ETSI TS 103 928 V1.1.1 (2023-07)

Cyber Security (CYBER);
Cyber Security for Home Gateways;
Conformance Assessment of Security Requirements
as vertical from Consumer Internet of Things

Reference
DTS/CYBER-0066

Keywords
home gateway, security, testing

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

The ETSI TS 103 848 [1] specifies security provisions for Home Gateway, which extends those of ETSI EN 303 645 [i.1] in a vertical specific manner.

The present document seeks to contribute to a harmonized approach to assessing the conformance of Home Gateway products against the ETSI TS 103 848 [1] using the methodology of the assessment specification ETSI TS 103 701 [2] for ETSI EN 303 645 [i.1].

1 Scope

The present document specifies a conformance assessment methodology for Home Gateway devices of their security risk mitigation and privacy protection measures against the ETSI TS 103 848 [1], addressing the mandatory provisions as well as conditions and complements of the standard by defining test cases and assessment criteria for each provision. The methodology is fully adapted from ETSI TS 103 701 [2] and the present document additionally covers the modifications and additions on provisions made in the ETSI TS 103 848 [1].

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

Multi-medium or highly targeted/sophisticated attacks and thus the invasive analysis of hard- and software modules is out of scope of the present document. The Test Scenarios (TSOs) are targeting basic effort regarding test depth and test circumference in accordance with the ETSI TS 103 848 [1] which addresses a baseline security level.

Due to the heterogeneity of Home Gateway devices, the ETSI TS 103 848 [1] and therefore the associated test groups in the present document are formulated in a generic manner. Thus, the present document does not describe specific tools or detailed step-by-step instructions. The test cases are intended to be performed by competent bodies that have the expertise to derive a suitable test plan.

2 References

2.1 Normative references

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

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

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

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

[1] ETSI TS 103 848 (V1.1.1): "Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things".

[2] ETSI TS 103 701 (V1.1.1): "CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

2.2 Informative references

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

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

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

[i.1] ETSI EN 303 645 (V2.1.1): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.2] ETSI TR 103 621 (V1.2.1): "Guide to Cyber Security for Consumer Internet of Things".

[i.3] NIST SP 800-90B (2018-01): "Recommendation for the Entropy Sources Used for Random Bit Generation".

[i.4] ETSI TS 119 312 (V1.4.2): "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.5] ETSI TS 103 645 (V2.1.2): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.6] SOGIS Agreed Cryptographic Mechanisms (V1.3): "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms".

[i.7] IEEE Std 802.11-2020™: "IEEE Standard for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Networks -- Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.8] IEEE Std 802.11b-1999™: "IEEE Standard for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Networks - Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band".

[i.9] IEEE Std 802.11g-2003™: "IEEE Standard for Information Technology -- Local and Metropolitan Area Networks-- Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band".

[i.10] IEEE Std 802.11n-2009™: "IEEE Standard for Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput".

[i.11] IEEE Std 802.11ax-2021™: "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in the ETSI TS 103 848 [1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in the ETSI TS 103 848 [1] and ETSI TS 103 701 [2] apply.

4 Conformance assessment methodology

4.1 Overview and document structure

4.1.0 General overview of the present document

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

Clause 4.3 describes the assessment procedure.

Clause 4.4 describes how to declare the conformity of the Home Gateway device to the provisions of ETSI TS 103 848 [1] in the Implementation Conformance Statement (ICS).

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

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

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

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

Clause 5 contains the TSOs for Home Gateway, where each TSO addresses a set of provisions from the ETSI TS 103 848 [1] and is composed of a set of test groups that describe the assessment for a single provision. Each test group is composed of a description of its objective and a set of test cases, where each test case describes how to assess a specific aspect of the corresponding provision. The number of the test case is appended to the test group number (e.g. Test case 5.1-3-2 for the second test case in Test group 5.1-3). Typically, the test cases distinguish two aspects:

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

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

Figure 1 illustrates the relation between the ETSI TS 103 848 [1] and the present document with respect to a conformance assessment process and the relation to ETSI EN 303 645 [i.1] and ETSI TS 103 701 [2]. The ETSI TS 103 848 [1] contains provisions concerning cyber security for Home Gateway.

NOTE: Terms, examples, notes, definitions and explanations from the ETSI TS 103 848 [1] are also valid and therefore not redundantly specified in the present document.

The present document is the basis for conformance assessment against the ETSI TS 103 848 [1] and defines the IXIT pro forma. ICS and IXIT are provided by the SO based on the ICS and IXIT pro forma to the TL. The TL uses these documents to derive a test plan.

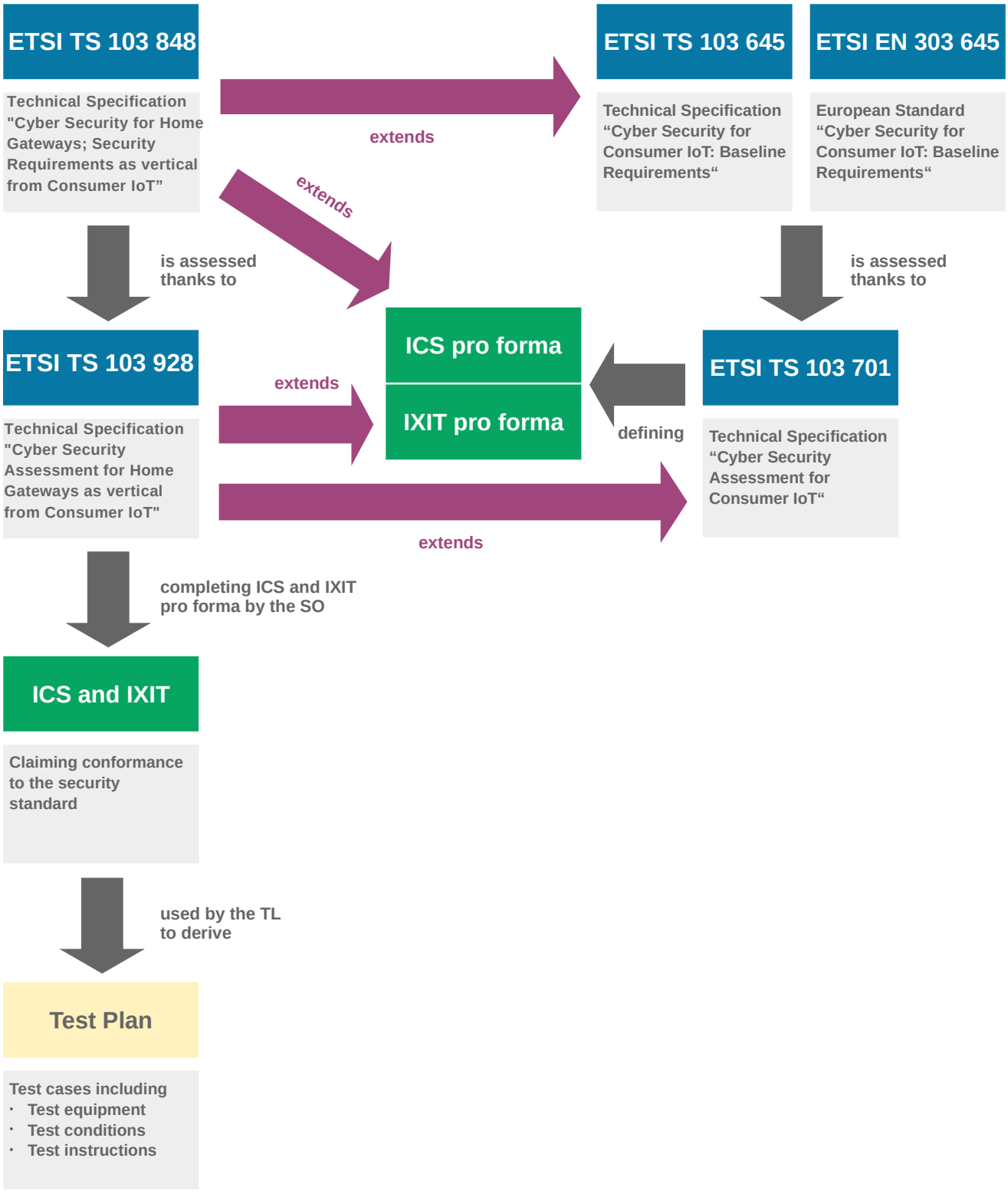

Figure 1: Relations of the present document with respect to a conformance assessment process

4.1.1 Handling of test groups

Each provision in ETSI EN 303 645 [i.1] corresponds to a test group in the ETSI TS 103 701 [2]. The ETSI TS 103 848 [1] contains modified and/or added provisions based on ETSI EN 303 645 [i.1], which correspond respectively to a test group in the present document.

Some modifications in the ETSI TS 103 848 [1] do not imply a replacement of the original provision from ETSI EN 303 645 [i.1] so that the corresponding test group from ETSI TS 103 701 [2] is still applicable. The present document lists the corresponding test groups that are applicable for mandatory provisions of ETSI TS 103 848 [1] in Table B.1. This table contains all provisions of the ICS.

4.1.2 Handling of IXIT entries

The following three bullet points explain how IXIT entries are handled in the present document based on the modified or added provisions in the ETSI TS 103 848 [1]:

- An existing IXIT entry (as defined in ETSI TS 103 701 [2]) is modified and added to an existing IXIT table or list from ETSI TS 103 701 [2].
- A new IXIT entry is created and added to an existing table or list from ETSI TS 103 701 [2].

NOTE: In both cases - modifying and adding an existing IXIT entry to an existing IXIT table or list from ETSI TS 103 701 [2] or adding a new IXIT entry to an existing IXIT table or list from ETSI TS 103 701 [2] - the corresponding IXIT table or list from ETSI TS 103 701 [2] is still valid. More precisely, this means that there is no IXIT entry and/or IXIT table or list from ETSI TS 103 701 [2] that is replaced as in both cases the new IXIT entries are simply added. For test groups and Table B.1 in the present document referring to added IXIT entries, all references are adapted accordingly to cover the new entries.

- A new table or list is added including the corresponding IXIT entries.

4.1.3 Naming conventions

The test group names within the TSOs in the present document are aligned with the provision names in the ETSI TS 103 848 [1].

New IXIT entries defined in the present document are labelled with "(added)".

4.2 Roles and objects

4.2.1 Device Under Test (DUT)

The text in clause 4.2.1 of ETSI TS 103 701 [2] also applies in the present document.

4.2.2 Supplier Organization (SO)

The text in clause 4.2.2 of ETSI TS 103 701 [2] also applies in the present document except for the fact that the SO requests a specific DUT to be tested against the provisions of ETSI TS 103 848 [1].

4.2.3 Test Laboratory (TL)

The text in clause 4.2.3 of ETSI TS 103 701 [2] also applies in the present document except for the fact that the reference to ETSI EN 303 645 [i.1] is to be replaced by the reference to the ETSI TS 103 848 [1].

4.3 Assessment procedure

The text in clause 4.3 of ETSI TS 103 701 [2] also applies in the present document except for the fact that the reference to ETSI EN 303 645 [i.1] is to be replaced by the reference to the ETSI TS 103 848 [1].

In addition, the ICS form is in the annex of ETSI TS 103 848 [1] and the matching table listing required IXIT entries for each provision (see Table B.1) is in the annex of the present document.

4.4 Implementation Conformance Statement (ICS)

The text in clause 4.4 of ETSI TS 103 701 [2] also applies in the present document except for the fact that the reference to ETSI EN 303 645 [i.1] is to be replaced by the reference to the ETSI TS 103 848 [1].

In addition, the ICS form is in the annex of ETSI TS 103 848 [1].

