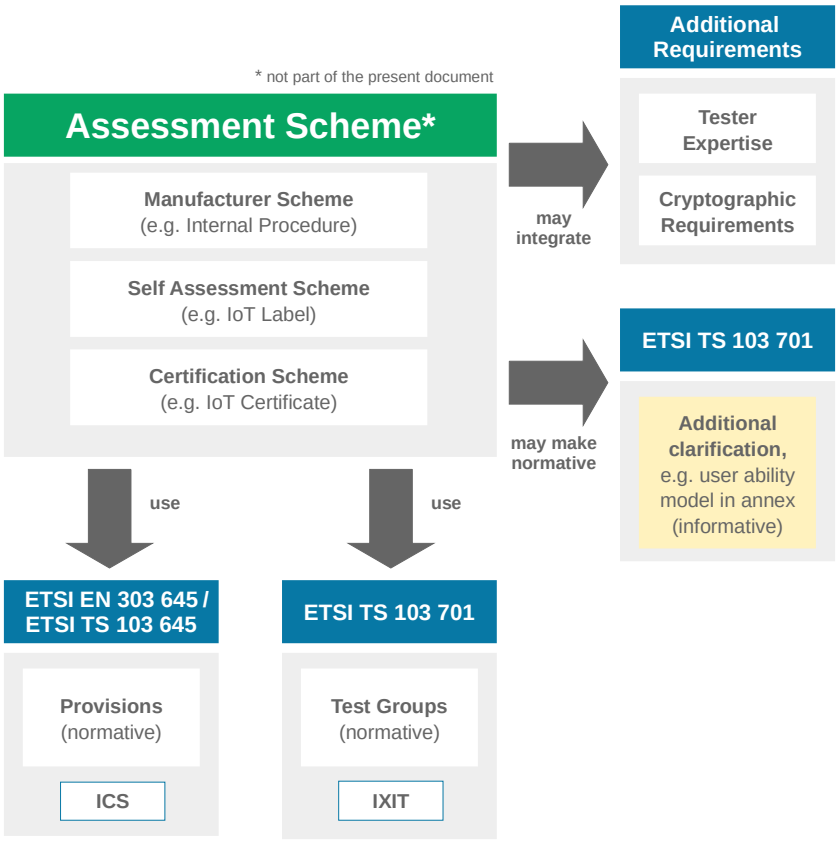

Figure 5: Role of an assessment scheme

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

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

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

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

5 Test scenarios for consumer IoT

5.0 TSO 4: Reporting implementation

5.0.1 Test group 4-1

5.0.1.0 Test group objective

The test group addresses the provision 4-1.

5.0.1.1 Test case 4-1-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1 TSO 5.1: No universal default passwords

5.1.1 Test group 5.1-1

5.1.1.0 Test group objective

The test group addresses the provision 5.1-1.

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

5.1.1.1 Test case 5.1-1-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.1.2 Test case 5.1-1-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.2 Test group 5.1-2

5.1.2.0 Test group objective

The test group addresses the provision 5.1-2.

5.1.2.1 Test case 5.1-2-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.2.2 Test case 5.1-2-2 (functional)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.3 Test group 5.1-3

5.1.3.0 Test group objective

The test group addresses the provision 5.1-3.

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

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

5.1.3.1 Test case 5.1-3-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

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

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

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.1.3.2 Test case 5.1-3-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.4 Test group 5.1-4

5.1.4.0 Test group objective

The test group addresses the provision 5.1-4.

5.1.4.1 Test case 5.1-4-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.4.2 Test case 5.1-4-2 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.5 Test group 5.1-5

5.1.5.0 Test group objective

The test group addresses the provision 5.1-5.

5.1.5.1 Test case 5.1-5-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.1.5.2 Test case 5.1-5-2 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

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

5.2.1 Test group 5.2-1

5.2.1.0 Test group objective

The test group addresses the provision 5.2-1.

5.2.1.1 Test case 5.2-1-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.2.1.2 Test case 5.2-1-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.2.2 Test group 5.2-2

5.2.2.0 Test group objective

The test group addresses the provision 5.2-2.

5.2.2.1 Test case 5.2-2-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

- a confirmation for the implementation is given.

The verdict FAIL is assigned otherwise.

5.2.3 Test group 5.2-3

5.2.3.0 Test group objective

The test group addresses the provision 5.2-3.

5.2.3.1 Test case 5.2-3-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3 TSO 5.3: Keep software updated

5.3.1 Test group 5.3-1

5.3.1.0 Test group objective

The test group addresses the provision 5.3-1.

