ICS 35.040, 35.240.99 SLOVENSKÁ TECHNICKÁ NORMA Február 2025

STN	**Kybernetika** **Kybernetická bezpečnosť pre spotrebiteľský internet vecí: Základné požiadavky**	**STN** **EN 303 645** **V3.1.3** 87 3645

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/25

Obsahuje: EN 303 645 V3.1.3:2024

obsahuje farebné strany

139661

ETSI EN 303 645 V3.1.3 (2024-09)

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

Reference
REN/CYBER-00127

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

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 11
3.3 Abbreviations 11
4 Implementation of the standard 12
5 Cyber security provisions for consumer IoT 12
5.0 Reporting implementation 12
5.1 No universal default passwords 13
5.2 Implement a means to manage reports of vulnerabilities 14
5.3 Keep software updated 16
5.4 Securely store sensitive security parameters 20
5.5 Communicate securely 21
5.6 Minimize exposed attack surfaces 22
5.7 Ensure software integrity 24
5.8 Ensure that personal data is secure 24
5.9 Make systems resilient to outages 25
5.10 Examine system telemetry data 25
5.11 Make it easy for users to delete user data 25
5.12 Make installation and maintenance of devices easy 26
5.13 Validate input data 27
6 Data protection provisions for consumer IoT 28
Annex A (informative): Basic concepts and models 30
A.1 Architecture 30
A.2 Device states 32
A.3 Interfaces 34
Annex B (informative): Implementation conformance statement pro forma 36
Annex C (informative): Change history 40
History 41

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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER).

National transposition dates	
Date of adoption of this EN:	11 September 2024
Date of latest announcement of this EN (doa):	31 December 2024
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 June 2025
Date of withdrawal of any conflicting National Standard (dow):	30 June 2025

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

As more devices in the home connect to the Internet, the cyber security and data protection of the Internet of Things (IoT) becomes a growing concern. People entrust their personal data to an increasing number of online devices and services. Products and appliances that have traditionally been offline are now connected and need to be designed to withstand cyber threats.

The present document brings together widely considered good practices in security for Internet-connected consumer devices in a set of high-level outcome-focused provisions. The objective of the present document is to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their products.

The provisions are primarily outcome-focused, rather than prescriptive, giving organizations the flexibility to innovate and implement security and data protection solutions appropriate for their products.

The present document is not intended to solve all security, data protection and privacy challenges associated with consumer IoT. It also does not focus on protecting against attacks that are prolonged/sophisticated or that require sustained physical access to the device. Rather, the focus is on the technical controls and organizational policies that matter most in addressing the most significant and widespread security shortcomings. Overall, a baseline level of security and data protection is considered; this is intended to protect against elementary attacks on fundamental design weaknesses (such as the use of easily guessable passwords).

The present document provides a set of baseline provisions applicable to all consumer IoT devices. It is intended to be complemented by other standards defining more specific provisions and fully testable and/or verifiable requirements for specific devices which, together with the present document, will facilitate the development of assurance schemes.

A clause in the present document in some cases begins with general information about the context of the following provisions. A provision is followed by explanatory text describing, where appropriate, the intent of the provision and how the provision might be implemented. Further information on implementation examples is given in ETSI TR 103 621 [i.31].

Many consumer IoT devices and their associated services process and store personal data, the present document can help in ensuring that these are compliant with the General Data Protection Regulation (GDPR) [i.7]. Security by design is an important principle that is endorsed by the present document.

ETSI TS 103 701 [i.19] provides guidance on how to assess and assure IoT products against provisions within the present document.

The provisions in the present document have been developed following a review of published standards, recommendations and guidance on IoT security and privacy, including: ETSI TR 103 305-3 [i.1], ETSI TR 103 309 [i.2], ENISA Baseline Security Recommendations [i.8], UK Department for Digital, Culture, Media and Sport (DCMS) Secure by Design Report [i.9], IoT Security Foundation Compliance Framework [i.10], GSMA IoT Security Guidelines and Assessment [i.11], ETSI TR 103 533 [i.12], DIN SPEC 27072 [i.20] and OWASP Internet of Things [i.23].

