Table C.23: Sample IXIT 23-ResMech (Resilience Mechanisms)

ID	Description	Type	Security Guarantees
ResMech-1	The DUT uses a built-in battery that can supply the DUT with power for 15 minutes. After 12 minutes of power outage the DUT initiates a graceful shutdown. However, to increase system stability the DUT also uses the UBIFS file system that was designed with tolerance against hard power-cuts.	Power outage	The DUT's main functions, the video and audio stream, completely remain operational during a power outage of max. 12 minutes. In case there is a hard power-cut, the DUT remains operational after booting up again and is not affected negatively by a corrupted file system.
ResMech-2	The DUT buffers its video and audio data for 5 minutes to provide resilience against network failures. After reconnection the video and audio data can be received by external devices normally.	Network connectivity	The DUT's main functions, the video and audio stream, completely remain operational during a network failures of max. 5 minutes.

Table C.24: Sample IXIT 24-TelData (Telemetry Data)

ID	Description	Purpose	Security Examination	Personal Data
TelData-1	Crash data in case of a service failure. In case of a crashed process the DUT writes a core dump file containing the state of a process when the process receives certain signals, e.g. segmentation fault or illegal instruction. The core dump contains a snapshot of the allocated memory and registers.	The data will be analysed by the Example Vendor Inc. to improve especially the system stability of its products.	The telemetry data is uploaded after a crash (caused by a security violation) without any user interaction to the associated services (cloud infrastructure) of Example Vendor Inc. so that it can be analysed what caused the crash and what code improvements are possible. The core dump is analysed with GDB and similar tools by the staff of Example Vendor Inc. to gain the necessary information.	PersData-3, PersData-4, PersData-5

ID	Description	Purpose	Security Examination	Personal Data
TelData-2	Crash data in case of a kernel failure. In case of a crashed kernel the DUT automatically boots into a second kernel using kexec and writes a crash dump file containing the whole volatile memory of the system (RAM). The DUT then automatically boots into the original kernel.	The data will be analysed by the Example Vendor Inc. to improve especially the system stability of its products.	The telemetry data is uploaded without any user interaction to the associated services (cloud infrastructure) of Example Vendor Inc. so that it can be analysed what caused the crash (caused by a security violation) and what code improvements are possible. The crash dump is analysed with GDB and similar tools by the staff of Example Vendor Inc. to gain the necessary information.	PersData-1, PersData-2, PersData-3, PersData-4, PersData-5, PersData-6
TelData-3	Meta data of the video stream. The video stream is continuously monitored for the following meta data: Compression rate, bitrate, framerate, and usage of CPU capacities. The data will be collected while the stream is played by a user.	The data is analysed by the Example Vendor Inc. to improve especially the performance of its products.	*N/A* *(The data is not used for security examination)*	None
TelData-4	Meta data of the audio stream: Compression rate, bitrate, and usage of CPU capacities.	The audio stream is continuously monitored for various meta data like compression rate, bitrate, and usage of CPU capacities. The data will be collected while the stream is played by a user. The data is analysed by the Example Vendor Inc. to improve especially the performance of its products.	*N/A* *(The data is not used for security examination)*	None

Table C.25: Sample IXIT 25-DelFunc (Deletion Functionalities)

ID	Description	Target Type	Initiation and Interaction	Confirmation
DelFunc-1	The user can choose to reset the DUT to factory defaults. In this case all configuration data created by the user or created by consequence of user-provided input is erased from the flash memory. All configuration data that is created in defined configuration files (SQLite databases) is deleted from the file system in the flash memory. Then new configuration files are created with empty content.	User data on the device	The user needs to select "Maintenance" -> "Reset" on the web interface or "Maintenance" -> "Reset" in the app.	Before starting the erasing the app or the web interface presents a notification about the erasing process and informs the user about a subsequent restart. After deletion the DUT is restarted and is in the factory default state after delivery then. The user can verify this by noticing that the DUT is no longer connected to the Wireless network and the user cannot login by its configured username/passwords combination on the web interface.
DelFunc-2	The user can choose to remove the user's online profile. In this case the user's account on the associated services (cloud infrastructure) and on the app is deleted. All data that is stored on the servers of Example Vendor Inc. connected with the user's account is removed.	Personal data on associated services	The user needs to select "Maintenance" -> "Delete account" on the web interface or "Maintenance" -> "Delete account" on the app.	Before starting the removal the app or the web interface presents a notification about the removal process and informs the user about a subsequent logout. After removing the account the user is automatically logged out in the app. Also, the web interface shows an account error. The user cannot use the remote services anymore.