4.5 Implementation eXtra Information for Testing (IXIT)

The text in clause 4.5 of ETSI TS 103 701 [2] also applies in the present document.

The matching table listing required IXIT entries for each provision (see Table B.1) is in the annex of the present document.

4.6 Assignment of verdicts

The text in clause 4.6 of ETSI TS 103 701 [2] also applies in the present document.

4.7 Usage of external evidences

The text in clause 4.7 of ETSI TS 103 701 [2] also applies in the present document.

4.8 Assessment scheme amendments

The text in clause 4.8 of ETSI TS 103 701 [2] also applies in the present document except for the fact that the reference to ETSI EN 303 645 [i.1] is to be replaced by the reference to the ETSI TS 103 848 [1] and the reference to the ETSI TS 103 701 [2] is to be replaced by the present document, respectively.

5 Test groups for adapted cyber security and data protection provisions for Home Gateway

5.0 TSO 4: Reporting implementation

5.0.1 Test group HG 4-1 (extended)

5.0.1.0 Test group objective

The present Test group HG 4-1 (extended) has the same objective as the Test group 4-1 in ETSI TS 103 701 [2]. The only difference is given by the fact that the present Test group HG 4-1 (extended) addresses the provision 4-1 (extended) of ETSI TS 103 848 [1] instead of the provision 4-1 of ETSI EN 303 645 [i.1].

5.0.1.1 Test case HG 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 HG 5.1-1 (extended)

5.1.1.0 Test group objective

The test group addresses the provision HG 5.1-1 (Extended).

This test group addresses the Wi-Fi® or administrator passwords preconfigured in factory default.

5.1.1.1 Test case HG 5.1-1 (extended)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the uniqueness of preconfigured passwords in factory default state.

Test units

a) For each authentication mechanism concerning Wi-Fi® or administrator (i.e. an administrator that performs management actions on the HG) in IXIT 1-AuthMech using factory default preconfigured passwords according to "Authentication Factor", the TL **shall** assess whether the generation mechanism in "Password Generation Mechanism" ensures that each password is unique per device.

Assignment of verdict

The verdict PASS is assigned if:

- Each factory default preconfigured password of a password-based authentication mechanism being used, is unique per device.

The verdict FAIL is assigned otherwise.

5.1.1.2 Test case HG 5.1-1 (extended)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the uniqueness of preconfigured passwords in factory default state.

Test units

a) For each authentication mechanism concerning Wi-Fi® or administrator (i.e. an administrator that performs management actions on the HG) in IXIT 1-AuthMech using preconfigured 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".

NOTE: The TL is required to assess whether at least two DUT samples use different pre-configured password. More samples may increase the accuracy of the assessment. The TL may reset the DUT to factory setting to ensure that the password is default one.

Assignment of verdict

The verdict PASS is assigned if:

- For each preconfigured password there is no indication, that its generation differs from the generation mechanism described in the IXIT.

The verdict FAIL is assigned otherwise.

5.1.2 Test group HG 5.1-4 (extended)-a

5.1.2.0 Test group objective

The present Test group HG 5.1-4 (extended)-a has the same content as the Test group 5.1-4 in ETSI TS 103 701 [2]. The only difference is given by the fact that the present Test group HG 5.1-4 (extended)-a in combination with Test group HG 5.1-4 (extended)-b and Test group HG 5.1-4 (extended)-c addresses the provision HG 5.1-4 (extended) a, b and c of ETSI TS 103 848 [1] instead of the provision 5.1-4 of ETSI EN 303 645 [i.1].

5.1.2.1 Test case HG 5.1-4 (extended)-a-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the capability to set the password in Wi-Fi® based on authentication mechanisms.

Test units

a) The TL **shall** assess whether the authentication mechanism in IXIT 1-AuthMech where "Description" indicates that the mechanism is used for user authentication with Wi-Fi®, the resource of "Documentation of Change Mechanisms" in IXIT 2-UserInfo contains description of Wi-Fi® password changing mechanism.

Assignment of verdict

The verdict PASS is assigned if:

- For each Wi-Fi® authentication mechanism the published resource contains Wi-Fi® password changing guidance.

The verdict FAIL is assigned otherwise.

5.1.3 Test group HG 5.1-4 (extended)-b

5.1.3.0 Test group objective

The present Test group HG 5.1-4 (extended)-b has the same content as the Test group 5.1-4 in ETSI TS 103 701 [2]. The only difference is given by the fact that the present Test group HG 5.1-4 (extended)-b in combination with Test group HG 5.1-4 (extended)-a and Test group HG 5.1-4 (extended)-c addresses the provision HG 5.1-4 (extended) a, b and c of ETSI TS 103 848 [1] instead of the provision 5.1-4 of ETSI EN 303 645 [i.1].

5.1.3.1 Test case HG 5.1-4 (extended)-b-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the mechanisms to change the Wi-Fi® password.

Test units

a) The TL **shall** assess whether the authentication mechanism in IXIT 1-AuthMech where "Description" indicates that the mechanism is used for user authentication with Wi-Fi®, the resource of "Documentation of Change Mechanisms" in IXIT 2-UserInfo considers the mechanism and describes how to change the Wi-Fi® password 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 each Wi-Fi® authentication mechanism the published resource describes how to change the Wi-Fi® password with a simple mechanism.

The verdict FAIL is assigned otherwise.

5.1.3.2 Test case HG 5.1-4 (extended)-b-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of each mechanism to change the Wi-Fi® password.

Test units

a) The TL **shall** perform a change of each Wi-Fi® password for the user authentication mechanism with Wi-Fi® 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 changing the Wi-Fi® password was successful.

Assignment of verdict

The verdict PASS is assigned if:

- each mechanism for the user to change the Wi-Fi® password for user authentication mechanisms works as described.

The verdict FAIL is assigned otherwise.

5.1.4 Test group HG 5.1-4 (extended)-c

5.1.4.0 Test group objective

The present Test group HG 5.1-4 (extended)-c has the same content as the Test group 5.1-4 in ETSI TS 103 701 [2]. The only difference is given by the fact that the present Test group HG 5.1-4 (extended)-c in combination with Test group HG 5.1-4 (extended)-a and Test group HG 5.1-4 (extended)-b addresses the provision HG 5.1-4 (extended) a, b and c of ETSI TS 103 848 [1] instead of the provision 5.1-4 of ETSI EN 303 645 [i.1].

5.1.4.1 Test case HG 5.1-4 (extended)-c-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of each mechanism to change the administrator password.

Test units

a) The TL **shall** assess whether IXIT 1-AuthMech contains the description of the authentication mechanism used for administrator authentication according to the "Description" entry of the table, and whether the resource of "Documentation of Change Mechanisms" in IXIT 2-UserInfo considers the mechanism and describes how to change the administrator password 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 the administrator authentication mechanism the published resource describes how to change the administrator password with a simple mechanism.

The verdict FAIL is assigned otherwise.

5.1.4.2 Test case HG 5.1-4 (extended)-c-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of each mechanism to change the administrator password.

Test units

a) The TL **shall** perform a change of the administrator password for each administrator authentication mechanism 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 changing the administrator password was successful.

Assignment of verdict

The verdict PASS is assigned if:

- The mechanisms for the user to change the administrator password for user authentication mechanisms work as described.

The verdict FAIL is assigned otherwise.

5.1.5 Test group HG 5.1-5 (refined)

The present Test group HG 5.1-5 (refined) has the same content as the Test group 5.1-5 in ETSI TS 103 701 [2]. The only difference is given by the fact that the present Test group HG 5.1-5 (refined) addresses the mandatory provision HG 5.1-5 (refined) of ETSI TS 103 848 [1] instead of the conditional provision 5.1-5 of ETSI EN 303 645 [i.1].

5.2 TSO 5.3: Keep software updated

5.2.1 Test group HG 5.3-1 (extended)-a

5.2.1.0 Test group objective

The test group addresses the provision HG 5.3-1 (extended) a.

This test group addresses the components that are not updatable.

5.2.1.1 Test case HG 5.3-1 (extended)-a-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of components that are not updateable.

Test units

a) For each software component in IXIT 6-SoftComp with an empty list in "Update Mechanism", the TL **shall** assess whether it has been noted and indicated in the resource from "Publication of Non-Updatable" in IXIT 2-UserInfo.

b) For each software component noted and indicated in "Publication of Non-Updatable", the TL **shall** assess whether the manufacture justifications for these un-updateable software components are sufficient to justify the design and assignment as un-updateable SW.

NOTE: Sufficient means that the choices of the un-updateable SW components made by the manufacture are reasonably acceptable to the TL according to the justifications.

Assignment of verdict

The verdict PASS is assigned if:

- each software component in IXIT 6-SoftComp with an empty list in "Update Mechanism" has been noted and indicated in "Publication of Non-Updatable" (i.e. each SW component of the HG is assigned either on the updateable or on the not-updateable list of components); and
- for each not-updatable software component, the TL confirms the sufficiency of the given justification as not updatable SW component.

The verdict FAIL is assigned otherwise.

5.2.2 Test group HG 5.3-1 (extended)-b

5.2.2.0 Test group objective

The test group addresses the provision HG 5.3-1 (extended) b.

This test group addresses the software version control for HG update.

5.2.2.1 Test case HG 5.3-1 (extended)-b-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the software version control for HG update.

Test units

a) The TL **shall** assess that for each operation of the update mechanism in IXIT 7-UpdMech, the software version control in the update mechanism verifies that the version of a provided software update has proven being valid, prior to installation according to the "Description" and the corresponding "Cryptographic Details".

EXAMPLE: The simplest form of version control is to check that the update provides software that has a higher version number than the currently installed software.

Assignment of verdict

The verdict PASS is assigned if:

- it is confirmed that each operation of the software version control mechanism described in update mechanism in IXIT 7-UpdMech verifies that the version of the software provided by the update has proven being valid prior to installation.

The verdict FAIL is assigned otherwise.

5.2.2.2 Test case HG 5.3-1 (extended)-b-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the version control for HG update.

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** perform an update with an invalid software version, but with a correct signature in order to test the rejection of invalid versions based on the "Description" and "Initiation and Interaction". Thereby, the TL has to ensure that the rejection of the update is for the reason of an invalid version number, and not for an integrity violation by the modified version number.

EXAMPLE: The TL can attempt to update the DUT with out-of-date software from manufacturer to check whether the software was rejected.

Assignment of verdict

The verdict PASS is assigned if:

- each version control within the update mechanism in IXIT 7-UpdMech can successfully validate the version of the software provided by the update; and
- version control effectively prevents installation of the old version software update.

The verdict FAIL is assigned otherwise.

5.2.3 Test group HG 5.3-2 (refined)

The present Test group HG 5.3-2 (refined) has the same content as the Test group 5.3-2 in ETSI TS 103 701 [2]. The only difference is that the present Test group HG 5.3-2 (refined) addresses the mandatory provision HG 5.3-2 (refined) of ETSI TS 103 848 [1] instead of the conditional provision 5.3-2 of ETSI EN 303 645 [i.1].

5.2.4 Test group HG 5.3-6 (extended)

5.2.4.0 Test group objective

The test group addresses the provision HG 5.3-6 (extended).

This test group addresses the default state of the update functionality and the ability to configure it.

5.2.4.1 Test case HG 5.3-6 (extended)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the configuration and the default state of update functionality.

Test units

a) For each update mechanism in IXIT 7-UpdMech that a not ISP-administrated HG device supports, the TL **shall** check whether the update functionality is enabled by default according to "Configuration".

b) For each update mechanism in IXIT 7-UpdMech that a not ISP-administrated HG device supports, the TL **shall** check whether it provides the user with the ability to configure its deactivation and its automation (e.g. enable, disable, or postpone the automatic installation of security updates) according to "Configuration" in IXIT 7-UpdMech.

