ETSI TS 103 848 V1.1.1 (2022-03)

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

Reference
DTS/CYBER-0069

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

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.

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 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.

[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™.

NOTE: Available at https://www.wi-fi.org/discover-wi-fi/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; 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 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 1: 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 (deprecated)

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 the clauses 7 and 8 that are not covered in ETSI EN 303 645 [1]. There is one type of new provisions, that 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 clauses 7 or 8 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.

NOTE 1: If an update fails and the previous state is reinstated, this is considered to be a reversion to the last known operational state and not a rollback attack.

EXAMPLE 2: If the currently installed software is v2.2 and v2.1 of the software is known to have an exploitable vulnerability, then reversion to v2.1 is considered to be a rollback attack.

Provision HG 5.3-2 (refined): The HG shall have an update mechanism for the secure installation of updates.

Provision HG 5.3-5 (refined): The HG should be configured by default to check after initialization, and then at least daily, whether updates are available.

NOTE 2: If the HG is ISP administered then **Provision HG 7.3-4 (added)** can also apply wherein the ISP pushes updates to the HG.

NOTE 3: It is assumed that the check for updates is configured at times with low service load.

Provision HG 5.3-6 (extended): If the HG is not an ISP-administrated device and supports the update functionality, then this functionality shall be enabled by default, configurable including its deactivation and its automation.

Provision HG 5.3-9 (promoted) a: The HG shall verify the authenticity and integrity of software updates.

NOTE 4: A time stamp can be added to the signature to allow the receiver to validate the freshness of the update after the authentication step.

NOTE 5: The authentication step thereby ensures that the signature preserving the integrity of the update stems from the allowed party of the supply chain and not from a threat agent.

Provision HG 5.3-9 (extended) b: The HG shall only install updates if the authentication and verification was successful.

NOTE 6: Authentication and verification, can be based on digital signatures. In the case of third-party software (**Provision HG 7.3-7 (added)**), it might not be possible in any case to check the trustworthiness of the origin.

Provision HG 5.3-11 (refined): The manufacturer should inform the local or remote administrator in a recognizable and apparent manner that an update is required together with information on the risks mitigated by that update.

NOTE 7: This notification can include the currently new available update version information, but does not necessarily need to name the older version information which is operated prior to the update.

Provision HG 5.3-14 (excluded): The provision is not applicable for HG and shall not apply.

Provision HG 5.3-15 (excluded): The provision is not applicable for HG and shall not apply.

Provision HG 5.3-16 (extended): Software version numbers shall only be retrievable by an administrator or an authenticated user on the LAN.

NOTE 8: The version information of the software can help an attacker.

NOTE 9: This provision is not applicable for users on guest Wi-Fi® or Community Wi-Fi®.

EXAMPLE 3: If the software release notes for any version includes information on vulnerabilities that have been fixed in the update an attacker can exploit those vulnerabilities in devices that have not been updated.

5.4 Securely store sensitive security parameters

An information to the provision from ETSI EN 303 645 [1], clause 5.4 is defined in the present document.

Provision HG 5.4-1 (information):

NOTE 1: See note in the ETSI EN 303 645 [1].

NOTE 2: Critical security parameters as defined by the ETSI EN 303 645 [1] is extended to the broader definition security critical data for the HG. These data include Wi-Fi®, user and administrator passwords, as well as access data to the ISP or similar infrastructures.

5.5 Communicate securely

Existing provisions from ETSI EN 303 645 [1], clause 5.5 are modified as follows.

NOTE 1: For the core purpose of the HG to maintain separation of LAN and WAN traffic, the provisions of clause 5.1 apply to ensure data from any connected device to the HG is protected.

Provision HG 5.5-1 (information):

NOTE 2: Best practice cryptography to communicate securely includes best practice cryptography for the Wi-Fi® encryption [i.4].

NOTE 3: The meaning of best practice cryptography is defined in ETSI EN 303 645 [1]. However, best practice is technology and time dependent and for that reason the manufacturer is expected to follow the guidance provided in the form of maintained cryptographic catalogues, for example by ENISA European certification schemes.

