ETSI TS 103 645 V1.1.1 (2019-02)

CYBER;
Cyber Security for Consumer Internet of Things

Reference
DTS/CYBER-0039

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

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 Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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) is becoming 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 becoming 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 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.

As many IoT devices and 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]. This present document can also help organizations implement a future EU common cybersecurity certification framework as proposed in the Cybersecurity Act [i.13] and the proposed IoT Cybersecurity Improvement Act in the United States.

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] and [i.12].

NOTE: Mappings of the landscape of IoT security standards, recommendations and guidance are available. See, for example, Mapping Security & Privacy in the Internet of Things (https://iotsecuritymapping.uk/) and ENISA Baseline Security Recommendations for IoT - Interactive Tool (https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-security-recommendations-for-iot-interactive-tool).

1 Scope

The present document specifies high-level provisions for the security of consumer devices that are connected to network infrastructure, such as the Internet or home network, and their associated services. A non-exhaustive list of examples include:

- connected children's toys and baby monitors;
- connected safety-relevant products such as smoke detectors and door locks;
- smart cameras, TVs and speakers;
- wearable health trackers;
- connected home automation and alarm systems;
- connected appliances (e.g. washing machines, fridges); and
- smart home assistants.

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

IoT products primarily intended to be employed in manufacturing, other industrial applications and healthcare are not in scope of the present document.

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: "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/publications/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".

NOTE: It is under development.

[i.13] Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

associated services: digital services that are linked to IoT devices, for example mobile applications, cloud computing/storage and third party Application Programming Interfaces (APIs) to services such as messaging

constrained device: device which has physical limitations that limit the ability of the device to process, communicate or store data

EXAMPLE: Limitations to the ability of the device, for example to receive and process software updates, can be due to battery life, processing power, physical access (e.g. if the device is embedded in concrete or otherwise inaccessible), limited functionality, limited memory or limited network bandwidth.

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

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

consumer IoT: network-connected (and network-connectable) devices and their associated services that are usually available for the consumer to purchase in retail and that are typically used in the home or as electronic wearables

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

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

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

security-sensitive data: data that is relevant to the security of a device or service, for example cryptographic keys, device identifiers and initialization vectors

3.2 Symbols

Void.

3.3 Abbreviations

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

API	Application Programming Interface
CVD	Coordinated Vulnerability Disclosure
CVRF	Common Vulnerability Reporting Framework
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Network and Information Security
EU	European Union
eUICC	embedded Universal Integrated Circuit Card
GDPR	General Data Protection Regulation
GSMA	GSM Association
IoT	Internet of Things
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
TEE	Trusted Execution Environment
TS	Technical Specification
UICC	Universal Integrated Circuit Card

4 Cyber security provisions for consumer IoT

4.1 No universal default passwords

Provision 4.1-1 All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.

Many IoT devices are being sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. This has been the source of many security issues in IoT and the practice needs to be discontinued. Following best practice on passwords and other authentication methods is encouraged. Device security can further be strengthened by having unique and immutable identities.

NOTE: For guidance see, for example, the NIST Special Publication on Digital Identity Guidelines, Authentication and Lifecycle Management [i.3].

4.2 Implement a means to manage reports of vulnerabilities

Provision 4.2-1 Companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues.

Provision 4.2-2 Disclosed vulnerabilities should be acted on in a timely manner.

A "timely manner" for acting on vulnerabilities varies considerably and is incident specific, however, the de facto standard for the vulnerability process to be completed is within 90 days. A hardware fix can take considerably longer to address than a software fix. Additionally, a fix that has to be deployed to devices can take time to roll out compared with a server software fix.

Provision 4.2-3 Companies should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate as part of the product security lifecycle.

Knowing about a security vulnerability allows companies to respond. Vulnerabilities are expected to be reported directly to the affected stakeholders in the first instance. If that is not possible vulnerabilities can be reported to national authorities. Companies are also encouraged to share information with competent industry bodies.

NOTE 1: Competent industry bodies include the GSMA and the IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure is available from the IoT Security Foundation which references the ISO/IEC 29147 standard on vulnerability disclosure [i.4]. The GSMA's industry level Coordinated Vulnerability Disclosure programme is located at: https://www.gsma.com/cvd.

Coordinated Vulnerability Disclosure (CVD) is standardized by the International Organization for Standardization (ISO), is simple to implement and has been proven to be successful in some large software companies around the world [i.4]. CVD is, however, still not established in the IoT industry and some companies are reticent about dealing with security researchers. CVD provides a way for security researchers to contact companies to inform them of security issues putting the company ahead of the threat of malicious exploitation and giving them an opportunity to resolve vulnerabilities in advance of a public disclosure.