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

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

5.3.1.1 Test case 5.3-1-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.1.2 Test case 5.3-1-2 (functional)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.2 Test group 5.3-2

5.3.2.0 Test group objective

The test group addresses the provision 5.3-2.

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

5.3.2.1 Test case 5.3-2-1 (conceptual)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.2.2 Test case 5.3-2-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.3 Test group 5.3-3

5.3.3.0 Test group objective

The test group addresses the provision 5.3-3.

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

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

5.3.3.1 Test case 5.3-3-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.4 Test group 5.3-4

5.3.4.0 Test group objective

The test group addresses the provision 5.3-4.

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

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

5.3.4.1 Test case 5.3-4-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

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

The verdict FAIL is assigned otherwise.

5.3.5 Test group 5.3-5

5.3.5.0 Test group objective

The test group addresses the provision 5.3-5.

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

5.3.5.1 Test case 5.3-5-1 (conceptual)

Test purpose

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

Test units

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

   - after initialization of the DUT; and

   - periodically.

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

Assignment of verdict

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

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

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

- the availability of software updates is checked periodically.

The verdict FAIL is assigned otherwise.

5.3.6 Test group 5.3-6

5.3.6.0 Test group objective

The test group addresses the provision 5.3-6.

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

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

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

5.3.6.1 Test case 5.3-6-1 (conceptual)

Test purpose

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

Test units

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

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

- enable; or
- disable; or
- postpone

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

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

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

- enable; or
- disable; or
- postpone

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.6.2 Test case 5.3-6-2 (functional)

Test purpose

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

Test units

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

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

   - enable; or
   - disable; or
   - postpone

   automatic installation of security updates.

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

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

   - enable; or
   - disable; or
   - postpone

   update notifications.

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.7 Test group 5.3-7

5.3.7.0 Test group objective

The test group addresses the provision 5.3-7.

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

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

5.3.7.1 Test case 5.3-7-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if for all update mechanisms:

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

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

The verdict FAIL is assigned otherwise.

5.3.8 Test group 5.3-8

5.3.8.0 Test group objective

The test group addresses the provision 5.3-8.

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

5.3.8.1 Test case 5.3-8-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.9 Test group 5.3-9

5.3.9.0 Test group objective

The test group addresses the provision 5.3-9.

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

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

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

5.3.9.1 Test case 5.3-9-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.10 Test group 5.3-10

5.3.10.0 Test group objective

The test group addresses the provision 5.3-10.

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

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

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

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

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.11 Test group 5.3-11

5.3.11.0 Test group objective

The test group addresses the provision 5.3-11.

5.3.11.1 Test case 5.3-11-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if for all update mechanisms:

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

The verdict FAIL is assigned otherwise.

5.3.12 Test group 5.3-12

5.3.12.0 Test group objective

The test group addresses the provision 5.3-12.

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

5.3.12.1 Test case 5.3-12-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if for each update mechanism:

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

The verdict FAIL is assigned otherwise.

5.3.13 Test group 5.3-13

5.3.13.0 Test group objective

The test group addresses the provision 5.3-13.

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

5.3.13.1 Test case 5.3-13-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.13.2 Test case 5.3-13-2 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.14 Test group 5.3-14

5.3.14.0 Test group objective

The test group addresses the provision 5.3-14.

5.3.14.1 Test case 5.3-14-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.14.2 Test case 5.3-14-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.15 Test group 5.3-15

5.3.15.0 Test group objective

The test group addresses the provision 5.3-15.

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

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

5.3.15.1 Test case 5.3-15-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.15.2 Test case 5.3-15-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.16 Test group 5.3-16

5.3.16.0 Test group objective

The test group addresses the provision 5.3-16.

5.3.16.1 Test case 5.3-16-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.3.16.2 Test case 5.3-16-2 (functional)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

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

The verdict FAIL is assigned otherwise.

5.4 TSO 5.4: Securely store sensitive security parameters

5.4.1 Test group 5.4-1

5.4.1.0 Test group objective

The test group addresses the provision 5.4-1.

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

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

5.4.1.1 Test case 5.4-1-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

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

The verdict FAIL is assigned otherwise.

5.4.1.2 Test case 5.4-1-2 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.4.2 Test group 5.4-2

5.4.2.0 Test group objective

The test group addresses the provision 5.4-2.