NOTE: Mappings of the landscape of IoT security standards, recommendations and guidance are available in ENISA Baseline Security Recommendations for IoT - Interactive Tool [i.15] and in Copper Horse Mapping Security & Privacy in the Internet of Things [i.14].

As consumer IoT products become increasingly secure, it is envisioned that future revisions of the present document will mandate provisions that are currently recommendations in the present document.

1 Scope

The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. A non-exhaustive list of examples of consumer IoT devices includes:

- connected children's toys and baby monitors;
- connected smoke detectors, door locks and window sensors;
- IoT gateways, base stations and hubs to which multiple devices connect;
- smart cameras, smart speakers and smart Televisions together with their remote controls;
- wearable health trackers;
- connected home automation and alarm systems, especially their gateways and hubs;
- connected appliances, such as washing machines and fridges; and
- smart home assistants.

Moreover, the present document addresses security considerations specific to constraints in device resources.

EXAMPLE: Typical device resources that might constrain the security capabilities are energy supply, communication bandwidth, processing power or (non-)volatile memory capacity.

The present document provides basic guidance through examples and explanatory text for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. Table B.1 provides a schema for the reader to give information about the implementation of the provisions.

Devices that are not consumer IoT devices, for example those that are primarily intended to be used in manufacturing, healthcare or other industrial applications, are not in scope of the present document.

The present document has been developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out here.

Annex A (informative) of the present document has been included to provide context to clauses 4, 5 and 6 (normative). Annex A contains examples of device and reference architectures and an example model of device states including data storage for each state.

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.

Not applicable.

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 TR 103 305-3: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 3: Internet of Things Sector".

[i.2] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.3] NIST Special Publication 800-63B: "Digital Identity Guidelines - Authentication and Lifecycle Management".

[i.4] ISO/IEC 29147: "Information technology - Security techniques - Vulnerability Disclosure".

[i.5] OASIS csaf-v2.0: "Common Security Advisory Framework", version 2.0,edited by Langley Rock, Stefan Hagen, and Thomas Schmidt, 18 November 2022 and the errata 01.

[i.6] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".

[i.7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.8] ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", November 2017, ISBN: 978-92-9204-236-3, doi: 10.2824/03228.

[i.9] UK Department for Digital, Culture, Media and Sport: "Secure by Design: Improving the cyber security of consumer Internet of Things Report", March 2018.

[i.10] IoT Security Foundation: "IoT Security Assurance Framework", Release 3.0, November 2021.

[i.11] GSMA: "GSMA IoT Security Guidelines and Assessment".

[i.12] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.13] Commission Notice 2016/C 272/01: "The "Blue Guide" on the implementation of EU products rules 2016" (Text with EEA relevance).

[i.14] Copper Horse: "Mapping Security & Privacy in the Internet of Things".

[i.15] ENISA: "Baseline Security Recommendations for IoT - Interactive Tool".

[i.16] IoT Security Foundation: "Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies".

[i.17] F-Secure: "IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks".

[i.18] W3C®: "Web of Things at W3C".

[i.19] ETSI TS 103 701: "CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.20] DIN SPEC 27072: "Information Technology - IoT capable devices - Minimum requirements for Information security".

[i.21] GSMA™: "Coordinated Vulnerability Disclosure (CVD) Programme".

[i.22] IoT Security Foundation: "Vulnerability Disclosure - Best Practice Guidelines".

[i.23] OWASP Internet of Things (IoT) Top 10 2018.

[i.24] IEEE 802.15.4-2015™/Cor 1-2018: "IEEE Standard for Low-Rate Wireless Networks, Corrigendum 1".

[i.25] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[i.26] GSMA™: "SGP.22 Technical Specification v2.2.1".

[i.27] ISO/IEC 27005:2022: "Information technology - Security techniques - Information security risk management".

[i.28] Microsoft® Corporation: "The STRIDE Threat Model".

[i.29] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.30] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.31] ETSI TR 103 621: " Guide to Cyber Security for Consumer Internet of Things".

[i.32] FIRST: "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure".

[i.33] ISO/IEC TR 5895: "Cybersecurity - Multi-party coordinated vulnerability disclosure and handling".

[i.34] ISO/IEC 16500-6:1999: "Information technology Generic digital audio-visual systems".