Draft ETSI TS 103 701 V 0.0.5 (2020-12-11)

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

The present document describes how to assess the conformance of consumer IoT products against ETSI TS 103 645 / ETSI EN 303 645.

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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 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 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 organisations in second party assessment, independent testing organisations 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 und thus the invasive analysis of hard- and software modules is not in the scope of the present document. The test scenarios 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.

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 1: 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: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements", Version 2.1.2, 2020-06.

[2] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements", Version 2.1.1, 2020-06.

NOTE 2: ETSI EN 303 645 is intended to be regularly synchronised 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 online at: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program.

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

NOTE: available online at: https://wiki.mozilla.org/Security/Server_Side_TLS.

[i.4] Overview of cryptographic key length recommendations

NOTE: available online at: https://www.keylength.com/.

[i.5] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.6] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.7] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[i.8] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

[i.9] 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.10] The Linux® Foundation, “Booting a self-signed Linux kernel”

NOTE: available online at https://www.linuxfoundation.org/blog/2013/09/booting-a-self-signed-linux-kernel/.

[i.11] Trusted Computing Group (TCG), “Hardware Requirements for a Device Identifier Composition Engine”

NOTE: available online at https://trustedcomputinggroup.org/resource/hardware-requirements-for-a-device-identifier-composition-engine/.

[i.12] Regulation 2019/881, “Cybersecurity Act”

NOTE: available online at https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

[i.13] Introduction to Hardware Security and Trust, Mohammad Tehranipoor and Cliff Wang, Eds., Springer, ISBN 978-1-4419-8079-3

NOTE: available online at: https://link.springer.com/book/10.1007%2F978-1-4419-8080-9.

[i.14] ETSI TR 103 621 V0.0.3 (2020-10, “CYBER; Guide to Cyber Security for Consumer Internet of Things“)

NOTE: not published yet

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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) proforma: 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 test laboratory to perform appropriate test activities

implementation extra information for testing (IXIT) proforma: document, in the form of a questionnaire, which when completed for a DUT becomes the IXIT

security guarantee: statement of the addressed security objectives

NOTE 1: In the present document security guarantees are used in an IXIT to describe the security objectives (e.g. confidentiality) which are realised by an implementation or process.

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

test action: named subdivision of a test case, constructed from test units and/or other test actions.

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

NOTE 2: The specification is considered to be complete if it is sufficient to enable a test 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 actions in isolation from other test cases.

test unit: indivisible unit of a specification of test actions

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 3: 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 supplier organization (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 4: The naming of test scenarios (sets of tests groups) and their corresponding sets of provisions coincide.

test verdict: statement of PASS, FAIL or INCONCLUSIVE, as specified in a test case, concerning conformance of the DUT with respect to that test case

3.2 Symbols

Void.

3.3 Abbreviations

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

API	Application Programming Interface
CVD	Coordinated Vulnerability Disclosure
CVRF	Common Vulnerability Reporting Framework
DDoS	Distributed Denial of Service
DUT	Device Under Test
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
GSMA	GSM Association
GUI	Graphical User Interface
ICS	Implementation Conformance Statement
IoT	Internet of Things
ISO	International Organization for Standardization

IXIT	Implementation eXtra Information for Testing
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
SO	Supplier Organization
TL	Test Laboratory
TEE	Trusted Execution Environment
TS	Technical Specification
TSO	Test Scenario

4 Conformance assessment methodology

4.1 Overview and document structure

4.1.1 Introduction

Section 4.1 describes the relevant roles and objects for the conformance assessment procedure.

Section 4.2 describes the assessment procedure.

Section 4.3 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).

Section 4.4 describes how to declare the corresponding security measures in the Implementation eXtra Information for Testing (IXIT) using IXIT proforma.

Section 4.5 describes the details for how to assign verdicts for test cases, test groups and finally, how to assign an overall verdict.

Section 4.6 describes how to use external evidences instead of the performing test groups in order to determine the conformance to a provision.

Section 4.7 highlights different aspects that assessment schemes typically address in addition of the content provided in the present document.

Sections 5 and 6 contain the test scenario, where each test scenario addresses a set of provisions from ETSI TS 103 645 [1] / ETSI EN 303 645 [2] and is composed of an IXIT proforma that describes the information required for the assessment and 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. 5.1-3-2 for the second test case in test group 5.1-3). Typically, the test cases distinguish to aspects:

- assessing conformity of the IXIT against the requirements of the provision (conformity of design); and
- assessing conformity of the DUT functionality, related 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 possibly nested test actions and an instruction on the assignment of the test verdict. Ultimately, test actions are constructed from indivisible test units. The test scenarios 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.

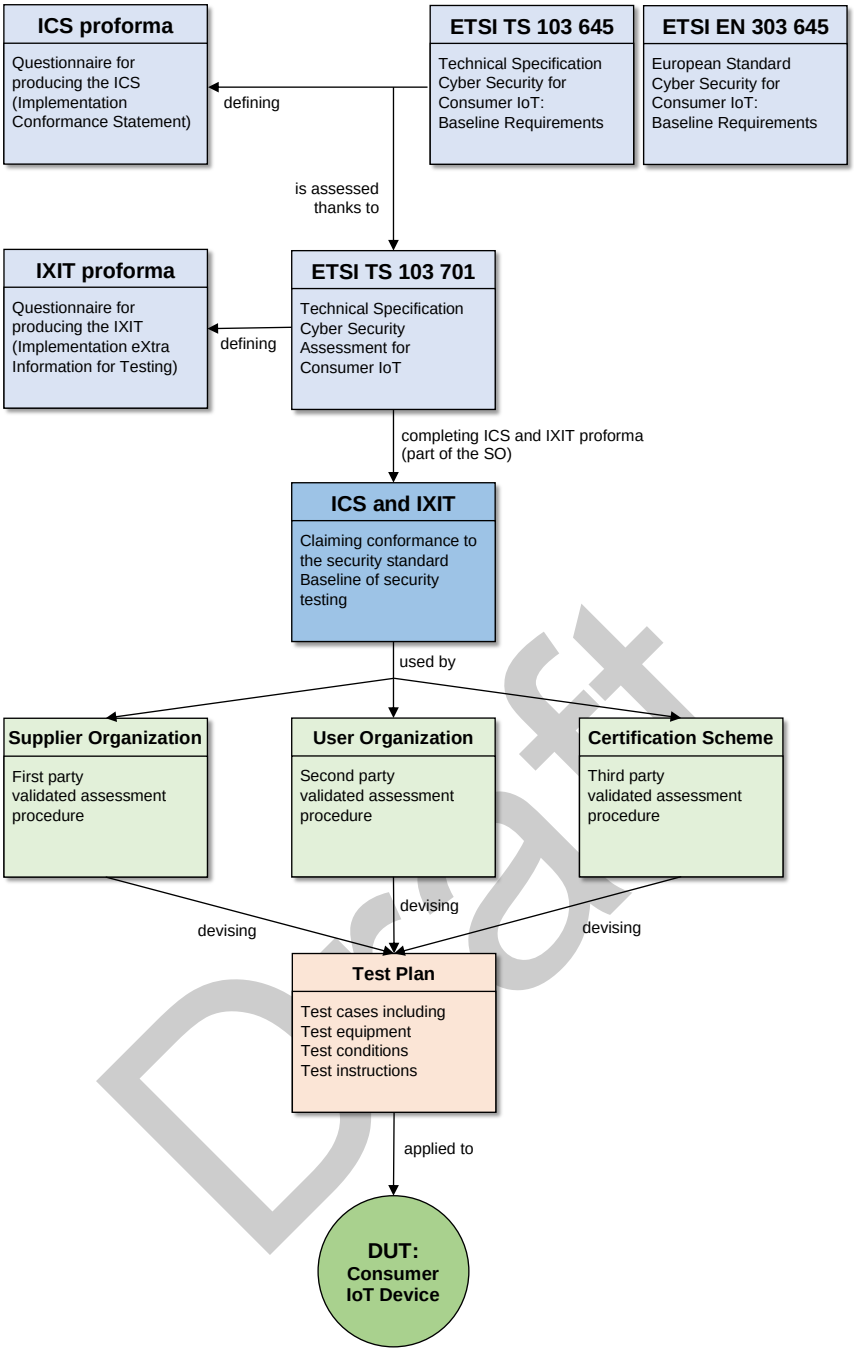

Figure 1: Relations of the present document with respect to a conformance assessment process Roles and Objects

4.1.2 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]. Test scenarios 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 **shall** 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 belongs to the DUT. An assessment in development state is also possible.

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

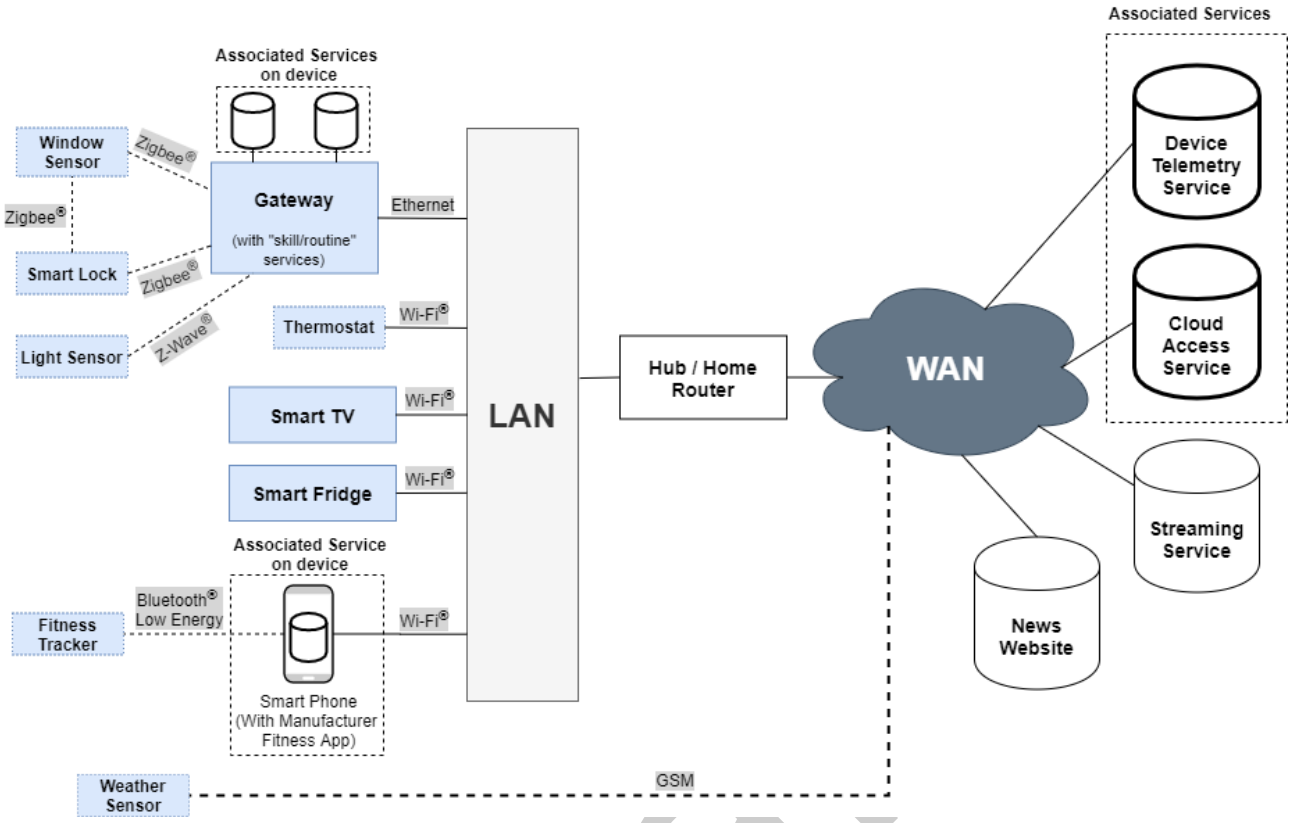

Figure 2: Challenges of assessing a wide range of implementations

4.1.3 Supplier Organization (SO)

The supplier organization (SO) requests a specific device under test (DUT) to be tested against the provisions of ETSI TS 103 645 [1] / ETSI EN 303 645 [2]. The SO may be the developer, manufacturer, vendor or distributor of the consumer IoT device. The SO usually serves as single point of contact to the test laboratory (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 test laboratory (TL) by providing all necessary information for the assessment.

4.1.4 Test Laboratory (TL)

The test laboratory (TL) is (a defined part of) an entity that carries out the conformance assessment of a device under test (DUT). The relation to accessioned 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]) . The TL **may** be a third party, a user organization, or an identifiable part of a supplier organization (SO). The TL is expected to operate competently and to be 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.

4.2 Assessment Procedure

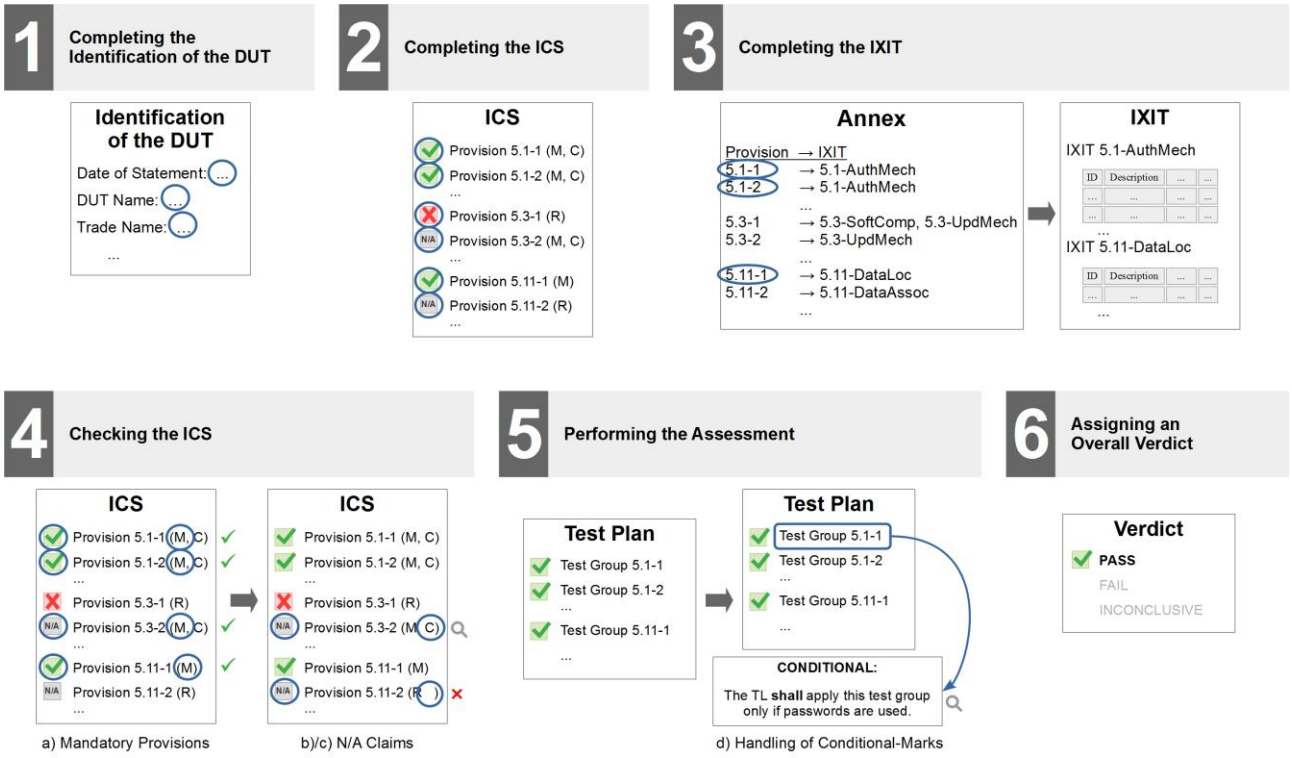

Figure 3: Phases of the Assessment Procedure (informative example)

The present section 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 3.

Phase 1: Completing the identification of the DUT

The SO **shall** complete the identification of the DUT. The questionnaire (part of the ICS proforma) to be filled and submitted by the SO is found in Annex B of the present document.

Phase 2: Completing the ICS

The SO **shall** complete the ICS (see section 4.3). The questionnaire (part of the ICS proforma) to be filled and submitted by the SO is found in Annex B of ETSI TS 103 645 [1] / ETSI EN 303 645 [2].

Phase 3: Completing the IXIT

The SO **shall** complete the necessary IXIT information (see section 4.4) for all provisions claimed as "Yes" in the ICS. The table in Annex 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 together with the SO.

Phase 4: Checking the ICS

The TL **shall** check the ICS by

a) verifying, that no mandatory provision (according to the status column in Annex B in ETSI TS 103 645 [1] / ETSI EN 303 645 [2]) is claimed as "No"; and
b) verifying, that for all conditional provision (according to the status column in Annex B in ETSI TS 103 645 [1] / ETSI EN 303 645 [2]) claimed as "N/A" the condition is indeed not fulfilled by the DUT; and
c) verifying, that there are no non-conditional provisions (according to the status column in Annex B in ETSI TS 103 645 [1] / ETSI EN 303 645 [2]) claimed as "N/A".

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. 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, test actions and test units. The TL **should** perform all test actions/units on its own. However, the present document does not preclude any alternative performance of the defined test actions/units.

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

If a test group is marked as "CONDITIONAL" (see d) in Figure 3), the TL **shall** evaluate, if the condition is fulfilled by the DUT before applying the test (e.g. a provision concerning passwords could not be applied to a DUT without password-based authentication even if it is claimed as "Yes" in the ICS).

The TL **shall** assign a verdict for each test case and test group as described in section 4.5.

Phase 6: Assigning an overall verdict

The TL **shall** assign an overall verdict according to Table 1 in section 4.5. 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, are fulfilled. When the assessment ends with the assigned verdict *FAIL*, at least one claimed provision is not fulfilled or the ICS is not fulfilled correctly.

The assigned verdict **shall** be published together with the ICS. This provides transparency concerning the treatment of recommended provisions.

NOTE: The details concerning the publication of the assessment results (e.g. definition of the specific content of an assessment report) is part of the assessment scheme.

4.3 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]. The ICS consists of a questionnaire (is found in Annex B of ETSI TS 103 645 [1] / ETSI EN 303 645 [2]) where the SO **shall** claim all provisions which are planned for the assessment. This is done by a written "Yes" in the "Support" column.

The mandatory provisions **shall** be claimed by the SO to enable 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 1: In terms of a conditional provision a constrained device (defined in ETSI TS 103 645 [1] / ETSI EN 303 645 [2]) represents a special case. It is possible to claim conformance against a conditional provisions even it is not necessary for a constrained device to fulfil the provision.

NOTE 2: Further guidance to fill in the ICS is given in Annex B of ETSI TS 103 645 [1] / ETSI EN 303 645 [2].

4.4 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 especially design details for the TL.

At the beginning of each TSO an IXIT proforma is provided which describes necessary information on the implementation of security measures addressing the corresponding provisions which in conjunction with the ICS (see section 4.3) give the necessary information for preparing and performing assessment activities.

The SO **shall** provide exhaustive and correct information on completing the IXIT. An *INCONCLUSIVE* verdict 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 distinctly reference to any entry in a table, e.g. sequential numbering.