Companies that provide internet-connected devices and services have a duty of care to consumers and third parties who can be harmed by their failure to have a CVD programme in place. Additionally, companies that share this information through industry bodies can assist others who can be suffering from the same problem.

Disclosures can comprise different approaches depending on the circumstances:

- Vulnerabilities related to single products or services: the problem is expected to be reported directly to the affected stakeholder (e.g. device manufacturer, IoT service provider or mobile application developer). The source of these reports can be security researchers or industry peers.

- Systemic vulnerabilities: a stakeholder, such as a device manufacturer, can discover a problem that is potentially systemic. Whilst fixing it in the device manufacturer's own product is crucial, there is significant benefit to industry and consumers from sharing this information. Similarly, security researchers can also seek to report such systemic vulnerabilities. In this case, a relevant competent industry body can coordinate a wider scale response.

NOTE 2: The Common Vulnerability Reporting Framework (CVRF) [i.5] can also be useful to exchange information on security vulnerabilities.

Cyber security threat information sharing can support organizations in developing and producing secure products [i.6].

4.3 Keep software updated

Provision 4.3-1 All software components in consumer IoT devices should be securely updateable.

Provision 4.3-2 The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required.

NOTE 1: The appropriate entity is decided by the relevant jurisdiction.

Provision 4.3-3 When software components are updateable, updates shall be timely.

Provision 4.3-4 When software components are updateable, an end-of-life policy shall be published for devices that explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. This policy shall be published in an accessible way that is clear and transparent to the consumer.

Provision 4.3-5 When software components are updateable, the need for each update should be made clear to consumers and an update should be easy to implement.

Developing and deploying software security updates in a timely manner is one of the most important actions a company can take to protect its customers and the wider technical ecosystem. Vulnerabilities often stem from software components that are not considered to be security related. It is good practice that all software is kept updated and well maintained.

"Timely" in the context of software updates can vary, depending on the particular issue and fix, as well as other factors, such as the ability to reach a device or constrained device considerations. For a non-critical bug, it can be acceptable to deliver a software update within a regular patch cycle; for a severe, remote code execution flaw, a more immediate update can be expected.

Software security updates can be provided for devices in a preventative manner, often as part of automatic updates, which can remove security vulnerabilities before they are exploited. Managing this can be complex, especially if there are parallel cloud service updates, device updates and other service updates to deal with. Therefore, a clear management and deployment plan is essential, as is transparency to consumers about the current state of update support.

In many cases, publishing software updates involves multiple dependencies on other organizations such as manufacturers of sub-components, however, this is not a reason to withhold updates. It is essential that the entire software supply chain is considered in the development and deployment of security updates.

Software updates are expected to be provided after the sale of a device and pushed to devices for a period appropriate to the device. When purchasing the product, the consumer expects this period of software update support to be made clear.

Software in consumer IoT devices can be one or more categories (this is a non-exhaustive list): firmware, platform software such as an operating system, services and applications. The update process can be different for the different categories of software.

Provision 4.3-6 When software components are updateable, updates should, where possible, maintain the basic functioning of the device, which can be critical to remain available during an update.

It can be critical for consumers that a device continues to operate during an update. This is why the provision above recommends to "maintain the basic functioning of the device" where possible. Particularly, devices that fulfil a safety-relevant function are expected not to turn completely off in the case of an update; some minimal system functional capability is expected.

EXAMPLE: During an update, a watch is expected to continue to tell the time, a home thermostat is expected to continue to be operable and heating settings changeable by users and a smart lock usable for unlocking and locking a door. This can become a critical safety issue for some types of devices and systems if not considered or managed correctly.

Provision 4.3-7 When software components are updateable, the provenance of software updates should be assured and security patches should be delivered over a secure channel.

NOTE 2: Software update mechanisms can present an attack vector.

Provision 4.3-8 For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.

Provision 4.3-9 For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period of hardware replacement support and an end-of-life policy should be published in an accessible way that is clear and transparent to the consumer.

There are some situations where devices cannot be patched. For constrained devices a replacement plan needs to be in place and be clearly communicated to the consumer. This plan would typically detail a schedule for when technologies will need to be replaced and, where applicable, when support for hardware and software ends.

4.4 Securely store credentials and security-sensitive data

Provision 4.4-1 Credentials and security-sensitive data shall be stored securely within services and on devices. Hard-coded credentials in device software shall not be used.

Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Secure, trusted storage mechanisms can be used to secure security-sensitive data, such as those provided by a Trusted Execution Environment (TEE) and associated trusted, secure storage, or the secure storage and processing capabilities of software running on a Universal Integrated Circuit Card UICC/embedded Universal Integrated Circuit Card (eUICC).

