Federal Office
for Information Security

BSI TR-03173: Amendments for Conformance Assessments based on ETSI EN 303 645/TS 103 701

Version: 1.0

Date: 27/04/2022

Document history

Version	*Date*	*Editor*	*Description*
1.0	27/04/2022	BSI	Public Release Version

Table 1: Document history

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: shs@bsi.bund.de
Internet: https://www.bsi.bund.de

Key Words

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in IETF RFC 2119 [1]. The key word “CONDITIONAL” is to be interpreted as follows:

CONDITIONAL: The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED.

Table of Contents

1 Introduction

The European standard “Cyber Security for Consumer Internet of Things: Baseline Requirements” (ETSI EN 303 645) [2] provides a set of baseline provisions for consumer IoT devices. The corresponding assessment specification “Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements” (ETSI TS 103 701) [3] specifies a conformance assessment methodology. These documents are essential to understand and apply the present document.

Manufacturers can consult the “Guide to Cyber Security for Consumer Internet of Things” (ETSI TR 103 621) [4] for implementation examples concerning the requirements of ETSI EN 303 645 [2]. Due to the generic character of ETSI EN 303 645 [2] and ETSI TS 103 701 [3] some amendments are necessary for the performance of a conformance assessment (see section 4.8 of ETSI TS 103 701 [3]) which are covered by the present document.

For example, the IT Security Label includes such a conformance assessment, where these amendments are applied. The IT Security Label allows manufacturers to label their IT products assuring those products have certain security features. This is accomplished by a self-declaration on the base of recognized security standards. The self-declaration is supplemented by a down-streamed process of market surveillance in which the BSI performs a random or event based check, to evaluate if the product does match the security features declared by the manufacturer.

2 Amendments

2.1 Best Practice Cryptography

The amendments in this section address the following provision of ETSI EN 303 645 [2] concerning best practice cryptography for:

- Provision 5.1-3: User Authentication
- Provision 5.3-7: Secure Update
- Provision 5.5-1, 5.5-6, 5.5-7, 5.8-1 and 5.8-2: Secure Communication

The standard ETSI EN 303 645 [2] does not contain specific cryptographic requirements. ETSI TS 103 701 [3] provides a methodology to assess whether cryptography can be considered as best practice with respect to the use case based upon reference catalogues or alternative evidences. Within this methodology only the following documents **shall** be used as reference catalogues:

- SOGIS-ACM [5]
- BSI TR-02102 [6] [7] [8] [9]

NOTE 1: The catalogues contain also cryptographic requirements or recommendations for use cases requiring security beyond the level basic.

NOTE 2: The methodology of ETSI TS 103 701 [3] allows to provide evidences to justify that the used cryptography is to be considered as best practice cryptography besides the listing in the reference catalogues.

NOTE 3: This amendment does not replace the methodology of ETSI TS 103 701 [3]. Only the term “reference catalogue” is concretised. Apart from that, the test groups concerning best practice cryptography apply unchanged as described in ETSI TS 103 701 [3].

Concerning the examination of cryptography defined in the methodology in ETSI TS 103 701 [3], the following non-exhaustive list of primitives and communication protocols **shall** be considered as known to be vulnerable to a feasible attack:

- SSL, TLS 1.0, TLS 1.1 for the use cases of communication with associated web services
- WEP for the use cases of Wi-Fi communication

2.2 Usability

The amendments in this section address the following provision of ETSI EN 303 645 [2] concerning usability:

- Provision 5.1-4: Changing authentication value
- Provision 5.3-3: Simple application of updates
- Provision 5.3-13: Publication of support period
- Provision 5.3-14: Publication of support period and replacement support for constraint devices
- Provision 5.8-3: Documentation of external sensing capabilities
- Provision 5.11-1: Erasing user data
- Provision 5.11-2: Removing personal data from associated service
- Provision 6.1-2: Obtaining the processing of personal data

The test cases in ETSI TS 103 701 [3] regarding the listed provisions refer to a “user with limited technical knowledge” to assess whether usability is given in the context of the provision. The model “user with limited technical knowledge” in Annex D.3 from ETSI TS 103 701 [3] **shall** be used for the related test cases.

2.3 Secure Storage

The amendments in this section address the following provision of ETSI EN 303 645 [2] concerning secure storage:

- Provision 5.4-1: Secure storage of sensitive security parameters

The test cases in ETSI TS 103 701 [3] regarding the listed provision refer to “suitable protection mechanism for the claimed security guarantees”. The “baseline attacker model” in Annex D.2 from ETSI TS 103 701 [3] **shall** be used for the related test cases to assess whether protection mechanisms are suitable for the claimed security guarantees.

2.4 Additional Applications

An IoT device can provide the capability to operate additional applications (first and third party apps). This is a special case which is not in the focus of ETSI EN 303 645 [2].

Preinstalled applications on an IoT device are to be considered as part of the Device under Test (DUT see ETSI TS 103 701 [3]).

The security of the applications on the DUT, which are installed by the user after initialization, are not part of the assessment. This includes applications, which are deactivated by default or prepared for installation (e.g. links to an app store). However, the interaction between the DUT and such types of application is addressed. The following clarifications apply:

- Provision 5.4-1: Secure storage of sensitive security parameters
  Consider the interaction of the application with the DUT concerning “Security Guarantees” and “Protection Schemes“ (see ETSI TS 103 701 [3]).
- Provision 5.13-1: Data Input Validation
  Consider the interface between the application and the DUT as API.

Bibliography

[1] IETF RFC 2119: Key words for use in RFCs to Indicate Requirement Levels.

[2] ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements v2.1.1.

[3] ETSI TS 103 701: Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements v1.1.1.

[4] ETSI TR 103 621: Guide to Cyber Security for Consumer Internet of Things v1.1.1.

[5] SOG-IS Crypto Working Group: Crypto Evaluation Scheme Agreed Cryptographic Mechanisms v1.2.

[6] BSI TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen.

[7] BSI TR-02102-2: Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS).

[8] BSI TR-02102-3: Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2).

[9] BSI TR-02102-4: Kryptographische Verfahren: Verwendung von Secure Shell (SSH).

NOTE: For references without version numbers, the currently published version of the referenced document applies.