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

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

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

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

5.4.2.1 Test case 5.4-2-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.4.2.2 Test case 5.4-2-2 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.4.3 Test group 5.4-3

5.4.3.0 Test group objective

The test group addresses the provision 5.4-3.

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

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

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

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

5.4.3.1 Test case 5.4-3-1 (conceptual)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.4.3.2 Test case 5.4-3-2 (functional)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.4.4 Test group 5.4-4

5.4.4.0 Test group objective

The test group addresses the provision 5.4-4.

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

5.4.4.1 Test case 5.4-4-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

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

The verdict FAIL is assigned otherwise.

5.5 TSO 5.5: Communicate securely

5.5.1 Test group 5.5-1

5.5.1.0 Test group objective

The test group addresses the provision 5.5-1.

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

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

5.5.1.1 Test case 5.5-1-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if for all communication mechanisms:

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

The verdict FAIL is assigned otherwise.

5.5.1.2 Test case 5.5-1-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.2 Test group 5.5-2

5.5.2.0 Test group objective

The test group addresses the provision 5.5-2.

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

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

5.5.2.1 Test case 5.5-2-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.2.2 Test case 5.5-2-2 (functional)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.3 Test group 5.5-3

5.5.3.0 Test group objective

The test group addresses the provision 5.5-3.

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

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

5.5.3.1 Test case 5.5-3-1 (conceptual)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.4 Test group 5.5-4

5.5.4.0 Test group objective

The test group addresses the provision 5.5-4.

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

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

5.5.4.1 Test case 5.5-4-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.4.2 Test case 5.5-4-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

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

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

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

The verdict FAIL is assigned otherwise.

5.5.5 Test group 5.5-5

5.5.5.0 Test group objective

The test group addresses the provision 5.5-5.

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

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

5.5.5.1 Test case 5.5-5-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.5.2 Test case 5.5-5-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.6 Test group 5.5-6

5.5.6.0 Test group objective

The test group addresses the provision 5.5-6.

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

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

5.5.6.1 Test case 5.5-6-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.5.6.2 Test case 5.5-6-2 (functional)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.7 Test group 5.5-7

5.5.7.0 Test group objective

The test group addresses the provision 5.5-7.

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

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

5.5.7.1 Test case 5.5-7-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.5.7.2 Test case 5.5-7-2 (functional)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.5.8 Test group 5.5-8

5.5.8.0 Test group objective

The test group addresses the provision 5.5-8.

5.5.8.1 Test case 5.5-8-1 (conceptual)

Test purpose

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

Test units

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

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

according to the processes in IXIT 14-SecMgmt.

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6 TSO 5.6: Minimize exposed attack surfaces

5.6.1 Test group 5.6-1

5.6.1.0 Test group objective

The test group addresses the provision 5.6-1.

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

5.6.1.1 Test case 5.6-1-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.1.2 Test case 5.6-1-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.2 Test group 5.6-2

5.6.2.0 Test group objective

The test group addresses the provision 5.6-2.

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

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

5.6.2.1 Test case 5.6-2-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if for every network interface:

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

The verdict FAIL is assigned otherwise.

5.6.2.2 Test case 5.6-2-2 (functional)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.3 Test group 5.6-3

5.6.3.0 Test group objective

The test group addresses the provision 5.6-3.

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

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

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

5.6.3.1 Test case 5.6-3-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.3.2 Test case 5.6-3-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.4 Test group 5.6-4

5.6.4.0 Test group objective

The test group addresses the provision 5.6-4.

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

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

5.6.4.1 Test case 5.6-4-1 (conceptual)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.4.2 Test case 5.6-4-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.5 Test group 5.6-5

5.6.5.0 Test group objective

The test group addresses the provision 5.6-5.

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

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

5.6.5.1 Test case 5.6-5-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.6 Test group 5.6-6

5.6.6.0 Test group objective

The test group addresses the provision 5.6-6.

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

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

5.6.6.1 Test case 5.6-6-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.7 Test group 5.6-7

5.6.7.0 Test group objective

The test group addresses the provision 5.6-7.

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

5.6.7.1 Test case 5.6-7-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.8 Test group 5.6-8

5.6.8.0 Test group objective

The test group addresses the provision 5.6-8.

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

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

5.6.8.1 Test case 5.6-8-1 (conceptual)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.6.9 Test group 5.6-9

5.6.9.0 Test group objective

The test group addresses the provision 5.6-9.

5.6.9.1 Test case 5.6-9-1 (conceptual)

Test purpose

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

Test units

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

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

- handling of third-party software providers.

according to the processes in IXIT 19-SecDev.