4.5 Assignment of verdicts

In general there are three kinds of verdicts: an overall verdict, group verdicts and test verdicts. The overall verdict is composed of the results of the applied test groups (the group verdicts) and some further criteria. The group verdicts are in turn composed of the results of the contained test cases (the test verdicts) and some further criteria. For the test verdicts there are dedicated criteria in each test case in the section "Assignment of verdict".

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

Overall verdict	Instruction
PASS	The verdict assigned when • for each provision claimed as "Yes" in the ICS the corresponding test group is assigned a *PASS* verdict; AND • no criterion for an overall verdict *FAIL* is fulfilled.
FAIL	The verdict assigned when • for at least one provision claimed as "Yes" in the ICS the corresponding test group is assigned a *FAIL* verdict; OR • at least one mandatory provision according to Annex B in ETSI TS 103 645 [1] / ETSI EN 303 645 [2] is claimed as "No" in the ICS; OR • at least one non-conditional provision according to Annex B in ETSI TS 103 645 [1] / ETSI EN 303 645 [2] is claimed as "Not Applicable" in the ICS; OR • at least one conditional provision according to Annex B in ETSI TS 103 645 [1] / ETSI EN 303 645 [2] is claimed as "Not Applicable" in the ICS, but the condition is, contrary to the ICS statement, not fulfilled.
INCONCLUSIVE	The verdict assigned when • for at least one provision claimed as "Yes" in the ICS the corresponding test group is assigned an *INCONCLUSIVE* verdict.

Table 1: Instructions for the assignment of the overall verdict

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

Group verdict	Instruction
PASS	The verdict assigned when • each test case of the test group is assigned a *PASS* verdict.
FAIL	The verdict assigned when • at least one test case of the test group is assigned a *FAIL* verdict; OR • the test group is marked as "CONDITIONAL" in the test group objective and claimed as "Yes" in the ICS, but the described condition is not fulfilled and does not enable the application of the test group.
INCONCLUSIVE	The verdict assigned when • at least one test case of the test group is assigned an *INCONCLUSIVE* verdict; OR • the information provided in the IXIT are not sufficient to allow a proper execution of the test cases in the test group or to allow a reliable assignment of a verdict.

Table 2: Instructions for the assignment of a group verdict

The performance of each test case results in a test verdict according to the criteria specified in that test case ("Assignment of verdict"). Generally these criteria are specified in accordance with the instructions of Table 3.

Test verdict	Instruction
PASS	The verdict assigned when the observed test outcome • demonstrates conformance according to the test purpose; AND • contains no violating test unit.
FAIL	The verdict assigned when the observed test outcome • demonstrates non-conformance according to the test purpose; OR • contains at least one violating test unit.
INCONCLUSIVE	The verdict assigned when • neither a *PASS* nor a *FAIL* verdict can be assigned.

Table 3: Instructions for the assignment of a test verdict

4.6 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) 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.

4.7 Assessment Scheme Amendments

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 cryptography. The specific cryptographic requirements are typically defined by the assessment scheme considering the properties of the technology, risk and usage and the corresponding information in the present document. 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 an another certification scheme) that is accepted within an assessment (see section 4.6).

5 Test scenarios for consumer IoT

5.0 TSO 4: Reporting implementation

5.0.0 IXIT proforma TSO 4

This TSO is based on the ICS only, i.e. IXIT is not needed.

5.0.1 Test group 4-1

5.0.1.0 Test group objective

The test group addresses the provision:

A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the consumer IoT device.

5.0.1.1 Test case 4-1-1

Test purpose

The purpose of this test case is to check the existence of a justification for each recommendation that is considered to be not applicable for or not fulfilled by the DUT.

Test actions

Assessing the existence of justifications in the ICS.

> **Test units**
>
> The TL **shall** verify that 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 FAIL is assigned if

- there is at least one recommendation that is considered to be not applicable for the DUT without justification; OR
- there is at least one recommendation that is considered to be not fulfilled by the DUT without justification.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1 TSO 5.1: No universal default passwords

5.1.0 IXIT proforma TSO 5.1

IXIT 5.1-AuthMech: Authentication Mechanisms

This IXIT lists all authentication mechanisms of the DUT. It may be 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.

  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 realised 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 (RFC 7235). 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 5.1-AuthInfo: User Information

- **Publication of Change Mechanisms**: Description of the way the change mechanisms are documented for the user, including all information to access the documentation.

  NOTE 2: Possible ways of publication are the website of the manufacturer and the corresponding URL and the user manual.

5.1.1 Test group 5.1-1

5.1.1.0 Test group objective

The test group addresses the provision:

Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

CONDITIONAL: The TL **shall** apply this test group only if passwords are used.

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

Test purpose

The purpose of this test case is to assess whether passwords used in all identified password-based authentication mechanism for user authentication are conformant to the provision based on the documentation.

Test actions

Assessing the conformity of design of the password-based authentication mechanisms.

> **Test units**
>
> The TL **shall** evaluate for all password-based user authentication mechanisms in **IXIT 5.1-AuthMech** where passwords that are not defined by the user according to "Authentication Factor" whether the "Password Generation Mechanism" ensures that passwords are unique per device.

Assignment of verdict

The verdict FAIL is assigned if

- a password of a password-based authentication mechanism being used, that is not defined by the user, is not unique per device.

The verdict PASS is assigned if

- each password of a password-based authentication mechanism being used, that is not defined by the user, is unique per device.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.1.2 Test case 5.1-1-2

Test purpose

Assessing the conformity of implementation of the password-based authentication mechanisms.

Test actions

Assessing the completeness of the IXIT information.

> **Test units**
>
> The TL **shall** inspect whether password-based authentication mechanisms that are not documented in **IXIT 5.1-AuthMech** are available via a network interface on the DUT.
>
> EXAMPLE: Network scanning tools allow for discovery of network-based authentication mechanisms.

Assessing the conformity of implementation of the passwords defined by the user.

> **Test units**
>
> The TL **shall** verify for each password-based user authentication mechanism in **IXIT 5.1-AuthMech** by functional evaluation that the user is required to define all passwords that are user-defined according to "Authentication Factor" before being used.

Assessing the conformity of implementation of the generation mechanisms.

> **Test units**
>
> The TL **shall** assess for plausibility by functional evaluation that all passwords of the DUT, that are not defined by the user, are generated according to the generation mechanisms described in "Password Generation Mechanism" in **IXIT 5.1-AuthMech**.

Assignment of verdict

The verdict FAIL is assigned if

- a password-based authentication mechanism is discovered, that is not listed in the IXIT; OR
- the user is not required to define a password before being used, that is stated as defined by the user in the IXIT; OR
- there are indications that a password of the DUT, that is not defined by the user, is not generated according to the generation mechanisms described in the IXIT.

The verdict PASS is assigned if

- no password-based authentication mechanism is discovered, that is not listed 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 are no indications that a password of the DUT, that is not defined by the user, is not generated according to the generation mechanisms described in the IXIT.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.2 Test group 5.1-2

5.1.2.0 Test group objective

The test group addresses the provision:

Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.

CONDITIONAL: The TL **shall** apply this test group only if pre-installed passwords are used.

5.1.2.1 Test case 5.1-2-1

Test purpose

The purpose of this test case is to assess whether the generation mechanisms of pre-installed passwords are conformant to the provision.

Test actions

Assessing the conformity of design of generation mechanisms.

Test units

The TL **shall** evaluate for each authentication mechanism in **IXIT 5.1-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) may be obvious regularities.

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

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

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

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

The TL **shall** verify that the generation mechanisms 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 passwords complexity.

Assignment of verdict

The verdict FAIL is assigned if

- a generation mechanism induces obvious regularities in the resulting passwords; OR
- a generation mechanism induces common strings or other common patterns in the resulting passwords; OR
- a generation mechanism induces passwords, that are related in an obvious way to public information; OR
- a mechanism used to generate passwords is not considered appropriate in terms of complexity.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.2.2 Test case 5.1-2-2

Test purpose

The purpose of this test case is to functionally verify that the pre-installed passwords are conformant to the generation mechanisms described in the IXIT**.**

Test actions

Assessing the conformity of implementation of the generation mechanisms.

> **Test units**
>
> The TL **shall** assess for plausibility by functional evaluation for each authentication mechanism in **IXIT 5.1-AuthMech** using pre-installed passwords according to "Authentication Factor", whether the generation mechanism is implemented in accordance to the description in "Password Generation Mechanism".

Assignment of verdict

The verdict FAIL is assigned if

- for any pre-defined password there is indication, that it is not generated by the generation mechanism described in the IXIT.

The verdict PASS is assigned if

- for each pre-defined password there is no indication, that it is not generated by the generation mechanism described in the IXIT.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.3 Test group 5.1-3

5.1.3.0 Test group objective

The test group addresses the provision:

Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.

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 indications 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

Test purpose

The purpose of this test case is to assess the use of best practice cryptography for all authentication mechanisms.

Test actions

Assessing the conformity of design of the stated cryptography to be suitable for the authentication of users against the DUT.

> **Test units**
>
> For each authentication mechanism in **IXIT 5.1-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.
>
> For each authentication mechanism in **IXIT 5.1-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.
>
> For each authentication mechanism in **IXIT 5.1-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 there is no reference catalogue for the corresponding cryptography (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.14]. Moreover general reference catalogue of best practice cryptography are available, for example: SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu).
>
> NOTE 3: If a cryptographic algorithm or primitive is considered to be deprecated with regard to its desired security property (e.g. SHA1 for collision resistance) or relies on a cryptographic parameter (e.g. key-size) that is considered to be not inappropriate for the intended lifetime of the DUT, it cannot be considered as best practice cryptography.

Assessing the conformity of design of the stated cryptography to be not known to be vulnerable to a feasible attack.

> **Test units**
>
> For each authentication mechanism in **IXIT 5.1-AuthMech** used to authenticate users against the DUT, the TL **shall** assess that the "Cryptographic Details" are not known to be vulnerable to a feasible attack 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.

Assignment of verdict

The verdict FAIL is assigned if for any user authentication mechanism

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

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.3.2 Test case 5.1-3-2

Test purpose

The purpose of this test case is to functionally evaluate the use of the described cryptography.

Test actions

Assessing the conformity of implementation of the used cryptography.

> **Test units**
>
> For each authentication mechanism in **IXIT 5.1-AuthMech** used to authenticate users against the DUT, the TL **shall** functionally evaluate whether the described "Cryptographic Details" are used by the DUT.
>
> EXAMPLE: Using a protocol analyser or packet sniffer tool.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any used cryptographic setting is not as described.

The verdict PASS is assigned if

- there are no indications that any used cryptographic setting is not as described.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.4 Test group 5.1-4

5.1.4.0 Test group objective

The test group addresses the provision:

Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.

CONDITIONAL: The TL **shall** apply this test group only if the device allows user authentication.

5.1.4.1 Test case 5.1-4-1

Test purpose

The purpose of this test case is to assess whether the provided mechanisms to change the authentication values are conformant to the provision.

Test actions

Assessing the conformity of design of the change mechanism.

> **Test units**
>
> The TL **shall** verify that for every authentication mechanism in **IXIT 5.1-AuthMech** where "Description" indicates that the mechanism is used for user authentication, the resource of "Publication of Change Mechanisms" in **IXIT 5.1-AuthInfo** considers the mechanism and describes how to change the authentication value for the mechanism in a manner that is understandable for a user without technical knowledge.

Assignment of verdict

The verdict FAIL is assigned if

- for any user based authentication mechanism the published resource does not describe how to change the authentication value for a user without technical knowledge.

The verdict PASS is assigned if

- for all user based authentication mechanisms the published resource describes how to change the authentication value for a user without technical knowledge.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.4.2 Test case 5.1-4-2

Test purpose

The purpose of this test case is to functionally verify that the mechanisms to change authentication values are conformant to the IXIT**.**

Test actions

Assessing the conformity of implementation of the change mechanism.

> **Test units**
>
> The TL **shall** change the authentication values for all user authentication mechanisms in **IXIT 5.1-AuthMech** as documented in the resource from "Publication of Change Mechanism" in **IXIT 5.1-AuthInfo**.
>
> The TL **shall** verify that all changes of user authentication values are successful.

Assignment of verdict

The verdict FAIL is assigned if

- any mechanism for the user to change the authentication value for user authentication mechanisms does not work as described; OR
- any change of a authentication value for user authentication is not successful, i.e. the old authentication value is still valid or the new authentication value is not valid after a change.

The verdict PASS is assigned if

- all mechanisms for the user to change authentication values for user authentication mechanisms work as described; AND
- all changes of authentication values for user authentication are successful, i.e. the old authentication value is no longer valid and the new authentication value is valid after a change.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.5 Test group 5.1-5

5.1.5.0 Test group objective

The test group addresses the provision:

When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.

5.1.5.1 Test case 5.1-5-1

Test purpose

The purpose of this test case is to assess whether the mechanisms for brute force protection of network-based authentication mechanisms are conformant to the provision.

Test actions

Assessing the conformity of design of the mechanisms for making brute force attacks impracticable.

> **Test units**

The TL **shall** evaluate for each authentication mechanism in **IXIT 5.1-AuthMech**, where "Description" indicates that the mechanism is directly addressable via a network interface, whether 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
- 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 FAIL is assigned if

- the documented mechanisms do not make brute force attacks via network interfaces impracticable.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.1.5.2 Test case 5.1-5-2

Test purpose

The purpose of this test case is to functionally verify that the mechanisms for brute force protection of the DUT are conformant to the IXIT**.**

Test actions

Assessing the completeness of the IXIT documentation.

The TL **shall** functionally check for further network-based authentication mechanisms, that are not listed in **IXIT 5.1-AuthMech**.

NOTE: Methods for functionally checking for network-based authentication methods are network scanners such as "nmap".

Assessing the conformity of implementation of the mechanisms to make brute force attacks via network interfaces impracticable.

Test units

The TL **shall** attempt to brute force every network-based authentication mechanisms described in **IXIT 5.1-AuthMech**.

Assignment of verdict

The verdict FAIL is assigned if

- any network-based authentication mechanism that is not documented in the IXIT is discovered; OR
- indication is found, that for any authentication mechanism via network interfaces brute force prevention is not implemented as documented.

The verdict PASS is assigned if

- no network-based authentication mechanism that is not documented in the IXIT is discovered; AND
- for all authentication mechanism via network interfaces no indication is found that brute force prevention is not implemented as documented.

Otherwise, the verdict INCONCLUSIVE is assigned.

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

5.2.0 IXIT proforma TSO 5.2

IXIT 5.2-VulnInfo: User Information

The entries in this IXIT are independent from each other. These entries may be filled out in form of a list.

- **Publication of Vulnerability Disclosure Policy**: Description of the way the vulnerability disclosure policy is published, including all information to access the publication.

  NOTE 1: Possible way of publication is the website of the manufacturer and the corresponding URL.

- **Support Period**: Time during which the product or service is maintained by the manufacturer, e.g. in terms of updates.

IXIT 5.2-VulnTypes: Relevant Vulnerabilities

This IXIT lists all types of vulnerabilities that are relevant for the DUT. It may be 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 ("VulnTypes-1") or labelling scheme ("VulnTypes-Firmw").

- **Description**: Brief description of the kind of vulnerability that is relevant for the DUT.

  NOTE 2: 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 3: Roll 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 2: 5 days for initial response and 90 days until publication of the patch.

IXIT 5.2-VulnMon: Vulnerability Monitoring

This IXIT lists all procedures for monitoring, identifying and rectifying vulnerabilities. It may be 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 3: 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. It may commonly include a responsible person, an approach to gather information and a workflow to perform in case a vulnerability is discovered.

5.2.1 Test group 5.2-1

5.2.1.0 Test group objective

The test group addresses the provision:

The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum:

- *contact information for the reporting of issues; and*
- *information on timelines for (1) initial acknowledgement of receipt and (2) status updates until the resolution of the reported issues.*

5.2.1.1 Test case 5.2-1-1

Test purpose

The purpose of this test case is to assess whether the type of publication of the vulnerability disclosure policy is conformant to the provision. It is required to be publicly available, which means that anyone has access to it.

Test actions

Assessing the conformity of design of the publication.

> **Test units**
>
> The TL **shall** evaluate whether access to the publication as described in "Publication of Vulnerability Disclosure Policy" in **IXIT 5.2-VulnInfo** 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 FAIL is assigned if

- the publication of the vulnerability disclosure policy is not available for anybody.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.2.1.2 Test case 5.2-1-2

Test purpose

The purpose of this test case is to assess whether the publication of the vulnerability disclosure policy is conformant to the IXIT and conformant to the provision.

Test actions

Assessing the conformity of implementation of the publication.

> **Test units**
>
> The TL **shall** functionally evaluate whether the vulnerability disclosure policy is publicly accessible as described in "Publication of Vulnerability Disclosure Policy" in **IXIT 5.2-VulnInfo**.
>
> The TL **shall** evaluate whether the policy contains
>
> - contact information; AND
> - information about timelines regarding acknowledgement of receipt and status updates.

Assignment of verdict

The verdict FAIL is assigned if

- the vulnerability disclosure policy is not publicly accessible; OR
- no contact information or information about timeliness regarding acknowledgement of receipt and status updates is found in the policy.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.2.2 Test group 5.2-2

5.2.2.0 Test group objective

The test group addresses the provision:

Disclosed vulnerabilities should be acted on in a timely manner.

5.2.2.1 Test case 5.2-2-1

Test purpose

The purpose of this test case is to conceptually evaluate whether the targeted time frame and the way of acting in case of a disclosed vulnerability facilitate a timely acting on vulnerability disclosures.

Test actions

Assessing the conformity of design of the manner in which vulnerabilities are acted on.

> **Test units**
>
> The TL **shall** examine the "Action" and the "Time Frame" of each disclosed vulnerability in **IXIT 5.2-VulnTypes** in order to determine that vulnerabilities are acted on in a timely manner.
>
> NOTE 1: The consideration of severity and criticality of the addressed vulnerabilities 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 an 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.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any described kind of vulnerability is not acted on timely.

The verdict PASS is assigned if

- there are no indications that any described kind of vulnerability is not acted on timely.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.2.2.2 Test case 5.2-2-2

Test purpose

The purpose of this test case is to make sure that disclosed vulnerabilities are acted on timely.

Test actions

Assessing the conformity of implementation of the manner in which vulnerabilities are acted on.

> **Test units**

The TL **shall** collect evidence for the manner in which vulnerabilities are acted on. Such evidence includes, but is not limited to,

- management audit reports, or
- records of the actions on disclosed vulnerabilities, or
- taking minutes of an interview with at least one person (that is part of the action) how the actions are established.

NOTE: If there has not been a disclosed vulnerability yet the interview method is an alternative to get an evidence on how the actions are generally established.

TL **shall** examine the collected evidence in order to determine that actions on disclosed vulnerabilities are applied in accordance with their "Action" in **IXIT 5.2-VulnTypes**.

TL **shall** examine the collected evidence in order to determine that disclosed vulnerabilities are acted on timely.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that actions on disclosed vulnerabilities are not applied in accordance with their description; OR
- there are indications that disclosed vulnerabilities are not acted on timely.

The verdict PASS is assigned if

- there are sufficient evidences that actions on disclosed vulnerabilities are applied in accordance with their description; AND
- there are sufficient evidences that disclosed vulnerabilities are acted on timely.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.2.3 Test group 5.2-3

5.2.3.0 Test group objective

The test group addresses the provision:

Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.