Assignment of verdict

The verdict PASS is assigned if:

- The DUT supports update functionality which is enabled in the default state and for all update mechanisms the user is provided with the ability to configure its deactivation and its automation.

The verdict FAIL is assigned otherwise.

5.2.4.2 Test case HG 5.3-6 (extended)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the configuration and the default state of update functionality.

Test units

a) For each update mechanism in IXIT 7-UpdMech that a not ISP-administrated HG device supports, the TL **shall** functionally check whether the update functionality is enabled in the default state of the DUT.

b) For each update mechanism in IXIT 7-UpdMech that a not ISP-administrated HG device supports, the TL **shall** perform a modification of the configuration as described in "Configuration" and assess whether the user is provided with the ability to configure its deactivation and its automation (e.g. enable, disable, or postpone the automatic installation of security updates).

Assignment of verdict

The verdict PASS is assigned if:

- The DUT supports update functionality which is enabled in the default state and for all update mechanisms the user can successfully modify the configuration as described.

The verdict FAIL is assigned otherwise.

5.2.5 Test group HG 5.3-9 (extended)-b

5.2.5.0 Test group objective

The test group addresses the Provision HG 5.3-9 (extended) b.

Authentication in this context means to have evidence that a software update stems from the true origin and not from another malicious source. Successful verification means that its integrity is proven, confirming that the received software update is exactly equal to the original before sending.

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

The assessment focuses on the verification of authenticity and integrity prior to the installation of the software update.

5.2.5.1 Test case 5.3-9 (extended)-b-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the verification of software updates concerning authenticity and integrity.

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" prior to the installation.

NOTE 1: There are different ways to verify the authenticity of a software update in regard to its source.

NOTE 2: The verification of authenticity by the DUT serves primarily for the rejection of integrity violated software updates stemming from other sources than the allowed.

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 primarily for the detection of injected malicious code, faults and other violations of integrity in a correctly chosen software update.

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

5.2.5.2 Test case 5.3-9 (extended)-b-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the verification of software updates concerning authenticity and integrity.

Test units

For each update mechanism in IXIT 7-UpdMech, the TL **shall** apply all **Test units** as specified in the Test Case HG 7.3-1 (added) and Test Case HG 7.3-7 (added) to each one of the update mechanisms.

Assignment of verdict

The verdict PASS is assigned if:

- the authenticity and integrity are effectively verified.

The verdict FAIL is assigned otherwise.

5.2.6 Test group HG 5.3-16 (extended)

5.2.6.0 Test group objective

The test group addresses the provision HG 5.3-16 (extended).

This test group addresses the access control of the software version numbers for different users from different interfaces.

5.2.6.1 Test case HG 5.3-16 (extended)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the access control of the software version numbers for different users connected from different interfaces.

Test units

a) The TL **shall** assess with the provided user guidance and other technical "description" whether the software version numbers of the DUT can be retrieved by an administrator (i.e. local administrator from LAN or remote administrator from WAN) according to "Software Version Numbers" in IXIT 2-UserInfo.

b) The TL **shall** assess with the provided user guidance and other technical "description" whether the software version numbers of the DUT can be retrieved by an authenticated user on the LAN according to "Software Version Numbers" in IXIT 2-UserInfo.

c) The TL **shall** assess with the provided user guidance and other technical "description" whether the software version numbers of the DUT can be retrieved by any other user role, if existing, and from guest Wi-Fi® according to "Software Version Numbers" in IXIT 2-UserInfo.

Assignment of verdict

The verdict PASS is assigned if:

- The access control policy ensures that only the administrator and authenticated user on the LAN, with the exception of Wi-Fi® guests, can retrieve the software version numbers.

The verdict FAIL is assigned otherwise.

Table 1: Ability to retrieve the software version numbers after authentication

Interface / User	LAN	WAN	Guest Wi-Fi
administrator	√	√	×
other users	√	N/A	×
NOTE: The authentication enforced on administrators and other users refers to the login check of the device management system/GUI, not the built-in mechanism of Wi-Fi® (e.g. WPA2).			

5.2.6.2 Test case HG 5.3-16 (extended)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the access control of the software version numbers for different users connected from different interfaces.

Test units

a) The TL **shall** functionally assess whether the software version numbers of the DUT can be retrieved by an administrator (i.e. local administrator from LAN or remote administrator from WAN) according to "Software Version Numbers" in IXIT 2-UserInfo.

b) The TL **shall** functionally assess whether the software version numbers of the DUT can be retrieved by an authenticated user on the LAN according to "Software Version Numbers" in IXIT 2-UserInfo.

c) The TL **shall** functionally assess whether the software version numbers of the DUT can be retrieved by any other user role, if existing, and from Guest Wi-Fi® according to " Software Version Numbers" in IXIT 2-UserInfo.

Assignment of verdict

The verdict PASS is assigned if:

- The software version numbers can exclusively be retrieved by an administrator or an authenticated user on the LAN, and that it cannot be retrieved by any other user role, if existing, and from users on a Wi-Fi® guest network.

The verdict FAIL is assigned otherwise.

5.3 TSO 5.6: Minimize exposed attack surfaces

5.3.1 Test group HG 5.6-1 (extended)

5.3.1.0 Test group objective

The present Test group HG 5.6-1 (extended) addresses the provision HG 5.6-1 (extended) of ETSI TS 103 848 [1] which is an extended provision to clause 5.6 of ETSI EN 303 645 [i.1].

This test group assesses the default setting of guest Wi-Fi® if the DUT support it.

5.3.1.1 Test case HG 5.6-1 (extended)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the default setting of the Guest Wi-Fi® functionality.

Test units

a) The TL **shall** assess whether IXIT 13-SoftServ contains a description of Guest Wi-Fi® functionality.

b) The TL **shall** assess whether the "Default Settings" of each Guest Wi-Fi® functionality provided in IXIT 13-SoftServ or other documentations indicates the functionality is disabled by default.

Assignment of verdict

The verdict PASS is assigned if:

- the HG support Guest Wi-Fi® functionality; and
- for the Guest Wi-Fi® functionality, the claimed IXIT table indicates it is disabled by default.

The verdict FAIL is assigned otherwise.

5.3.1.2 Test case HG 5.6-1 (extended)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the Guest Wi-Fi® functionality.

Test units

a) The TL shall functionally assess whether each Guest Wi-Fi® functionality provided in IXIT 13-SoftServ "Default Settings" is implemented according to the IXIT documentation. If multiple Guest(s) Wi-Fi ® are supported, all of them shall be tested.

Assignment of verdict

The verdict PASS is assigned if:

- For each Guest Wi-Fi® functionality, there is no indication that the implementation of the default settings differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

5.4 TSO 5.9: Make systems resilient to outages

5.4.1 Test group HG 5.9-2 (promoted)

The present Test group HG 5.9-2 (extended) addresses the provision HG 5.9-2 (extended) of ETSI TS 103 848 [1] which is a promoted provision to clause 5.9 of ETSI EN 303 645 [i.1].

This test group assesses the resilience mechanism concerning outages of network and power. Test Group 5.9-2 from ETSI TS 103 701 [2] can be reused.

6 Test Groups for additional cyber security provisions for Home Gateway

6.0 Overview

Additional test groups are defined in the present clause referring to the added provisions in the ETSI TS 103 848 [1]. These additional test groups are defined in the following clauses.

6.1 TSO 7.3: Keep software updated

6.1.1 Test group HG 7.3-1 (added)

6.1.1.0 Test group objective

The test group addresses the provision HG 7.3-1 (added).

This test group addresses the pre-installed public verification key of the manufacturer or software provider in the default state.

6.1.1.1 Test case HG 7.3-1 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the pre-installed public verification key of the manufacturer or software provider in the default state.

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** conceptually check whether the public verification key was pre-installed by default according to " Cryptographic Details", the corresponding "Security Guarantees" and "Description".

Assignment of verdict

The verdict PASS is assigned if:

- The DUT has the public verification key of the manufacturer or software provider pre-installed in the default state.

The verdict FAIL is assigned otherwise.

6.1.1.2 Test case HG 7.3-1 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the pre-installed public verification key of the manufacturer or software provider in the default state.

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** devise functional attacks in the default state of the HG to circumvent or abuse the pre-installed manufacturer public key.

b) The TL **shall** functionally check whether the pre-installed public verification key is effectively used to verify the integrity and signature of the update package to prevent the misuse of software updates.

EXAMPLE: If applicable the TL should try to provide a manipulated update package or an inappropriate signed update package to the DUT. Inappropriate means either the signature was generated with a mismatched private key to the public key, or the signed hash does not meet the SW update package.

Assignment of verdict

The verdict PASS is assigned if:

- The public verification key was pre-installed by default and can effectively verify integrity and signature of the update package to prevent the misuse of software updates.

The verdict FAIL is assigned otherwise.

6.1.2 Test group HG 7.3-4 (added)

6.1.2.0 Test group objective

This test group applies only if the HG is an ISP administrated device.

The test group addresses the provision HG 7.3-4 (added).

This test group addresses the remote configurable update service of the HG and its transparency.

6.1.2.1 Test case HG 7.3-4 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the remote configurable update as ISP administration service and its transparency to the local user.

Test units

a) The TL **shall** assess whether the update can be made available when required by an ISP-administrator according to "Description" and "Status" in IXIT 13-SoftServ.

b) The TL **shall** assess whether the update service needs any local user interactions and configurations according to the "Allows Configuration" in IXIT 13-SoftServ.

Assignment of verdict

The verdict PASS is assigned if:

- the DUT has a remote ISP administrated update service which can be configured as required by the ISP-administrator; and
- the ISP administrated update service is enabled by default and needs no local user interactions or configurations.

The verdict FAIL is assigned otherwise.

6.1.2.2 Test case HG 7.3-4 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the remote configurable update as an ISP administration service and its transparency to the local user.

Test units

a) The TL **shall** trigger a remote update and check whether the update can be performed successfully as configured by the HG.

b) The TL **shall** check whether the procedure of the update needs any local user interaction.

Assignment of verdict

The verdict PASS is assigned if:

- the update is/was successfully performed and the version of the DUT was successfully upgraded as configured; and
- the procedure of the update is totally transparent to the local user. This includes also HG service-stop and reboot - if required for the update.

The verdict FAIL is assigned otherwise.

6.1.3 Test group HG 7.3-6 (added)

6.1.3.0 Test group objective

The test group addresses the provision HG 7.3-6 (added).

This test group addresses the installation of the 3rd-party SW.

6.1.3.1 Test case HG 7.3-6 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the installation of the 3rd-party SW concerning the default configuration (a), the interaction with the administrator (b) and the SW-restore mechanism (c).

Test units

a) For each 3rd-party SW in IXIT 31-ThiParSoft (added), the TL **shall** conceptually check in the original delivery condition the existence of the option to install 3rd-party SW, and if present, this option shall be disabled.

b) For each 3rd-party SW in IXIT 31-ThiParSoft (added), the TL **shall** conceptually check, in case the option to install 3rd-party SW is present and active, that:

   1) the HG triggers a warning to the administrator; and

   2) requires administrator's consent according to the "Initiation and Interaction" prior installation of any 3rd-party SW.

c) For each 3rd-party SW in IXIT 31-ThiParSoft (added), the TL **shall** conceptually check whether the HG can be restored to the OEM SW state according to "Software Restore".

NOTE: Restore to OEM SW state means on one hand that the HG has all 3rd-party SW completely removed along with all its configuration and data. On the other hand it means that the user configuration files, security patches and everything else in the system remains or get recovered after the factory status restore installation.