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

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

Assignment of verdict

The verdict PASS is assigned if the secure development covers:

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

The verdict FAIL is assigned otherwise.

5.7 TSO 5.7: Ensure software integrity

5.7.1 Test group 5.7-1

5.7.1.0 Test group objective

The test group addresses the provision 5.7-1.

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

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

5.7.1.1 Test case 5.7-1-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.7.1.2 Test case 5.7-1-2 (functional)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.7.2 Test group 5.7-2

5.7.2.0 Test group objective

The test group addresses the provision 5.7-2.

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

5.7.2.1 Test case 5.7-2-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.7.2.2 Test case 5.7-2-2 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.8 TSO 5.8: Ensure that personal data is secure

5.8.1 Test group 5.8-1

5.8.1.0 Test group objective

The test group addresses the provision 5.8-1.

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

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

5.8.1.1 Test case 5.8-1-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.8.1.2 Test case 5.8-1-2 (functional)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.8.2 Test group 5.8-2

5.8.2.0 Test group objective

The test group addresses the provision 5.8-2.

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

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

5.8.2.1 Test case 5.8-2-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.8.2.2 Test case 5.8-2-2 (functional)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.8.3 Test group 5.8-3

5.8.3.0 Test group objective

The test group addresses the provision 5.8-3.

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

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

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

5.8.3.1 Test case 5.8-3-1 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.9 TSO 5.9: Make systems resilient to outages

5.9.1 Test Group 5.9-1

5.9.1.0 Test group objective

The test group addresses the provision 5.9-1.

5.9.1.1 Test case 5.9-1-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.9.1.2 Test case 5.9-1-2 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.9.2 Test Group 5.9-2

5.9.2.0 Test group objective

The test group addresses the provision 5.9-2.

5.9.2.1 Test case 5.9-2-1 (conceptual)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.9.2.2 Test case 5.9-2-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.9.3 Test Group 5.9-3

5.9.3.0 Test group objective

The test group addresses the provision 5.9-3.

This test group considers the capabilities:

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

5.9.3.1 Test case 5.9-3-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.9.3.2 Test case 5.9-3-2 (functional)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.10 TSO 5.10: Examine system telemetry data

5.10.1 Test Group 5.10-1

5.10.1.0 Test group objective

The test group addresses the provision 5.10-1.

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

5.10.1.1 Test case 5.10-1-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

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

5.11.1 Test group 5.11-1

5.11.1.0 Test group objective

The test group addresses the provision 5.11-1.

5.11.1.1 Test case 5.11-1-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

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

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.11.1.2 Test case 5.11-1-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.11.2 Test group 5.11-2

5.11.2.0 Test group objective

The test group addresses the provision 5.11-2.

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

5.11.2.1 Test case 5.11-2-1 (conceptual)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.11.2.2 Test case 5.11-2-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

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

Assignment of verdict

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

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

The verdict FAIL is assigned otherwise.

5.11.3 Test group 5.11-3

5.11.3.0 Test group objective

The test group addresses the provision 5.11-3.

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

5.11.3.1 Test case 5.11-3-1 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if every deletion functionality:

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

The verdict FAIL is assigned otherwise.

5.11.4 Test group 5.11-4

5.11.4.0 Test group objective

The test group addresses the provision 5.11-4.

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

5.11.4.1 Test case 5.11-4-1 (functional)

Test purpose

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

Test units

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.12 TSO 5.12: Make installation and maintenance of devices easy

5.12.1 Test group 5.12-1

5.12.1.0 Test group objective

The test group addresses the provision 5.12-1.

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

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

5.12.1.1 Test case 5.12-1-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.12.1.2 Test case 5.12-1-2 (functional)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.12.2 Test group 5.12-2

5.12.2.0 Test group objective

The test group addresses the provision 5.12-2.

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

5.12.2.1 Test case 5.12-2-1 (functional)

Test purpose

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

Test units

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.12.3 Test group 5.12-3

5.12.3.0 Test group objective

The test group addresses the provision 5.12-3.

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

5.12.3.1 Test case 5.12-3-1 (functional)

Test purpose

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

Test units

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.13 TSO 5.13: Validate input data

5.13.1 Test group 5.13-1

5.13.1.0 Test group objective

The test group addresses the provision 5.13-1.