NOTE 4: WPA3™ is the most recent version (as of the date of publication of the present document), but will not be supported by some legacy or existing devices that try to connect to the HG. In such cases, WPA2-PSK hybrid mode or similar is an appropriate compromise between security and availability.

Provision HG 5.5-3 (information):

NOTE 5: Updatability of cryptographic algorithms and primitives depends on the algorithms and key sizes supported in the hardware and for relevant protocols.

Provision HG 5.5-4 (extended)-a: The HG should support TLS [i.8] for device management via a web-portal by the local administrator.

EXAMPLE 1: NMS device management services are enabled by a protocol such as the Customer-Premises Equipment (CPE) WAN Management Protocol [i.9].

Provision HG 5.5-4 (extended)-b: The HG should support TLS [i.8] with mutual authentication using a pre-installed device certificate for the Network Management System (NMS) and remote device management by the ISP-administrator.

Provision HG 5.5-5 (information): Accessibility includes both credentials managed by the ISP for connection to the ISP, and credentials managed on the home network for connections related to the home network side of the HG.

5.6 Minimize exposed attack surfaces

Existing provisions from ETSI EN 303 645 [1], clause 5.6 are modified as follows.

As a guide to the HG developer, the default configuration settings for the HG puts it into a condition where the best protection against the attacks outlined in ETSI TR 103 309 [i.5] is achieved, taking due note of the analysis provided in ETSI TR 103 743 [i.1]. It is best practice for the product designer to keep the security by default configuration as a principle in mind during product development.

Provision HG 5.6-1 (extended): The guest Wi-Fi® access, if present, shall be disabled by default.

NOTE 1: Only the ISP administrator will have the ability to enable or disable the community Wi-Fi®.

HGs between the ISP and user LAN are exposed to attacks at all times. For that reason, Provision EN 5.6-5 from ETSI EN 303 645 [1] is upgraded to a mandatory requirement.

Provision HG 5.6-5 (promoted): The manufacturer shall only enable software services that are used or required for the intended use or operation of the device.

Third party application and plug-ins are potential high-risk software which can incur attacks to the HG. Applying techniques for process isolation provides an isolated environment such as a closed container or a sandbox for operation. Operation in such closed compartments mitigates attacks originated from third party applications and plug ins.

Provision HG 5.6-7 (extended): If the HG supports installation of third-party applications and plug-ins, the HG should support a container or sandbox for third party applications and plug-in isolation.

NOTE 2: Not all HGs will support the installation of third-party applications and plug-ins, thus this provision only applies to relevant HGs.

Vulnerabilities of the HG can be a result of coding without security considerations or simply by implemented faults. Therefore, applying secure coding is an essential good practice for all R&D engineers to improve the security of the product code and decreasing potential vulnerabilities which could enable the undesired modification of the code. Additionally, secure coding practices habitually prohibit the implementation of hard-coded cryptographic keys which could enable disclosure of code and data and their modification from being abused.

Provision HG 5.6-9 (information) a: This provision is more detailed by following examples:

EXAMPLE 1: Secure compiling flags such as stack protection, Relocation Read-Only (RELRO), PIE, and Stack-Smashing-Protector techniques.

EXAMPLE 2: Memory protection features such as the use of Non-eXecutable (NX) memory and Kernel Address Space Layout Randomization (KASLR).

EXAMPLE 3: Secure variants of functions provided by the latest versions of programming languages. For example, the function gets() in C/C++ [i.11] can lead to a buffer overflow if the string being read is longer than the variable assigned, whereas the function fgets() is bounded to read a fixed length string.

Provision HG 5.6-9 (extended) b: The firmware should use best-practice programming techniques to mitigate tampering, fault and leakage attacks.

It is recognized that manufacturers can choose to develop their products on the basis of open source software. When this is the case the same provisions apply to open source software with respect to good programming practice. In particular where faults or vulnerabilities exist in the open source resource they are reported and fixed in the same manner as any other code development.

5.7 Ensure software integrity

Existing provisions from ETSI EN 303 645 [1], clause 5.7 are modified as follows.

