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

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

Reference

DTS/CYBER-0050

Keywords

cybersecurity, IoT, privacy

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

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

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

1 Scope

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

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

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

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

2 References

2.1 Normative references

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

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

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

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

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

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

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

2.2 Informative references

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE: Not published yet.

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

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

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

assess: generate a result by analysis using evaluator expertise

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

check: generate a result by a simple comparison

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

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

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

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

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

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

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

security guarantee: statement of the addressed security objectives

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

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

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

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

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

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

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

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

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

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

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

test unit: indivisible unit of a specification of test activities

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

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

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

3.2 Symbols

Void.

3.3 Abbreviations

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

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

NOTE: In context of addressing.

MAC	Message Authentication Code

NOTE: In context of cryptography.

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

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

4 Conformance assessment methodology

4.1 Overview and document structure

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

Clause 4.3 describes the assessment procedure.

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

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

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

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

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

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

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

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

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

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

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

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

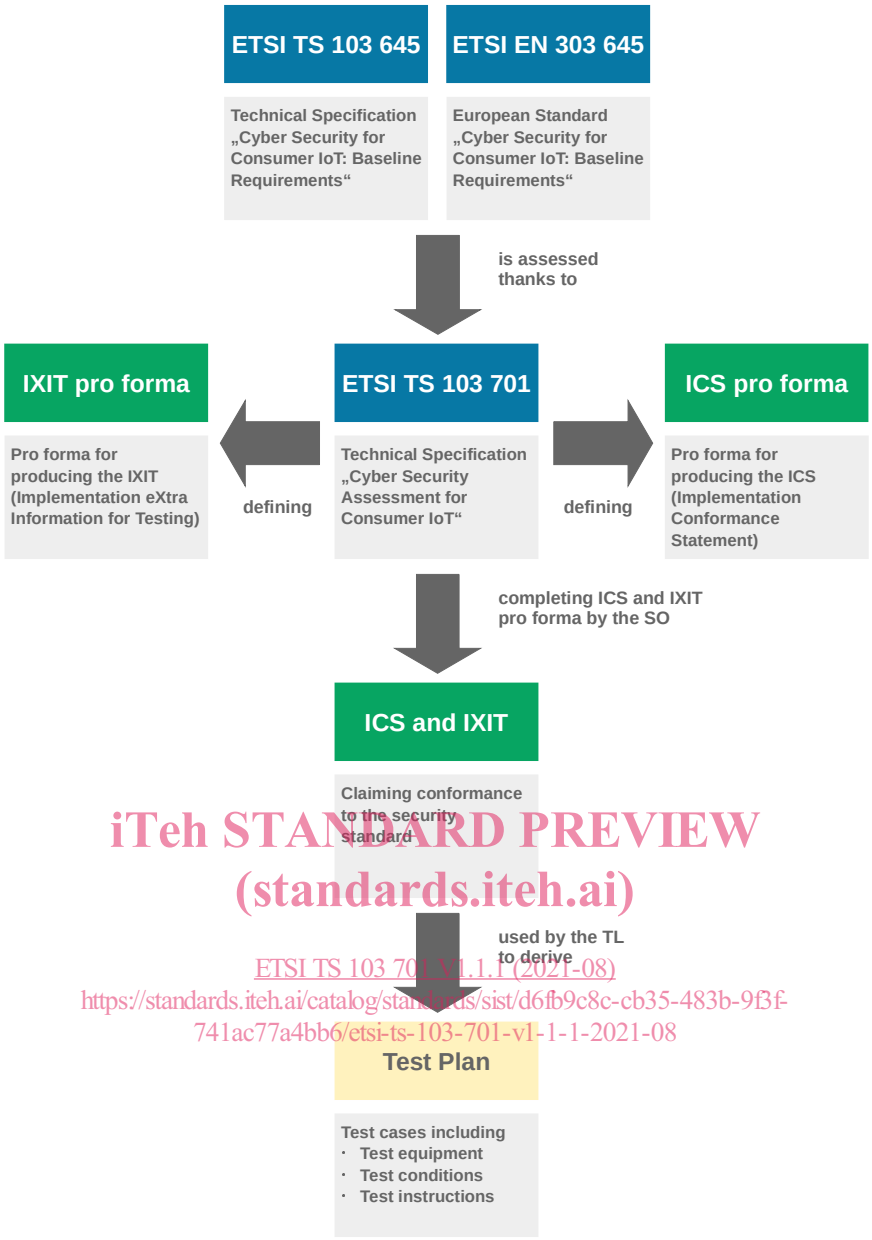

Figure 1: Relations of the present document with respect to a conformance assessment process