Assignment of verdict

The verdict PASS is assigned if:

- the DUT has the installation of the 3rd-party SW disabled by default:

  1) clear warning; and

  2) the request for consent; and

  3) the required input of the user consent prior to installation; and

- the DUT devises a clear way to restore to OEM SW state.

The verdict FAIL is assigned otherwise.

6.1.3.2 Test case HG 7.3-6 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the installation of the 3rd-party SW concerning the default configuration (a), the interaction with the administrator (b-c) and the SW-restore mechanism (d).

Test units

a) The TL **shall** check that in the original delivery condition, the option to install 3rd-party SW is disabled.

b) The TL **shall** perform a 3rd-party SW installation and functionally check whether the administrator receives a clear warning about the upcoming installation and the related risks the installation induces.

c) The TL **shall** functionally check whether the installation can be launched only with the consent of the administrator.

d) The TL **shall** functionally check whether the SW installation can be restored to the OEM state.

EXAMPLE: Restore the SW installation to the OEM state by installing a FW from a trustworthy manufacture source verified with the on board public key.

Assignment of verdict

The verdict PASS is assigned if:

- the DUT has the installation of the 3rd-party SW disabled by default; and
- clear warning about the installation, and the risk the installation induces, is prominently displayed to the current user; and
- the installation can be launched only with the consent of the administrator; and
- the DUT can successfully install a SW-update from a trustworthy manufacture source and be restored to the OEM SW state.

The verdict FAIL is assigned otherwise.

6.1.4 Test group HG 7.3-7 (added)

6.1.4.0 Test group objective

The test group addresses the provision HG 7.3-7 (added).

This test group addresses the signature of the update packages.

6.1.4.1 Test case HG 7.3-7 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the signature of each update package.

In contrast to 3rd-party-SW, each update package is supplied under liability of the HG manufacturer.

Test units

a) For each update mechanism in IXIT 7-UpdMech, the TL **shall** conceptually check whether each update package was digitally signed before releasing it to the public according to "Cryptographic Details", the corresponding "Security Guarantees" and "Description".

Assignment of verdict

The verdict PASS is assigned if:

- The HG manufacturers and/or trustworthy software providers have signed the update package before it is released to the public.
- The digital signature should proof to be verifiable and authentic.

The verdict FAIL is assigned otherwise.

6.1.4.2 Test case HG 7.3-7 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the signature of the update packages.

Test units

For each update mechanism in IXIT 7-UpdMech, the TL **shall** apply all **Test units** as specified in the Test Case HG 7.3-1 (added) to each one of the update mechanisms.

a) The TL **shall** perform an update with an appropriate signed update package and check whether the update signature can be successfully verified.

b) The TL **shall** perform a code modification of only one sign or bit of a signed update package and try to conduct an update with the modified package. In that case, the signature verification shall proof to fail and output according error messages. The modified update package shall be rejected and not installed.

NOTE: Appropriate means:

1) that the signature was generated with the private key of the manufacture or trusted software provider; and

2) the signed hash value equals to the hash value computed on the received update package.

Assignment of verdict

The verdict PASS is assigned if:

- the public verification key was pre-installed in the DUT and can effectively verify and authenticate the signature of the update package; and
- the signature of the original appropriately signed update package gets successfully verified and the update is performed successfully;
- the signature verification of the tampered signed update package failed with matching error messages and the update package was rejected and not installed, not even in parts.

The verdict FAIL is assigned otherwise.

6.1.5 Test group HG 7.3-8 (added)

6.1.5.0 Test group objective

The test group addresses the Provision HG 7.3-8 (added).

According to ETSI EN 303 645 [i.1] 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.

This test group addresses the best-practice techniques used for protecting the confidentiality of the update package containing sensitive data.

This test group applies only if the HG software contains sensitive data. Any discovery of the sensitive data is beyond the scope.

6.1.5.1 Test case 7.3-8 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptography used for encrypting updates 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 updates with sensitive data. The confidentiality of sensitive data in updates is required to be protected.

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 updates with sensitive data 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 that the cryptography is appropriate as best practice for the use case. In such a 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.2]. Moreover general reference catalogues of best practice cryptography are available, for example: SOGIS Agreed Cryptographic Mechanisms [i.6] (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 crypto agility, 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 basis 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 in ETSI TS 103 701 [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 updates with sensitive 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 for the desired security property.

The verdict FAIL is assigned otherwise.

6.2 TSO 7.4: Securely store sensitive security parameters

6.2.1 Test group HG 7.4-1 (added)

6.2.1.0 Test group objective

The present Test group HG 7.4-1 (added) addresses the provision HG 7.1-5 (refined) of ETSI TS 103 848 [1] which is an additional provision to clause 5.4 of ETSI EN 303 645 [i.1].

This test group assesses whether the access to Wi-Fi® and local administrator credentials is restricted to authenticated local administrator of the HG.

6.2.1.1 Test case HG 7.4-1 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the access control to Wi-Fi® and local administrator credentials.

Test units

a) The TL **shall** assess whether the declaration in "Type" of the Wi-Fi® and local administrator credentials, provided in IXIT 10-SecParam is consistent with the "Description".

b) The TL **shall** assess whether the "Security Guarantees" of the Wi-Fi® and local administrator credentials provided in IXIT 10-SecParam contain a description of access control concerning the credentials.

c) The TL **shall** assess whether the "Protection Scheme" of the Wi-Fi® and local administrator credentials provided in IXIT 10-SecParam contains the requirement to access to the credentials.

Assignment of verdict

The verdict PASS is assigned if:

- for the Wi-Fi® and local administrator credentials, the declarations are consistent with their description; and
- for the Wi-Fi® and local administrator credentials, the claimed security guarantees cover access control to the credentials; and
- for the Wi-Fi® and local administrator credentials, the claimed protection scheme indicates that only authenticated local administrator can access the credentials.

The verdict FAIL is assigned otherwise.

6.2.1.2 Test case HG 7.4-1 (added)-2 (functional)

Test purpose

The purpose of this test case is the conceptual assessment of the access control to Wi-Fi® and local administrator credentials.

Test units

a) The TL **shall** functionally assess whether the credentials for the Wi-Fi® and local administrator, provided in IXIT 10-SecParam "Protection Scheme", are implemented according to the IXIT documentation.

Assignment of verdict

The verdict PASS is assigned if:

- for the Wi-Fi® and local administrator credentials, there is no indication that the implementation of the corresponding protection scheme differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

6.2.2 Test group HG 7.4-2 (added)

6.2.2.0 Test group objective

The present Test group HG 7.4-2 (added) addresses the provision HG 7.4-2 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.4 of ETSI EN 303 645 [i.1].

This test group assesses whether the access to ISP administrator credentials is restricted to authenticated ISP administrator of the HG.

6.2.2.1 Test case HG 7.4-2 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the access control to ISP administrator credentials.

Test units

a) The TL **shall** assess whether the declaration in "Type" of the ISP administrator credentials, provided in IXIT 30-User is consistent with the "Description".

b) The TL **shall** assess whether the "Security Guarantees" of the ISP administrator credentials provided in IXIT 30-User contain a description of access control to the credentials.

c) The TL **shall** assess whether the "Protection Scheme" of the ISP administrator credentials provided in IXIT 30-User indicates the access protection to the ISP administrator credentials is based on authentication.

Assignment of verdict

The verdict PASS is assigned if:

- for the ISP administrator credentials, the declarations are consistent with their description; and
- for the ISP administrator credentials, the claimed security guarantees cover access control to the credentials; and
- for the ISP administrator credentials, the claimed protection scheme indicates that only an authenticated ISP administrator can access the credentials.

The verdict FAIL is assigned otherwise.

6.2.2.2 Test case HG 7.4-2 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the access control to ISP administrator credentials.

Test units

a) The TL **shall** functionally assess whether ISP administrator credentials provided in IXIT 30-User "Protection Scheme" are implemented according to the IXIT documentation.

Assignment of verdict

The verdict PASS is assigned if:

- For the ISP administrator credentials, there is no indication that the implementation of the corresponding protection scheme differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

6.2.3 Test group HG 7.4-3 (added)

6.2.3.0 Test group objective

The present Test group HG 7.4-3 (added) addresses the provision HG 7.4-3 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.4 of ETSI EN 303 645 [i.1].

This test group assesses whether the HG has different management strategies for user data and security critical data.

NOTE: ETSI EN 303 645 [i.1] defines sensitive security parameters as security-related secret information whose disclosure or modification can compromise the security of a security module. Some examples are secret cryptographic keys, network access authentication values such as pre-shared keys, or private components of certificates.

6.2.3.1 Test case HG 7.4-3 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment that user data and critical security parameters are managed independently.

Test units

a) The TL **shall** assess whether the declaration in "Type" of each critical security parameter, provided in IXIT 30-User is consistent with the "Description".

b) The TL **shall** assess whether the "Security Guarantees" and "Protection Scheme" of each critical security parameter, provided in IXIT 30-User contains a description of a management strategy for the parameter.

c) The TL **shall** assess whether the "Security Guarantees" and "Protection Scheme" of each user data, provided in IXIT 30-User contains a description of a management strategy for the data.

d) The TL **shall** assess whether the management strategy of critical security parameters and user data is different and complies with the management metric defined in ETSI TS 103 848 [1].

Assignment of verdict

The verdict PASS is assigned if:

- for each security parameter, the declaration is consistent with its description; and
- for each security parameter, the claimed security guarantee covers a management strategy for the parameter; and
- for all user data, the claimed security guarantee covers a management strategy for the user data; and
- for critical security parameters and user data, the management strategy complies with the metric from ETSI TS 103 848 [1].

The verdict FAIL is assigned otherwise.

6.2.3.2 Test case HG 7.4-3 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the difference of the management strategy for user data and critical security parameters.

Test units

a) The TL **shall** functionally assess whether the "Security Guarantee" and "Protection Scheme" to each critical security parameter provided in IXIT 30-User are implemented correctly according to the IXIT documentation.

b) The TL **shall** functionally assess whether the "Security Guarantee" and "Protection Scheme" to general user data provided in IXIT 30-User are implemented correctly according to the IXIT documentation.

Assignment of verdict

The verdict PASS is assigned if:

- for all critical security parameters, there is no indication that the implementation of the corresponding security guarantee and protection scheme differs from its IXIT documentation; and
- for all user data, there is no indication that the implementation of the corresponding security guarantee and protection scheme differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

6.2.4 Test group HG 7.4-9 (added)

6.2.4.0 Test group objective

The present Test group HG 7.4-9 (added) addresses the provision HG 7.4-9 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.4 of ETSI EN 303 645 [i.1].

This test group assesses whether the HG is able to produce random bits with an appropriate entropy in compliance to publicly available standard quality metrics.

6.2.4.1 Test case HG 7.4-9 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the generation of random number.

Test units

a) The TL **shall** assess whether the declaration in "Generation Mechanism" of the security parameters, provided in IXIT 30-User contains description of random a/the data generator and its entropy sources.

b) The TL **shall** assess whether the random data generating mechanism described in "Generation Mechanism" of the security parameters provided in IXIT 30-User meets the requirements of publicly available standard quality metrics.

EXAMPLE: A widely accepted quality metric can be found in NIST SP 800-90B [i.3], ETSI TS 119 312 [i.4] and in other national guidance.

Assignment of verdict

The verdict PASS is assigned if:

- for the security parameters provided in IXIT 30-User, the declarations contain a description of a random data generator and its entropy sources; and
- for each security parameter with a random number generator involved in data generation, the claimed random number generating mechanism meets the requirements of publicly available standard quality metrics.

The verdict FAIL is assigned otherwise.

6.2.4.2 Test case HG 7.4-9 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the generation of random number.

Test units

a) The TL **shall** functionally assess whether the claimed IXIT 30-User "Generation Mechanism" meets the requirements of the claimed public standard quality metrics.