5.2.3.1 Test case 5.2-3-1

Test purpose

The purpose of this test case is to assess whether the way of continuous monitoring, identifying and rectifying security vulnerabilities is conformant to the provision.

Test actions

Assessing the conformity of design of the way of continuous monitoring for security vulnerabilities.

Test units

The TL **shall** evaluate whether the way of continuously monitoring for security vulnerabilities documented in **IXIT 5.2-VulnMon** is suited to systematically gather information about security vulnerabilities that potentially may affect the DUT.

Assessing the conformity of design of the way of identifying security vulnerabilities.

Test units

The TL **shall** evaluate whether the way of identifying security vulnerabilities documented in **IXIT 5.2-VulnMon** is suited determine if and how a security vulnerability may affect the DUT.

Assessing the conformity of design of the way of rectifying security vulnerabilities.

> **Test units**
>
> The TL **shall** evaluate whether the way of rectifying security vulnerabilities documented in **IXIT 5.2-VulnMon** is suited to address and mitigate the susceptibility of a DUT against a security vulnerability.

Assessing the conformity of design of the time span the way of monitoring, identifying and rectifying security vulnerabilities is designed for.

> **Test units**
>
> The TL **shall** evaluate whether the way of monitoring, identifying and rectifying security vulnerabilities documented in **IXIT 5.2-VulnMon** is designed to be utilized for the entire duration of the "Support Period" described in **IXIT 5.2-VulnInfo**.

Assignment of verdict

The verdict FAIL is assigned if

- the described way is not suited for continuously monitoring for security vulnerabilities; OR
- the described way is not suited for identifying security vulnerabilities; OR
- the described way is not suited for rectifying security vulnerabilities.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.2.3.2 Test case 5.2-3-2

Test purpose

The purpose of this test case is to make sure that the described way for continuously monitoring security vulnerabilities is applied.

Test actions

Assessing the conformity of implementation of the way of continuous monitoring, identifying and rectifying security vulnerabilities.

> **Test units**
>
> The TL **shall** collect evidence for the application of the way of continuous monitoring, identifying and rectifying security vulnerabilities. Such evidence includes, but is not limited to,
>
> - management audit reports, or
> - records of the way of continuous monitoring, identifying and rectifying security vulnerabilities or
> - taking minutes of an interview with at least one person (that is part of the described way) concerning how the way of monitoring, identifying and rectifying security vulnerabilities is established.
>
> TL **shall** examine the collected evidence in order to determine that the way of continuous monitoring, identifying and rectifying security vulnerabilities is applied in accordance with its "Description" in **IXIT 5.2-VulnMon**.
>
> TL **shall** examine the collected evidence in order to determine that security vulnerabilities are monitored, identified and rectified.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that the way of continuously monitoring, identifying and rectifying security vulnerabilities is not applied in accordance with its description; OR

- there are no sufficient evidences that security vulnerabilities are monitored, identified and rectified.

The verdict PASS is assigned if

- there are no indications that the way of continuously monitoring, identifying and rectifying security vulnerabilities is not applied in accordance with its description; AND
- there are sufficient evidences that security vulnerabilities are monitored, identified and rectified.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3 TSO 5.3: Keep software updated

5.3.0 IXIT proforma TSO 5.3

IXIT 5.3-SoftComp: Software Components

This IXIT lists all software components of the DUT. It may be filled out in form of a table.

NOTE 1: The 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. The scope of implemented update mechanism might define a reasonable level of abstraction.

- **ID**: Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

  EXAMPLE 1: Sequential numbering (“SoftComp-1”) or labelling scheme (“SoftComp-Firmw”).

- **Description**: Brief description of the software component.

  NOTE 2: BIOS, firmware and boot loader are possible software components of the DUT.

- **Update Mechanism**: Reference to update mechanisms in **IXIT 5.3-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, a brief statement is included, that side effects of updating those algorithms and primitives are considered by the manufacturer.

IXIT 5.3-UpdMech: Update Mechanisms

This IXIT lists all update mechanisms of the DUT. It may be 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 2: 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 3: Depending on the complexity it may be useful to divide the description into the steps in which the update is performed.

  EXAMPLE 3: 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 realised 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 4: 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 5: Authenticity and integrity of a software update is realised by a signed firmware package based on RFC 3852. For the signature SHA-256 with RSA 2048 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 device.

- **Initiation and Interaction**: Brief description of the procedure an update is initiated and a brief description of the user interaction, which is necessary to initiate and apply an update.

  NOTE 4: 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 5: 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 6: HTTPS query for latest stable Firmware version to EXAMPLE.ORG and comparison to installed version after initialisation 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 realised by the DUT itself.

  NOTE 6: Notifications via user interfaces and push messages are possible ways to inform the user.

IXIT 5.3-UpdProc: Update Procedures

This IXIT lists procedures of the manufacturer for the management of security updates. It may be 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 7: 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 5.3-UpdInfo: User Information

This IXIT lists information about updates provided to users. The entries in this IXIT are independent from each other. These entries may be filled out in form of a list.

- **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 7: 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 8: Possible way of publication is the website of the manufacturer and the corresponding URL.

- **Publication of Replacement**: If the DUT is not updatable: Description of the way the guidance to isolate the device and the hardware replacement plan is documented for the user, including all information to access the documentation.

  NOTE 9: Possible ways of publication are the website of the manufacturer and the corresponding URL and the user manual.

- **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.

5.3.1 Test group 5.3-1

5.3.1.0 Test group objective

The test group addresses the provision:

All software components in consumer IoT devices should be securely updateable.

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

Test purpose

The purpose of this test case is to assess whether for all software components exist an update mechanism and the design of software update mechanisms is secure, i.e. there are adequate measures to prevent an attacker misusing the update mechanisms.

Assessing the conformity of design of the absence of software updates.

> **Test units**
>
> For each software component in **IXIT 5.3-SoftComp** with an empty list of "Update Mechanisms", the TL **shall** examine the justification for the absence of software updates in order to determine that the implementation of software updates is beyond practicability or for a security reason.
>
> EXAMPLE 1: An IoT device can contain separate microcontrollers from the main system which are only internally addressable. Those microcontroller typically acts as an internal service provider (e.g. temperature controller of a smart wine rack) sometimes without update functionality. A software update for those components could 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.

Assessing the conformity of design of the update mechanisms.

> **Test units**
>
> All test units as specified in the test action on conformity of design of the update mechanisms in test case 5.3-2-1 **shall** be applied to every referenced "Update Mechanism" in **IXIT 5.3-SoftComp**.

Assignment of verdict

The verdict FAIL is assigned if

- for at least one software component software updates are absent, but there is no practicability reason or security reason; OR
- at least one update mechanism can be misused by an attacker.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.1.2 Test case 5.3-1-2

Test purpose

The purpose of this test case is to functionally verify the effectiveness of the update mechanisms to avoid misuse.

Test actions

Assessing the conformity of implementation: Effectiveness of the update mechanisms against misuse.

> **Test units**
>
> All test units as specified in the test case 5.3-2-2 **shall** be applied to every referenced "Update Mechanism" in **IXIT 5.3-SoftComp**.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that a misuse of at least one update mechanism is possible.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.2 Test group 5.3-2

5.3.2.0 Test group objective

The test group addresses the provision:

When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.

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

Test purpose

The purpose of this test case is to assess whether the design of a least one update mechanism is secure, i.e. there are adequate measures to prevent an attacker misusing the update installation on the DUT.

Test actions

Assessing the conformity of design of the update installation mechanisms.

> **Test units**
>
> For each update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** examine the "Security Guarantees", the corresponding "Description", "Cryptographic Details" and "Initiation and Interaction" in order to determine that the

design of the update mechanism prevents misuse from an attacker. The examination **shall** be based on the defined "Security Guarantees" in **IXIT 5.3-UpdMech**.

NOTE: The consideration of the baseline attacker model described in Annex A is helpful for the examination.

EXAMPLE: A misuse may 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 FAIL is assigned if

- all update mechanisms of the DUT can be misused by an attacker.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.2.2 Test case 5.3-2-2

Test purpose

The purpose of this test case is to functionally verify the effectiveness of the update mechanism to avoid misuse.

Test actions

Assessing the conformity of implementation: Effectiveness of the update mechanisms against misuse.

Test units

For each update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** devise functional attacks to misuse the update mechanism based on the "description".

EXAMPLE: If applicable try a man-in-the-middle attack (MITM) between the DUT and the update server.

NOTE: An attack may be trying to resume the sequence of update steps after some failure of a specific update step.

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

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that a misuse of all update mechanism of the DUT is possible.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.3 Test group 5.3-3

5.3.3.0 Test group objective

The test group addresses the provision:

An update shall be simple for the user to apply.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

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.

NOTE: The focus of the provision is on the triggering of the update from user perspective.

5.3.3.1 Test case 5.3-3-1

Test purpose

The purpose of this test case is to assess whether update mechanisms are simple for the user to apply.

Test actions

Assessing the conformity of design of the simplicity the apply software updates.

Test units

The TL **shall** examine the "Initiation and Interaction" of each update mechanism in **IXIT 5.3-UpdMech** whether it is simple for the user to apply 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 without technical knowledge.

Assignment of verdict

The verdict FAIL is assigned if

- any update mechanism is not simple for the user to apply.

The verdict PASS is assigned if

- all update mechanisms are simple for the user to apply.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.4 Test group 5.3-4

5.3.4.0 Test group objective

The test group addresses the provision:

Automatic mechanisms should be used for software updates.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

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

5.3.4.1 Test case 5.3-4-1

Test purpose

The purpose of this test case is to assess whether the description of automation is suitable for automatic software updates.

Test actions

Assessing the conformity of design of the update mechanisms.

Test units

For each update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** assess whether the mechanism allows the performance of updates without requiring any user interaction according to "Initiation and Interaction".

For each update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** assess whether the mechanism allows the "Update Checking" without requiring any user interaction.

For each update mechanism in **IXIT 5.3-UpdMech** with the capability to configure the automation according to "Configuration", the TL **shall** assess whether the automatic mechanisms are enabled by default.

Assignment of verdict

The verdict FAIL is assigned if

- any update mechanism requires any user interaction for performing an update; OR
- any update mechanism requires any user interaction for checking the availability of an update; OR
- for any update mechanism automatic mechanisms are not enabled by default.

The verdict PASS is assigned if

- every update mechanism does not require any user interaction for performing an update; AND
- every update mechanism does not require any user interaction for checking the availability of an update; AND
- for every update mechanism automatic mechanisms are enabled by default.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.5 Test group 5.3-5

5.3.5.0 Test group objective

The test group addresses the provision:

The device should check after initialization, and then periodically, whether security updates are available.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

5.3.5.1 Test case 5.3-5-1

Test purpose

The purpose of this test case is to assess whether the update mechanisms check for available security updates triggered by the DUT after initialization, and then periodically .

Test actions

Assessing the conformity of design of the occurrence of security update checking.

Test units

For each "Update Mechanism" in **IXIT 5.3-UpdMech** the TL **shall** examine the schedule for querying for security updates in "Update Checking" in order to determine that the availability of security updates is checked

- after initialisation of the DUT; AND
- periodically.

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

Assignment of verdict

The verdict FAIL is assigned if for any update mechanism

- the checking of the availability of software updates is not triggered by the DUT itself; OR
- the availability of software updates is not checked after initialisation of the DUT; OR
- the availability of software updates is not checked periodically.

The verdict PASS is assigned if for every update mechanism

- the checking of the availability of software updates is triggered by the DUT itself; AND
- the availability of software updates is checked after initialisation of the DUT; AND
- the availability of software updates is checked periodically.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.6 Test group 5.3-6

5.3.6.0 Test group objective

The test group addresses the provision:

If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented and the device supports automatic updates and/or update notifications.

NOTE 1: The entry "Initiation and Interaction" in **IXIT 5.3-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 5.3-UpdMech** indicates whether it supports update notifications.

NOTE 3: The provisions addresses two different functionalities ("automatic updates" und "update notification") of an update mechanism. Furthermore, the provisions 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

Test purpose

The purpose of this test case is to assess whether automatic updates and/or update notifications are configurable by the user.

Test actions

Assessing the conformity of design of the configuration of automatic updates.

> **Test units**
>
> The TL **shall** apply all test units in test case 5.3-4-1 to identify all automatic update mechanisms in **IXIT 5.3-UpdMech**.
>
> For each update mechanism in **IXIT 5.3-UpdMech** that provides automatic software updates, the TL **shall** examine the description of "Configuration" in **IXIT 5.3-UpdMech** in order to determine that it provides the user with the ability to
>
> - enable,
> - disable, or
> - postpone
>
> automatic installation of security updates.

Assessing the conformity of design of the configuration of update notifications.

> **Test units**
>
> For each update mechanism in **IXIT 5.3-UpdMech** that provides update notifications according to "User Notification" the TL **shall** examine the description of "Configuration" in **IXIT 5.3-UpdMech** in order to determine that it provides the user with the ability to
>
> - enable,
> - disable, or

- postpone

update notifications.

Assignment of verdict

The verdict FAIL is assigned if for at least one update mechanism that supports automatic updates and/or update notifications the given functionality

- does not provide the user with the ability to enable, disable or postpone automatic installation of security updates; AND/OR
- does not provide the user with the ability to enable, disable or postpone update notifications.

The verdict PASS is assigned if for all update mechanism that supports automatic updates and/or update notifications the given functionality

- does not provide the user with the ability to enable, disable or postpone automatic installation of security updates; AND/OR
- does not provide the user with the ability to enable, disable or postpone update notifications.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.6.2 Test case 5.3-6-2

Test purpose

The purpose of this test case is to functionally verify the configuration of automatic updates and/or update notifications.

Test actions

Assessing the conformity of implementation of the configuration of automatic updates.

Test units

For each update mechanism in **IXIT 5.3-UpdMech** that provides automatic software updates (compare identification in test case 5.3-6-1) the TL **shall** verify that automatic updates are configured to be enabled in the initialized state of the DUT.

For each update mechanism in **IXIT 5.3-UpdMech** that provides automatic software updates (compare identification in test case 5.3-6-1) the TL **shall** modify the configuration of automatic update in order to determine that the user is provided with the ability to

- enable,
- disable, or
- postpone

automatic installation of security updates.

Assessing the conformity of implementation of the configuration of update notifications.

Test units

For each update mechanism in **IXIT 5.3-UpdMech** that provides update notifications according to “User Notification” the TL **shall** verify that update notifications are configured to be enabled in the initialized state of the DUT.

For each update mechanism in **IXIT 5.3-UpdMech** that provides update notifications according to “User Notification” the TL **shall** modify the configuration of update notifications in order to determine that the user is provided with the ability to

- enable,
- disable, or
- postpone

update notifications.

Assignment of verdict

The verdict FAIL is assigned if for at least one update mechanism that supports automatic updates and/or update notifications for the given functionality

- the configuration of automatic updates is not enabled in the initialized state of the DUT or cannot be modified by the user as described; AND/OR
- the configuration of update notifications is not enabled in the initialized state of the DUT or cannot be modified by the user as described.

The verdict PASS is assigned if for all update mechanism that support automatic updates or update notifications for the given functionality

- the configuration of automatic updates is enabled in the initialized state of the DUT and can be modified by the user as described; AND/OR
- the configuration of update notifications is enabled in the initialized state of the DUT and can be modified by the user as described.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.7 Test group 5.3-7

5.3.7.0 Test group objective

The test group addresses the provision:

The device shall use best practice cryptography to facilitate secure update mechanisms.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

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 indications 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

Test purpose

The purpose of this test case is to assess the use of best practice cryptography for the update mechanisms.

Test actions

Assessing the conformity of design of the stated cryptography to be suitable for secure update mechanisms.

> **Test units**
>
> For each update mechanism in **IXIT 5.3-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.
>
> For each update mechanism in **IXIT 5.3-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.
>
> For each update mechanism in **IXIT 5.3-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 there is no reference catalogue for the corresponding cryptography (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.14]. Moreover general reference catalogue of best practice cryptography are available, for example: SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu).

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

Assessing the conformity of design of the stated cryptography to be not known to be vulnerable to a feasible attack.

Test units

For each update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** assess that the "Cryptographic Details" are not known to be vulnerable to a feasible attack 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.

Assignment of verdict

The verdict FAIL is assigned if for any update mechanism

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

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.8 Test group 5.3-8

5.3.8.0 Test group objective

The test group addresses the provision:

Security updates shall be timely.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

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

Test purpose

The purpose of this test case is to assess whether security updates are deployed in a timely manner.

Test actions

Assessing the conformity of design of the procedures for deploying security updates timely.

Test units

The TL **shall** examine the "Description" and the "Time Frame" of each security update procedure in **IXIT 5.3-UpdProc** in order to determine that security updates are deployed in a timely manner.

NOTE 1: The consideration of severity and criticality of the addressed security vulnerabilities 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 an indicators for a timely deployment.

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

Assignment of verdict

The verdict FAIL is assigned if any update mechanism

- there are no indications that the described management procedure does allow a timely deployment of security updates

The verdict PASS is assigned if every update mechanism

- there are indications that the described management procedure does allow a timely deployment of security updates

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.8.2 Test case 5.3-8-2

Test purpose

The purpose of this test case is to assess the application of security update procedures.

Test actions

Assessing the conformity of implementation of the procedures for deploying security updates timely.

Test units

The TL **shall** collect evidence for the application of security update procedures. Such evidence includes, but is not limited to,

- management audit reports, or
- records of the application of security update procedures, or
- records of the timing of deployment of security updates or
- taking minutes of an interview with at least one person (that is part of the security update procedures) concerning how the procedure is established.

TL **shall** examine the collected evidence in order to determine that security update procedures are applied in accordance with their "Description" in **IXIT 5.3-UpdProc**.

Assignment of verdict

The verdict FAIL is assigned if for any update mechanism

- there are indications that the security update procedures are not applied in accordance with their description; OR
- there are no indications that security updates are deployed timely.

The verdict PASS is assigned if for every update mechanism

- there are indications that the security update procedures are applied in accordance with their description; AND
- there are indications that security updates are deployed timely.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.9 Test group 5.3-9

5.3.9.0 Test group objective

The test group addresses the provision:

The device should verify the authenticity and integrity of software updates.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

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

Test purpose

The purpose of this test case is to assess whether the authenticity and integrity of software updates is suitably verified.

Test actions

Assessing the conformity of design of the verification of authenticity of software updates.

> **Test units**
>
> For each update mechanism in **IXIT 5.3-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.

Assessing the conformity of design of the verification of integrity of software updates.

> **Test units**
>
> For each update mechanism in **IXIT 5.3-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.

Assessing the conformity of design of the performing entity.

> **Test units**
>
> For each update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** examine that the authenticity verification is performed by the DUT itself according to "Security Guarantees".
>
> For each update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** examine that the integrity verification is performed by the DUT itself according to "Security Guarantees".

Assignment of verdict

The verdict FAIL is assigned if

- at least one update mechanism is not effective for the verification of authenticity of software updates; OR

- at least one update mechanism is not effective for the verification of integrity of software updates; OR
- the verification of authenticity or integrity of software updates is not performed by the DUT itself.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.10 Test group 5.3-10

5.3.10.0 Test group objective

The test group addresses the provision:

Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented and updates are delivered over a network interface.