4.5 Communicate securely

Provision 4.5-1 Security-sensitive data, including any remote management and control, should be encrypted in transit, with such encryption appropriate to the properties of the technology and usage.

Provision 4.5-2 All keys should be managed securely.

The use of open, peer-reviewed standards is strongly encouraged.

It is expected that products meet the needs of users whilst remaining resilient to attacks on encryption. However, appropriateness of security controls and the use of encryption is dependent on many factors including the usage context. As security is ever-evolving it is difficult to give prescriptive advice about encryption measures without the risk of such advice quickly becoming obsolete.

4.6 Minimize exposed attack surfaces

The "principle of least privilege" is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

Provision 4.6-1 Unused software and network ports should be closed.

Provision 4.6-2 Hardware should not unnecessarily expose access to attack (e.g. open serial access, ports or test points).

Provision 4.6-3 Software services should not be available if they are not used.

Provision 4.6-4 Code should be minimized to the functionality necessary for the service/device to operate.

Provision 4.6-5 Software should run with least necessary privileges, taking account of both security and functionality.

4.7 Ensure software integrity

Provision 4.7-1 Software on IoT devices should be verified using secure boot mechanisms, which require a hardware root of trust.

Provision 4.7-2 If an unauthorized change is detected to the software, the device should alert the consumer and/or administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

The ability to remotely recover from these situations can rely on a known good state, such as locally storing a known good version to enable safe recovery and updating of the device. This will avoid denial of service and costly recalls or maintenance visits, whilst managing the risk of potential takeover of the device by an attacker subverting update or other network communications mechanisms.

If an IoT device detects something unusual has happened with its software, it will be able to inform the right person. In some cases, devices can have the ability to be in administration mode - for example, there can be a user mode for a thermostat in a room that prevents other settings being changed. In these cases, an alert to the administrator is appropriate as that person has the ability to act on the alert.

4.8 Ensure that personal data is protected

Provision 4.8-1 Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

Provision 4.8-2 Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.

Provision 4.8-3 Consumers who gave consent for the processing of their personal data shall be given the opportunity to withdraw it at any time.

It is expected that the appropriate entity, such as the service provider or device manufacturer, ensures that personal data is processed in accordance with applicable data protection law, for example the GDPR [i.7], and also in accordance with applicable legislation regarding security and regulatory matters.

Obtaining consent "in a valid way" normally involves giving consumers a free, obvious and explicit opt-in choice of whether their personal data can be used for a specified purpose.

Consumers expect to be provided with means to preserve their privacy by means of configuring IoT device and service functionality appropriately.

4.9 Make systems resilient to outages

Provision 4.9-1 Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power.

Provision 4.9-2 As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power.

Provision 4.9-3 Devices should be able to return to a network in an expected, operational and stable state and in an orderly fashion, rather than in a massive-scale reconnect.

IoT systems and devices are relied upon by consumers for increasingly important use cases that can be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures can include building redundancy into associated services as well as mitigations against, for example, Distributed Denial of Service (DDoS) attacks or signalling storms which can be caused by mass-reconnections of devices following an outage. It is expected that the level of resilience necessary is proportionate and determined by usage, with consideration given to others that rely on the system, service or device given that an outage can have a wider impact than expected.

The aim of the above provisions is to ensure that IoT services are kept up and running as the adoption of IoT devices across all aspects of a consumer's life increases, including in functions that are relevant to personal safety. The impact on people's lives could be prevalent if, for example, an internet connection is lost to a connected door and someone is locked outside. Another example is a home heating system that turns off because of a DDoS attack against a cloud service. It is important to note that other safety-related regulations can apply, but the key is to avoid making outages the cause of these problems and to design products and services ready for these challenges.

4.10 Examine system telemetry data

Provision 4.10-1 If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.

Provision 4.10-2 If telemetry data is collected from IoT devices and services, the processing of personal data should be kept to a minimum and such data should be anonymized.

Provision 4.10-3 If telemetry data is collected from IoT devices and services, consumers shall be provided with information on what telemetry data is collected and the reasons for this.

Examining telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimizing security risk and allowing quick mitigation of problems.

4.11 Make it easy for consumers to delete personal data

Provision 4.11-1 Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it, when the consumer wishes to remove a service from the device and/or when the consumer wishes to dispose of the device.

Provision 4.11-2 Consumers should be given clear instructions on how to delete their personal data.

Provision 4.11-3 Consumers should be provided with clear confirmation that personal data has been deleted from services, devices and applications.