Assignment of verdict

The verdict PASS is assigned if:

- For all security parameters generated by a random number generator, the randomization meets the requirements of publicly available standard quality metrics.

The verdict FAIL is assigned otherwise.

6.3 TSO 7.5: Communicate securely

6.3.1 Test group HG 7.5-6 (added)

6.3.1.0 Test group objective

The present Test group HG 7.5-6 (added) addresses the provision HG 7.5-6 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.5 of ETSI EN 303 645 [i.1].

This test group assesses whether the default configuration settings of the HG firewall are the most restrictive settings to protect a layman user.

6.3.1.1 Test case HG 7.5-6 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the security of default firewall configuration settings.

Test units

a) The TL **shall** assess whether IXIT 13-SoftServ contains a description of firewall functionality.

b) The TL **shall** assess whether the "Default Settings" of the firewall functionality provided in IXIT 13-SoftServ provide sufficient security to HG.

NOTE: The most restrictive firewall settings depend on the implemented design of firewall and should be assessed and determined by the TL.

Assignment of verdict

The verdict PASS is assigned if:

- the HG support firewall functionality; and
- for the firewall functionality, the claimed default settings provide maximum security to user.

The verdict FAIL is assigned otherwise.

6.3.1.2 Test case HG 7.5-6 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the security of default firewall configuration settings.

Test units

a) The TL **shall** functionally assess whether the firewall functionality provided in IXIT 13-SoftServ "Default Settings" is implemented according to the IXIT documentation.

Assignment of verdict

The verdict PASS is assigned if:

- For the firewall functionality, there is no indication that the implementation of the default settings differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

6.3.2 Test group HG 7.5-7 (added)

6.3.2.0 Test group objective

The present Test group HG 7.5-7 (added) addresses the provision HG 7.5-7 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.4 of ETSI EN 303 645 [i.1].

This test group assesses the configuration of port forwarding rules in the HG factory default state.

6.3.2.1 Test case HG 7.5-7 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the default setting of the port forwarding rules.

Test units

a) The TL **shall** assess whether IXIT 13-SoftServ contains description of firewall functionality.

b) The TL **shall** assess whether the "Default Settings" of the firewall functionality provided in IXIT 13-SoftServ indicates no port forwarding rules are configured in the initialized state.

Assignment of verdict

The verdict PASS is assigned if:

- the HG support firewall functionality; and
- for the firewall functionality, the claimed default settings contain no port forwarding rule.

The verdict FAIL is assigned otherwise.

6.3.2.2 Test case HG 7.5-7 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the default setting of the port forwarding rules.

Test units

a) The TL **shall** functionally assess whether the default forwarding rule configuration of the firewall functionality provided in IXIT 13-SoftServ "Default settings" is implemented according to the IXIT documentation.

Assignment of verdict

The verdict PASS is assigned if:

- For the firewall functionality, there is no indication that the implementation of the forwarding rule default settings differs from its IXIT documentation.

The verdict FAIL is assigned otherwise.

6.4 TSO 7.6: Minimize exposed attack surfaces

6.4.1 Test group HG 7.6-1 (added)

6.4.1.0 Test group objective

The present Test group HG 7.6-1 (added) addresses the provision HG 7.6-1 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 7.6 of ETSI EN 303 645 [i.1].

This test group assesses the physical interfaces of the DUT. The physical debug or other test interface used during development, such as JTAG connector (and the software components), shall be permanently disabled or physically removed from the PCB.

6.4.1.1 Test case HG 7.6-1 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the physical debug interfaces during development.

Test units

a) For each physical interface in IXIT 15-Intf or other documentations that is described as a debug interface during development according to "Description", the TL **shall** check whether the interface is disabled permanently or physical removed according to "Status".

b) The TL **shall** ensure that any hardware interface including also non-IXIT interfaces is documented. This may include opening of the housing to inspect for internal connectors.

Assignment of verdict

The verdict PASS is assigned if:

- For every physical debug interface during development, the interface is permanently disabled or physically removed.
- At the point in time, the device leaves development premises, all physical debug interfaces are disabled permanently or physical removed according to "Status".

The verdict FAIL is assigned otherwise.

6.4.1.2 Test case HG 7.6-1 (added)-2 (functional)

Test purpose

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

Test units

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

b) The TL **shall** functionally assess whether common physical debugging interfaces can be used for debugging purposes although it is not claimed as a "Debug Interface" in IXIT 15-Intf.

EXAMPLE: Common physical debugging interfaces include JTAG, SWD, etc.

NOTE: The TL can assess the accessibility of the physical debugging interfaces by checking the accessibility of both physical connectors and software components.

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

6.4.2 Test group HG 7.6-2 (added)

6.4.2.0 Test group objective

The present Test group HG 7.6-2 (added) addresses the provision HG 7.6-2 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.6 of ETSI EN 303 645 [i.1].

This test group assesses the software debug interfaces of the DUT. The software debug interface used during development, such as gdb and hexdump, shall be permanently disabled, locked or removed before delivery.

6.4.2.1 Test case HG 7.6-2 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the software debug interfaces during development.

Test units

a) For each software interface in IXIT 15-Intf that is described as a debug interface during development according to "Description", the TL **shall** check whether the interface is disabled, locked or removed permanently according to "Status".

b) The TL **shall** ensure that any software debug and test interface including also non-IXIT interfaces is documented.

Assignment of verdict

The verdict PASS is assigned if:

- For every software debug interface that is indicated as intermittently required during development, the interface is disabled, locked or removed.
- The TL has confirmed that any software debug interface and any other software interface has been documented and none is missing in the documentation.

The verdict FAIL is assigned otherwise.

6.4.2.2 Test case HG 7.6-2 (added)-2 (functional)

Test purpose

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

Test units

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

b) For each software 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.

Assignment of verdict

The verdict PASS is assigned if:

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

The verdict FAIL is assigned otherwise.

6.4.3 Test group HG 7.6-3 (added)

6.4.3.0 Test group objective

The present Test group HG 7.6-3 (added) addresses the provision HG 7.6-3 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.6 of ETSI EN 303 645 [i.1].

This test group assesses the isolation between different types of Wi-Fi® subnets. The DUT shall use different keys to encrypt traffic data transmitted in different Wi-Fi® subnets.

6.4.3.1 Test case HG 7.6-3 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the cryptographic isolation between different types of Wi-Fi® SSID the DUT supports.

Test units

a) The TL **shall** check the "Description" of IXIT 11-ComMech or other documentation to assess the types of Wi-Fi® the DUT supports.

b) If the DUT supports guest Wi-Fi® or community Wi-Fi®, the TL **shall** check the "Cryptographic Details" of IXIT 11-ComMech or other documentation to assess whether data transmitted in different Wi-Fi® SSID is cryptographically isolated from each other.

Assignment of verdict

The verdict PASS is assigned if:

- the DUT supports guest Wi-Fi® and/or community Wi-Fi® according to IXIT 11-ComMech or other documentation; and
- the DUT provides cryptographic isolation for each types of Wi-Fi® SSID according to IXIT 11-ComMech or other documentation.

The verdict FAIL is assigned otherwise.

6.4.3.2 Test case HG 7.6-3 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the cryptographic isolation between different types of Wi-Fi® the DUT supports.

Test units

a) For each Wi-Fi® type the DUT supports according to IXIT 11-ComMech or other documentation, the TL **shall** functionally check whether the Wi-Fi® SSID is cryptographically isolated from others as claimed.

NOTE 1: Methods for capturing data transmitted in different Wi-Fi® SSID include wireless packet sniffers for IEEE 802.11™ such as "aircrack".

NOTE 2: To assess cryptographic isolation between different SSID, the TL should ensure that the data sent is known plaint text - to be verified by the recipient with an application - and that the wireless packets of different SSID send the same data.

Assignment of verdict

The verdict PASS is assigned if:

- Each Wi-Fi® SSID the DUT supports is cryptographically isolated from each other as claimed.

The verdict FAIL is assigned otherwise.

6.4.4 Test group HG 7.6-4 (added)

6.4.4.0 Test group objective

The present Test group HG 7.6-4 (added) addresses the provision HG 7.6-4 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.6 of ETSI EN 303 645 [i.1].

This test group assesses if it is feasible for any user not connected to the normal Wi-Fi®, such as users of a guest Wi-Fi® or community Wi-Fi® to access any assets only available to normal users.

6.4.4.1 Test case HG 7.6-4 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the accessibility of user devices connected in user host network from guest or community Wi-Fi® SSID.

Test units

a) The TL **shall** check the "Description" of IXIT 11-ComMech or other documentation to assess the types of Wi-Fi® the DUT supports.

b) If the DUT supports guest Wi-Fi® or community Wi-Fi®, the TL **shall** check the "Security Guarantees" entry of IXIT 11-ComMech or other documentation to assess whether assets from the host Wi-Fi® are not accessible for a guest or community network user.

Assignment of verdict

The verdict PASS is assigned if:

- the DUT supports guest Wi-Fi® or community Wi-Fi® according to IXIT 11-ComMech or other documentation; and
- assets from the host Wi-Fi® are not accessible for a guest or community user according to IXIT 12-NetSecImpl or other documentation.

The verdict FAIL is assigned otherwise.

6.4.4.2 Test case HG 7.6-4 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the feasibility of user's device under different types of Wi-Fi® SSID.

Test units

a) The TL **shall** functionally assess whether a guest or community Wi-Fi® user can access assets from the host Wi-Fi®.

Assignment of verdict

The verdict PASS is assigned if:

- assets from the host Wi-Fi® are not accessible to a guest or community Wi-Fi® user as claimed in IXIT 12-NetSecImpl or other documentation.

EXAMPLE: The TL can log into a guest or community network with knowledge of network-addresses of devices in the user host-network and try to connect to them to assess the accessibility.

The verdict FAIL is assigned otherwise.

6.4.5 Test group HG 7.6-9 (added)

6.4.5.0 Test group objective

The present Test group HG 7.6-9 (added) addresses the provision HG 7.6-9 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.6 of ETSI EN 303 645 [i.1].

This test group assesses the configuration of Access Control Lists (ACLs) for host Wi-Fi® and guest Wi-Fi®. The ACLs for host and guest Wi-Fi® shall be accessible only to an authenticated local or remote ISP administrator.

6.4.5.1 Test case HG 7.6-9 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the accessibility of the configuration of ACLs for host Wi-Fi® and guest Wi-Fi®.

Test units

a) The TL **shall** check the "Description" of IXIT 13-SoftServ or other documentation to judge whether the DUT supports Wi-Fi® and guest Wi-Fi® feature.

b) For host Wi-Fi® and guest Wi-Fi®, the TL **shall** check the "Allows Configuration" of IXIT 13-SoftServ or other documentation to judge whether the DUT supports configuration of ACLs.

c) For host Wi-Fi® and guest Wi-Fi®, the TL **shall** check the "Authentication Mechanism" of IXIT 13-SoftServ to assess whether the configuration of ACLs is only accessible to an authenticated local or remote ISP administrator.

Assignment of verdict

The verdict PASS is assigned if:

- the DUT supports Wi-Fi® and guest Wi-Fi; and
- the DUT supports configuration of ACLs for host Wi-Fi® and guest Wi-Fi; and
- for host Wi-Fi® and guest Wi-Fi, the configuration of ACLs is only accessible for an authenticated local or remote ISP administrator.

The verdict FAIL is assigned otherwise.

6.4.5.2 Test case HG 7.6-9 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the configuration of ACLs for host Wi-Fi® and guest Wi-Fi®.