NOTE: The entry "Description" in **IXIT 5.3-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

Test purpose

The purpose of this test case is to assess whether the authenticity and integrity of software updates is suitably verified and whether the verification relies on a valid trust relationship.

Test actions

Assessing the conformity of design of the verification of authenticity and integrity of software updates.

> **Test units**
>
> All test units as specified in the test action on "conformity of design of the verification of authenticity of software updates" in test case 5.3-9-1 **shall** be applied.
>
> All test units as specified in the test action on "conformity of design of the verification of integrity of software updates" in test case 5.3-9-1 **shall** be applied.

Assessing the conformity of design of the performing entity.

> For each network based update mechanism in **IXIT 5.3-UpdMech**, the TL **shall** check the "Description" and "Security Guarantees" in order to determine that the verification of integrity and authenticity relies on a valid trust relationship. 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.

Assignment of verdict

The verdict FAIL is assigned if

- at least one update mechanism is not effective for the verification of authenticity of software updates; OR
- at least one update mechanism is not effective for the verification of integrity of software updates; OR
- the verification of authenticity or integrity of software updates is not based on a valid trust relationship verified by the DUT itself.

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 verified by the DUT itself.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.11 Test group 5.3-11

5.3.11.0 Test group objective

The test group addresses the provision:

The manufacturer should inform the user in a recognisable and apparent manner that a security update is required together with information on the risks mitigated by that update.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

5.3.11.1 Test case 5.3-11-1

Test purpose

The purpose of this test case is to assess whether the method and content of information for the user about required security updates conforms to the provision.

Test actions

Assessing the conformity of design of the method and content of information for the user about required security updates.

> **Test units**
>
> The TL **shall** examine the "User Notification" for each update mechanism in **IXIT 5.3-UpdMech** in order to determine that the method to inform the user about the availability of required security updates is recognisable and apparent.
>
> EXAMPLE 1: A notification via user interface, push message, e-mail is recognisable.
>
> EXAMPLE 2: A sufficiently sized pop-up using short and concise language is apparent.
>
> The TL **shall** examine the "User Notification" for each update mechanism in **IXIT 5.3-UpdMech** in order to determine that the user notification on required security updates includes information about the risks mitigated by the update.

Assignment of verdict

The verdict FAIL is assigned if for any update mechanism

- the method to inform the user about required security updates is not recognisable or apparent; OR
- the notification on required security updates does not include information about the risks mitigated by the update.

The verdict PASS is assigned if

- the method to inform the user about required security updates is recognisable and apparent; AND

- the notification on required security updates includes information about the risks mitigated by the update.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.12 Test group 5.3-12

5.3.12.0 Test group objective

The test group addresses the provision:

The device should notify the user when the application of a software update will disrupt the basic functioning of the device.

CONDITIONAL: The TL **shall** apply this test group only if an update mechanism is implemented.

Each update mechanisms is required to notify the user in case of a disruptive software update.

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

Test purpose

The purpose of this test case is to assess whether each update mechanism notifies the user about the disruption of basic functioning during the software update.

Test actions

Assessing the conformity of design of user notification in case of disruptive software updates.

> The TL **shall** evaluate each update mechanism in **IXIT 5.3-UpdMech** in order to determine if it supports user notification in case of disruptive software updates according to "User Notification" and it is indicated as realised on the DUT itself.

Assignment of verdict

The verdict FAIL is assigned if for at least one update mechanism

- the user is not appropriately notified about the disruption of basic functioning during the software update; OR
- the user notification is not realised on the DUT itself.

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 realised on the DUT itself.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.13 Test group 5.3-13

5.3.13.0 Test group objective

The test group addresses the provision:

The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.

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

Test purpose

The purpose of this test case is to assess whether the publication of software update support period is accessible, clear and transparent to the user.

Test actions

Assessing the conformity of design of the publication of software update support period.

> **Test units**
>
> The TL **shall** examine the "Publication of Support Period" in **IXIT 5.3-UpdInfo** in order to determine that the access to the publication is understandable and comprehensible for a user without technical knowledge.
>
> EXAMPLE: With help of the model designation of the DUT the user may find the support period over a search engine on website of the manufacturer.

Assignment of verdict

The verdict FAIL is assigned if

- the publication of software update support period is not understandable or comprehensible for a user without technical knowledge.

The verdict PASS is assigned if

- the publication of software update support period is understandable and comprehensible for a user without technical knowledge.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.13.2 Test case 5.3-13-2

Test purpose

The purpose of this test case is to functionally verify the publication of software update support period**.**

Test actions

Assessing the conformity of implementation of the publication of software update support period.

> **Test units**
>
> The TL **shall** inspect the user information on accessing the resource for publishing the defined support period according to "Publication of Support Period" in **IXIT 5.3-UpdInfo** in order to determine that the information is provided as described.
>
> The TL **shall** inspect the resource for publishing the defined support period according to "Publication of Support Period" in **IXIT 5.3-UpdInfo** in order to determine that it is accessible without restrictions (like e.g. a registration prior to the access).
>
> The TL **shall** inspect the published support period according to "Publication of Support Period" in **IXIT 5.3-UpdInfo** in order to determine that it actually defines the support period with respect to the updateable software components as described in "Support Period" in **IXIT 5.2-VulnInfo**.

Assignment of verdict

The verdict FAIL is assigned if

- the access to the resource for publishing the defined support period to the user is not provided as described in the IXIT; OR
- the access to the resource for publishing the defined support period is restricted; OR
- the defined support period is not published.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.14 Test group 5.3-14

5.3.14.0 Test group objective

The test group addresses the provision:

For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.

CONDITIONAL: The TL **shall** apply this test group only if software components are not updateable.

5.3.14.1 Test case 5.3-14-1

Test purpose

The purpose of this test case is to assess whether the publication of the rationale for absence of updates and hardware replacement support is accessible, clear and transparent to the user.

Test actions

Assessing the conformity of design of the publication of the rationale for absence of updates and hardware replacement support.

> **Test units**
>
> The TL **shall** examine the "Publication of Non-Updatable" and "Publication of Replacement" in **IXIT 5.3-UpdInfo** in order to determine that the access to the publications is understandable for a user without technical knowledge.

Assignment of verdict

The verdict FAIL is assigned if

- the publication of the rationale for absence of updates or hardware replacement support is not understandable for a user without technical knowledge.

The verdict PASS is assigned if

- the publication of the rationale for absence of updates and hardware replacement support is understandable for a user without technical knowledge.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.14.2 Test case 5.3-14-2

Test purpose

The purpose of this test case is to functionally verify the publication of the rationale for absence of updates and hardware replacement support**.**

Test actions

Assessing the conformity of implementation of the publication of the rationale for absence of updates and hardware replacement support.

Test units

The TL **shall** inspect 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 "Publication of Replacement" in **IXIT 5.3-UpdInfo** in order to determine that the information is provided as described.

The TL **shall** inspect the resource for publishing the rationale for absence of updates and hardware replacement support according to "Publication of Non-Updatable" and "Publication of Replacement" in **IXIT 5.3-UpdInfo** in order to determine that it is accessible without restrictions (like e.g. a registration prior to the access).

The TL **shall** inspect the published rationale for absence of updates according to "Publication of Non-Updatable" in **IXIT 5.3-UpdInfo** in order to determine that it contains the rationale for the absence of software updates.

The TL **shall** inspect the published hardware replacement support according to "Publication of Replacement" in **IXIT 5.3-UpdInfo** in order to determine that it 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.

The TL **shall** inspect the published rationale for absence of updates according to "Publication of Non-Updatable" in **IXIT 5.3-UpdInfo** in order to determine that it contains a defined support period.

Assignment of verdict

The verdict FAIL is assigned if

- the access to the resource for publishing the rationale for absence of updates and hardware replacement support to the user is not provided as described in the IXIT; OR
- the access to the resource for publishing the rationale for absence of updates and hardware replacement support is restricted; OR
- the rationale for the absence of software updates is not published; OR
- the period and method of hardware replacement support is not published; OR
- a support period is not published.

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 not 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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.15 Test group 5.3-15

5.3.15.0 Test group objective

The test group addresses the provision:

For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.

CONDITIONAL: The TL **shall** apply this test group only if software components are not updateable.

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

Test purpose

The purpose of this test case is to assess whether the IoT product is isolable and the hardware replaceable.

Test actions

Assessing the conformity of design of the isolation and hardware replacement support.

> **Test units**
>
> The TL **shall** examine the resource in "Publication of Replacement" in **IXIT 5.3-UpdInfo** in order to determine that the described method of hardware replacement 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.
>
> The TL **shall** examine the resource in "Publication of Replacement" in **IXIT 5.3-UpdInfo** in order to determine that the described method of hardware replacement is suitable to be able to replace the hardware.

Assignment of verdict

The verdict FAIL is assigned if

- the method of hardware replacement is not suited for the isolation of the IoT product; OR
- the method of hardware replacement is not suited for the replacement of the hardware.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.15.2 Test case 5.3-15-2

Test purpose

The purpose of this test case is to functionally verify that the IoT product is isolable and the hardware replaceable.

Test actions

Assessing the conformity of implementation of the isolation capabilities.

> **Test units**
>
> The TL **shall** set up the IoT product in the intended environment.
>
> The TL **shall** apply the method of hardware replacement as described in the resource of "Publication of Replacement" in **IXIT 5.3-UpdInfo** 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.
>
> The TL **shall** examine the isolated IoT product in order to determine that
>
> - 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 in a self-contained environment with other devices: the integrity of devices within that environment is ensured.

Assessing the conformity of implementation of the hardware replacement.

> **Test units**
>
> The TL **shall** apply the method of hardware replacement as described in the resource of "Publication of Replacement" in **IXIT 5.3-UpdInfo** in order to replace the hardware in the intended environment.

The TL **shall** examine the replaced DUT in order to determine that the connectivity and associated functionality can be regained.

Assignment of verdict

The verdict FAIL is assigned if

- the IoT product cannot be isolated successfully according to the hardware replacement plan; OR
- the hardware cannot be replaced successfully according to the hardware replacement plan.

The verdict PASS is assigned if

- the IoT product can be isolated successfully according to the hardware replacement plan; AND
- the hardware can be replaced successfully according to the hardware replacement plan.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.3.16 Test group 5.3-16

5.3.16.0 Test group objective

The test group addresses the provision:

The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.

5.3.16.1 Test case 5.3-16-1

Test purpose

The purpose of this test case is to functionally verify that the model designation can be clearly recognized**.**

Test actions

Assessing the conformity of implementation of the way of recognition of model designation and its given format.

Test units

The TL **shall** apply the described way of recognition in "Model Designation" in **IXIT 5.3-UpdInfo** in order to obtain the model designation of the DUT either by clearly recognizable labelling on the device or via a physical interface.

The TL **shall** examine that the obtained model designation is available in simple text and that it corresponds with the excepted model designation described in "Model Designation" in **IXIT 5.3-UpdInfo**.

Assignment of verdict

The verdict FAIL is assigned if

- the model designation of the DUT cannot be extracted according to the described way of recognition either by labelling on the device or via a physical interface; OR
- the model designation is not available in simple text; OR
- the model designation is not corresponding with the expected model designation according to the IXIT.

The verdict PASS is assigned if

- the model designation of the DUT can be extracted according to the described way of recognition either by labelling on the device or via a physical interface; AND
- the model designation is available in simple text; AND
- the model designation is corresponding with the expected model designation according to the IXIT.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.4 TSO 5.4: Securely store sensitive security parameters

5.4.0 IXIT proforma TSO 5.4

IXIT 5.4-SecParam: Security Parameters

This IXIT lists all sensitive (public and critical) security parameters that are persistently stored on the DUT during intended usage. It may be 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 ("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: Public and critical security parameters are defined in ETSI TS 103 645 [1] / ETSI EN 303 645 [2].

- **Security Guarantees**: Description of the realised 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 during the operation of the DUT.

  NOTE: 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 5.5-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 2: References to a standard random number generator and applicable design documents.

5.4.1 Test group 5.4-1

5.4.1.0 Test group objective

The test group addresses the provision:

Sensitive security parameters in persistent storage shall be stored securely by the device.

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 1: Threat modelling e.g. provided by the SO and the baseline attacker model described in Annex A 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

Test purpose

The purpose of this test case is to assess whether the security objectives are addressed by the security mechanisms based on the documentation.

Test actions

Assessing the conformity of design of the security claims for secure storage of and access to sensitive security parameters.

> **Test units**
>
> The TL **shall** assess whether the declaration in "Type" of each sensitive security parameter provided in **IXIT 5.4-SecParam** is consistent with the "Description".
>
> The TL **shall** assess whether the "Security Guarantees" of each sensitive security parameter provided in **IXIT 5.4-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.

Assessing the conformity of design of the secure storage of and access to sensitive security parameters with respect to the security claims.

> The TL **shall** assess whether the "Protection Scheme" of each sensitive security parameter provided in **IXIT 5.4-SecParam** provides the claimed "Security Guarantees".
>
> NOTE 2: Consider the usage of external evidences (see section 4.6) to (partially) cover the provision if a secure element is used.

Assessing the completeness of the IXIT documentation.

> **Test units**
>
> The TL **shall** evaluate the completeness of the sensitive security parameters in **IXIT 5.4-SecParam** by considering indications for sensitive security parameters in the provided information in all other IXITs.

Assignment of verdict

The verdict FAIL is assigned if

- for any sensitive security parameter the declaration is not consistent with its description; OR
- for any sensitive security parameter the security guarantees claimed do not match its minimal protection needs; OR
- for any sensitive security parameter the protection scheme is not suitable to deliver the claimed security guarantees; OR
- indications are found, that the listed sensitive security parameters in the IXIT are incomplete.

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 security guarantees claimed match its minimal protection needs; AND
- every sensitive security parameter has a suitable protection mechanism for the claimed security guarantees; AND
- no indications are found, that the listed sensitive security parameters are incomplete.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.4.1.2 Test case 5.4-1-2

Test purpose

The purpose of this test case is to assess whether the security objectives are addressed by the security mechanisms based on functional evaluation.

Test actions

Assessing the conformity of implementation of the secure storage of sensitive security parameters.

> **Test units**
>
> The TL **shall** inspect whether for all sensitive security parameters provided in **IXIT 5.4-SecParam** "Protection Scheme" is implemented according to the 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, indications for non-conformity of the implementation can be found, if existing on a basic level.

Assignment of verdict

The verdict FAIL is assigned if

- for any sensitive security parameter indication is found that any protection scheme is not implemented according to the documentation.

The verdict PASS is assigned if

- for every sensitive security parameter indication is found that the corresponding protection scheme is implemented according to the documentation.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.4.2 Test group 5.4-2

5.4.2.0 Test group objective

The test group addresses the provision:

Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.

CONDITIONAL: The TL **shall** apply this test group only if a hard-coded unique per device identify is used for security purposes.

It addresses the identification of hard-coded device identities and potential hard-coded information the identity is derived from and whether adequate protection needs are identified. A functional evaluation for tamper proof storage by any means is not in focus of this test scenario.

NOTE 1: The conceptual evaluation of protection schemes for tamper-resistance of hard-coded identities and an inspection for indications 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 might be derived from a – potentially secret – piece of information that persists in hardware (e.g. a seed value for a randomization algorithm). This information may be considered as part of a device identity

5.4.2.1 Test case 5.4-2-1

Test purpose

The purpose of this test case is to assess whether the protection scheme is providing tamper resistance.

Test actions

Assessing the conformity of design of tamper-resistant storage of hard-coded identities.

Test units

The TL **shall** assess whether for each sensitive security parameter in **IXIT 5.4-SecParam** where the "Description" indicates that it is used as an hard-coded identity, a corresponding explicit statement is provided.

The TL **shall** assess whether for each hard-coded identity as indicated in "Description" in **IXIT 5.4-SecParam** the corresponding "Security Guarantee" provides 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 section 4.6) to (partially) cover the provision if a secure element is used.

Assessing the conformity of tamper-resistant storage of hard-coded identities.

Test units

The TL **shall** assess whether the "Protection Scheme" of each hard-coded identity as indicated in "Description" in **IXIT 5.4-SecParam** provides the claimed "Security Guarantees" with respect to tamper-resistance.

Assignment of verdict

The verdict FAIL is assigned if

- indication is found that any hard-coded identity is not documented as such; OR
- for any hard-coded identity the security guarantee does not include tamper-resistance; OR
- any hard-coded identity has no suitable protection mechanism for tamper-resistance.

The verdict PASS is assigned if

- no indication is found 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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.4.2.2 Test case 5.4-2-2

Test purpose

The purpose of this test case is to assess whether the protection scheme that is providing tamper resistance for hard-coded identities is implemented based on functional evaluation.

Test actions

Assessing the conformity of implementation of the protection scheme that is providing tamper resistance for hard-coded identities.

Test units

The TL **shall** inspect whether for all each hard-coded identity as indicated in "Description" in **IXIT 5.4-SecParam** the "Protection Scheme" with respect to tamper-resistance is implemented according to the 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, indications for non-conformity of the implementation can be found, if existing on a basic level.

Assignment of verdict

The verdict FAIL is assigned if

- for any hard-coded identity, indication is found that any protection scheme with respect to tamper-resistance is not implemented according to the documentation.

The verdict PASS is assigned if

- for every hard-coded identity, no indication is found that any protection scheme with respect to tamper-resistance is not implemented according to the documentation.

5.4.3 Test group 5.4-3

5.4.3.0 Test group objective

The test group addresses the provision:

Hard-coded critical security parameters in device software source code shall not be used.

This test group assesses whether there are indications 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 device. This approach cannot provide strong assurance for completeness of the documentation concerning the identification of hard-coded critical security parameters in device software source code.

We note 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 may be embedded in the object code of the software of the DUT.

5.4.3.1 Test case 5.4-3-1

Test purpose

The purpose of this test case is to assess whether all documented critical security parameter that are hard-coded in device software source code are identified and that corresponding provisioning mechanisms ensure that hard-coded critical security parameter in device software source code are not used during the operation of the DUT.

Test actions

Assessing the conformity of design of the critical security parameters.

> **Test units**
>
> The TL **shall** assess whether for all critical security parameters provided in **IXIT 5.4-SecParam** where "Provisioning Mechanism" indicates that it is hard coded in device software source code, the fact is reflected in "Description".
>
> The TL **shall** assess whether for all critical security parameters in **IXIT 5.4-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 device.

Assignment of verdict

The verdict FAIL is assigned if

- indication is found that any critical security parameter hard-coded in device software source code is not documented; OR
- for any critical security parameter hard-coded in device software source code, the "Provisioning Mechanism" does not ensure that it is not used during the operation of the device.

The verdict PASS is assigned if

- no indication is found that any critical security parameter hard-coded in device software source code is not documented; 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 device.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.4.3.2 Test case 5.4-3-2

Test purpose

The purpose of this test case is to assess whether for all critical security parameter that are hard-coded in device software source code the documented provision mechanism is applied.

Test actions

Assessing the conformity of implementation of the critical security parameters.

> **Test units**
>
> The TL **shall** inspect whether for all critical security parameters hard-coded in device software source code documented in "Description" of **IXIT 5.4-SecParam**, the "Provisioning Mechanism" is indeed applied during the operation of the DUT.