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

5.13.1.1 Test case 5.13-1-1 (conceptual)

Test purpose

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

Test units

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.13.1.2 Test case 5.13-1-2 (functional)

Test purpose

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

Test units

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

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

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

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

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

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

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

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

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.14 TSO 6: Data protection for consumer IoT

5.14.1 Test group 6-1

5.14.1.0 Test group objective

The test group addresses the provision 6-1.

5.14.1.1 Test case 6-1-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.14.1.2 Test case 6-1-2 (functional)

Test purpose

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

Test units

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

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

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

d) The TL **shall** functionally assess whether the obtained information describe how personal data is being used, by whom, and for what purposes in a way understandable for a user with limited technical knowledge (see clause D.3).

Assignment of verdict

The verdict PASS is assigned if:

- the information about processing personal data can be obtained as described; and
- the obtained information about processing personal data match their description; and
- the personal data being processed is clearly and transparently described; and
- it is clearly and transparently described how personal data is being used, by whom, and for what purposes.

The verdict FAIL is assigned otherwise.

5.14.2 Test group 6-2

5.14.2.0 Test group objective

The test group addresses the provision 6-2.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2], obtaining consent "in a valid way" normally involves giving consumers a free, obvious and explicit opt-in choice of whether their personal data is used for a specified purpose.

5.14.2.1 Test case 6-2-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** assess whether the opt-in choice:

   - is given freely; and
   - is given obviously; and
   - is given explicitly

according to the description of "Obtaining Consent".

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- it is described how to express consent (opt-in choice) to the processing of personal data for specific purposes; and

- the opt-in choice is given freely, obviously and explicitly.

The verdict FAIL is assigned otherwise.

5.14.2.2 Test case 6-2-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** functionally assess whether consumers' consent to processing personal data is obtained as described in the IXIT.

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- the way of obtaining consumers' consent matches the description.

The verdict FAIL is assigned otherwise.

5.14.3 Test group 6-3

5.14.3.0 Test group objective

The test group addresses the provision 6-3.

According to ETSI TS 103 645 [1]/ETSI EN 303 645 [2], withdrawing consent at any time normally involves configuring IoT device and service functionality appropriately.

5.14.3.1 Test case 6-3-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of withdrawing consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** assess whether the information on "Withdrawing Consent" describes how to withdraw consent to the processing of personal data at any time by configuring IoT device and service functionality appropriately.

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- it is described how to withdraw consent to the processing of personal data at any time.

The verdict FAIL is assigned otherwise.

5.14.3.2 Test case 6-3-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of withdrawing consumers' consent for the processing of personal data.

Test units

a) For each personal data in IXIT 21-PersData that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL **shall** functionally assess whether consumers' consent to processing personal data can be withdrawn as described in "Withdrawing Consent".

Assignment of verdict

The verdict PASS is assigned if for each category of personal data that is processed on the basis of consumers' consent:

- the way of withdrawing consumers' consent matches the description.

The verdict FAIL is assigned otherwise.

5.14.4 Test group 6-4

5.14.4.0 Test group objective

The test group addresses the provision 6-4.

5.14.4.1 Test case 6-4-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the processing of telemetry data.

Test units

a) The TL **shall** assess whether the personal data in IXIT 21-PersData that are referenced in "Personal Data" in IXIT 24-TelData is necessary for the intended functionality as described in the "Purpose" of collecting the data.

NOTE: Telemetry data are considered to be necessary for the intended functionality if and only if they are needed for achieving the processing purposes.

Assignment of verdict

The verdict PASS is assigned if for each telemetry data:

- their processing is necessary for the intended functionality.

The verdict FAIL is assigned otherwise.

5.14.5 Test group 6-5

5.14.5.0 Test group objective

The test group addresses the provision 6-5.

5.14.5.1 Test case 6-5-1 (conceptual)

Test purpose

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

Test units

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

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.14.5.2 Test case 6-5-2 (functional)

Test purpose

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

Test units

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

b) The TL **shall** functionally assess whether the obtained information about processing telemetry data accessing the "Documentation of Telemetry Data" in IXIT 2-UserInfo match their "Purpose" described in IXIT 24-TelData.

c) The TL **shall** functionally check whether the obtained information describes what telemetry data is collected.

d) The TL **shall** functionally check whether the obtained information describes how telemetry data is being used, by whom, and for what purposes.

Assignment of verdict

The verdict PASS is assigned if:

- the information about processing telemetry data can be obtained as described; and
- the obtained information about processing telemetry data match their description; and
- the telemetry data being collected is described; and
- it is completely described how telemetry data is being used, by whom, and for what purposes.

The verdict FAIL is assigned otherwise.