Test units

a) For host Wi-Fi® and guest Wi-Fi®, the TL **shall** functionally check whether the configuration of ACLs is not accessible for normal users other than an authenticated local or remote ISP administrator.

b) As an administrative user allowed to configure the ACL, the TL **shall** remove login permission of a user in guest or community Wi-Fi® and check that the HG follows the modified ACL. The removed user shall not be able to log into the host Wi-Fi® and guest Wi-Fi® after the changed ACL became active.

Assignment of verdict

The verdict PASS is assigned if:

- the configuration of ACLs for host Wi-Fi® and guest Wi-Fi® is only accessible to an authenticated local or remote ISP administrator;

- the ACL is implemented correctly on the DUT.

The verdict FAIL is assigned otherwise.

6.5 TSO 7.12: Make installation and maintenance of devices easy

6.5.1 Test group HG 7.12-1 (added)

6.5.1.0 Test group objective

The present Test group HG 7.12-1 (added) addresses the provision HG 7.12-1 (added) of ETSI TS 103 848 [1] which is an additional provision to clause 5.12 of ETSI EN 303 645 [i.1].

This test group assesses the Telnet interfaces of the DUT. The Telnet service provides text-based interactive communication for administrators to configure the HG. It shall be disabled by default since it can easily be exploited by an attacker to access the HG.

6.5.1.1 Test case HG 7.12-1 (added)-1 (conceptual)

Test purpose

The purpose of this test case is the conceptual assessment of the default status of the Telnet service.

Test units

a) The TL **shall** check the "Description" and "Status" of IXIT 13-SoftServ or other documentation to assess the default status of the Telnet service.

Assignment of verdict

The verdict PASS is assigned if:

- There is no Telnet service installed on the DUT or the Telnet service is disabled by default according to IXIT 13-SoftServ or other documentation.

The verdict FAIL is assigned otherwise.

6.5.1.2 Test case HG 7.12-1 (added)-2 (functional)

Test purpose

The purpose of this test case is the functional assessment of the default status of Telnet service.

Test units

a) The TL **shall** functionally assess whether the default status claimed in IXIT 13-SoftServ "Status" or other documentation is implemented correctly.

EXAMPLE: The TL can perform a full portscan of DUT to assess whether the Telnet service is accessible.

Assignment of verdict

The verdict PASS is assigned if:

- The Telnet service is disabled by default as claimed.

The verdict FAIL is assigned otherwise.

Annex A (normative): Home Gateway Pro formas for the SO

A.1 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the Identification of the DUT pro forma, ICS pro forma and IXIT pro forma in this annex so that they can be used for their intended purposes and may further publish the completed pro formas.

A.2 Identification of the DUT pro forma for Home Gateway

Clause A.2 in ETSI TS 103 701 [2], which specifies the DUT pro forma, also applies in the present document.

A.3 Implementation Conformance Statement (ICS) pro forma for Home Gateway

Table A.1 provides a mechanism for the user of the present document (who is expected to be an entity involved in the development or manufacturing of Home Gateway) to give information about the implementation of the provisions within ETSI TS 103 848 [1].

The provision column gives reference to the provisions in ETSI EN 303 645 [i.1] and ETSI TS 103 848 [1].

The status column indicates the status of a provision. The following notations are used:

M	the provision is a mandatory requirement
R	the provision is a recommendation
M C	the provision is a mandatory requirement and conditional
R C	the provision is a recommendation and conditional

NOTE: Where the conditional notation is used, this is conditional on the text of the provision. The conditions are provided at the bottom of the table with references provided for the relevant provisions to help with clarity.

The support column can be filled in by the user of the present document. The following notations are used:

Y	supported by the implementation
N	not supported by the implementation
N/A	the provision is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the product in question)

The detail column can be filled in by the user of the present document:

- If a provision is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.
- If a provision is not supported by the implementation, the entry in the detail column is to contain information on the reasons why implementation is not possible or not appropriate.

- If a provision is not applicable, the entry in the detail column is to contain the rationale for this determination.

Table A.1: Implementation of provisions for HG security

Clause number and title			
Provision	**Status**	**Support**	**Detail**
4.1 Reporting implementation			
HG 4.1 (extended)	M		
5.1 No universal default passwords			
HG 5.1-1 (extended)	M C		
Provision 5.1-2	M C		
Provision 5.1-3	M C		
HG 5.1-4 (extended) a	M		
HG 5.1-4 (extended) b	M		
HG 5.1-4 (extended) c	M		
HG 5.1-5 (refined)	M		
5.2 Implement a means to manage reports of vulnerabilities			
HG 5.2-1 (information)	M		
HG 5.2-2 (information)	R		
Provision 5.2-3	R		
5.3 Keep software updated			
HG 5.3-1 (extended) a	M C (1)		
HG 5.3-1 (extended) b	M (1)		
HG 5.3-2 (refined)	M (1)		
Provision 5.3-3	M C		
Provision 5.3-4	R C		
HG 5.3-5 (refined)	R (1)		
HG 5.3-6 (extended)	M C (1)		
Provision 5.3-7	M C		
Provision 5.3-8	M C		
HG 5.3-9 (promoted) a	M (1)		
HG 5.3-9 (extended) b	M C (1)		
Provision 5.3-10	M		
HG 5.3-11 (refined)	R (1)		
Provision 5.3-12	R C		
Provision 5.3-13	M		
HG 5.3-14 (excluded)	Not applicable		
HG 5.3-15 (excluded)	Not applicable		
HG 5.3-16 (extended)	M		
5.4 Securely store sensitive security parameters			
HG 5.4-1 (information)	M		
Provision 5.4-2	M C		
Provision 5.4-3	M		
Provision 5.4-4	M		
5.5 Communicate securely			
HG 5.5-1 (information)	M		
Provision 5.5-2	R		
HG 5.5-3 (information)	R		
HG 5.5-4 (extended) a	R		
HG 5.5-4 (extended) b	R		
HG 5.5-5 (information)	M		
Provision 5.5-6	R		
Provision 5.5-7	M		
Provision 5.5-8	M		
5.6 Minimize exposed attack surfaces			
HG 5.6-1 (extended)	M C (3)		
Provision 5.6-2	R		
Provision 5.6-3	R		
Provision 5.6-4	R		
HG 5.6-5 (promoted)	M		
Provision 5.6-6	R		
HG 5.6-7 (extended)	R C		
Provision 5.6-8	R		
HG 5.6-9 (extended) b	R		

Clause number and title			
Provision	**Status**	**Support**	**Detail**
5.7 Ensure software integrity			
HG 5.7-1 (extended)	R		
HG 5.7-2 (extended)	R		
5.8 Ensure that personal data is secure			
Provision 5.8-1	R		
Provision 5.8-2	M		
Provision 5.8-3	M		
5.9 Make systems resilient to outages			
Provision 5.9-1	R		
HG 5.9-2 (promoted)(refined)	M C (5)		
HG 5.9-3 (extended)	R C (5)		
5.10 Examine system telemetry data			
Provision 5.10-1	R C		
5.11 Make it easy for users to delete user data			
Provision 5.11-1	M		
Provision 5.11-2	R		
Provision 5.11-3	R		
Provision 5.11-4	R		
5.12 Make installation and maintenance of devices easy			
HG 5.12-1 (extended)	R		
Provision 5.12-2	R		
Provision 5.12-3	R		
5.13 Validate input data			
Provision 5.13-1	M		
6 Adapted Data protection provisions for the HGs			
Provision 6.1	M		
Provision 6.2	M C		
Provision 6.3	M		
Provision 6.4	R C		
Provision 6.5	M C		
7.1 No universal default passwords			
HG 7.1-1 (added)	R		
7.2 Implement a means to manage reports of vulnerabilities			
7.3 Keep software updated			
HG 7.3-1 (added)	M		
HG 7.3-2 (added)	R C		
HG 7.3-3 (added)	R C (4)		
HG 7.3-4 (added)	M		
HG 7.3-5 (added)	R C		
HG 7.3-6 (added)	M C		
HG 7.3-7 (added)	M		
HG 7.3-8 (added)	M C		
7.4 Securely store sensitive security parameters			
HG 7.4-1 (added)	M		
HG 7.4-2 (added)	M		
HG 7.4-3 (added)	M		
HG 7.4-4 (added)	R		
HG 7.4-5 (added)	R C		
HG 7.4-6 (added)	R C		
HG 7.4-7 (added)	R C		
HG 7.4-8 (added)	R		
HG 7.4-9 (added)	M		
HG 7.4-10 (added)	R		
HG 7.4-11 (added)	R C		
HG 7.4-12 (added)	R		
7.5 Communicate securely			
HG 7.5-1 (added)	R		
HG 7.5-2 (added)	R		
HG 7.5-3 (added)	R		
HG 7.5-4 (added)	R		
HG 7.5-5 (added)	R C		
HG 7.5-6 (added)	M C		
HG 7.5-7 (added)	M C		

Clause number and title			
Provision	**Status**	**Support**	**Detail**
HG 7.5-8 (added)	R		
HG 7.5-9 (added)	R		
HG 7.5-10 (added)	R		
HG 7.5-11 (added)	R		
7.6 Minimize exposed attack surfaces			
HG 7.6-1 (added)	M		
HG 7.6-2 (added)	M		
HG 7.6-3 (added)	M C (3)		
HG 7.6-4 (added)	M C (3)		
HG 7.6-5 (added)	R (4)		
HG 7.6-6 (added)	R C		
HG 7.6-7 (added)	R C		
HG 7.6-8 (added)	R		
HG 7.6-9 (added)	M C		
7.7 Ensure software integrity			
HG 7.7-1 (added)	R		
HG 7.7-2 (added)	R		
7.8 Ensure that personal data is secure			
7.9 Make system resilient to outages			
7.10 Collecting log data			
HG 7.10-1 (added)	R		
HG 7.10-2 (added)	R		
HG 7.10-3 (added)	R		
HG 7.10-4 (added)	R		
HG 7.10-5 (added)	R		
HG 7.10-6 (added)	R		
7.11 Make it easy for users to delete user data			
7.12 Make installation and maintenance of devices easy			
HG 7.12-1 (added)	M		
7.13 Validate input data			
Conditions: 1) An update mechanism is implemented. 2) Open source software or 3rd-party software is used. 3) A guest or community Wi-Fi® channel is enabled. 4) The programming language contains unsecure functions that have been superseded by secure counterparts. 5) The HG device fails in its function due to power loss or similar failure.			

A.4 Implementation eXtra Information for Testing (IXIT) pro forma for Home Gateway

In the following, modified IXIT entries, new IXIT entries and/or new IXIT tables or lists are specified based on the modified and added provisions in the ETSI TS 103 848 [1] according to clause 4.1.2 of the present document:

- A new IXIT entry is created and added to an existing table or list from ETSI TS 103 701 [2].

IXIT 2-UserInfo: User Information

The following IXIT entry is new and is added to the original IXIT table IXIT 2-UserInfo from ETSI TS 103 701 [2]:

- **Software Version Numbers** (added): Software version numbers of the DUT and a brief description of which user and how the user can retrieve the software version numbers of the DUT.

IXIT 13-SoftServ: Software Services

The following IXIT entry is new and is added to the original IXIT table IXIT 13-SoftServ from ETSI TS 103 701 [2]:

- **Default Settings** (added): List of default settings to specific software service.

IXIT 30-UserData: User data in transmission and in storage

The completed IXIT lists all types of user data that are transmitted or persistently stored on the DUT during intended usage. The pro forma contains the following entries and is typically filled out in form of a table:

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
- **Description:** Brief description of the user data, including its purpose.
- **Security Guarantees:** Description of the realized baseline security objectives and threats the security parameter is protected against during persistent storage.
- **Protection Scheme:** Description of the measures that are applied to achieve the "Security Guarantees". This includes the principals and roles through which access to the parameter is possible, including the privileges associated to each role.