Assignment of verdict

The verdict FAIL is assigned if

- for any critical security parameter hard-coded in device software source code there are indications, that the "Provisioning Mechanism" not applied as documented.

The verdict PASS is assigned if

- for all critical security parameter hard-coded in device software source code there are sufficient indications that the "Provisioning Mechanism" is applied as documented.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.4.4 Test group 5.4-4

5.4.4.0 Test group objective

The test group addresses the provision:

Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.

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

Test purpose

The purpose of this test case is to assess whether the documented generation mechanisms are conformant to the provision.

Test actions

Assessing the conformity of design of generation mechanisms.

> **Test units**
>
> The TL **shall** assess whether all critical security parameter provided in **IXIT 5.4-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".
>
> The TL **shall** assess for all critical security parameters provided in **IXIT 5.4-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) may 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. Standardisation bodies offer publicly available sources of information on suitable generation mechanisms, e.g. 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 may be keener with, Mozilla® publicly lists configuration profiles for TLS [i.3]. Finally, there are publicly available catalogs of references to relevant standards, e.g. the KeyLength catalog [i.4] that indexes standards published by NIST, ANSSI, BSI, etc. on the matter of cryprographic key length.

Assignment of verdict

The verdict FAIL is assigned if

- any critical security parameter where the purpose in “Description” indicates that the critical security parameter is used for integrity and authenticity checks of software updates or for protection of communication with associated services is not documented as such in “Generation Mechanism”; OR
- for any critical security parameter the “Generation Mechanism” does not ensure 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.

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 Mechanisms” ensure 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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5 TSO 5.5: Communicate securely

5.5.0 IXIT proforma TSO 5.5

IXIT 5.5-ComMech: Communication Mechanisms

This IXIT lists all communication mechanisms of the DUT. It may be 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 (“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 1: A possible communication mechanism is the use of Bluetooth, WiFi or NFC for a local connection between an mobile application and the DUT.

- **Security Guarantees**: Description of the realised security objectives and the threats the mechanism is protected against.

  NOTE 2: 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 3: 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.

IXIT 5.5-NetSecImpl: Network and Security Implementations

This IXIT lists all implementations of network and security functionalities of the DUT. It may be 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 3: 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 4: 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), the stakeholders involved, and the way defects are reported. 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 5: The outcome of the review or evaluation may not 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 5.5-SecMgmt: Secure Management Processes

This IXIT lists all secure management processes for critical security parameters implemented by the SO for the DUT. It can be 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 4: Sequential numbering ("SecMgmt-1") or labelling scheme ("SecMgmt-Passwd").

- **Description**: Brief description of the secure management process for critical security parameters. If an existing standard is used, a reference to the corresponding standard is provided.

5.5.1 Test group 5.5-1

5.5.1.0 Test group objective

The test group addresses the provision:

The consumer IoT device shall use best practice cryptography to communicate securely.

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 indications 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

Test purpose

The purpose of this test case is to assess the use of best practice cryptography for all communication mechanisms.

Test actions

Assessing the conformity of design of the stated cryptography to be suitable for the communication.

> **Test units**
>
> For each communication mechanism in **IXIT 5.5-ComMech**, the TL **shall** assess whether the "Security Guarantees" are appropriate for the use case of the communication.
>
> For each communication mechanism in **IXIT 5.5-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.
>
> For each communication mechanism in **IXIT 5.5-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 there is no reference catalogue for the corresponding cryptography (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.14]. Moreover general reference catalogue of best practice cryptography are available, for example: SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu).
>
> NOTE 3: If a cryptographic algorithm or primitive is considered to be deprecated with regard to its desired security property (e.g. SHA1 for collision resistance) or relies on a cryptographic parameter (e.g. key-size) that is considered to be not inappropriate for the intended lifetime of the DUT, it cannot be considered as best practice cryptography.

Assessing the conformity of design of the stated cryptography to be not known to be vulnerable to a feasible attack.

> **Test units**
>
> For each communication mechanism in **IXIT 5.5-ComMech**, the TL **shall** assess that the "Cryptographic Details" are not known to be vulnerable to a feasible attack 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.

Assignment of verdict

The verdict FAIL is assigned if for any communication mechanism

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

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.1.2 Test case 5.5-1-2

Test purpose

The purpose of this test case is to functionally evaluate the use of the described cryptography.

Test actions

Assessing the conformity of implementation of the used cryptography.

> **Test units**
>
> For each communication mechanism in **IXIT 5.5-ComMech**, the TL **shall** functionally evaluate whether the described "Cryptographic Details" are used by the DUT.
>
> EXAMPLE: Using a protocol analyser or packet sniffer tool.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any used cryptographic setting is not as described.

The verdict PASS is assigned if

- there are no indications that any used cryptographic setting is not as described.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.2 Test group 5.5-2

5.5.2.0 Test group objective

The test group addresses the provision:

The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.

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 recognised certification scheme.

The objective of this test case is to assess, firstly, whether the evaluation of an implementation covers the necessary security measures and mitigation identified by the SO and, secondly, whether the review of an implementation covers the implementation in full and is effective.

5.5.2.1 Test case 5.5-2-1

Test purpose

The purpose of this test case is to assess whether an evaluation of an implementation covers the necessary security measures and mitigations identified by the SO and whether a review of an implementation covers the implementation scope in full, and it is effective.

Test actions

Assessing the conformity of design of the evaluation method associated to an implementation with respect to proper coverage of the implementation and identified security measures and mitigations.

> **Test units**
>
> For each evaluation method associated to an implementation in **IXIT 5.5-NetSecImpl**, the TL **shall** assess whether the evaluation method in "Review/Evaluation Method" covers, or has been applied to, the implementation scope as described in "Description".
>
> For each evaluation method associated to an implementation in **IXIT 5.5-NetSecImpl**, the TL **shall** assess whether the evaluation method in "Review/Evaluation Method" covers the security measures and mitigations identified in "Description".

Assessing the conformity of design of the review method associated to an implementation with respect to coverage of the implementation scope and effectiveness.

> **Test units**
>
> For each implementation in **IXIT 5.5-NetSecImpl**, the TL **shall** assess whether the review method in "Review/Evaluation Method" and its "Report" covers the related implementation scope as described in "Description".
>
> For each implementation in **IXIT 5.5-NetSecImpl**, the TL **shall** assess whether the "Report" of the review considers a collection of identified defects and optionally an analysis of the implementation.
>
> For each review method associated to an implementation in **IXIT 5.5-NetSecImpl**, the TL **shall** assess whether the "Report" of the review considers a collection of bug fixes and recommendations.

Assignment of verdict

The verdict FAIL is assigned if

- any of the evaluation methods do not cover, or has not been applied to, the scope of the related implementation; OR
- any of the evaluation methods do not cover the security measures and mitigations identified by the SO for the related implementation; OR
- any review method does not match the related implementation in scope; OR
- any review report does not consider a collection of identified defects; OR
- any review report does not consider any collection of bug fixes or recommendations.

The verdict PASS is assigned if

- all evaluation methods cover, or have been applied to, the scope of the related implementation; AND
- all evaluation methods cover the security measures and mitigations identified by the SO for the related implementation; AND
- every review method matches the related implementation in scope; AND
- every review report considers a collection of identified defects; AND
- every review report considers a collection of bug fixes or recommendations.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.2.2 Test case 5.5-2-2

Test purpose

The purpose of this test case is to assess whether a provided implementation is conformant to the certificate or evaluation report provided for it as part of an evaluation and to the results of its review.

Test actions

Assessing the conformity of implementation of the certificate provided in the IXIT documentation.

> **Test units**

For each implementation associated with a review method in **IXIT 5.5-NetSecImpl**, the TL **shall** assess whether the identification of the implementation (name and version) on the device matches the identification of the implementation provided in the evaluation certificate or report.

Assessing the conformity of implementation of the review report provided in the IXIT documentation.

Test units

For each implementation associated with a review method in **IXIT 5.5-NetSecImpl**, the TL **shall** assess whether the identification of the implementation (name and version) on the device matches the identification of the implementation provided in the review report.

Assignment of verdict

The verdict FAIL is assigned if

- the name or version of any provided implementation does not match the name or version provided in the related certificate or report.

The verdict PASS is assigned if

- the name and version of every provided implementation matches the name and version provided in the related certificate or report; OR
- the device does not provide any information on the implementation name and version.

Otherwise the verdict INCONCLUSIVE is assigned.

5.5.3 Test group 5.5-3

5.5.3.0 Test group objective

The test group addresses the provision:

Cryptographic algorithms and primitives should be updateable.

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 higher-level 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

Test purpose

The purpose of this test case is to assess whether cryptographic algorithms and primitives, as described in the IXIT documentation, are updatable.

Test actions

Assessing the conformity of design of the implementations providing cryptographic algorithms and primitives described in the IXIT documentation with regard to the updatability.

Test units

For each software component in **IXIT 5.3-SoftComp** indicating “Cryptographic Usage”, the TL **shall** assess whether an “Update Mechanism” to update the software component is referenced.

For each software component in **IXIT 5.3-SoftComp** indicating “Cryptographic Usage”, the TL **shall** assess 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 FAIL is assigned if

- for any software component indicating cryptographic usage an update mechanism is not referenced; OR
- side effects of updating those algorithms and primitives is not considered by the manufacturer.

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 is considered by the manufacturer.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.4 Test group 5.5-4

5.5.4.0 Test group objective

The test group addresses the provision:

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

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 two 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 authorisation step is effective.

5.5.4.1 Test case 5.5-4-1

Test purpose

The purpose of this test case is firstly, to assess whether an authentication mechanism can discriminate between authentication subjects, is effective, and is resistant to adversaries and, secondly, whether the related authorisation process is effective.

Test actions

Assessing the conformity of design of the authentication mechanism with regard to the ability to discriminate between subjects, effectiveness and resistance to adversary.

Test units

For each device functionality in **IXIT 5.6-SoftServ** indicated as accessible via network interface in the initialized state according to “Description”, the TL **shall** assess whether there is at least one “Authentication Mechanism” referenced.

For each “Authentication Mechanism” referenced in **IXIT 5.6-SoftServ**, the TL **shall** assess whether the authentication mechanism described in **IXIT 5.1-AuthMech** allows to discriminate between two 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.

For each “Authentication Mechanism” referenced in **IXIT 5.6-SoftServ**, the TL **shall** assess whether the means protecting the authentication mechanism in “Cryptographic Details” in **IXIT 5.1-AuthMech** provide the “Security Guarantees” identified for the mechanism and are resistant to attempts at compromising the mechanism.

Assessing the conformity of design of the authorisation process with regard to effectiveness and protection of the authentication result.

> **Test units**
>
> For each "Authentication Mechanism" referenced in **IXIT 5.6-SoftServ**, the TL **shall** assess whether the authorization process described in "Description" in **IXIT 5.1-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 FAIL is assigned if

- no authentication mechanism is referenced for any device functionality accessible via network interface in the initialized state; OR
- an authentication mechanism does not allow to discriminate between two authentication subjects or to reject authentication attempts based on invalid identities and/or authentication factors; OR
- the means used to protect an authentication mechanism do not provide the expected security guarantees or are not resistant at attempts to compromise the mechanism; OR
- an authorisation mechanism does not allow access to authenticated subjects with proper access rights; OR
- an authorisation mechanism allows access to authenticated subjects with inadequate access rights or to unauthenticated subjects.

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 two 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 authorisation mechanism allows access to authenticated subjects with proper access rights; AND
- every authorisation mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.4.2 Test case 5.5-4-2

Test purpose

The purpose of this test case is to assess whether the implementation of the authentication and authorisation mechanisms protecting device functionalities is conformant to the IXIT documentation.

Test actions

Assessing the conformity of implementation of the authentication and authorisation mechanisms.

> **Test units**
>
> For each "Authentication Mechanism" referenced in **IXIT 5.6-SoftServ**, the TL **shall** functionally verify that an unauthenticated subject and a subject with invalid identity or credentials and an authenticated subject without appropriate access rights cannot access the device functionality.
>
> NOTE: This test unit cannot in principle distinguish between the authentication and the authorisation step – implementation aiming at reducing information leak will not disclose which step would fail to the subject.
>
> For each "Authentication Mechanism" referenced in **IXIT 5.6-SoftServ**,-the TL **shall** functionally verify that an authenticated subject with appropriate access rights can access the device functionality.
>
> For each "Authentication Mechanism" referenced in **IXIT 5.6-SoftServ**, the TL **shall** functionally verify that the protection of the authentication mechanism conforms to the description in "Security Guarantees" and "Cryptographic Details" in **IXIT 5.1-AuthMech**.

Assignment of verdict

The verdict FAIL is assigned if for any device functionality accessible via network interface in the initialized state

- an unauthenticated subject, a subject with invalid identity or invalid credentials or an authenticated subject without appropriate access rights can access the functionality ; OR
- an authenticated subject with appropriate access rights cannot access the device functionality; OR
- there are indications that the mechanism to secure the authentication does not conform to the IXIT documentation.

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; AND
- an authenticated subject with appropriate access rights can access the device functionality; AND
- there are no indications that the mechanism to secure the authentication does not conform to the IXIT documentation.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.5 Test group 5.5-5

5.5.5.0 Test group objective

The test group addresses the provision:

Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.

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 authorisation 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 authorisation step is effective.

5.5.5.1 Test case 5.5-5-1

Test purpose

The purpose of this test case is firstly, to assess whether an authentication mechanism can discriminate between authentication subjects, is effective, and is resistant to adversaries and, secondly, whether the related authorisation mechanism is effective.

Test actions

Assessing the conformity of design of the authentication mechanism with regard to the ability to discriminate between subjects, effectiveness and resistance to adversary.

> **Test units**
>
> All test actions as specified in test case 5.5-4-1 **shall** be applied with restriction to the functionalities that allow security-relevant changes according to “Allows Configuration” in **IXIT 5.6-SoftServ**.

Assignment of verdict

The verdict FAIL is assigned if

- an authentication mechanism does not allow to discriminate between two authentication subjects or to reject authentication attempts based on invalid identities and/or authentication factors; OR

- the means used to protect an authentication mechanism do not provide the expected security guarantees or are not resistant at attempts to compromise the mechanism; OR
- an authorisation mechanism does not allow access to authenticated subjects with proper access rights; OR
- an authorisation mechanism allows access to authenticated subjects with inadequate access rights or to unauthenticated subjects.

The verdict PASS is assigned if

- every authentication mechanism allows to discriminate between two 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 authorisation mechanism allows access to authenticated subjects with proper access rights; AND
- every authorisation mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.5.2 Test case 5.5-5-2

Test purpose

The purpose of this test case is to assess whether the implementation of the authentication and authorisation mechanisms protecting device functionalities is conformant to the IXIT documentation.

Test actions

Assessing the conformity of implementation of the authentication and authorisation mechanisms according to the IXIT documentation.

> **Test units**
>
> All test actions as specified in test case 5.5-4-2 **shall** be applied with restriction to the functionalities that allow security-relevant changes according to "Allows Configuration" in **IXIT 5.6-SoftServ**.

Assignment of verdict

The verdict FAIL is assigned if for any device functionality accessible via network interface and allowing security-relevant configuration changes

- an unauthenticated subject, a subject with invalid identity or invalid credentials or an authenticated subject without appropriate access rights can access the functionality; OR
- an authenticated subject with appropriate access rights cannot access the device functionality; OR
- there are indications that the mechanism to secure the authentication does not conform to the IXIT documentation.

The verdict PASS is assigned if for every device functionality accessible via network interface and allowing security-relevant configuration changes

- 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 are no indications that the mechanism to secure the authentication does not conform to the IXIT documentation.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.6 Test group 5.5-6

5.5.6.0 Test group objective

The test group addresses the provision:

Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.

In difference to test group 5.5-1, the use case in this provision is precised 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

Test purpose

The purpose of this test case is to assess the use of best practice cryptography for all communication mechanisms transmitting critical security parameters.

Test actions

Assessing the conformity of design of the stated cryptography to be suitable for the communication of critical security parameters.

> **Test units**
>
> For all "Communication Mechanisms" in **IXIT 5.5-ComMech** referenced in any critical security parameter in **IXIT 5.4-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 FAIL is assigned if for any communication mechanism used for communicating critical security parameters

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

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

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.6.2 Test case 5.5-6-2

Test purpose

The purpose of this test case is to functionally evaluate the use of the described cryptography.

Test actions

Assessing the conformity of implementation of the used cryptography.

> **Test units**
>
> For all "Communication Mechanisms" in **IXIT 5.5-ComMech** referenced in any critical security parameter in **IXIT 5.4-SecParam**, the TL **shall** apply all test units as specified in the test case 5.5-1-2.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any used cryptographic setting is not as described.

The verdict PASS is assigned if

- there are no indications that any used cryptographic setting is not as described.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.7 Test group 5.5-7

5.5.7.0 Test group objective

The test group addresses the provision:

The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.

In difference to test group 5.5-1 and 5.5-6, the use case in this provision is precised 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

Test purpose

The purpose of this test case is to assess the use of best practice cryptography for all communication mechanisms transmitting critical security parameters via remotely accessible network interfaces.

Test actions

Assessing the conformity of design of the stated cryptography to be suitable for the communication of critical security parameters via remotely accessible network interfaces.

> **Test units**
>
> For all “Communication Mechanisms”, that are remotely accessible according to their “Description” in **IXIT 5.5-ComMech** referenced in any critical security parameter in **IXIT 5.4-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 FAIL is assigned if for any communication mechanism used for communicating critical security parameters via remotely accessible network interfaces

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

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.7.2 Test case 5.5-7-2

Test purpose

The purpose of this test case is to functionally evaluate the use of the described cryptography.

Test actions

Assessing the conformity of implementation of the used cryptography.

> **Test units**
>
> For all "Communication Mechanisms", that are remotely accessible according to their "Description" in **IXIT 5.5-ComMech** referenced in any critical security parameter in **IXIT 5.4-SecParam**, the TL **shall** apply all test units as specified in the test case 5.5-1-2.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any used cryptographic setting is not as described.

The verdict PASS is assigned if

- there are no indications that any used cryptographic setting is not as described.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.8 Test group 5.5-8

5.5.8.0 Test group objective

The test group addresses the provision:

The manufacturer shall follow secure management processes for critical security parameters that relate to the device.

5.5.8.1 Test case 5.5-8-1

Test purpose

The purpose of this test case is to assess whether the secure management processes are conformant to the requirements of the provision.

Test actions

Assessing conformity of design of the secure management processes.

> **Test units**
>
> The TL **shall** assess whether the secure management of critical security parameters covers the whole life cycle of an critical security parameter considering its
>
> - generation,
> - provisioning,
> - storage,
> - updates,
> - decommissioning, archival, and destruction, and
> - processes to handle the expiration and compromise
>
> according to the processes in **IXIT 5.5-SecMgmt**.

Assignment of verdict

The verdict FAIL is assigned if

- the secure management does not cover the whole life cycle of a critical security parameter according to its processes.

The verdict PASS is assigned if

- the secure management covers the whole life cycle of a critical security parameter according to its processes.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.5.8.2 Test case 5.5-8-2

Test purpose

The purpose of this test case is to assess whether the secure management processes are applied as described.

Test actions

Assessing conformity of implementation of the secure management processes.