Table C.26: Sample IXIT 26-UserDec (User Decisions)

ID	Description	Options	Triggered By
UserDec-1	The user needs to set a new password for the admin user. This is the first action the user has to make to setup the DUT.	The user needs to choose a password that complies with the password rules (no default). The strength of the chosen password is displayed to the user.	The user wants to access the DUT via the app or the web interface for the first time. The decision cannot be triggered by the user.
UserDec-2	The user can add additional user accounts for the web interface. This is the second action the user has to make to setup the DUT. After initialization the user can still add or remove user accounts for the web interface independently from any other configuration workflow.	The user needs to choose a username/password combination that complies with the password rules (no default). The strength of the chosen password is displayed to the user.	The user wants to access the DUT via the app or the web interface for the first time. In this case the decision is triggered automatically. Additionally the decision can be triggered by the user after initialization.
UserDec-3	The user needs to enter his/her full name and email address. This is the third action the user has to make to setup the DUT. After initialization the user can still edit his/her full name and email address independently from any other configuration workflow.	The user needs to choose a valid name and email format (no default).	The user wants to access the DUT via the app or the web interface for the first time. In this case the decision is triggered automatically. Additionally the decision can be triggered by the user after initialization.
UserDec-4	The user can enter his/her age independently from any other configuration workflow.	The user needs to choose a valid age format (empty by default).	The user wants to access the DUT via the app or the web interface for the first time or he/she enters the configuration menu on the app or the web interface. The decision can be triggered by the user.
UserDec-5	The user can configure the transmission of GPS data from the DUT to the associated services (cloud infrastructure).	The user can choose between "on" (default) and "off". If "on", GPS data is transmitted according to PersData-3.	The user enters the configuration menu on the app or the web interface. The decision can be triggered by the user.
UserDec-6	The user can configure the behaviour of the DUT's motion sensor.	The user can choose between "active", "inactive" (default) and "time-based".	The user enters the configuration menu on the app or the web interface. The decision can be triggered by the user.
UserDec-7	The user can configure the time frame the DUT uses for applying firmware updates.	The user can choose between "never, manually" (default), "automatically within the time period …".	The user enters the configuration menu on the app or the web interface. The decision can be triggered by the user.
UserDec-8	The user can create a client certificate for enabling the SSH access.	The user can choose between "SSH disabled" (default) and "Enable SSH and generate certificate".	The user enters the configuration menu on the web interface. The decision can be triggered by the user.

Table C.27: Sample IXIT 27-UserIntf (User Interfaces)

ID	Description
UserIntf-1	The user can enter configuration data on the web interface accessible on remote port 443.
UserIntf-2	The user can enter configuration data on the app which is then transferred over the associated services (cloud infrastructure) to the DUT.

Table C.28: Sample IXIT 28-ExtAPI (External APIs)

ID	Description
ExtAPI-1	The DUT offers a SOAP interface that can be used by other devices to control the movement of the DUT's camera and receive audio and video streams via a direct connection on remote port 8085.

Table C.29: Sample IXIT 29-InpVal (Data Input Validation)

ID	Description
InpVal-1	For each user data transferred to the DUT over one of its APIs a defined validation rule is applied. A validation rule consists of at least one regular expression which receives the input data and gives back whether the input matches the expression. In case the input is more complex, the input can be matched against not just one but a set of regular expressions so that only valid values are processed by the DUT. Invalid values are rejected. The regular expressions are applied on any data received from the web interface, the SOAP interface, and the app.

Annex D (informative): Additional assessment information

D.1 Threat model

Threat modelling is widely recognized as one of the most important activities in information systems security. Threat modelling informs the discovery of actions and sequences thereof that a malicious actor possibly undertakes in order to impair, detriment, or otherwise compromise the value of an information system.

Threat modelling is concerned with the disciplined development and application of a representation of adversarial threats, i.e. sources, scenarios, and events specific to those. Such threats can target or affect an asset, be that a device, an application, a system, a network, a business function (and the corresponding supporting systems), or any other assets as defined within the scope of concern.

Like any model, a threat model is an abstract representation of the domain that involves threats and the primary concerns associated to those threats. In this regard, a threat model is used to capture knowledge in a structured manner, to provide a common language that supports a discourse about that knowledge, and to perform analyses and inference in the respective domain.

The key concepts of a threat model, include threat events, threat source, threat scenario, and consequences. Alternative wordings are also possible and frequent in the literature, e.g. the term impact is also used in the place of consequences.

Threats are events that can cause harm to the confidentiality, integrity, or availability of information or information systems, through unauthorized disclosure, misuse, alteration, or destruction of information or information systems. According to ISO/IEC 15408 [i.5], a threat is a potential cause of an incident that can result in harm to a system or organization. A threat consists of an asset, a threat agent and an adverse action of that threat agent on that asset. Moreover, a threat is enacted by a threat agent, and can lead to an unwanted incident breaking certain pre-defined security objectives.

A threat event is a situation that has the potential for causing undesirable consequences or impact upon a particular piece of information, a particular set of information systems, or both.

A threat scenario is a set of discrete threat events, associated a specific set of one or more threat sources, and which are partially ordered in time.

Several approaches and techniques for threat modelling are available. The Common Criteria (CC) for security assurance and evaluation defined in ISO/IEC 15408 [i.5] is one established approach.

