SLOVENSKI STANDARD
oSIST prEN 303 645 V2.0.0:2020

01-februar-2020

CYBER - Kibernetska varnost za uporabnike interneta stvari

CYBER - Cyber Security for Consumer Internet of Things

Ta slovenski standard je istoveten z: **ETSI EN 303 645 V2.0.0 (2019-11)**

ICS:

35.030 Informacijska varnost IT Security

oSIST prEN 303 645 V2.0.0:2020 **en**

Draft ETSI EN 303 645 V2.0.0 (2019-11)

CYBER;
Cyber Security for Consumer Internet of Things

Reference
REN/CYBER-0048

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER) in co-operation with CEN/CENELEC JTC 13 (Cybersecurity and Data Protection) and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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 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 practice 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 solutions appropriate for their products.

The present document is not intended to solve all security challenges associated with consumer IoT. 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 is considered; this is intended to protect against elementary attacks on fundamental design weaknesses (such as the use of easily guessable passwords).

As much of consumer IoT and the 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.20] 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 review of published standards, recommendations and guidance on IoT security and privacy [i.1], [i.2], [i.8], [i.9], [i.10], [i.11], [i.12], [i.20] and [i.23].

NOTE: Mappings of the landscape of IoT security standards, recommendations and guidance are available [i.14] and [i.15].

1 Scope

The present document specifies high-level provisions for the security of consumer IoT devices, that are connected to network infrastructure (such as the Internet or home network) and their relationships to associated services. These relationships encompass both network communications and handling of personal data. A non-exhaustive list of examples of consumer IoT devices include:

- connected children's toys and baby monitors;
- connected safety-relevant products such as smoke detectors and door locks;
- IoT base stations and hubs to which multiple devices connect;
- smart cameras, TVs and speakers;
- 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 constrained devices, such as sensors and actuators. Such devices typically have limited ability to process, communicate or store data, or limited user interfaces, which affects security considerations.

EXAMPLE: Window contact sensors, flood sensors and energy switches are typically constrained devices.

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.

Applicability of these provisions depends on risk analysis; this is performed by the device manufacturer and/or other relevant entities and is out of scope of the present document. For certain use cases and following risk assessment, it can be appropriate to apply additional provisions than those contained within the present document. The present document provides a foundation level of security for such higher assurance level use cases.

IoT products primarily intended to be used in manufacturing, healthcare or for 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 main clause 4 (normative). Annex A contains examples of device and reference architectures, an example model of device states including data storage for each state and additional description of key stakeholders.

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; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations".

[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".

NOTE: Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

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

NOTE: Available at https://www.iso.org/standard/45170.html.

[i.5] CSAF: "Common Vulnerability Reporting Framework (CVRF)".

NOTE: Available at http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html.

[i.6] ETSI TR 103 331: "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.

NOTE: Available at https://www.gov.uk/government/collections/secure-by-design.

[i.10] IoT Security Foundation: "IoT Security Compliance Framework", Release 2 December 2018.

NOTE: Available at https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf.

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

NOTE: Available at https://www.gsma.com/iot/iot-security/iot-security-guidelines/.

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

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

NOTE: Available in the Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2016:272:TOC.

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

NOTE: Available at https://iotsecuritymapping.uk/.

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

NOTE: Available at https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/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".

NOTE: Available at https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability-Disclosure-Design-v4.pdf.

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

NOTE: Available at https://blog.f-secure.com/iot-threats/.

[i.18] W3C: "Web of Things at W3C".

NOTE: Available at https://www.w3.org/WoT/.

[i.19] ETSI TS 103 701: "CYBER; Cybersecurity assessment for consumer IoT products".

NOTE: It is under development.

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

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

NOTE: Available at https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/.

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

NOTE: Available at https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf.

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

NOTE: Available at https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10.

[i.24] IEEE™ 802.15.4-2015: "IEEE Standard for Low-Rate Wireless Networks".

NOTE: Available at https://standards.ieee.org/content/ieee-standards/en/standard/802_15_4-2015.html.

