ETSI TR 103 621 V1.2.1 (2022-09)

Guide to Cyber Security for Consumer Internet of Things

Reference
RTR/CYBER-0084

Keywords
cybersecurity, IoT

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

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 Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**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

The growth of the Internet of Things has spurred the development of security requirements for IoT devices. ETSI EN 303 645 [i.1] provides baseline cyber security provisions for a wide range of Consumer IoT products and remains outcome focused. While ETSI TS 103 701 [i.3] deals with the assessment of conformance of IoT products against the provisions of ETSI EN 303 645 [i.1], the present document has been developed to guide manufacturers on its implementation, by providing non-exhaustive examples of practical solutions that can be used to meet these provisions. Additionally, the examples provided herein are not limitative; it is possible to meet the provisions in ETSI EN 303 645 [i.1] by using other solutions.

1 Scope

The present document serves as guidance to help manufacturers and other stakeholders in meeting the cyber security provisions defined for Consumer IoT devices in ETSI EN 303 645 [i.1] and ETSI TS 103 645 [i.2].

The present document is complementary to ETSI EN 303 645 [i.1] and ETSI TS 103 701 [i.3]. It explains the relationship between these specifications and how they can be used together. It also provides a non-exhaustive set of example implementations that can be used to meet the provisions of ETSI EN 303 645 [i.1] and ETSI TS 103 645 [i.2], noting that not all possible implementations are included. Where relevant, pointers to supporting specifications are provided. Usage by industry players as well as future development of standards, such as specialisation into precise use cases, or certification aspects, are being given consideration.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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

[i.2] ETSI TS 103 645 (V2.1.2): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

NOTE: The technical content of ETSI TS 103 645 (V2.1.2) is exactly the same as in ETSI EN 303 645 (V2.1.1).

[i.3] ETSI TS 103 701 (V1.1.1): "CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.4] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.5] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[i.6] GNU Bison.

NOTE: Available at https://www.gnu.org/software/bison/.

[i.7] W3C® Recommendation: "W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures".

NOTE: Available at https://www.w3.org/TR/xmlschema11-1/.

[i.8] JSON Schema.

NOTE: Available at https://json-schema.org/.

[i.9] Article 29 Working Party: "Guidelines on transparency under Regulation 2016/679".

[i.10] Article 29 Working Party: "Guidelines on consent under Regulation 2016/679".

NOTE: Available at https://edpb.europa.eu.

[i.11] IETF RFC 1034: "DOMAIN NAMES - CONCEPTS AND FACILITIES".

[i.12] Microsoft™ SDL: "Security Development Lifecycle".

NOTE: Available at https://www.microsoft.com/sdl.

[i.13] ISO/IEC 27034-3: "Information technology -- Application security -- Part 3: Application security management process".

[i.14] ISO/IEC 29147: "Information technology -- Security techniques -- Vulnerability disclosure".

[i.15] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.16] IETF RFC 7516: "JSON Web Encryption (JWE)".

[i.17] ETSI TR 103 838: "Cyber security; Guide to Coordinated Vulnerability Disclosure".

[i.18] IoT Security Foundation: "Vulnerability Disclosure Best Practice Guidelines".

NOTE: Available at https://www.iotsecurityfoundation.org/best-practice-guidelines/.

[i.19] HackerOne®, vulnerability disclosure service.

NOTE: Available at https://www.hackerone.com/.

[i.20] NCSC: "Setting up two-factor authentication (2FA)".

NOTE: Available at https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa.

[i.21] NCSC: "Secure development and deployment guidance".

NOTE: Available at https://www.ncsc.gov.uk/collection/developers-collection.

[i.22] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.23] NIST SP800-90A: "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

[i.24] AIS 20/31: "A proposal for: Functionality classes for random number generators".

[i.25] ANSI/ISA-62443: "Security for industrial automation and control systems".

[i.26] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[i.27] IEEE 802.11w™-2009: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames".

[i.28] IEEE 802.11i™-2004: "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements".

[i.29] IETF RFC 6238: "TOTP: Time-Based One-Time Password Algorithm".

[i.30] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

NOTE: Available at https://eur-lex.europa.eu/.