> **Test units**
>
> The TL **shall** collect evidence for the application of the secure management processes. Such evidence includes, but is not limited to,
>
> - management audit reports, or
> - records of the secure management processes, or
> - taking minutes of an interview with at least one person (that is part of the process) concerning how the secure management processes are established.
>
> TL **shall** examine the collected evidence in order to determine that the secure management processes are applied in accordance with their "Description" in **IXIT 5.5-SecMgmt**.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any secure management process is not applied in accordance with its description.

The verdict PASS is assigned if

- there are no indications that any secure management process is not applied in accordance with its description.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6 TSO 5.6: Minimize exposed attack surfaces

5.6.0 IXIT proforma TSO 5.6

IXIT 5.6-Intf: Interfaces

This IXIT lists all interfaces of the DUT. It may be 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 ("Intf-1") or labelling scheme ("Intf-LanPort").

- **Description**: Brief description of the interface, including purpose. For physical interfaces, it is described additionally whether the interface is always required, never required or required only in specific cases, which are briefly described then.

- **Type**: Indication of the type of the interface.

  NOTE 1: Interface types might be network, logical, physical, air.

- **Status**: Indication whether the interface is enabled or disabled by default. 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.
- **Debug Interface**: If the interface is a physical interface: Indication whether the interface is a debug interface.
- **Protection**: If the interface is a physical interface: Description of the protection methods necessary to limit exposure of the interface.

  NOTE 2: For debug interfaces a description of the software mechanism used to disable the interface is expected.

IXIT 5.6-SoftServ: Software Services

This IXIT lists all software services of the DUT. It may be 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 2: 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 if this is the case in the initialized state.
- **Status**: Indication whether the service is enabled or disabled.
- **Justification**: If the service is enabled: Justification why the service is necessary for the intended use or operation of the device.
- **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 5.1-AuthMech** that are used for authentication prior the use of the service.

IXIT 5.6-CodeMin: Code Minimization

This IXIT lists all methods for minimizing code. It may be 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 3: Sequential numbering ("CodeMin-1") or labelling scheme ("CodeMin-DeadCode").
- **Description**: Brief description of the method used to minimize code to the necessary functionality.

IXIT 5.6-PrivlCtrl: Privilege Control

This IXIT lists all privilege control mechanisms. It may be 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 4: Sequential numbering ("PrivlCtrl-1") or labelling scheme ("PrivlCtrl-OS").
- **Description**: Brief description of the mechanism to control privileges of software on the DUT.

IXIT 5.6-AccCtrl: Access Control

This IXIT lists all access control mechanisms for memory on hardware-level. It may be 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 5: 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 5.6-SecDev: Secure Development Processes

This IXIT lists all secure development processes implemented by the SO for the DUT. It can be 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 ("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.

5.6.1 Test group 5.6-1

5.6.1.0 Test group objective

The test group addresses the provision:

All unused network and logical interfaces shall be disabled.

In principle a logical interface may 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 to have 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

Test purpose

The purpose of this test case is to assess whether the statuses of network and logical interfaces are compatible with the interface purposes described.

Test actions

Assessing the conformity of design of the status of each network and logical interface of the DUT.

> **Test units**
>
> For each network and logical interface in **IXIT 5.6-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 FAIL is assigned if

- for any network or logical interface that is marked as enabled in the IXIT documentation, there is no purpose that provides a valid justification for the interface to be enabled

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.1.2 Test case 5.6-1-2

Test purpose

The purpose of this test case is to assess whether the statuses of network and logical interfaces on the DUT match the description in the IXIT documentation.

Test actions

Assessing the conformity of implementation of the status of each network and logical interface of the DUT.

> **Test units**
>
> For each network and logical interface in **IXIT 5.6-Intf**, the TL **shall** assess by functional evaluation 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.

Assessing the completeness of the IXIT information.

> **Test units**
>
> The TL **shall** inspect whether network or logical interfaces that are not documented in **IXIT 5.6-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 FAIL is assigned if

- any documented network or logical interface that is marked as disabled in the IXIT documentation is found to be enabled or accessible on the DUT; OR
- there is indication that any network or logical interface is available that is not documented.

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
- there is no indication that any network or logical interface is available that is not documented

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.2 Test group 5.6-2

5.6.2.0 Test group objective

The test group addresses the provision:

In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.

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 comply to standardised 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

Test purpose

The purpose of this test case is to assess whether security-relevant information disclosed by logical interfaces without authentication in the initialized state is properly identified and whether disclosure of the information is necessary for device operation.

Test actions

Assessing the conformity of design of the disclosed information described in the IXIT documentation.

> **Test units**
>
> For each logical interface in **IXIT 5.6-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.
>
> For each logical interface in **IXIT 5.6-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 device operation.

Assignment of verdict

The verdict FAIL is assigned if

- for any logical interface, there is information disclosed by the interface without authentication in the initialized state that is security-relevant and not documented as such; OR
- for any logical interface, there is security-relevant information disclosed by the interface without authentication in the initialized state that is not necessary for device operation.

The verdict PASS is assigned if

- for every logical interface, there is no information disclosed by the interface without authentication in the initialized state that is security-relevant and not documented as such; AND
- for every logical interface, all security-relevant information disclosed by the interface without authentication in the initialized state is necessary for device operation.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.2.2 Test case 5.6-2-2

Test purpose

The purpose of this test case is to assess whether information disclosed by the logical interfaces of the DUT in the initialized state and without authentication matches the description in the IXIT documentation.

Test actions

Assessing the conformity of implementation of the information disclosed by the logical interfaces of the DUT in the initialized state and without authentication.

> **Test units**
>
> For each logical interface in **IXIT 5.6-Intf**, the TL **shall** assess whether 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 FAIL is assigned if

- for any logical interface, information can be observed that is not described in the IXIT documentation

The verdict PASS is assigned if

- for every logical interface, only information can be observed that is described in the IXIT documentation

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.3 Test group 5.6-3

5.6.3.0 Test group objective

The test group addresses the provision:

Device hardware should not unnecessarily expose physical interfaces to attack.

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).

It is to be noted that protection through the casing is not efficient for physical 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, firstly, whether physical port and/or air interfaces that never require exposure are protected by the device casing, secondly, whether physical air interfaces that never require exposure are disabled and, thirdly, whether physical interfaces that are exposed but intermittently necessary are disabled by default and can be enabled and disabled via a trusted mechanism.

5.6.3.1 Test case 5.6-3-1

Test purpose

The purpose of this test case is to assess whether the protection of physical port and/or air interfaces conforms to the provision.

Test actions

Assessing the conformity of design of physical interfaces that do not require exposure.

> **Test units**
>
> For each physical interface in **IXIT 5.6-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.
>
> NOTE: For physical air interfaces it is acceptable that the antenna part remains outside of the device casing.
>
> For each physical air interface in **IXIT 5.6-Intf** that does not require exposure according to "Description", the TL **shall** assess whether the interface is disabled according to "Status".

Assessing the conformity of design of physical interfaces that do not require permanent exposure.

> **Test units**
>
> For each physical interface in **IXIT 5.6-Intf** that does not require permanent exposure according to "Description", the TL **shall** assess whether the interface is disabled by default according to "Status".
>
> For each physical interface in **IXIT 5.6-Intf** that does not require permanent exposure according to "Description", the TL **shall** assess whether the interface can be enabled and disabled via a trusted mechanism.

Assignment of verdict

The verdict FAIL is assigned if

- for any physical interface that does not require exposure, the protection means of the interface does not include protection by the device casing; OR
  for any physical air interface that does not require exposure, the interface is not disabled; OR

- for any physical interface that does not require permanent exposure, the interface is not disabled by default; OR
- for any physical interface that does not require permanent exposure, there is no trusted mechanism to enable and disable the interface.

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; AND
- for every physical 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 by default; AND
- for any physical interface that does not require permanent exposure, there is a trusted mechanism to enable and disable the interface.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.3.2 Test case 5.6-3-2

Test purpose

The purpose of this test is to assess whether physical interfaces on the DUT and their protection match the description provided in the IXIT documentation.

Test actions

Assessing the conformity of implementation of the physical interfaces of the DUT.

> **Test units**
>
> For each physical interface identified on the DUT the TL **shall** assess whether exposed physical interfaces on the DUT are described as required or intermittently required in "Description" of **IXIT 5.6-Intf**.
>
> For each physical interface identified on the DUT that does not require exposure according to "Description" the TL **shall** inspect whether physical interfaces on the DUT are protected by device casing.
>
> NOTE: For physical air interfaces it is acceptable that the antenna part remains outside of the device casing.
>
> For each physical interface identified on the DUT the TL **shall** inspect whether physical air interfaces on the DUT are enabled or disabled as indicated in "Status" in **IXIT 5.6-Intf**.
>
> For each physical interface identified on the DUT the TL **shall** inspect whether a trusted mechanism exist on the DUT to enable or disable physical interfaces that are not permanently required.

Assessing the completeness of the IXIT documentation.

> **Test units**
>
> The TL **shall** assess whether all exposed physical interfaces and all physical air interfaces on the DUT have been accounted for in **IXIT 5.6-Intf**.

Assignment of verdict

The verdict FAIL is assigned if

- for any exposed physical interface on the DUT, the interface is not described as "required" or "intermittently required" in the IXIT documentation; OR
- for any physical interface that is identified as never requiring exposure in the IXIT documentation, the interface is not protected by the device casing; OR
- for any physical air interface that is enabled on the DUT, the interface is not marked as "required" or "intermittently required" in the IXIT documentation; OR
- for any physical interface that is marked as "intermittently required" in the IXIT documentation, there is not a trusted mechanism on the DUT to enable and disable the interface; OR
- for any exposed physical port interface on the DUT, there is no information for the interface in the IXIT documentation; OR
- for any physical air interface on the DUT, there is no information for the interface in the IXIT documentation.

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; AND
- all physical 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, there is a trusted mechanism on the DUT to enable and disable the interface; AND
- for all exposed physical port interfaces on the DUT, there is information for the interface in the IXIT documentation; AND
- for all physical air interfaces on the DUT, there is information for the interface in the IXIT documentation.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.4 Test group 5.6-4

5.6.4.0 Test group objective

The test group addresses the provision:

Where a debug interface is physically accessible, it shall be disabled in software.

CONDITIONAL: The TL **shall** apply this test group only if a debug interface is physically accessible.

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 could be permanently disabled in software or, if it is foreseen that the it may 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

Test purpose

The purpose of this test case is to assess whether physically accessible debug interfaces are disabled in software in the IXIT documentation.

Test actions

Assessing the conformity of design of the control of physically accessible debug interfaces by software.

> **Test units**
>
> For each physical interface in **IXIT 5.6-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.
>
> For each physical interface in **IXIT 5.6-Intf** that is described as an accessible debug interface, that is not indicated as intermittently required according to “Description”, the TL **shall** assess whether the interface is disabled permanently according to “Status”.
>
> For each physical interface in **IXIT 5.6-Intf** that is described as an accessible debug interface, that is indicated as intermittently required according to “Description”, the TL **shall** assess whether the interface is disabled by default according to “Status”.

Assignment of verdict

The verdict FAIL is assigned if

- for any accessible physical debug interface, there is no software mechanism described to disable the interface; OR
- for any accessible physical debug interface that is not indicated as intermittently required, the interface is not permanently disabled; OR
- for any accessible physical debug interface that is indicated as intermittently required, the interface is not disabled by default.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.4.2 Test case 5.6-4-2

Test purpose

The purpose of this test case is to assess whether physically accessible debug interfaces on the DUT are disabled.

Test actions

Assessing the completeness of the IXIT information.

> **Test units**
>
> For each accessible physical interface on the DUT the TL **shall** inspect whether the interface can be used for debugging purposes although it is not indicated as "Debug Interface" in **IXIT 5.6-Intf**.
>
> NOTE 1: For this test unit the TL may attempt to use the interface as a debug interface using standard methods and tools.

Assessing the conformity of implementation of the status of physically accessible debug interfaces on the DUT.

> **Test units**
>
> For each accessible physical interface on the DUT indicated as "Debug Interface" in **IXIT 5.6-Intf**, the TL **shall** inspect whether the interface is disabled.
>
> NOTE 2: For this test unit the TL is to ensure that the interface is in its default state.

Assignment of verdict

The verdict FAIL is assigned if

- a physical interface can be used as debug interface and is not indicated as such in the IXIT; OR
- any accessible physical debug interface is not disabled.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.5 Test group 5.6-5

5.6.5.0 Test group objective

The test group addresses the provision:

The manufacturer should only enable software services that are used or required for the intended use or operation of the device.

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 though such service may actually be 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 may be services that are enabled by default by an IoT platform provider. In such situation the SO may list the services that are enabled along with a reason why they are.

5.6.5.1 Test case 5.6-5-1

Test purpose

The purpose of this test case is to assess whether the enabled software services are necessary for the intended use or operation of the device.

Test actions

Assessing the conformity of design of the enabled services with regard to the intended use or operation of the device.

> **Test units**
>
> For each software service in **IXIT 5.6-SoftServ** that is enabled according to "Status", the TL **shall** assess whether the service is necessary for the intended use or operation of the device according to the purpose in "Description" and the "Justification" for enabling the service.

Assignment of verdict

The verdict FAIL is assigned if

- for any enabled software service, the service is not necessary for the intended use or operation of the device.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.6 Test group 5.6-6

5.6.6.0 Test group objective

The test group addresses the provision:

Code should be minimized to the functionality necessary for the service/device to operate.

There exist many options to minimize code. Within large software projects, automated tools may 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 may give options to what is included in the packaging, compilation or installation of their software.

Code minimization may be assessed in terms of effectiveness, i.e. 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] may be referred to.

5.6.6.1 Test case 5.6-6-1

Test purpose

The purpose of this test case is to assess whether the code minimization techniques described in the IXIT documentation are effective.

Test actions

Assessing the conformity of design of code minimization techniques.

> **Test units**
>
> For each code minimization technique in **IXIT 5.6-CodeMin** the TL **shall** assess whether the technique can help in minimizing code.
>
> For each code minimization technique in **IXIT 5.6-CodeMin** the TL **shall** assess whether the application of the technique has resulted in a reduction of code that reduces the security risk.

Assignment of verdict

The verdict FAIL is assigned if

- for any code minimization technique, the technique cannot help in minimizing code; OR
- for any code minimization technique, the application of the technique has not resulted in a reduction of code that reduces the security risk.

The verdict PASS is assigned if

- for every code minimization technique, the technique can help in minimizing code; AND
- for every code minimization technique, the application of the technique has resulted in a reduction of code that reduces the security risk.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.7 Test group 5.6-7

5.6.7.0 Test group objective

The test group addresses the provision:

Software should run with least necessary privileges, taking account of both security and functionality.

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 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

Test purpose

The purpose of this test case is to assess whether the privilege control mechanisms described in the IXIT allow to implement the separation of duty, need to know and minimization of privilege principles.

Test actions

Assessing the conformity of design of the mechanisms to control privileges of software on the DUT.

> **Test units**
>
> The TL **shall** assess whether the combination of each mechanism to control privileges of software on the DUT in **IXIT 5.6-PrivlCtrl** facilitates the principles of separation of duty, need to know and minimization of privilege.

Assignment of verdict

The verdict FAIL is assigned if

- the described privilege control mechanisms are not adequate to facilitate the principles of separation of duty, need to know and minimization of privilege.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.8 Test group 5.6-8

5.6.8.0 Test group objective

The test group addresses the provision:

The device should include a hardware-level access control mechanism for memory.

Many options exists that may be combined to provide hardware-level access control mechanisms for memory. At the level of grey-box testing this may be evaluation based on documentation provided by the manufacturer (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, firstly, whether the identified hardware-level mechanisms do provide for access control to memory and, secondly, whether these are used by the device software.

5.6.8.1 Test case 5.6-8-1

Test purpose

The purpose of this test case is to assess whether the device hardware-level mechanisms for access control to memory are effective.

Test actions

Assessing the conformity of design of hardware-level mechanisms for access control to memory.

> **Test units**
>
> For each hardware-level access control mechanism for memory in **IXIT 5.6-AccCtrl**, the TL **shall** assess whether the mechanism is implemented at the level of the hardware.
>
> NOTE: Implementation at the level of the hardware may include software embedded in the hardware.
>
> For each hardware-level access control mechanism for memory in **IXIT 5.6-AccCtrl**, the TL **shall** assess whether the mechanism allows to control access to memory.

Assignment of verdict

The verdict FAIL is assigned if

- for any hardware-level access control mechanism for memory, the mechanism is not implemented at the level of the hardware; OR
- for any hardware-level access control mechanism for memory, the mechanism does not allow to control access to memory.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.9 Test group 5.6-9

5.6.9.0 Test group objective

The test group addresses the provision:

The manufacturer should follow secure development processes for software deployed on the device.

5.6.9.1 Test case 5.6-9-1

Test purpose

The purpose of this test case is to assess whether the described secure development processes are conformant to the requirements of the provision.

Test actions

Assessing conformity of design of the secure development processes.

> **Test units**
>
> The TL **shall** assess whether the secure development of software covers
>
> - security training of developers,
> - the requirement and design phases of the software,
> - secure coding techniques and security tooling for the implementation phase,
> - security testing,
> - security review as well as archival of assets and information relevant to maintaining security of the software before the software is released,
> - secure deployment and incident response processes, and
> - handling of third-party software providers
>
> according to the processes in **IXIT 5.6-SecDev**.

Assignment of verdict

The verdict FAIL is assigned if the secure development does not cover

- security training of personnel; OR
- the requirement and design phases of the software; OR
- secure coding techniques and security tolling for the implementation phase; OR
- security testing; OR
- security reviews or archival of assets and information relevant to maintaining security of the software before the software is released; OR
- secure deployment and incident response processes; OR
- handling of third-party software providers.

The verdict PASS is assigned if the secure development covers

- security training of personnel; OR
- the requirement and design phases of the software; OR
- secure coding techniques and security tolling for the implementation phase; OR
- security testing; OR
- security reviews or archival of assets and information relevant to maintaining security of the software before the software is released; OR
- secure deployment and incident response processes; OR
- handling of third-party software providers.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.6.9.2 Test case 5.6-9-2

Test purpose

The purpose of this test case is to assess whether the secure development processes are applied as described.

Test actions

Assessing conformity of implementation of the secure development processes.

> **Test units**
>
> The TL **shall** collect evidence for the application of the secure development processes. Such evidence includes, but is not limited to,
>
> - management audit reports, or
> - records of the secure development processes, or
> - taking minutes of an interview with at least one person (that is part of the process) concerning how the secure development processes are established.
>
> TL **shall** examine the collected evidence in order to determine that the secure development processes are applied in accordance with their "Description" in **IXIT 5.6-SecDev**.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any secure development process is not applied in accordance with its description.

The verdict PASS is assigned if

- there are no indications that any secure development process is not applied in accordance with its description.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.7 TSO 5.7: Ensure software integrity

5.7.0 IXIT proforma TSO 5.7

IXIT 5.7-SecBoot: Secure Boot Mechanisms

This IXIT lists all secure boot mechanisms of the DUT. It may be 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 ("SecBoot-1") or labelling scheme ("SecBoot-TEE").

- **Description**: Brief description of the mechanism (incl. 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 realised security objectives of the mechanism.

  EXAMPLE 2: The mechanisms realises 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 2: 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) are possible ways to inform the user.