[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".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

administrator: consumer who is at least intermittently a user and has the highest-privilege level in relation to the device and is able to change any configuration related to the intended functionality

associated services: digital services that, together with the device, are part of the overall consumer IoT product and that are typically required to provide the product's intended functionality

EXAMPLE: Associated services can include mobile applications, cloud computing/storage and third party Application Programming Interfaces (APIs).

authentication mechanism: method used to prove the authenticity of a consumer

EXAMPLE: An authentication mechanism can be the requesting of a password, scanning a QR code, or use of a biometric fingerprint scanner.

authentication value: individual value of an attribute used by an authentication mechanism

EXAMPLE: When the authentication mechanism is to request a password, the authentication value can be a character string. When the authentication mechanism is a biometric fingerprint recognition, the authentication value can be the index fingerprint of the left hand.

best practice cryptography: cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques

NOTE: This does not refer only to the cryptographic primitives used, but also implementation, key generation and handling of keys.

EXAMPLE: The device manufacturer uses a communication protocol and cryptographic library provided with the IoT platform and where that library and protocol have been assessed against feasible attacks, such as replay.

constrained device: device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user

NOTE: Physical limitations can be due to power supply, battery life, processing power, physical access, limited functionality, limited memory or limited network bandwidth. These limitations can require a constrained device to be supported by another device, such as a base station or companion device.

EXAMPLE 1: A window sensor's battery cannot be charged or changed by the user; this is a constrained device.

EXAMPLE 2: The device cannot have its software updated due to storage limitations, resulting in hardware replacement or network isolation being the only options to manage a security vulnerability.

EXAMPLE 3: A low-powered device uses a battery to enable it to be deployed in a range of locations. Performing high power cryptographic operations would quickly reduce the battery life, so it relies on a base station or hub to perform validations on updates.

EXAMPLE 4: The device has no display screen to validate binding codes for Bluetooth pairing.

EXAMPLE 5: The device has no ability to input, such as via a keyboard, authentication information.

consumer: natural person who is acting for purposes that are outside her/his trade, business, craft or profession

NOTE: Organizations, including businesses of any size, use consumer IoT. For example, smart TVs are frequently deployed in meeting rooms, and home security kits can protect the premises of small businesses.

consumer IoT devices: network-connected (and network-connectable) devices that have relationships to associated services and are used by the consumer typically in the home or as electronic wearables

NOTE: Consumer IoT devices are often available for the consumer to purchase in retail environments. Consumer IoT devices can also be commissioned and/or installed professionally.

critical security parameter: security-related secret information whose disclosure or modification can compromise the security of a security module

EXAMPLE: Secret cryptographic keys, authentication values such as passwords, PINs, certificates or other trust anchors.

defined support period: minimum length of time, expressed as a period or by an end-date, for which a device will receive security updates

device manufacturer: entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers

factory default: state of the device after reset or following final production/assembly

initialization: process that activates the network connectivity of the device for operation and optionally sets authentication features for a user or for network access

initialized state: state of the device after initialization

isolable: able to be removed from the network it is connected to, without causing functionality loss, so that any compromise affects only itself; alternatively, able to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured

logical interface: software that utilizes a network interface to communicate over the network via channels or ports

manufacturer: relevant economic operator in the supply chain (including the device manufacturer)

NOTE: This definition acknowledges the variety of actors involved in the consumer IoT ecosystem and the complex ways by which they can share responsibilities. Beyond the device manufacturer, such entities can also be, for example and depending on a specific case at hand: importers, distributors, integrators, component and platform providers, software providers, IT and telecommunications service providers, managed service providers and providers of associated services.

network interface: physical interface that can be used to access the functionality of consumer IoT via a network

owner: consumer who owns or who purchased the device

personal data: any information relating to an identified or identifiable natural person

physical interface: physical port or radio used to communicate with the device at the physical layer

EXAMPLE: Radios, ethernet ports, serial interfaces such as USB, and those used for debugging purposes including test points, UART, SWD or JTAG.

public security parameter: security related public information whose modification can compromise the security of a security module

EXAMPLE: A public key to verify the authenticity/integrity of software updates

remotely accessible: intended to be accessible via wide area networks such as the Internet

security module: set of hardware, software, and/or firmware that implements security functions

EXAMPLE: A device contains a hardware root of trust, a cryptographic software library that operates within a trusted execution environment, and software within the operating system that enforces security such as user separation and the update mechanism. These all make up the security module.

security update: software update that addresses security vulnerabilities either discovered by or reported to the manufacturer

NOTE: Software updates can be purely security updates if the severity of the vulnerability requires a higher priority fix.

sensitive security parameters: critical security parameters and public security parameters

software service: software component of a device that is used to support functionality

EXAMPLE: A runtime for the programming language used within the device software or a daemon that exposes an API used by the device software, e.g. a cryptographic module's API.