[i.31] Mayhew, Joe, and Hamid Jahankhani: "Current Challenges of Modern-Day Domestic Abuse", Policing in the Era of AI and Smart Societies. Springer, Cham, 2020. 267-282.

[i.32] Datta Burton, S. et al.: "The UK Code of Practice for Consumer IoT Cybersecurity: where we are and what next" (2021).

[i.33] 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.34] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 303 645 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 303 645 [i.1] and the following apply:

ACM	Agreed Cryptographic Mechanisms
AES	Advanced Encryption Standard
AIS	Application notes and Interpretation of the Scheme
ANSI	American National Standards Institute
ARM	Advanced RISC Machine
BLE	Bluetooth® Low Energy
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CPU	Central Processing Unit
CSA	Coordination and Support Action
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ECRYPT	European Network of Excellence for Cryptology
EN	European Standard
FAQ	Frequently Asked Question
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
GHz	GigaHertz
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISA	International Society of Automation
IV	Initialization Vector
JSON	JavaScript Object Notation
KDF	Key Derivation Function
MAC	Message Authentication Code
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSK	Pre-Shared Key

RAM	Random-Access Memory
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
SAE	Simultaneous Authentication of Equals
SHA	Securing Hash Algorithm
SMS	Short Message Service
SOGIS	Senior Officials Group on Information Security
TOTP	Time-based One-Time-Password
TPM	Trusted Platform Module
WAN	Wide Area Network
WLAN	Wireless LAN
WPA	Wi-Fi® Protected Access
XOR	exclusive OR
XTS	XOR-Encrypt-XOR-Based Tweaked-Codebook Mode with Ciphertext Stealing

4 Using the present document

4.1 Purpose

The present document provides guidance to implement the provisions in ETSI EN 303 645 [i.1] in the form of examples illustrating possible solutions. The intent is to help implementers better understand how each provision can be met. It is reminded that ETSI EN 303 645 [i.1] and ETSI TS 103 645 [i.2] both provide guidance text and examples. These can be referred to when considering the examples provided herein. These examples are provided in clauses 6 and 7.

In ETSI EN 303 645 [i.1] and ETSI TS 103 645 [i.2] recommendations are expected to be followed by manufacturers unless there exists a justification for not doing so. Examples of situation where it might be difficult to follow a given recommendation are provided in clause 8.

4.2 Relationship to ETSI EN 303 645

The examples provided in the present document are tailored to the outcome-focused nature of ETSI EN 303 645 [i.1]. It is acknowledged that ETSI EN 303 645 [i.1] can be specialised into more precise domains of applicability, for example smart locks. In such case, the example solutions to meet the new set of provisions can be better tailored to this specific IoT domain. It is expected that these examples would be included in an update to the present document, or to a future, dedicated guidance document.

4.3 Relationship to ETSI TS 103 701

ETSI TS 103 701 [i.3] provides a framework for the assessment of the provisions defined in ETSI EN 303 645 [i.1]. As such, they can be used (when implemented) to inform the definition of test scenarios and the development of a test plan based on ETSI TS 103 701 [i.3]. As described in clauses 4.1 and 4.2, a specialisation of ETSI EN 303 645 [i.1] for a specific application domain can allow more precise examples to be provided which, when implemented, would allow more precise test scenarios and test plan, leading to stronger certainty on the test expectations and outcomes.

5 Guidance on implementation

Clauses 6 and 7 provide examples for implementing the provisions laid out in ETSI EN 303 645 [i.1]. The examples provided herein are not exhaustive or limitative; it is possible to meet the provisions in ETSI EN 303 645 [i.1] by using other solutions or variants of the provided examples.

For each provision, the examples are not given in a specific qualitative order (therefore, example 1 is not necessarily qualitatively better than example(s) 2 or 3) but are ordered by usage, from the most widely applicable examples to the more specific ones. While most examples are meant to cover a large spectrum of IoT cases, those that relate to a specific type of IoT device, constrained device, or a given use case are indicated as such.

The examples in clauses 6 and 7 of the present document provide guidance on the implementation of cybersecurity mainly protecting users from unknown other users. However, consumer IoT devices can be misused, e.g. by intimate partners, which makes it even more difficult to find appropriate security measures.