IXIT 31-ThiParSoft (added): 3rd-party Software

The completed IXIT lists all standalone 3rd-party SW of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

NOTE 1: There can be two different types of the 3rd-party SW, the first type is the integrated 3rd-party SW incorporated in the firmware component and released by the OEM or trusted software provider. This type of 3rd-party SW was an included part of the OEM development, released for the HG and will be installed along with the software component to constitute the complete HG device. The user of the HG cannot distinguish between the parts the OEM firmware is constituted from.
And, the second type is a, from the HG manufacturer development separated, extra 3rd-party SW which can optionally be chosen and installed by the owner or his administrator of the HG. This 3rd-party SW is out of the responsibility of the HG manufacturer and can implement a security risk if installed.
The test group targets the separated, extra 3rd-party SW installed on owner or administrator discretion.

EXAMPLE: The owner or administrator of the HG could decide to download, install and execute an application that measures and logs the available bandwidth. On top, that application provides its records via a dedicated web-interface.

- **ID:** Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
- **Description:** If the HG provides functionality to download and install 3rd-party SW, then the HG should provide user guidance for the correct installation and is required to explicit output a warning and require consent prior to download and installation.
For the testing of the HG, the TL requires a brief description of the 3rd-party SW including its functionality and interfaces.
- **Security Provision:** Description of the realized security objectives and the threats the installation is protected against.

NOTE 2: The installation of 3rd-party SW only starts after the administrator has confirmed his awareness of the potential risk and has given his consent. If "signature verification" configuration has been chosen, the public key of the 3rd-party software provider needs to be installed prior to the 3rd-party SW installation. Further, the download server of the 3rd-party SW needs to be listed within to the "URI list" configuration, if an online installation has been chosen.

- **Initiation and Interaction:** The HG delivery shall provide commensurate user guidance of the procedures of the initiation, HG configuration, installation and user interaction. If the HG provides functionality for the download and installation of 3rd-party SW then this shall be part of the user guidance too.
- **Configuration:** The default configuration of the HG disables the 3rd-party-download and installation. Enable/disable 3rd-party SW installation and the URI list of download servers are possible configurations or options to choose from. But, if 3rd-party SW installation is enabled, then the SW signature verification shall always be enabled.

- **Software Restore:** The software recovery mechanism supports the authenticated and authorized user or administrator to remove all after delivery installed 3rd-party SW from the HG, and recovers all SW stemming from the OEM. The recovery mechanism may also include the installation of SW-updates from the OEM server or trustworthy SW provider.

NOTE 3: If 3rd-party SW gets executed, the HG manufacturer is out of scope and control of the device The liability is persistently moved to the HG's owner or user/admin, as the HG was modified without manufacturer acceptance and the HG is in a unknown status. For the case, the software recovery mechanism is provided by the HG manufacturer, and the SW source is trustworthy, then all restored SW can be verified by means of digital signature using the HG-on-board public key. Provided, the HG hardware remains untouched, and if the HG is after the conduct of the software recovery mechanism either in the original delivery status or in the current OEM provided updated status, the HG manufacturer remains liable.

Annex B (informative): Matching tables for Home Gateway

B.1 Overview of required IXIT entries per provision for Home Gateway

As described in the assessment procedure in clause 4.3 of ETSI TS 103 701 [2], Table B.1 describes for each provision in ETSI TS 103 848 [1] which IXIT entries are required to perform the corresponding test group.

Table B.1: Required IXIT entries per provision

Provisions from the ETSI TS 103 848 [1]	Required IXIT entries
HG 4.1 (extended)	None
HG 5.1-1 (extended)	**IXIT 1-AuthMech:** ID, Description, Authentication Factor, Password Generation Mechanism
HG 5.1-4 (extended)-a	**IXIT 1-AuthMech:** ID, Description, Authentication Factor **IXIT 2-UserInfo:** Documentation of Change Mechanisms
HG 5.1-4 (extended)-b	**IXIT 1-AuthMech:** ID, Description, Authentication Factor **IXIT 2-UserInfo:** Documentation of Change Mechanisms
HG 5.1-4 (extended)-c	**IXIT 1-AuthMech:** ID, Description, Authentication Factor **IXIT 2-UserInfo:** Documentation of Change Mechanisms
HG 5.1-5 (refined)	**IXIT 1-AuthMech:** ID, Description, Brute Force Prevention
HG 5.3-1 (extended) a	**IXIT 6-SoftComp:** ID, Update Mechanism **IXIT 2-UserInfo:** ID, Publication of Non-Updatable
HG 5.3-1 (extended) b	**IXIT 7-UpdMech:** ID, Description, Cryptographic Details, Initiation and Interaction
HG 5.3-2 (refined)	**IXIT 7-UpdMech:** ID, Description, Security Guarantees, Cryptographic Details, Initiation and Interaction
HG 5.3-6 (extended)	**IXIT 7-UpdMech:** ID, Description, Initiation and Interaction, Configuration, User Notification
HG 5.3-9 (extended) b	**IXIT 7-UpdMech:** ID, Description, Security Guarantees, Cryptographic Details
HG 5.3-16 (extended)	**IXIT 2-UserInfo:** Software Version Numbers (added)
HG 5.6-1 (extended)	**IXIT 13-SoftServ:** ID, Description, Type, Security Guarantees, Protection Scheme
HG 5.9-2 (promoted)	**IXIT 23-ResMech:** ID, Description, Type, Security Guarantees
HG 7.3-1 (added)	**IXIT 7-UpdMech:** ID, Cryptographic Details, Security Guarantees, Description
HG 7.3.4 (added)	**IXIT 13-SoftServ:** ID, Description, Status, Justification, Allows Configuration, Authentication Mechanism
HG 7.3-6 (added)	**IXIT 31-ThiParSoft (added):** ID, Description, Configuration, Initiation and Interaction, Security Guarantee
HG 7.3-7 (added)	**IXIT 7-UpdMech:** ID, Cryptographic Details, Security Guarantees, Description
HG 7.3-8 (added)	**IXIT 7-UpdMech:** ID, Description, Security Guarantees, Cryptographic Details
HG 7.4-1 (added)	**IXIT 10-SecParam:** ID, Description, Type, Security Guarantees, Protection Scheme
HG 7.4-2 (added)	**IXIT 10-SecParam:** ID, Description, Type, Security Guarantees, Protection Scheme
HG 7.4-3 (added)	**IXIT 10-SecParam:** ID, Description, Type, Security Guarantees, Protection Scheme **IXIT 30-UserData:** ID, Description, Type, Security Guarantees, Protection Scheme
HG 7.4-9 (added)	**IXIT 10-SecParam:** ID, Description, Type, Generation Mechanism
HG 7.5-6 (added)	**IXIT 13-SoftServ:** ID, Description, Status, Default Settings
HG 7.5-7 (added)	**IXIT 13-SoftServ:** ID, Description, Status, Default Settings
HG 7.6-1 (added)	**IXIT 15-Intf:** ID, Description, Type, Status, Debug Interface, Protection
HG 7.6-2 (added)	**IXIT 15-Intf:** ID, Description, Type, Status, Debug Interface, Protection
HG 7.6-3 (added)	**IXIT 11-ComMech:** ID, Description, Cryptographic details
HG 7.6-4 (added)	**IXIT 1-ComMech:** ID, Description, Security Guarantees
HG 7.6-9 (added)	**IXIT 13-SoftServ:** ID, Description, Allows Configuration, Authentication Mechanism
HG 7.12-1 (added)	**IXIT 13-SoftServ:** ID, Description, Status

B.2 Overview of required test groups per provision for Home Gateway

Table B.2: Required test groups per provision

Provisions from the ETSI TS 103 848 [1]	Test groups for a conformance assessment of the corresponding provision
Provision HG 5.1-1 (extended)	Test group HG 5.1-1 (extended)
Provision 5.1-2	Test group 5.1-2 from ETSI TS 103 701 [2]
Provision 5.1-3	Test group 5.1-3 from ETSI TS 103 701 [2]
Provision HG 5.1-4 (extended)-a	Test group HG 5.1-4 (extended)-a
Provision HG 5.1-4 (extended)-b	Test group HG 5.1-4 (extended)-b
Provision HG 5.1-4 (extended)-c	Test group HG 5.1-4 (extended)-c
Provision HG 5.1-5 (refined)	Test group HG 5.1-5 (refined)
Provision 5.2-1	Test group 5.2-1 from ETSI TS 103 701 [2]
Provision HG 5.3-1 (extended)-a	Test group HG 5.3-1 (extended)-a
Provision HG 5.3-1 (extended)-b	Test group HG 5.3-1 (extended)-b
Provision HG 5.3-2 (refined)	Test group HG 5.3-2 (refined)
Provision 5.3-3	Test group 5.3-3 from ETSI TS 103 701 [2]
Provision HG 5.3-6 (extended)	Test group HG 5.3-6 (extended)
Provision 5.3-7	Test group 5.3-6 from ETSI TS 103 701 [2]
Provision 5.3-8	Test group 5.3-7 from ETSI TS 103 701 [2]
Provision HG 5.3-9 (promoted)-a	Test group 5.3-9 from ETSI TS 103 701 [2]
Provision HG 5.3-9 (extended)-b	Test group HG 5.3-9 (extended)-b
Provision 5.3-10	Test group 5.3-10 from ETSI TS 103 701 [2]
Provision 5.3-13	Test group 5.3-13 from ETSI TS 103 701 [2]
Provision HG 5.3-16 (extended)	Test group HG 5.3-16 (extended)
Provision 5.4-1	Test group 5.4-1 from ETSI TS 103 701 [2]
Provision 5.4-2	Test group 5.4-2 from ETSI TS 103 701 [2]
Provision 5.4-3	Test group 5.4-3 from ETSI TS 103 701 [2]
Provision 5.4-4	Test group 5.4-4 from ETSI TS 103 701 [2]
Provision 5.5-1	Test group 5.5-1 from ETSI TS 103 701 [2]
Provision 5.5-5	Test group 5.5-5 from ETSI TS 103 701 [2]
Provision 5.5-7	Test group 5.5-7 from ETSI TS 103 701 [2]
Provision 5.5-8	Test group 5.5-8 from ETSI TS 103 701 [2]
Provision HG 5.6-1 (extended)	Test group HG 5.6-1 (extended)
Provision HG 5.6-5 (promoted)	Test group 5.6-5 from ETSI TS 103 701 [2]
Provision 5.8-2	Test group 5.8-2 from ETSI TS 103 701 [2]
Provision 5.8-3	Test group 5.8-3 from ETSI TS 103 701 [2]
Provision HG 5.9-2 (promoted)(refined)	Test group HG 5.9-2 (promoted)(refined)
Provision 5.11-1	Test group 5.11-1 from ETSI TS 103 701 [2]
Provision 5.13-1	Test group 5.13-1 from ETSI TS 103 701 [2]
Provision 6.1	Test group 6.1 from ETSI TS 103 701 [2]
Provision 6.2	Test group 6.2 from ETSI TS 103 701 [2]
Provision 6.3	Test group 6.3 from ETSI TS 103 701 [2]
Provision 6.5	Test group 6.5 from ETSI TS 103 701 [2]
Provision HG 7.3-1 (added)	Test group HG 7.3-1 (added)
Provision HG 7.3-4 (added)	Test group HG 7.3-4 (added)
Provision HG 7.3-6 (added)	Test group HG 7.3-6 (added)
Provision HG 7.3-7 (added)	Test group HG 7.3-7 (added)
Provision HG 7.3-8 (added)	Test group HG 7.3-8 (added)
Provision HG 7.4-1 (added)	Test group HG 7.4-1 (added)
Provision HG 7.4-2 (added)	Test group HG 7.4-2 (added)
Provision HG 7.4-3 (added)	Test group HG 7.4-3 (added)
Provision HG 7.4-9 (added)	Test group HG 7.4-9 (added)
Provision HG 7.5-6 (added)	Test group HG 7.5-6 (added)
Provision HG 7.5-7 (added)	Test group HG 7.5-7 (added)
Provision HG 7.6-1 (added)	Test group HG 7.6-1 (added)
Provision HG 7.6-2 (added)	Test group HG 7.6-2 (added)
Provision HG 7.6-3 (added)	Test group HG 7.6-3 (added)
Provision HG 7.6-4 (added)	Test group HG 7.6-4 (added)
Provision HG 7.6-9 (added)	Test group HG 7.6-9 (added)
Provision HG 7.12-1 (added)	Test group HG 7.12-1 (added)

Annex C (informative): Sample IXIT for Home Gateway

The sample IXIT in ETSI TS 103 701 [2] provides examples for completing the IXIT pro formas and demonstrates the scope and level of detail of the IXIT entries of ETSI TS 103 701 [2].