IoT devices often change ownership and will eventually be recycled or disposed of. Mechanisms can be provided that allow the consumer to remain in control and remove personal data from services, devices and applications. When a consumer wishes to completely remove their personal data, they also expect this to include backup copies that the service provider may hold.

Deleting personal data from a device or service is not simply achieved by resetting a device back to its factory settings. There are many use cases where the consumer is not the owner of a device, but wishes to delete their own personal data from the device and all associated services such as cloud services or mobile applications.

EXAMPLE: A user can have temporary usage of consumer IoT products within a rented apartment. Carrying out a factory reset of the product can remove configuration settings or disable the device to the detriment of the apartment owner and a future user. It would be an inappropriate technical mechanism to delete all personal data in this context.

4.12 Make installation and maintenance of devices easy

Provision 4.12-1 Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.

Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats.

4.13 Validate input data

Provision 4.13-1 Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

i) Not of the expected type, for example executable code rather than user inputted text.

ii) Out of range, for example a temperature value which is beyond the limits of a sensor.

Annex A (informative): Implementation pro forma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the pro forma in the present annex so that it can be used for its intended purposes and may further publish the completed annex including table A.1.

The purpose of table A.1 is to provide a mechanism for the user of the present document (for example an entity involved in the development or manufacturing of consumer IoT) to give information about the implementation of the provisions within the present document.

The reference column gives reference to the provisions in the present document.

The status column indicates the status of a provision. The following notations are used:

M	the provision is a mandatory requirement
R	the provision is a recommendation
M C	the provision is a mandatory requirement and conditional
R C	the provision is a recommendation and conditional

NOTE: Where the conditional notation is used, this is conditional on the text of the provision.

The support column can be filled in by the user of the present document. The following notations are used:

Y	supported by the implementation
N	not supported by the implementation
N/A	the provision is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the product in question)

The detail column can be filled in by the user of the present document.

- If a provision is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.
- If a provision is not supported by the implementation, the entry in the detail column is to contain information on the reasons why implementation is not possible or not appropriate.
- If a provision is not applicable, the entry in the detail column is to contain the rationale for this determination.

Table A.1: Implementation of provisions for consumer IoT security

Clause number and title			
Reference	**Status**	**Support**	**Detail**
4.1 No universal default passwords			
Provision 4.1-1	M		
4.2 Implement a means to manage reports of vulnerabilities			
Provision 4.2-1	M		
Provision 4.2-2	R		
Provision 4.2-3	R		
4.3 Keep software updated			
Provision 4.3-1	R		
Provision 4.3-2	R		
Provision 4.3-3	M C (see note 1)		
Provision 4.3-4	M C (see note 1)		
Provision 4.3-5	R C (see note 1)		
Provision 4.3-6	R C (see note 1)		
Provision 4.3-7	R C (see note 1)		
Provision 4.3-8	R C (see note 2)		
Provision 4.3-9	R C (see note 2)		
4.4 Securely store credentials and security-sensitive data			
Provision 4.4-1	M		
4.5 Communicate securely			
Provision 4.5-1	R		
Provision 4.5-2	R		
4.6 Minimize exposed attack surfaces			
Provision 4.6-1	R		
Provision 4.6-2	R		
Provision 4.6-3	R		
Provision 4.6-4	R		
Provision 4.6-5	R		
4.7 Ensure software integrity			
Provision 4.7-1	R		
Provision 4.7-2	R		
4.8 Ensure that personal data is protected			
Provision 4.8-1	M		
Provision 4.8-2	M		
Provision 4.8-3	M		
4.9 Make systems resilient to outages			
Provision 4.9-1	R		
Provision 4.9-2	R		
Provision 4.9-3	R		
4.10 Examine system telemetry data			
Provision 4.10-1	R C (see note 3)		
Provision 4.10-2	R C (see note 3)		
Provision 4.10-3	M C (see note 3)		
4.11 Make it easy for consumers to delete personal data			
Provision 4.11-1	R		
Provision 4.11-2	R		
Provision 4.11-3	R		
4.12 Make installation and maintenance of devices easy			
Provision 4.12-1	R		
4.13 Validate input data			
Provision 4.13-1	M		
NOTE 1: Provisions 4.3-3, 4.3-4, 4.3-5, 4.3-6 and 4.3-7 are conditional on software components being updateable. NOTE 2: Provisions 4.3-8 and 4.3-9 are conditional on the inability to update the software of constrained devices. NOTE 3: Provisions 4.10-1, 4.10-2 and 4.10-3 are conditional on telemetry data being collected.			

History

Document history		
V1.1.1	February 2019	Publication