The following list provides examples of related threats using consumer IoT devices:

- audio control (i.e. recording and/or replying);
- video control (i.e. recording and/or displaying);
- data control (i.e. collection, manipulation, unintended disclosure);
- access to shared accounts linked to the consumer IoT device and therefore providing the possibility for social stalking (e.g. social media);
- other remote control threats (e.g. heating control, door lock control).

The exploitation of the aforementioned threats might result in coercive control (e.g. isolation from friends and family, spying, deprivation of vital and basic means such as medical services and food, controlling finances, etc.).

In this regard, the following measures could help to mitigate domestic abuse by using consumer IoT devices [i.31]:

- introduction of legal policy to prosecute abusers and protect victims of domestic abuse in cases of digital coercive control;
- development of technology that at least provides evidence of activity in cases of domestic abuse, however, without violating data protection/privacy regulations;
- creation of awareness to improve prevention, and establish contact possibilities in cases of domestic abuse to support the victims by providing appropriate advice.

Privacy and data protection related legislation only cover a small part of the first of the aforementioned measures as requirements are set against personal data in terms of transparency in processing as well as purpose limitation, accuracy, integrity and confidentiality.

The second item referring to technology depends on the specific application scenario and can be considered during the development of corresponding solutions or verticals based on ETSI EN 303 645 [i.1] appropriate to the properties of the technology, risk, benefit and usage. Designing ways to prevent the misuse of the device intends to mitigate the risk of its misuse, but it is understood that it might not eliminate the risk entirely.

The item regarding awareness can be realized by training and by reaching out to all stakeholders of consumer IoT products, for instance by advertisements or by including the domestic abuse matter into guidelines as in the present document.

NOTE: The UK Code of Practice for Consumer IoT Security [i.32] provides statistics and references to the current state of the art regarding research in consumer IoT tech abuse. It also references to industry actors providing guidelines to prevent that technology is being used for domestic abuse.

6 Examples to meet cyber security provisions for consumer IoT

6.1 Provision 5.1-1

"Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user". (ETSI EN 303 645 [i.1])

NOTE 1: An example for this provision is also provided in ETSI EN 303 645 [i.1].

EXAMPLE 1: The consumer IoT device password for the factory default state is printed on a sticker under the device casing. During the initialization phase, the user is requested to provide a new password and the procedure cannot complete without the new password being different from the default state password.

EXAMPLE 2: The consumer IoT device has no password in the factory default state and generates a password for the user during the initialization phase. The device is not constrained and the password generation process is based on a cryptographically secure pseudorandom number generator where the entropy source is an on-device ring oscillator.

NOTE 2: For simpler and constrained devices, a less advanced MCU does not provide the same cryptographic acceleration and entropy.

EXAMPLE 3: The consumer IoT device prompts a user to create a password, choosing any complexity requirements such that a user can create a memorable password with a strength appropriate to the device's capabilities and the security necessary for the application.

6.2 Provision 5.1-2

"Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device". (ETSI EN 303 645 [i.1])

NOTE 1: An example for this provision is also provided in ETSI EN 303 645 [i.1].

EXAMPLE 1: The password is generated using a cryptographically secure pseudorandom number generator present on a chip in the device. The password complexity is such that the password cannot be guessed through an exhaustive search attack (including optimized variants such as dictionary attacks) via the quickest authentication method available on the device, at least during its expected lifetime. The password is concatenated with a per-device salt and hashed. The device uses a well-known widely implemented hashing algorithm with no known weaknesses, appropriate to the device's capabilities and the security necessary for the application.

NOTE 2: A guidance on the choice of hashing algorithms is given in ETSI TS 119 312 [i.22].

EXAMPLE 2: The manufacturer generates pre-installed passwords within the factory environment using a critical security parameter, stored within a hardware security module, concatenated with either the serial number or MAC address of the device. The resultant string is hashed and the last 8 bytes, as represented in hexadecimal to be human-readable, are taken to be the default password for that device.

EXAMPLE 3: The device is provisioned with a private-public key pair. Upon initialization, a critical security parameter is sent from the factory environment to the device, encrypted with the public key of the device. The device decrypts this message to get the critical security parameter. The device concatenates the critical security parameter with either the serial number or MAC address of the device. The resultant string is hashed and the last 8 bytes, as represented in hexadecimal to be human-readable, are taken to be the device password. This allows a manufacturer to update the device's password throughout its lifetime using a cryptographically secure generation method which would not be available on the device.

