

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

Medieninhaber und Hersteller:

ÖVE Österreichischer Verband für Elektrotechnik
Austrian Standards Institute

Copyright © ÖVE/Austrian Standards Institute – 2020.

Alle Rechte vorbehalten! Nachdruck oder Vervielfältigung,
Aufnahme auf oder in sonstige Medien oder Datenträger nur
mit Zustimmung gestattet!

**Verkauf von in- und ausländischen Normen und
technischen Regelwerken durch**

Austrian Standards Institute
Heinestraße 38, 1020 Wien
E-Mail: sales@austrian-standards.at
Internet: www.austrian-standards.at
Webshop: www.austrian-standards.at/webshop
Tel.: +43 1 213 00-300
Fax: +43 1 213 00-818

Alle Regelwerke für die Elektrotechnik auch erhältlich bei
ÖVE Österreichischer Verband für Elektrotechnik
Eschenbachgasse 9, 1010 Wien
E-Mail: verkauf@ove.at
Internet: www.ove.at
Webshop: www.ove.at/shop
Tel.: +43 1 587 63 73

ICS 33.040

Ident (IDT) mit ETSI EN 303 645 V2.1.1 (2020-06)

zuständig ÖVE/Komitee
TK IT-EG
Informationstechnologie, Telekommunikation und
Elektronik

Nationales Vorwort

Diese Europäische Norm EN 303 645 V2.1.1:2020 hat sowohl den Status einer nationalen elektrotechnischen Norm gemäß ETG 1992 als auch den einer nationalen Norm gemäß NormG 2016. Bei ihrer Anwendung ist dieses Nationale Vorwort zu berücksichtigen.

Für den Fall einer undatierten normativen Verweisung (Verweisung auf einen Standard ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste Ausgabe dieses Standards.

Für den Fall einer datierten normativen Verweisung bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Standards.

Der Rechtsstatus dieser nationalen (elektrotechnischen) Norm ist den jeweils geltenden Verordnungen zum Elektrotechnikgesetz zu entnehmen.

Bei mittels Verordnungen zum Elektrotechnikgesetz verbindlich erklärten nationalen (elektrotechnischen) Normen ist zu beachten:

- Hinweise auf Veröffentlichungen beziehen sich, sofern nicht anders angegeben, auf den Stand zum Zeitpunkt der Herausgabe dieser nationalen (elektrotechnischen) Norm. Zum Zeitpunkt der Anwendung dieser nationalen (elektrotechnischen) Norm ist der durch die Verordnungen zum Elektrotechnikgesetz oder gegebenenfalls auf andere Weise festgelegte aktuelle Stand zu berücksichtigen.
- Informative Anhänge und Fußnoten sowie normative Verweise und Hinweise auf Fundstellen in anderen, nicht verbindlichen Texten werden von der Verbindlicherklärung nicht erfasst.

Europäische Normen (EN) von ETSI werden gemäß den „Gemeinsamen Regeln“ von CEN/CENELEC durch Veröffentlichung eines identen Titels und Textes in das Gesamtwerk der nationalen (elektrotechnischen) Normen übernommen, wobei der Nummerierung der Zusatz ÖVE/ÖNORM vorangestellt wird.

Der von ETSI übermittelte Normentext wird in englischer Sprache veröffentlicht, da davon ausgegangen werden kann, dass die Anwender der Norm über ausreichende englische Sprachkenntnisse verfügen.

ETSI EN 303 645 V2.1.1 (2020-06)



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

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2020.

All rights reserved.

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.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Symbols.....	11
3.3 Abbreviations	12
4 Reporting implementation.....	12
5 Cyber security provisions for consumer IoT	13
5.1 No universal default passwords.....	13
5.2 Implement a means to manage reports of vulnerabilities	14
5.3 Keep software updated	15
5.4 Securely store sensitive security parameters	18
5.5 Communicate securely	19
5.6 Minimize exposed attack surfaces.....	20
5.7 Ensure software integrity.....	21
5.8 Ensure that personal data is secure	22
5.9 Make systems resilient to outages	22
5.10 Examine system telemetry data	23
5.11 Make it easy for users to delete user data.....	23
5.12 Make installation and maintenance of devices easy	24
5.13 Validate input data.....	24
6 Data protection provisions for consumer IoT.....	24
Annex A (informative): Basic concepts and models	26
A.1 Architecture.....	26
A.2 Device states.....	28
Annex B (informative): Implementation conformance statement pro forma	31
History	34

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

National transposition dates	
Date of adoption of this EN:	19 June 2020
Date of latest announcement of this EN (doa):	30 September 2020
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2021
Date of withdrawal of any conflicting National Standard (dow):	31 March 2021

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. 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 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.

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. The associated services are out of scope. 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, 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 security considerations specific to constrained devices.

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.

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.