- **Notification Functionality**: Brief description of the network functionalities necessary to notify a user.

  EXAMPLE 3: SMTP protocol (in case of email notifications), RFCOMM protocol details (in case of Bluetooth notifications).

5.7.1 Test group 5.7-1

5.7.1.0 Test group objective

The test group addresses the provision:

The consumer IoT device should verify its software using secure boot mechanisms.

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

NOTE : Threat modelling and the baseline attacker model described in Annex A is 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

Test purpose

The purpose of this test case is to assess whether the secure boot mechanisms are suitable to verify the claimed software based on the provided security guarantees.

Test actions

Assessing the conformity of design of the secure boot mechanisms.

> **Test units**
>
> The TL **shall** assess whether the "Security Guarantees" of each secure boot mechanism in **IXIT 5.7-SecBoot** provide at least verification of integrity and authenticity of device software.
>
> The TL **shall** assess whether for each secure boot mechanism in **IXIT 5.7-SecBoot** the "Description" and corresponding "Detection Mechanisms" are suitable to provide the "Security Guarantees" it is used.

Assignment of verdict

The verdict FAIL is assigned if

- any secure boot mechanism does not provide the security guarantees of integrity or authenticity verification of the device software; OR
- any secure boot mechanism and its detection mechanisms is not suitable to provide the described security guarantees.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.7.1.2 Test case 5.7-1-2

Test purpose

The purpose of this test case to functionally verify that the mechanisms for the verification of the software is applied as described.

Test actions

Assessing the conformity of implementation of the secure boot mechanisms.

> **Test units**
>
> The TL **shall** inspect whether the verification of the device software is implemented according to the information in **IXIT 5.7-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.

Assignment of verdict

The verdict FAIL is assigned if

- indications are found, that any secure boot mechanism is not implemented as described in the IXIT.

The verdict PASS is assigned if

- no indications are found, that any secure boot mechanism is not implemented as described in the IXIT.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.7.2 Test group 5.7-2

5.7.2.0 Test group objective

The test group addresses the provision:

If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.

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.

5.7.2.1 Test case 5.7-2-1

Test purpose

The purpose of this test case is to assess the alerting and restricting mechanisms in case of detecting an unauthorized software change.

Test actions

Assessing the conformity of design of the alerting mechanisms.

> **Test units**
>
> 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.

Assessing the conformity of design of the communication restriction.

> **Test units**
>
> The TL **shall** assess whether every “Notification Functionality” in **IXIT 5.7-SecBoot** is necessary for the described method of “User Notification”.

Assignment of verdict

The verdict FAIL is assigned if

- the described way of user notification is not sufficient to inform the user and/or administrator about unauthorized changes in device software; OR
- any described notification functionality is not necessary for the user notification in case of detecting unauthorized software changes.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.7.2.2 Test case 5.7-2-2

Test purpose

The purpose of this test case is to assess whether alerting and restricting mechanisms in case of detecting an unauthorized software change are implemented according to the IXIT.

Test actions

Assessing the conformity of implementation of the alerting mechanisms.

> **Test units**
>
> The TL **shall** inspect whether alerting takes place as described in "User Notification" in **IXIT 5.7-SecBoot** after the detection of an unauthorised change in device software.

Assessing the conformity of implementation of the communication restriction.

> **Test units**
>
> The TL **shall** functionally evaluate whether the communication capabilities of the DUT to wider networks are restricted to the ones described in "Notification Functionality" in **IXIT 5.7-SecBoot** after the detection of an unauthorised change in device software.
>
> NOTE: Methods for functional evaluation of the communication capacities may 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 FAIL is assigned if

- there are indications that any alerting mechanism of the DUT is not implemented as described; OR
- any communication to wider networks is detected after detection of unauthorised changes, that is not described as necessary.

The verdict PASS is assigned if

- there are no indications that any alerting mechanism of the DUT is not implemented as described; AND
- only communication to wider networks is detected after detection of unauthorised changes, that is described as necessary.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.8 TSO 5.8: Ensure that personal data is secure

5.8.0 IXIT proforma TSO 5.8

IXIT 5.8-PersData: Personal Data

This IXIT lists all personal data communicated by the DUT. It may be 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 ("PersData-1") or labelling scheme ("PersData-PayInfo").

- **Description**: Brief description of the category of personal data being communicated by the DUT.

  EXAMPLE 2: Configuration settings of the DUT, log data on the usage of the DUT, payment information, timestamped location data, audio input stream or biometric data.

  NOTE 1: 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 2: 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 3: Advertisement (direct marketing) is a form of communicating an offer, where organizations communicate directly to a pre-selected customer and supply a method for a direct response.

- **Communication Mechanisms**: Reference to communication mechanisms in **IXIT 5.5-ComMech** that are used for communicating the personal data and an indication of the recipient.

- **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 5.8-ExtSens: External Sensors

This IXIT lists all external sensing capabilities of the DUT. It may be 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 3: Sequential numbering ("ExtSens-1") or labelling scheme ("ExtSens-Cam").

- **Description**: Brief description of the sensing capability.

  NOTE 4: Such sensing capabilities may be a microphone or camera.

IXIT 5.8-SensInfo: User Information

- **Publication 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 5: Possible ways of publication are the website of the manufacturer and the corresponding URL and the user manual.

5.8.1 Test group 5.8-1

5.8.1.0 Test group objective

The test group addresses the provision:

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

In difference to test group 5.5-1, the use case in this provision is precised on the communication of personal data, which requires at least confidentiality and authenticity.

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

Test purpose

The purpose of this test case is to assess the use of best practice cryptography for all communication mechanisms transmitting personal data.

Test actions

Assessing the conformity of design of the stated cryptography to be suitable for the communication of personal data.

> **Test units**
>
> For all "Communication Mechanisms" in **IXIT 5.5-ComMech** referenced in any personal data in **IXIT 5.8-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 and authenticity is required to be fulfilled.

Assignment of verdict

The verdict FAIL is assigned if for any communication mechanism used for communicating personal data

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

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

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.8.1.2 Test case 5.8-1-2

The purpose of this test case is to functionally evaluate the use of the described cryptography.

Test actions

Assessing the conformity of implementation of the used cryptography.

> **Test units**
>
> For all "Communication Mechanisms" in **IXIT 5.5-ComMech** referenced in any personal data in **IXIT 5.8-PersData**, the TL **shall** apply all test units as specified in the test case 5.5-1-2.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that any used cryptographic setting is not as described.

The verdict PASS is assigned if

- there are no indications that any used cryptographic setting is not as described.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.8.2 Test group 5.8-2

5.8.2.0 Test group objective

The test group addresses the provision:

The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.

In difference to test group 5.5-1 and 5.8-1, the use case in this provision is precised on the communication of critical security parameters between the device and associated services, which requires at least confidentiality and authenticity.

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

Test purpose

The purpose of this test case is to assess the use of best practice cryptography for all communication mechanisms transmitting sensitive personal data between the device and associated services.

Test actions

Assessing the conformity of design of the stated cryptography to be suitable for the communication of sensitive personal data between the device and associated services.

> **Test units**
>
> For all “Communication Mechanisms” in **IXIT 5.5-ComMech** referenced in any sensitive personal data in **IXIT 5.8-PersData** according to “Sensitive”, where the recipient 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 and authenticity is required to be fulfilled.

Assignment of verdict

The verdict FAIL is assigned if for any communication mechanism used for communicating sensitive personal data between the device and an associated service

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

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 not appropriate for the use case of communicating sensitive personal data between the device and an associated service; AND
- the mechanism is not appropriate to achieve the security guarantees with respect to the use case; AND

- any used cryptographic details are not considered as best practice for the use case; AND
- any used cryptographic details are known to be vulnerable to a feasible attack.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.8.2.2 Test case 5.8-2-2

Test purpose

The purpose of this test case is to functionally evaluate the use of the described cryptography.

Test actions

Assessing the conformity of implementation of the used cryptography.

> **Test units**
>
> For all "Communication Mechanisms" in **IXIT 5.5-ComMech** referenced in any sensitive personal data in **IXIT 5.8-PersData** according to "Sensitive", where the recipient 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 FAIL is assigned if

- there are indications that any used cryptographic setting is not as described.

The verdict PASS is assigned if

- there are no indications that any used cryptographic setting is not as described.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.8.3 Test group 5.8-3

5.8.3.0 Test group objective

The test group addresses the provision:

All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.

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, and document it 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 device 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 device.

5.8.3.1 Test case 5.8-3-1

Test purpose

The purpose of this test case is to make sure the external sensing capabilities are documented in the fashion the documentation states.

Test actions

Assessing the conformity of implementation of the documentation of external sensing capabilities.

Test units

The TL **shall** functionally verify that the documentation of external sensing capabilities is accessible as documented in "Publication of Sensors" in **IXIT 5.8-SensInfo**.

NOTE 1: This can be done by accessing the documentation according to the IXIT information.

The TL **shall** inspect whether the documentation of external sensing capabilities as documented in "Publication of Sensors" in **IXIT 5.8-SensInfo** is understandable for a user without technical knowledge.

Assessing the completeness of the IXIT documentation.

The TL **shall** inspect whether all obvious sensing capabilities of the DUT are documented in **IXIT 5.8-ExtSens**.

NOTE 2: Such check can include a visual inspection of the DUT for detecting obvious sensors.

Assignment of verdict

The verdict FAIL is assigned if

- the documentation is not accessible according to the IXIT; OR
- the documentation is not understandable for a user without technical knowledge; OR
- at least one obvious sensing capability provided by the DUT is not documented.

The verdict PASS is assigned if

- the documentation is accessible according to the IXIT; AND
- the documentation is understandable for a user without technical knowledge; AND
- each obvious sensing capability provided by the DUT is documented.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.9 TSO 5.9: Make systems resilient to outages

5.10 TSO 5.10: Examine system telemetry data

5.10.0 IXIT proforma TSO 5.10

IXIT 5.10-TelData: Telemetry Data

This IXIT lists all telemetry data collected by the DUT. It may be 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: Sequential numbering ("TelData-1") or labelling scheme ("TelData-CrashLog").

- **Description**: Brief description of the telemetry data being collected.

- **Collector**: Description of functions and services that collect the telemetry data. It is indicated additionally for what purpose the data is collected.

- **Security Examination**: Description of how the telemetry data are examined for security anomalies and how it helps the manufacturer to identify issues or information related to device usage.

  NOTE 1: The security anomaly examination may be realised outside the DUT, i.e. by associated services.

  NOTE 2: A device telemetry service (collector) 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 5.8-PersData** that are processed in the telemetry data.

5.10.1 Test Group 5.10-1

5.10.1.0 Test group objective

The test group addresses the provision:

If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.

CONDITIONAL: The TL **shall** apply this test group only if telemetry data is collected.

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

EXAMPLE: A consumer IoT device reports software malfunctions to the manufacturer enabling them to identify and remedy the cause.

5.10.1.1 Test case 5.10-1-1

Test purpose

The purpose of this test case is the evaluation of the suitability of the security anomaly examination that is applied to the telemetry data collected from the device.

Test actions

Assessing the conformity of design of the security anomaly examination.

> **Test units**
>
> For each “Collector” of telemetry data in **IXIT 5.10-TelData**, the TL **shall** assess whether it is suitable for the collection of the associated telemetry data in “Description”.
>
> For each “Security Examination” of telemetry data in **IXIT 5.10-TelData**, the TL **shall** assess whether the associated telemetry data in “Description” are suited for the described security examination.
>
> For each “Security Examination” of telemetry data in **IXIT 5.10-TelData**, the TL **shall** assess whether it is suited to help the manufacturer identify issues or information related to device usage.

Assignment of verdict

The verdict FAIL is assigned if

- at least one telemetry collector is not suited for collecting the associated telemetry data; OR
- at least one security anomaly examination is not suited for examining the associated telemetry data; OR
- at least one security anomaly examination is not suited to help the manufacturer identify issues or information related to device usage.

The verdict PASS is assigned if

- each telemetry collector is suited for collecting the associated telemetry data; AND
- each security anomaly examination is suited for examining the associated telemetry data; AND
- each security anomaly examination is suited to the manufacturer identify issues or information related to device usage.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.10.1.2 Test case 5.10-1-2

Test purpose

The purpose of this test case is to assess by functional evaluation whether the IXIT is complete and correct, i. e. whether all telemetry data that is collected from the DUT is examined for security anomalies.

Test actions

Assessing the conformity of implementation of the security anomaly examination.

> **Test units**
>
> For each "Collector" of telemetry data in **IXIT 5.10-TelData**, the TL **shall** functionally verify that all associated telemetry data in "Description" is actually collected.
>
> For each "Collector" of telemetry data in **IXIT 5.10-TelData**, the TL **shall** functionally verify that all telemetry data collected from the DUT is actually documented in "Description".
>
> The TL **shall** collect evidence for the application of the "Security Examination" as described in **IXIT 5.10-TelData**. Such evidence includes, but is not limited to,
>
> - management audit reports, or
> - records of the security anomaly examination, or
> - taking minutes of an interview with a least one person (that is part of the process) concerning how the process is applied.
>
> TL **shall** examine the collected evidence in order to determine that the "Security Examination" is applied in accordance with its description in **IXIT 5.10-TelData**.

Assignment of verdict

The verdict FAIL is assigned if

- for at least one telemetry collector and associated telemetry data the collected telemetry data differs from its description in the IXIT; OR
- there are indications that at least one security anomaly examination is not applied in accordance with it description in the IXIT.

The verdict PASS is assigned if

- for each telemetry collector and associated telemetry data the collected telemetry data coincides with its description in the IXIT; AND
- there are no indications that any security anomaly examination is not applied in accordance with it description in the IXIT.

Otherwise, the verdict INCONCLUSIVE is assigned.

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

5.11.0 IXIT proforma TSO 5.11

IXIT 5.11-ErasFunc: Erasure Functionalities

- **ID**: Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

  EXAMPLE 1: Sequential numbering ("ErasFunc-1") or labelling scheme ("ErasFunc-Config").

- **Description**: Brief description of the functionality used to erase user data, including the concerning user data, which will be erased by applying the functionality.

  NOTE 1: Such user data may be configuration data, cryptographic material or personal data.

  NOTE 2: A functionality to erase user data may be a factory reset, which overwrites all user data with a random value.

- **Initiation and Interaction**: Brief description of the user interaction, which is necessary to initiate and apply the erasing functionality.

5.11.1 Test group 5.11-1

5.11.1.0 Test group objective

The test group addresses the provision:

The user shall be provided with functionality such that user data can be erased from the device in a simple manner.

5.11.1.1 Test case 5.11-1-1

Test purpose

The purpose of this test case is to assess whether the user data erasure functionalities are conformant to the requirements of the provision.

Test actions

Assessing conformity of design of the user data erasure functionalities.

> **Test units**
>
> The TL **shall** assess whether at least one functionality is provided according to **IXIT 5.11-ErasFunc**, which can be performed by the user without technical knowledge according to "Description" and "Initiation and Interaction" to erase user data.
>
> The TL **shall** assess whether each functionality in **IXIT 5.11-ErasFunc** is adequate to erase the targeted user data.
>
> NOTE 1: Erasure can be realised by overwriting with a pre-defined value or by internal permanent blocking of all access to the data on the device.
>
> The TL **shall** assess whether the functionalities to erase user data in **IXIT 5.11-ErasFunc** cover personal data, user configuration and cryptographic material such as passwords or keys stored in the device.
>
> NOTE 2: The information in **IXIT 5.4-SecParam**, **IXIT 5.8-PersData** and other IXITs is helpful to identify user data.

Assignment of verdict

The verdict FAIL is assigned if

- no simple functionality to erase user data is provided to the user; OR
- the described functionality is not adequate to erase the targeted user data; OR
- personal data, user configuration or cryptographic material is not covered by the functionalities to erase user data.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

5.11.1.2 Test case 5.11-1-2

Test purpose

The purpose of this test case is to assess whether the user data erasure functionalities are implemented as described on the DUT.

Test actions

Assessing conformity of implementation of user data erasure functionalities of the DUT.

Test units

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

NOTE 1: Such data can be personal data, user configuration or cryptographic material such as user passwords or keys, which differ from the standard configuration.

The TL **shall** perform each functionality to erase user data in **IXIT 5.11-ErasFunc** and evaluate whether the "Initiation and Interaction" is as described in the IXIT.

The TL **shall** perform each functionality to erase user data in **IXIT 5.11-ErasFunc** and verify whether the corresponding user data still exists after completing the operation.

NOTE 2: The comparison between the configuration before and after the erasure may be helpful to identify not erased user data.

Assignment of verdict

The verdict FAIL is assigned if for any functionality to erase user data

- the initiation and interaction of the user differs from the descriptions in the IXIT; OR
- there are indications that the corresponding user data is not erased successfully.

The verdict PASS is assigned if for any functionality to erase user data

- the initiation and interaction of the user is as described in the IXIT; AND
- there are no indications that the corresponding user data is not erased successfully.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.12 TSO 5.12: Make installation and maintenance of devices easy

5.13 TSO 5.13: Validate input data

5.13.0 IXIT proforma TSO 5.13

IXIT 5.13-UserIntf: User Interfaces

This IXIT lists all user interfaces of the DUT, which enable input from the user. It can be 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 ("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 5.13-InpVal: Data Input Validation

This IXIT lists all data input validation methods of the DUT. It can be 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 2: 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. It is indicated additionally which of the sources for data input are addressed by the method.

  NOTE: To validate the data input, it may be checked whether it is of an allowed type (format and structure), of allowed value, an allowed cardinality or an allowed ordering.

5.13.1 Test group 5.13-1

5.13.1.0 Test group objective

The test group addresses the provision:

The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

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

Test purpose

The purpose of this test case is to assess whether the data input validation methods are conformant to the requirements of the provision.

Test actions

Assessing conformity of design of the data input validation methods.

> **Test units**
>
> The TL **shall** assess whether the combination of data input validation methods in **IXIT 5.13-InpVal** covers all sources for data input according to the user interfaces in **IXIT 5.13-UserIntf** and APIs and network communications, which receive data input according to the corresponding remotely accessible communication methods in **IXIT 5.5-ComMech**.
>
> For each data input validation method in **IXIT 5.13-InpVal**, the TL **shall** assess whether it is effective to validate 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 FAIL is assigned if

- the data input validation methods do not cover data input via user interfaces, transmitted via APIs or between networks in services and devices; OR
- any described data input validation method is not effective for validating the corresponding data input.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

5.13.1.2 Test case 5.13-1-2

Test purpose

The purpose of this test case is to functionally assess whether the data input validation methods are implemented as described.

Test actions

Assessing the conformity of implementation of the data input validation.

Test units

The TL **shall** choose randomly a representative number of sources for data input and devise functional attacks to misuse the data input based on the "Description" of its data input validation method in **IXIT 5.13-InpVal**.

NOTE 1: Ideally at least one source of data input may be chosen from each category, i.e. one user interface, one API and one communication method transferring data input between networks in services and the devices.

The TL **shall** attempt to misuse each data input validation method in **IXIT 5.13-InpVal** on the base of the devised misuse action and evaluate whether the validation methods protect against the action.

NOTE 2: Automated tools may be used to find data which does not suit to the expected input, e.g. in format and structure, value, cardinality or ordering.

Assessing the completeness of the user interfaces and APIs.

