ETSI TS 103 848 V1.2.1 (2025-02)

Cyber Security for Home Gateways;
Security Requirements
as vertical from Consumer Internet of Things

Reference
RTS/CYBER-00148

Keywords
cybersecurity, home gateway, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

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 on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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.

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.

1 Scope

The present document defines security provisions for Home Gateways resulting from the analysis presented in ETSI TR 103 743 [i.1], and extending from the provisions for consumer IoT devices defined in ETSI EN 303 645 [1].

NOTE 1: The Home Gateway (HG) is not an IoT device as defined in ETSI EN 303 645 [1]. However, due to its generic character, ETSI EN 303 645 [1] is appropriate as baseline for the HG. The present document therefore is an adaption of the provisions of ETSI EN 303 645 [1] for the specific capabilities of a HG.

EXAMPLE: The HG is responsible for network management and is therefore subject to higher requirements than a consumer IoT device concerning the role of an administrator having a higher level of privilege than a user.

NOTE 2: The adoption of ETSI EN 303 645 [1] as a baseline does not infer that a Home Gateway (HG) is an IoT device according to the ETSI EN 303 645 [1] definition.

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 in the ETSI docbox.

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.

[1] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

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 103 743: "CYBER; Home Gateway Security Threat Analysis".

[i.2] Wi-Fi Easy Connect™.

[i.3] NIST SP 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation".

[i.4] IEEE 802.11™-2020: "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".

NOTE: The above reference supersedes IEEE 802.11i™ and incorporates the latest security mechanisms as originally found in IEEE 802.11i™.

[i.5] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.6] ETSI TR 103 305-2: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing".

[i.7] ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.8] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

NOTE: Earlier versions of TLS still apply.

[i.9] Broadband Forum Technical Report 069 (TR-069): "CPE WAN Management Protocol (CWMP)".

[i.10] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

[i.11] ISO/IEC 14882:2020(E): "Programming Language C++".

[i.12] ETSI TS 119 312: "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

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 [1], ETSI TR 103 743 [i.1] and the following apply:

community Wi-Fi®: Wi-Fi® channel made available from the HG independently of the user and guest provisions to allow public access to the Internet

Hardware-Based Root of Trust (HBRT): hardware component that provides a tamper-proof unique per device identity and can perform cryptographic functions in an isolated environment

EXAMPLE: A hardware-based Trusted Platform Module (TPM) can be used as a hardware-based root of trust.

Home Gateway (HG): physical device that lies between the in-home network and the public network with a primary purpose of managing traffic between these networks

IPsec tunnel: protective communication protocol and technology on which a VPN can be built

NOTE: Each IP packet gets encrypted and authenticated prior sending. Authenticated means that an encrypted or signed hash-value is attached, which only the receiving entity can decrypt and verify. Prior sending, the packet is then encapsulated into a new packet with a packet header and sent. This establishes a confidentiality and integrity protection between two network entities.

local administrator: administrator that performs management actions on the HG from the LAN connection

EXAMPLE: A local administrator generates and manages the LAN Wi-Fi® accounts and interfaces.

remote administrator: administrator that performs management actions on the HG from the WAN connection

NOTE: The remote administrator can include the role of the ISP in managing elements of the HG required for access to the WAN.

security log data: log data that is related to security events only

NOTE: These data can contain MAC-, IP-addresses and other data types which could constitute or be related to personal data.

security critical data: all data comprising security parameters, keys, authentication credentials, security relevant device configuration settings and any similar values, suitable either to compromise the HG, jeopardize the user LAN, or even the ISP network.

traffic management log data: log data that is related to traffic management events only

transmission log data: log data that is related to transmission events only

Virtual Private Network (VPN): protected and managed communication channel between one or more entities traversing a public network

NOTE: The protection of each communication link within a VPN relies usually on preparation steps: The entities have been identified, authenticated, authorized, negotiated a common session symmetric key, and have means in place to preserve the integrity of the subsequent communication. The identification, authentication and authorization of each entity is usually based on security credentials managed by the VPN operator. All these protection means constitute a VPN.

EXAMPLE: An IPsec tunnel is one means of implementing a VPN.

3.2 Symbols

Void.