In the following, sample IXIT entries are provided for all new and/or modified IXIT entries as defined in the present document.

Table C.1: Sample IXIT 1-AuthMech (Authentication Mechanisms)

ID	Description	Authentication Factor	Password Generation Mechanism	Security Guarantees	Cryptographic Details	Brute Force Prevention
AuthMech-1	A user can connect to the HG Wi-Fi® with a pre-installed password or a password configured by the local administrator. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a Wi-Fi® interface.	Wi-Fi® password (pre-installed and used in initialized state or set by user)	The default password is generated randomly and is unique per device. The password has a length of 16 and consists of upper case characters, lower case characters and numbers. The password is generated by use of /dev/urandom on a UNIX configuration system during manufacturing phase.	The password is transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Wi-Fi® authentication is implemented in accordance with IEEE 802.11 [i.7]. Two link-level types of authentication are supported: Open System and Shared Key. The device supports the following shared key authentication: WEP, WPA, WPA2, WPA3.	*N/A*
AuthMech-2	A user can login over HTTPS on port 443 to gain access to the web frontend. (A user can request a login over HTTP on port 80 but is forwarded automatically to HTTPS on port 443.) The authentication on the login page is needed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	Administrator username and password (default one printed on the label or configured by the administrator)	The administrator's username is fixed "admin". The password is generated randomly and is unique per device. The password has a length of 16 and consists of upper case characters, lower case characters and numbers. The password is generated by use of /dev/urandom on a UNIX configuration system during manufacturing phase.	The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Authentication is performed via a form-based HTML interface by an internal PHP script in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	After 3 invalid login attempts the login interface is inaccessible for 5 minutes.

Table C.2: Sample IXIT 2-UserInfo (User Information)

Software version numbers	The software version numbers "V1.0.0" are provided to the user at the HTTPS web page under "Device Info". Also, the software version numbers can be retrieved from the SSH session using the "show version" command and from the SOAP data exchange interactions. The access control policies for the software version numbers are as below: 1) For local administrator and other users from LAN interface, they will have the access to the web service and/or SSH service after authentication and will be granted to retrieve the software version numbers. 2) For remote administrator from the WAN interface, only the remote administrator will have the access to the SOAP service after authentication and will be granted to retrieve the software version numbers. 3) For any other users from the Guest Wi-Fi® interface, none of them will be granted to retrieve the software version numbers because the endpoints connected to the Guest Wi-Fi® will have no authorization to the web or SSH services.

Table C.3: Sample IXIT 10-SecParam (Security Parameters)

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism
SecParam-11	Wi-Fi® password set by a local administrator of the HG. This password is used to verify the identity of a user attempting to connect to the HG and access network service.	critical	The Wi-Fi® credential's confidentiality is ensured and cannot be accessed by an attacker	The only user role that has access rights to read and to modify the Wi-Fi® password is the local administrator who has successfully passed the authentication.	The Wi-Fi® password is stored in the memory of the HG and can be read and modified in the web frontend by an authenticated local administrated only.	*N/A (The security parameter is not transmitted)*	*N/A (The Wi-Fi® password is required to be configured by a local administrator at first login.)*
SecParam-12	Local administrator credential for authentication against the web frontend.	critical	The local administrator credential's confidentiality is ensured and cannot be accessed by an attacker	The only user role that has access rights to modify the local administrator password is the local administrator who has successfully passed the authentication.	The local administrator credential is stored in the memory of the HG and can be modified in the web frontend by an authenticated local administrated only.	*N/A (The security parameter is not transmitted)*	*N/A (The local administrator credential is required to be configured by a local administrator at first login.)*

Table C.4: Sample IXIT 11-ComMech (Communication Mechanisms)

ID	Description	Security Guarantees	Cryptographic Details	Resilience Measures
ComMech-5	The DUT offers 2.4 GHz wireless connection for its guest Wi-Fi® feature. The wireless connection is based on IEEE 802.11 b [i.8], IEEE 802.11g [i.9], IEEE 802.11n [i.10] and IEEE 802.11ax [i.11]	Guest Wi-Fi® connections only allow guest user to access the internet. Devices connected to the host Wi-Fi® are isolated from other subnets such as the guest Wi-Fi®. It is infeasible for devices on the other network to access any assets of the host Wi-Fi®.	Guest Wi-Fi® supports security policies including Wired Equivalent Privacy (WEP), Wi-Fi® Protected Access (WPA), WPA2, and WPA3. Data encryption keys for the guest Wi-Fi® channel is different with that of host Wi-Fi®.	The connection uses the well-defined IEEE 802.11 b [i.8], IEEE 802.11g [i.9], IEEE 802.11n [i.10] and IEEE 802.11ax [i.11] protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. The DUT also support CPU overload protection to deal with mass connections.

Table C.5: Sample IXIT 13-SoftServ (Software Services)

ID	Description	Status	Default Settings	Justification	Allows Configuration	Authentication Mechanism
SoftServ-1	Callable update service for downloading and applying firmware updates. The service is triggered by the remote call from the authenticated ISP-administrator and responsible for checking specific remote for specific firmware updates as required. The service is accessible over the network. The service is accessible in the initialized state.	Enabled	--	The service is enabled by default for security and administration reasons.	No.	AuthMech-2
SoftServ-5	Guest Wi-Fi® providing network service to guest user is isolated from host Wi-Fi®.	Disabled	*N/A* *(No SSID and password assigned)*	The service is necessary to provide protection to host network while providing limited network access to guest user.	Yes. The user can: • Enable or disable Guest Wi-Fi®. • Guest Wi-Fi® SSID and password.	AuthMech-1, AuthMech-2
SoftServ-6	Firewall services provide protection from normal network attacks.	Enabled	DoS Protection: On TCP SynAttack Protection: On Port forwarding rules: empty	The service is necessary to provide the user the security of network attack.	Yes. The user can: • Configure the protection level of the firewall. • Configure port forwarding rules.	AuthMech-1, AuthMech-2
SoftServ-7	Guest Wi-Fi® providing network service to guest user is isolated from host Wi-Fi®.	Disabled by default	No SSID and password assigned Access control lists is empty.	The service is necessary to provide protection to host network while providing limited network access to guest user.	Yes. The administrator can: • Enable or disable Guest Wi-Fi®. • Guest Wi-Fi® SSID and password. • Configure access control lists to allow/block devices with specific MAC address.	AuthMech-1, AuthMech-2
SoftServ-8	Telnet service providing interactive communication for ISP administrator to configure the HG.	Disabled by default	*N/A*	Telnet service provides text-based interactive communication for ISP administrator to configure the HG.	Yes. The administrator can enable or disable Telnet service.	AuthMech-1, uthMech-2

Table C.6: Sample IXIT 30-User (User data in transmission and in storage)

ID	Description	Security Guarantees	Protection Scheme
UserData-1	General user data transmitted by the HG. The data stream can consist of different types of data such as voice, video and high-speed internet data generated by over-the-top user application and any other user data source.	Only the correct use can access the user data in-transit.	User data is encrypted in transmission between CPE and HG. Local data not for transmission remain stored in the HG. The HG does not implement an interface enabling an ISP admin and the local admin to access user data in-transit.
UserData-2	User configuration data stored in HG including Wi-Fi® SSID, LAN host IP address, DHCP setting, etc.	Only the authenticated local administrator can access the user configuration data in-storage.	User configuration data is stored in the encrypted file system of the HG. The only user role that has access rights to user configuration data is the local successfully authenticated administrator.
UserDate-3	For the operation of an ISP administrated HG, the HG stores ISP-related configuration and credentials to access the ISP network and to allow the ISP administrator to remotely access the HG.	Only the ISP administrator can have remote access to the IPS administrated HG and to the ISP credentials. The ISP administration traffic is confidentiality and integrity protected.	The ISP-related data are stored in the encrypted file system of the HG. The only user role that has access rights to these data is the remotely successfully authenticated ISP administrator.

Table C.7: Sample IXIT 31-ThiParSoft (3rd-party Software)

ID	Description	Security Provision	Initiation and Interaction	Configuration	Software Restore
ThiParSoft -1	The HG executes a SW developed by a 3rd-party supplier. For example, the SW provides the HG with the functions to manage and control the IoT devices connected to the HG, such as smart door locks and smart socket. The SW can be downloaded and installed from a management platform at https://example.com/resources/download/example.tgz or can be installed using a USB storage. In that case, a clear warning about the upcoming installation is sent to the administrator and the installation does not start without consent from the administrator. The signature of the SW package needs to be verified successfully before an installation can be done. The "smart home service" is a premium service purchased by the user and provided by the ISP, and this 3rd-party SW is the essential software component to help the ISP to fulfil the contract.	The installation does not start until the administrator confirmed awareness of the potential risk and has given his consent. The SW can only be downloaded from the configured URI (i.e. https://example.com/resources/download/example.jar). The authenticity and integrity of the SW was verified by means of digital signature generated by the SW provider and pre-installed on the HG.	User-initiated SW installation over web interface. The user can: a) login to a webpage, select and remotely download the SW package; b) manually select the SW package from a local storage (USB); or c) input the URI of the download server to download the SW package. In all cases the installation starts if the digital signature verification was successful. When a 3rd-party SW selection is done and the download is the next step, the administrator will be warned about the detail of the forthcoming installation and the potential risk to install this SW, and the HG requires the consent prior the download. The administrator agrees, he can start the download and installation process by pressing the button "Fully aware and start", or cancel the installation by pressing the button "Cancel".	The user can configure the DUT to enable/disable the installation of 3rd-party SW, and can configure the URI list of download server to download SW packages. If the installation of 3rd-party SW is active, then the SW signature verification is always enabled. The default option is that the installation of 3rd-party SW is disabled.	The authenticated and authorized user can recover the SW of the HG to the OEM SW state by click the button "restore". Then on one hand, all 3rd-party SW gets removed from the HG, and on the other hand, the newest SW-update will be downloaded and installed. This OEM installation is done automatically from the trustworthy OEM or trusted SW provider source. The digital signature on the SW-update is verified using the on-board public key to ensure authenticity and integrity.

Annex D (informative): Additional assessment information for Home Gateway

D.1 Threat model

Clause D.1 in the annex of ETSI TS 103 701 [2] applies also in the present document.

D.2 Baseline attacker model

Clause D.2 in the annex of ETSI TS 103 701 [2] applies also in the present document.

D.3 Model for a "user with limited technical knowledge"

Clause D.3 in the annex of ETSI TS 103 701 [2] applies also in the present document.

History

Document history		
V1.1.1	July 2023	Publication