Test units

The TL **shall** functionally evaluate whether all user interfaces of the DUT are described in **IXIT 5.13-UserIntf** according to the documentation for the user, e.g. user manual.

The TL **shall** functionally evaluate whether all APIs of the DUT are covered by a communication method described in **IXIT 5.5-ComMech**.

NOTE 3: APIs using remotely accessible communication may be found using a port scanner.

Assignment of verdict

The verdict FAIL is assigned if

- there are indications that data input via user interfaces, transmitted via APIs or between networks in services and devices is not validated accordingly; OR
- user interfaces are found, which are not documented in the IXIT; OR
- APIs are found, which are remotely accessible, but their communication mechanism is not described in the IXIT.

The verdict PASS is assigned if

- there are no indications that data input via user interfaces, transmitted via APIs or between networks in services and devices is not validated accordingly; OR
- no user interfaces are found, which are not documented in the IXIT; OR
- no APIs are found, which are remotely accessible, and their communication mechanism is not described in the IXIT.

Otherwise, the verdict INCONCLUSIVE is assigned.

6 TSO 6: Data protection test scenario for consumer IoT

6.0 IXIT proforma TSO 6

IXIT 6-DataInfo: User Information

The entries in this IXIT are independent from each other. These entries may be filled out in form of a list.

- **Publication 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 1: Possible ways of publication are the website of the manufacturer and the corresponding URL and the user manual.

- **Publication 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 2: Possible ways of publication are the website of the manufacturer and the corresponding URL and the user manual.

6.1 Test group 6-1

6.1.0 Test group objective

The test group addresses the provision:

The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

6.1.1 Test case 6-1-1

Test purpose

The purpose of this test case is to verify that the information about the processing of personal data is clear and transparent and that this information is suitably provided to the consumer.

Test actions

Assessing the conformity of design concerning how the information about processing personal data is provided to the consumer.

> **Test units**
>
> The TL **shall** assess whether the "Publication of Personal Data" in **IXIT 6-DataInfo** is suitable for the consumer to obtain the information about processing personal data.

Assignment of verdict

The verdict FAIL is assigned if

- the information about processing personal data is not suitably provided to the consumer.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

6.1.2 Test case 6-1-2

Test purpose

The purpose of this test case is to verify that the information about the processing of personal data is actually provided to the consumer as described.

Test actions

Assessing the conformity of implementation concerning how the information about processing personal data is provided to the consumer.

> **Test units**
>
> The TL **shall** functionally verify that the information about processing personal data is provided as described "Publication of Personal Data" in **IXIT 6-DataInfo**.

Assessing the conformity of implementation concerning the processing of personal data.

> **Test units**

The TL **shall** functionally verify that the obtained information about processing personal data accessing the "Publication of Personal Data" in **IXIT 6-DataInfo** match their description in "Processing Activities" in **IXIT 5.8-PersData**.

The TL **shall** assess whether the obtained information clearly and transparently describes what personal data is processed.

The TL **shall** assess whether the obtained information clearly and transparently describe how personal data is being used, by whom, and for what purposes.

Assignment of verdict

The verdict FAIL is assigned if

- the information about processing personal data cannot be obtained as described; OR
- the obtained information about processing personal data does not match their description; OR
- the personal data being processed is not clearly and transparently described; OR
- it is not clearly and transparently described how personal data is being used, by whom, and for what purposes.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

6.2 Test group 6-2

6.2.0 Test group objective

The test group addresses the provision:

Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.

CONDITIONAL: The TL **shall** apply this test group only if personal data is processed on the basis of consumers' consent.

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 may be used for a specified purpose.

6.2.1 Test case 6-2-1

Test purpose

The purpose of this test case is to verify that consumers' consent to the processing of personal data is obtained in a valid way.

Test actions

Assessing the conformity of design of obtaining consumers' consent for the processing of personal data.

Test units

For each personal data in **IXIT 5.8-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 FAIL is assigned if for at least on category of personal data that is processed on the basis of consumers' consent

- it is not described how to express consent (opt-in choice) to the processing of personal data for specific purposes;
OR
- the opt-in choice is not given freely, obviously and explicitly.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

6.2.2 Test case 6-2-2

Test purpose

The purpose of this test case is to verify that consumers' consent to the processing of personal data is actually obtained as described.

Test actions

Assessing the conformity of implementation of obtaining consumers' consent to processing personal data.

> **Test units**
>
> For each personal data in **IXIT 5.8-PersData** that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** functionally verify that consumers' consent to processing personal data is obtained as described.

Assignment of verdict

The verdict FAIL is assigned if for at least on category of personal data that is processed on the basis of consumers' consent

- the way of obtaining consumers' consent doesn't match the description.

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 match the description.

Otherwise, the verdict INCONCLUSIVE is assigned.

6.3 Test group 6-3

6.3.0 Test group objective

The test group addresses the provision:

Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.

CONDITIONAL: The TL **shall** apply this test group only if personal data is processed on the basis of consumers' consent.

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.

6.3.1 Test case 6-3-1

Test purpose

The purpose of this test case is to verify that consumers' consent for the processing of personal data can be withdrawn at any time.

Test actions

Assessing the conformity of design of withdrawing consumers' consent to the processing of personal data.

> **Test units**
>
> For each personal data in **IXIT 5.8-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 FAIL is assigned if for at least on category of personal data that is processed on the basis of consumers' consent

- it is not described how to withdraw consent to the processing of personal data at any time.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

6.3.2 Test case 6-3-2

Test purpose

The purpose of this test case is to verify that consumers' consent to the processing of personal data can be actually withdrawn as described.

Test actions

Assessing the conformity of implementation concerning how consumers' consent to processing personal data is obtained.

> **Test units**
>
> For each personal data in **IXIT 5.8-PersData** that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** functionally verify that consumers' consent to processing personal data can be withdrawn as described in "Withdrawing Consent".

Assignment of verdict

The verdict FAIL is assigned if for at least on category of personal data that is processed on the basis of consumers' consent

- the way of withdrawing consumers' consent doesn't match the description.

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 match the description.

Otherwise, the verdict INCONCLUSIVE is assigned.

6.4 Test group 6-4

6.4.0 Test group objective

The test group addresses the provision:

If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.

CONDITIONAL: The TL **shall** apply this test group only if telemetry data is collected.

6.4.1 Test case 6-4-1

Test purpose

The purpose of this test case is to verify that the information about the processing of telemetry data is kept to the minimum necessary for the intended functionality.

Test actions

Assessing the conformity of design concerning the processing of telemetry data.

Test units

The TL **shall** assess whether the personal data in **IXIT 5.8-PersData** that are referenced in "Personal Data" in **IXIT 5.10-TelData** is necessary for the intended functionality as described in the purpose of collecting the data in "Collector".

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 FAIL is assigned if for at least on category of telemetry data

- their processing is not necessary for the intended functionality.

The verdict PASS is assigned if for each category of telemetry data

- their processing is necessary for the intended functionality.

Otherwise, the verdict INCONCLUSIVE is assigned.

6.5 Test group 6-5

6.5.0 Test group objective

The test group addresses the provision:

If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.

CONDITIONAL: The TL **shall** apply this test group only if telemetry data is collected.

6.5.1 Test case 6-5-1

Test purpose

The purpose of this test case is to verify that the information about the processing of telemetry data is completely and suitably provided to the consumer.

Test actions

Assessing the conformity of design concerning how the information about processing telemetry data is provided to the consumer.

Test units

The TL **shall** assess whether the "Publication of Telemetry Data" in **IXIT 6-DataInfo** is suitable for the consumer to obtain the information about processing telemetry data.

Assignment of verdict

The verdict FAIL is assigned if

- the information about processing telemetry data is not suitably provided to the consumer.

The verdict PASS is assigned if

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

Otherwise, the verdict INCONCLUSIVE is assigned.

6.5.2 Test case 6-5-2

Test purpose

The purpose of this test case is to verify that the information about the processing of telemetry data is actually provided to the consumer as described.

Test actions

Assessing the conformity of implementation concerning how the information about processing telemetry data is provided to the consumer.

Test units

The TL **shall** functionally verify that the information about processing telemetry data is provided as described in "Publication of Telemetry Data" in **IXIT 6-DataInfo**.

Assessing the conformity of implementation concerning the processing of telemetry data.

Test units

The TL **shall** functionally verify that the obtained information about processing telemetry data accessing the "Publication of Telemetry Data" in **IXIT 6-DataInfo** match their purpose described in "Collector" in **IXIT 5.10-TelData**.

The TL **shall** assess whether the obtained information describes what telemetry data is collected.

The TL **shall** assess whether the obtained information describes how telemetry data is being used, by whom, and for what purposes.

Assignment of verdict

The verdict FAIL is assigned if

- the information about processing telemetry data cannot be obtained as described; OR
- the obtained information about processing telemetry data does not match their description; OR
- the telemetry data being collected is not described; OR
- it is not completely described how telemetry data is being used, by whom, and for what purposes.

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.

Otherwise, the verdict INCONCLUSIVE is assigned.

Annex A (informative)

Threat model

Threat modeling is widely recognized as one of the most important activities in information systems security. Threat modeling informs the discovery of actions and sequences therereof that a malicious actor might undertake in order to impair, detriment, or otherwise compromise the value of an information system.

Threat modeling 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 may 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 could 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 [i.5], a threat is a potential cause of an incident that may 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 may 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 for security assurance and evaluation defined in ISO/IEC 15408 [i.5], [i.6], [i.7], [i.8] is one established approach.

The Threat, Vulnerability and Risk Analysis is another standard method used to develop a threat model [i.9]. 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 may exploit them, and the unwanted incidents that may result.

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.

Baseline Attacker Model

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 section.

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 characterised by a combination of ability and motivation of the attacker.

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.

Ability of the attacker

The ability of an attacker is characterised by expertise and resources. It is quantified as attack potential which is determined by the following factors (bearing resemblance to CC [i.10] and CEM [i.11]):

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 may 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 restricted information concerning the DUT, e.g. knowledge that is controlled within the developer organisation and shared with other organisations under a non-disclosure agreement.
Opportunity	Opportunity has a relationship to the elapsed time factor. Identification or exploitation of a vulnerability may require considerable amounts of access to a DUT that may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the DUT to exploit. Access may 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.	The acquisition is limited to specialised equipment that is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment, or development of more extensive attack scripts or programs.

Assurance levels

In alignment to widely accepted principles of risk management, the EU Cybersecurity Act [i.12] recommends that "the assurance level should be commensurate with the level of the risk associated with the intended use of an ICT product, ICT service or ICT process".

According to the EU Cybersecurity Act [i.12], the assurance level of a certification scheme is a basis for confidence that an ICT artefact, whether a product, a service or a process, meets specific security requirements (e.g. such as those of a specific European cybersecurity certification scheme). The EU Cybersecurity Act [i.5] considers that a European cybersecurity certification scheme should be able to specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each such European cybersecurity certificate might refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity might only refer to the assurance level 'basic'.

According to the EU Cybersecurity Act [i.4], the assurance levels would provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service or ICT process and would be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents.

The case for differentiated rigour and depth in evaluation applies in the case of embedded systems. Because there is no straightforward way to evaluate the hardware security of a semiconductor device, one applies different attack methods and observe the result [i.6]. The more attacks are tested, the more confidence one may have in the result. Therefore, in order to estimate the level of security protection several tamper protection levels are introduced [i.13].

Annex B

Identification of the DUT

Identification of the DUT **shall** be filled in so as to provide as much detail as possible regarding version numbers and configuration options. A person who can answer queries regarding information supplied in the ICS should be named as the contact person.

Date of the statement

DUT identification

DUT name:	
Brand/Trade Name(s) 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):	

The following documentation **shall** be declare and justify a constrained device.

Constrained Device	Yes/No
Justification	(detailed)

The justification **shall** match the requirements referring to this in ETSI TS 103 645 [1] / ETSI EN 303 645 [2].

SO

Name:	
Address:	
Telephone number:	
E-mail address:	
Additional information:	

ICS contact person

Name:	
Telephone number:	
E-mail address:	
Additional information:	

Annex C

As described in the assessment procedure in section 4.2, the following Table 4 describes for each provision which IXIT entries are required to perform the corresponding test group.

Provision	Required IXIT entries
4-1	(none)
5.1-1	**IXIT 5.1-AuthMech**: ID, Description, Authentication Factor, Password Generation Mechanism
5.1-2	**IXIT 5.1-AuthMech**: ID, Description, Authentication Factor, Password Generation Mechanism
5.1-3	**IXIT 5.1-AuthMech**: ID, Description, Security Guarantees, Cryptographic Details
5.1-4	**IXIT 5.1-AuthMech**: ID, Description **IXIT 5.1-AuthInfo**: Publication of Change Mechanisms
5.1-5	**IXIT 5.1-AuthMech**: ID, Description, Brute Force Prevention
5.2-1	**IXIT 5.2-VulnInfo**: Publication of Vulnerability Disclosure Policy
5.2-2	**IXIT 5.2-VulnTypes**: ID, Description, Process, Time Frame

5.2-3	**IXIT 5.2-VulnMon**: ID, Description **IXIT 5.2-VulnInfo**: Support Period
5.3-1	**IXIT 5.3-SoftComp**: ID, Description, Update Mechanism **IXIT 5.3-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details, Initiation and Interaction
5.3-2	**IXIT 5.3-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details, Initiation and Interaction
5.3-3	**IXIT 5.3-UpdMech**: ID, Description, Initiation and Interaction
5.3-4	**IXIT 5.3-UpdMech**: ID, Description, Initiation and Interaction, Configuration
5.3-5	**IXIT 5.3-UpdMech**: ID, Description, Update Checking
5.3-6	**IXIT 5.3-UpdMech**: ID, Description, Initiation and Interaction, Configuration, User Notification
5.3-7	**IXIT 5.3-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details
5.3-8	**IXIT 5.3-UpdProc**: ID, Description, Time Frame
5.3-9	**IXIT 5.3-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details
5.3-10	**IXIT 5.3-UpdMech**: ID, Description, Security Guarantees, Cryptographic Details
5.3-11	**IXIT 5.3-UpdMech**: ID, Description, User Notification
5.3-12	**IXIT 5.3-UpdMech**: ID, Description, User Notification
5.3-13	**IXIT 5.3-UpdInfo**: Publication of Support Period **IXIT 5.2-VulnInfo**: Support Period
5.3-14	**IXIT 5.3-UpdInfo**: Publication of Non-Updatable, Publication of Replacement
5.3-15	**IXIT 5.3-UpdInfo**: Publication of Replacement
5.3-16	**IXIT 5.3-UpdInfo**: Model Designation
5.4-1	**IXIT 5.4-SecParam**: ID, Description, Type, Security Guarantees, Protection Scheme
5.4-2	**IXIT 5.4-SecParam**: ID, Description, Type, Security Guarantees, Protection Scheme
5.4-3	**IXIT 5.4-SecParam**: ID, Description, Type, Provisioning Mechanism
5.4-4	**IXIT 5.4-SecParam**: ID, Description, Type, Generation Mechanism
5.5-1	**IXIT 5.5-ComMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-2	**IXIT 5.5-NetSecImpl**: ID, Description, Review/Evaluation Method, Report
5.5-3	**IXIT 5.3-SoftComp**: ID, Description, Update Mechanism, Cryptographic Usage **IXIT 5.3-UpdMech**: ID, Description
5.5-4	**IXIT 5.6-SoftServ**: ID, Description, Authentication Mechanism **IXIT 5.1-AuthMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-5	**IXIT 5.6-SoftServ**: ID, Description, Allows Configuration, Authentication Mechanism **IXIT 5.1-AuthMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-6	**IXIT 5.4-SecParam**: ID, Description, Type, Communication Mechanisms **IXIT 5.5-ComMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-7	**IXIT 5.4-SecParam**: ID, Description, Type, Communication Mechanisms **IXIT 5.5-ComMech**: ID, Description, Security Guarantees, Cryptographic Details
5.5-8	**IXIT 5.5-SecMgmt**: ID, Description
5.6-1	**IXIT 5.6-Intf**: ID, Description, Type, Status
5.6-2	**IXIT 5.6-Intf**: ID, Description, Type, Disclosed Information
5.6-3	**IXIT 5.6-Intf**: ID, Description, Type, Status, Protection
5.6-4	**IXIT 5.6-Intf**: ID, Description, Type, Status, Debug Interface, Protection
5.6-5	**IXIT 5.6-SoftServ**: ID, Description, Status, Justification
5.6-6	**IXIT 5.6-CodeMin**: ID, Description
5.6-7	**IXIT 5.6-PrivlCtrl**: ID, Description
5.6-8	**IXIT 5.6-AccCtrl**: ID, Description
5.6-9	**IXIT 5.6-SecDev**: ID, Description
5.7-1	**IXIT 5.7-SecBoot**: ID, Description, Security Guarantees, Detection Mechanisms
5.7-2	**IXIT 5.7-SecBoot**: ID, Description, User Notification, Notification Functionality
5.8-1	**IXIT 5.8-PersData**: ID, Description, Communication Mechanisms **IXIT 5.5-ComMech**: ID, Description, Security Guarantees, Cryptographic Details

5.8-2	**IXIT 5.8-PersData**: ID, Description, Processing Activities, Communication Mechanisms, Sensitive **IXIT 5.5-ComMech**: ID, Description, Security Guarantees, Cryptographic Details
5.8-3	**IXIT 5.8-ExtSens**: ID, Description **IXIT 5.8-SensInfo**: Publication of Sensors
5.9-1	tbd
5.9-2	tbd
5.9-3	tbd
5.10-1	**IXIT 5.10-TelData**: ID, Description, Collector, Security Examination
5.11-1	**IXIT 5.11-ErasFunc**: ID, Description, Initiation and Interaction
5.11-2	tbd
5.11-3	tbd
5.11-4	tbd
5.12-1	tbd
5.12-2	tbd
5.12-3	tbd
5.13-1	**IXIT 5.13-UserIntf**: ID, Description **IXIT 5.13-InpVal**: ID, Description **IXIT 5.5-ComMech**: ID, Description
6-1	**IXIT 6-DataInfo**: Publication of Personal Data **IXIT 5.8-PersData**: ID, Description, Processing Activities
6-2	**IXIT 5.8-PersData**: ID, Description, Obtaining Consent
6-3	**IXIT 5.8-PersData**: ID, Description, Obtaining Consent, Withdrawing Consent
6-4	**IXIT 5.10-TelData**: ID, Description, Collector, Personal Data **IXIT 5.8-PersData**: ID, Description
6-5	**IXIT 6-DataInfo**: Publication of Telemetry Data **IXIT 5.10-TelData**: ID, Description, Collector

Table 4: Required IXIT entries per provision

7 History

Document history		
Version	Date	Description
0.0.0	07/2019	Initial Draft UK
0.0.1	10/2019	Kick-off Web Conference
0.0.1b	11/2019	Presented at Cyber#18
0.0.2	01/2020	
0.0.2-5	04/2020	Presented at Rapporteurs Call 05/2020
0.0.2-7	05/2020	Preview to be presented at Cyber#20
0.0.3	05/2020	Presented at Cyber#20
0.0.4	09/2020	Presented at Cyber#21
0.0.4-1	11/2020	Presented at Cyber#22
0.0.4-9	12/2020	Presented at Rapporteurs Call 12/2020
0.0.5	12/2020	Public Draft