3.3 Abbreviations

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

ACL	Access Control List(s)
CPE	Customer Premises Equipment
DoS	Denial of Service
EN	European Standard
HBRT	Hardware-Based Root of Trust
HG	Home Gateway
HMEE	Hardware Mediated Execution Enclave
HSM	Hardware Security Module
ISP	Internet Service Provider
IT	Information Technology
KASLR	Kernel Address Space Layout Randomization
LTS	Long-Term Support
N/A	Not applicable
NMS	Network Management System
NTP	Network Time Protocol
NVM	None-Volatile Memory
OS	Operating System
PIE	Position Independent Executable
PSK	Pre-Shared-Key
RELRO	Relocation Read Only
R&D	Research and Development
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SW	Software
TLS	Transport Layer Security
TPM	Trusted Platform Module
VPN	Virtual Private Network
Wi-Fi®	Wireless Fidelity
WPA	Wi-Fi® Protected Access

4 Methodology and general requirements

4.1 Introduction

A Home Gateway (HG) is connected on one side to the Internet Service Provider (ISP) network and on the other side to the user's Local Area Network (LAN). On the ISP network side, the HG is exposed to other risks and attacks as an IoT device, which justifies the promotions, refinements, extensions and additions of the provisions of ETSI EN 303 645 [1].

For the purposes of the present document, the ETSI EN 303 645 [1] sets a security baseline that has been adopted for the Home Gateway (HG) independently of a potential classification of an HG as an IoT device.

The provisions specified in the present document are supported by the threat analysis in clauses 5 and 6 of ETSI TR 103 743 [i.1].

4.2 Handling of provisions

The present document adopts the provisions of ETSI EN 303 645 [1] as a baseline for the HG. The methodology used for the adoption is described in the present clause, which includes different operations to modify provisions from ETSI EN 303 645 [1] and add new provisions specific to the present document.

All provisions from ETSI EN 303 645 [1] shall apply in the present document, unchanged, to the HG, unless otherwise noted in the present document.

Consumer IoT devices in the vertical domain of a HG are not constrained devices. Consequently, all provisions from ETSI EN 303 645 [1] regarding constrained devices are adjusted accordingly.

There are different types of modifications indicated by a naming convention as described in clause 4.3. Within clauses 5 and 6 of the present document, the following modifications can be applied to the set of provisions defined in ETSI EN 303 645 [1]:

- **Information:** Providing additional information (in the form of informative text) to an unmodified provision. The original provision in ETSI EN 303 645 [1] is still valid.

- **Promotion:** Promoting a recommendation to a mandatory provision. The wording of the provision remains as in the original provision, but the promoted modal verb is replaced by the new modal verb (e.g. "should" is replaced by "shall"). The original provision in ETSI EN 303 645 [1] is replaced by the promotion and is not valid anymore.

- **Refinement:** Refining a provision with additions or modifications to its normative definition text, including stronger scoping of conditionality. The original scope and spirit remain in force. The original provision in ETSI EN 303 645 [1] is replaced by the refinement and is not valid anymore.

NOTE: A refinement can be used to scope the conditionality of a provision, i.e. to remove one or more conditions from the provision, as part of the clarification on the provision's constraints.

- **Extension:** Extending an existing provision with one or more new sub-provisions. The original provision in ETSI EN 303 645 [1] is still valid.

- **Substitution:** Replacing a recommendation that is not applicable for the HG with another recommendation of equivalent effect (that provides, possibly in combination with other recommendations or provisions, the same security outcome as the replaced recommendation). The original provision in ETSI EN 303 645 [1] is replaced by the substitution and is not valid anymore.

- **Exclusion** (only possible for recommendations and conditional provisions): Declaring a recommendation or conditional provision as "not applicable" for the HG. The original provision in ETSI EN 303 645 [1] is excluded and is not valid anymore.

The present document allows to define new provisions within clause 7 that are not covered in ETSI EN 303 645 [1]. There is one type of new provisions, which is also covered by the naming convention in clause 4.3:

- **Addition:** Defining a new provision specific to the HG that cannot be linked to any provision in ETSI EN 303 645 [1].

4.3 Naming conventions

The provisions in the present document are named following the naming conventions described in the present clause.

Each provision contains an acronym representing the HG. The acronym for the HG is set to HG.

Names for provisions that are specific to the present document are constructed as follows:

- The name starts with the string "Provision" to which the acronym "HG" is appended.
- A provision identifier (id) is appended. An example id is 5.1-1.
- One or more suffixes are appended (according to the types of provisions as described in clause 4.2).

NOTE: A provision can be at the same time promoted and refined, in which case the two suffixes are appended to its name.

- For provisions that are extensions, an alphabetical index is appended, that is unique to the provision, for example, "-a". The alphabetical index is appended only in cases where there is more than one extension to a given provision.