6.3 Provision 5.1-3

"Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage". (ETSI EN 303 645 [i.1])

EXAMPLE 1: The authentication protocol between the device control application and the device is protected by TLS 1.2 [i.15] or a higher version, using cipher suites and other security parameters in recommendations issued by a governmental agency for security or by prominent industry crypto-catalogues adapted to the usage context of the device, considering the date of implementation and the expected lifecycle of the device.

EXAMPLE 2: The consumer IoT device provides a password-based user authentication mechanism, so that the user can login and connect to the consumer IoT device using a mobile application. The authentication mechanism is IP-based and uses the HTTP authentication framework (IETF RFC 7235 [i.26]), and TLS 1.2 with a PKI-based authentication is implemented. The consumer IoT device stores two certificates imported during the manufacturing process; one is an individual client certificate (Signature Algorithm ECDSA, key length 224, SHA-224) and the other is the root certificate (Signature Algorithm ECDSA, key length 224, SHA-224) of the PKI. The TLS 1.2 cryptographic configuration for the connection is TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. Within the connection establishment, the IoT device and the mobile application exchange their certificates and verify them against the root certificate, ensuring the authenticity of the connection. The AES session encryption with 128 bits key length in GCM mode ensures the confidentiality and integrity of the data exchange. The cryptography is suitable for the corresponding use case regarding the needed security guarantees. There are no published feasible attacks with regard to current readily available techniques (State 17 February 2021). The used cryptography is part of the public cryptographic catalogue SOGIS-ACM (State 17 February 2021).

EXAMPLE 3: The consumer IoT device provides a password-based user authentication mechanism via an IP-based web interface. The IP connection is offered wireless (Wi-Fi® protocol per default) or wired (Ethernet). The underlying use case is that the user connects to the consumer IoT device, located in the home, using a web browser for the login. The authentication mechanism is implemented via HTTP authentication framework (IETF RFC 7235 [i.26]) and WPA2 (IEEE 802.11i [i.28]) with Protected Management Frames support (IEEE 802.11w™ [i.27]). The WPA2 implementation uses AES/CCMP. For wireless connection, WPA2 with the out-of-band exchange of the network key ensures that the communication is authenticated. The AES session encryption with 128 bits key size ensures the security guarantees, confidentiality and integrity of the password transmission. The cryptography is suitable for the corresponding use case regarding the needed security guarantees. There are no published feasible attacks with regard to current readily available techniques (State 17 February 2021). The used cryptography is part of the public cryptographic catalogue ECRYPT CSA and compliant to FIPS PUB 140-2 [i.34] (State 17 February 2021). For a wired connection, the authenticity and confidentiality are ensured by physical measures and network separation (LAN/WAN), and the risk assessment model that only trustworthy devices operate in the home environment. Therefore, the cryptography is suitable for the corresponding use case.

NOTE: Example 3 bases on the assumption of a trustworthy home environment where the connection to the consumer IoT device using a physical interface is considered to be secure.

EXAMPLE 4: Password-based authentication schemes for connection to a wireless network rely on cryptographic schemes ensuring forward secrecy to prevent offline brute-force attacks of the password based on wireless traffic that has been eavesdropped upon then recorded (e.g. WPA3-SAE was introduced to prevent offline attacks on a recorded Wi-Fi® exchange relying on WPA2-PSK).

6.4 Provision 5.1-4

"Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used".(ETSI EN 303 645 [i.1])

NOTE: Examples for this provision are also provided in ETSI EN 303 645 [i.1].

EXAMPLE 1: During the initialization process, a user is asked to provide a PIN for password reset purposes. A user can reset the password for their consumer IoT device using this PIN through one or more of the following methods: online, through an application, via email or a dedicated phone hotline. Each of these methods triggers an email or SMS sent to the user's registered details, which contains a link to reset the password.

EXAMPLE 2: The device's Graphical User Interface provides each user a prominent widget on the home screen to manage user authentication values. The widget takes the user to a management process, which is limited to the steps required to change the value, including re-authentication if necessary. When the user is an administrator, they can go through the same process to change their own authentication value or that of another user.