The Threat, Vulnerability and Risk Analysis is another standard method used to develop a threat model [i.6]. Threat Vulnerability and Risk Analysis (TVRA) follows a structured approach through the following steps:

1) Identification of the Target Of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.

2) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.

3) Identification of the functional security requirements, derived from the objectives from step 2.

4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.

5) Identification and classification of the vulnerabilities in the system, the threats that potentially exploit them, and the resulting unwanted incidents.

6) Quantifying the occurrence likelihood and impact of the threats.

7) Establishment of the risks.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8.

10) Specification of detailed requirements for the security services and capabilities from step 9.

D.2 Baseline attacker model

D.2.1 Overview

Many test cases of the present document require an assessment of whether the strength of a security mechanism from the DUT is sufficient. To facilitate the evaluation, the relevant properties of an attacker on a baseline level are described in this clause.

In general the present document addresses a baseline security level. It is intended to contribute to the protection of consumer IoT products against the most common cybersecurity threats especially over network interfaces. Multi-medium or highly targeted/sophisticated attacks are not in scope. The attacker model is characterized by a combination of ability and motivation of the attacker.

D.2.2 Motivation of the attacker

The aim of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] is that a compliant device is protected against elementary attacks on fundamental design weaknesses especially concerning network based attacks. A typical attack scenario is that an attacker intents to compromise a class of devices for the integration into a botnet to attack third parties. The attacker is not intended to compromise the particular DUT. If the attacker discovers that the DUT has no fundamental vulnerabilities, he will generally address a different device. Accordingly, the motivation of the attacker is basic to compromise the DUT.

D.2.3 Characterization of the attacker

The ability of an attacker is characterized by expertise and resources. It is quantified as attack potential which is determined by the following factors described in Table D.1.

Table D.1: Attacker characterization

Factor	Description	Baseline Attacker Potential
Elapsed time for identification and exploitation	Elapsed time is the total amount of time taken by an attacker to identify that a particular potential vulnerability can exist in the DUT, to develop an attack method and to sustain effort required to mount the attack against the DUT.	The elapsed time is limited to less than one month.
Expertise	Expertise refers to the level of generic knowledge of the underlying principles, product type or attack methods.	The level of expertise is limited to a proficient person that is familiar with the security behaviour of the product type.
Knowledge of the DUT (design and operation)	Knowledge of the DUT refers to specific expertise in relation to the DUT. This is distinct from generic expertise, but not unrelated to it.	The knowledge of the DUT is limited to public information concerning the DUT and information provided to a user, e.g. user manual. Knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement is excluded.

Factor	Description	Baseline Attacker Potential
Opportunity	Opportunity has a relationship to the elapsed time factor. Identification or exploitation of a vulnerability can require considerable amounts of access to a DUT that can increase the likelihood of detection. Some attack methods can require considerable effort off-line, and only brief access to the DUT to exploit. Access can also need to be continuous, or over a number of sessions.	The opportunity is limited to a moderate level, i.e. access to the DUT is required for less than one month and the number of DUT samples required to perform the attack is less than one hundred.
Equipment required for exploitation	Equipment required for exploitation refers to the acquisition by the attacker.	Specialized equipment that is not readily available to the attacker, but can be acquired without undue effort and/or at reasonable cost, forms the upper limit concerning the acquisition. This can include purchase of moderate amounts of equipment, or development of more extensive attack scripts or programs.

D.3 Model for a "user with limited technical knowledge"

D.3.1 Overview

Many test cases of the present document require an assessment of whether the usability of a security-relevant mechanism from the DUT is given and user documentations are understandable for a common user. To facilitate the evaluation, the relevant properties of a corresponding user are described in this clause.

D.3.2 Characterization of a "user with limited technical knowledge"

The following Table D.2 describes assumptions on the ability of a user with limited technical knowledge.

Table D.2: User characterization

Factor	Description	User Potential
Expertise	Expertise refers to the level of generic knowledge of the underlying principles and product type.	The level of expertise is limited to baseline expertise described by the following key data: • The user is able to use a web browser. • The user able to navigate through the public internet and fill out forms. • The user knows how to change settings in a smartphone OS. • The user has baseline security knowledge (e.g. is able to use a virus scanner or password, such as a wireless network password). • The user has baseline knowledge about security updates (e.g. knows the intention, knows that updates have to be transmitted/installed and knows the meaning of a support period). • The user is able to pair devices (e.g. wireless ear plugs with a smartphone). • The user generally knows what a camera or microphone is.

Factor	Description	User Potential
Knowledge of the DUT	Knowledge of the DUT refers to specific expertise in relation to the DUT. This is distinct from generic expertise, but not unrelated to it.	The knowledge of the DUT is limited to all information that are provided or referenced together with the DUT (e.g. a user manual) and what is public available from the website of the SO. The user knows the intended functionality of the DUT.
Equipment for DUT usage	Equipment required for the usage of the DUT.	The equipment of the user is limited to what is provided with the DUT (e.g. additional software). Further, the user possesses a PC or smartphone or gateways and hubs if necessary.

History

Document history		
V1.1.1	August 2021	Publication