



EUROPEAN STANDARD

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

ReferenceREN/CYBER-0048

Keywordscybersecurity, 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/CommitteeSupportStaff.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.....	21
5.9 Make systems resilient to outages	22
5.10 Examine system telemetry data.....	22
5.11 Make it easy for users to delete user data.....	23
5.12 Make installation and maintenance of devices easy	23
5.13 Validate input data.....	24
6 Data protection provisions for consumer IoT.....	24
Annex A (informative): Basic concepts and models	25
A.1 Architecture.....	25
A.2 Device states.....	27
Annex B (informative): Implementation conformance statement pro forma	29
History	32

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 final draft European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER), and is now submitted for the 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. 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 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.