The following list describes the suffixes depending on the type of the provision as described in clause 4.2:

- **Information:** The id is the id of the original provision in ETSI EN 303 645 [1] additional informative information is provided for. The suffix is "(information)".
- **Promotion:** The id is the id of the original provision in ETSI EN 303 645 [1] that is promoted. The suffix is "(promoted)".
- **Refinement:** The id is the id of the original provision in ETSI EN 303 645 [1] that is refined. The suffix is "(refined)".
- **Extension:** The id is the id of the original provision in ETSI EN 303 645 [1] that is extended. The suffix is "(extended)".
- **Substitution:** The id is the id of the original provision in ETSI EN 303 645 [1] that is substituted. The suffix is "(substituted)".
- **Exclusion:** The id is the id of the original provision in ETSI EN 303 645 [1] that is excluded. The suffix is "(excluded)".
- **Addition:** The id is a new and unique id added in clause 7 that reflects the clause in which it is defined. The suffix is "(added)".

4.4 Reporting implementation

Provision HG 4-1 (extended): A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the device.

5 Adapted cyber security provisions for the HG

5.1 No universal default passwords

Existing provisions from ETSI EN 303 645 [1], clause 5.1 are modified as follows.

In an HG, it is broadly assumed that a user and administrator can be the same person (not all users will be the same person as the administrator) but for the purposes of the present document the terms user and administrator refer to roles with respect to the HG, with the administrator having a higher level of privilege than a user.

EXAMPLE: An administrator account allows direct modification of some operational parameters of the HG. It is recognized that an HG can have more than one administrator account: one for the LAN side, and one for the ISP side. When separate local and ISP administrator accounts exist, it is assumed that these are suitably isolated from each other.

Provision HG 5.1-1 (extended): Where Wi-Fi® or administrator passwords are preconfigured in factory default, these preconfigured passwords shall be unique per HG.

Provision HG 5.1-4 (extended) a: HGs shall allow an administrator to set the Wi-Fi® password.

Provision HG 5.1-4 (extended) b: The HG shall provide to the local administrator a simple mechanism to change the Wi-Fi® password.

Provision HG 5.1-4 (extended) c: The HG shall provide to an administrator a simple mechanism to change the administrator password (local to local, remote to remote).

Provision HG 5.1-5 (refined): The HG shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.

5.2 Implement a means to manage reports of vulnerabilities

Existing provisions from ETSI EN 303 645 [1], clause 5.2 are modified as follows.

Provision HG 5.2-1 (information) and Provision HG 5.2-2 (information):
The above-named provisions in clause 5.2 of ETSI EN 303 645 [1] require the manufacturer to publish a policy for vulnerability disclosure and recommends handling vulnerabilities in a timely manner. The following clarifies these provisions for the HG, as the HG manufacturer can instantiate different parties and relations between them in the HG supply chain. Specifically, it is not a user problem to think about where to feedback a discovered vulnerability back to the manufacturer.

Thus provision 5.2-1 of ETSI EN 303 645 [1] holds true, but needs an explanation for HGs, as those can be subject to the peculiarities of supply chains that may or may not modify, or personalize, or in other ways alter, the manufacturer supplied HG. Users will probably address identified vulnerabilities to the instance where they have purchased the HG which is not necessarily the manufacturer in all cases.

EXAMPLE 1: If the HG is provided through a retail channel, or any other supply chain channel in addition to direct sales, the manufacturer enables all instances in that supply chain towards the customer to receive vulnerability reports by the user and handle them.

EXAMPLE 2: Whilst being made available to the manufacturer, the logs and vulnerability reports are made available through the supply chain for analysis. The supply chain in due course makes reports available to the manufacturer.

NOTE: Some of the provisions in this group are subject to constraints applied under consumer protection law in some jurisdictions.

EXAMPLE 3: In many jurisdictions the retail outlet has a primary duty of care for a period of time after sale and the user ought to be directed to the retail outlet to fix any problems within that period.

5.3 Keep software updated

Existing provisions from ETSI EN 303 645 [1], clause 5.3 are modified as follows.

Provision HG 5.3-1 (extended) a: If not all software components are updateable, those components affected shall be noted and indicated in the user guidance.

Provision HG 5.3-1 (extended) b: The HG shall implement software version control and verify that the version of the software provided by the update is valid prior to installation.

EXAMPLE 1: The simplest form of version control is to check that the update provides software that has a higher version number than the currently installed software. Such version control can also be used for rollback protection.