Provision HG 5.7-1 (extended): The HG should not provide any command or API to disable the secure boot feature or to circumvent this feature and boot from other sources.

Provision HG 5.7-2 (extended): If any integrity verification fails during the secure booting the HG should reset and retry the secure booting using the firmware backup image. If secure boot using the firmware backup image fails, the HG should be disabled from further operation.

5.8 Ensure that personal data is secure

No modifications to the provisions from ETSI EN 303 645 [1], clause 5.8 are defined in the present document.

5.9 Make systems resilient to outages

Existing provisions from ETSI EN 303 645 [1], clause 5.9 are modified as follows.

Having firmware and log file backups mitigates against the consequences of a data integrity failure. In the event of a failure, the original data can be recovered from an uncorrupted copy stored on a different device.

Provision HG 5.9-2 (promoted)(refined): The HG shall remain operating and locally functional in the case of a loss of network access and shall automatically recover to the previous connectivity and configuration state without user action in the case of restoration of a loss of power.

The HG is exposed to the internet by design and can be under attack as described in ETSI TR 103 743 [i.1]. The following requirement extends Provision EN 5.9-3 from ETSI EN 303 645 [1] to address specific sources of functional outages that impact system resilience.

Provision HG 5.9-3 (extended): When the HG is overloaded, it should buffer unprocessed traffic management packets in order to maintain availability.

5.10 Examine system telemetry data

No modifications to the provisions from ETSI EN 303 645 [1], clause 5.10 are defined in the present document.

The timely examination of telemetry, including log data, is often useful for security evaluation and can allow problems (e.g. faults or attacks) to be identified early and dealt with, minimizing security risk and allowing mitigation of problems.

Whilst an HG can use telemetry data for some traffic management tasks, e.g. routing optimization, the present document focusses on the recording of security events.

Security event data include, but are not restricted to: log-in failures, firmware updates, and memory area accesses. As telemetry and security data are different, the event records are stored in discrete log files. The present document addresses the requirements for generating and maintaining security log data and the resulting security log file.

The additional provisions and a description of the log data are given in clause 7.10.

5.11 Make it easy for users to delete user data

No modifications to the provisions from ETSI EN 303 645 [1], clause 5.11 are defined in the present document.

5.12 Make installation and maintenance of devices easy

Existing provisions from ETSI EN 303 645 [1], clause 5.12 are modified as follows.

Provision HG 5.12-1 (extended): The HG should use secure interfaces for remote configuration during initial device setup.

EXAMPLE 1: Initial configuration by the ISP via Simple Network Management Protocol (SNMP).

EXAMPLE 2: Initial configuration by the administrator via a secure web-portal that is only accessible from the LAN.

5.13 Validate input data

No modifications to the provisions from ETSI EN 303 645 [1], clause 5.13 are defined in the present document.

6 Adapted data protection provisions for HGs

No modifications to the provisions from ETSI EN 303 645 [1], clause 6 are defined in the present document.

7 Additional cybersecurity provisions for HGs

7.1 No universal default passwords

Provision HG 7.1-1 (added): The supply chain should be designed in such a way that leakage of the HG specific credentials is prevented.

NOTE 1: Clause 7 of ETSI TR 103 743 [i.1] describes attacks across the supply chain.

EXAMPLE: A HG requires that Wi-Fi®, user and administrator passwords comply with a local password policy specifying a minimum length, or the inclusion of specific elements from the password alphabet (upper- and lower-case letters, numbers, symbols).

NOTE 2: For the purposes of testing some care is needed to ensure that credentials specific to the test environment are not used for normal operation.

7.2 Implement a means to manage reports of vulnerabilities

No additions to the provisions from ETSI EN 303 645 [1], clause 5.2 are defined in the present document.

7.3 Keep software updated

Provision HG 7.3-1 (added): The public verification key of the manufacturer or software provider shall be pre-installed on the HG.

EXAMPLE 1: The pre-installed public key for the integrity verification and validation of the SW update package is used.

Provision HG 7.3-2 (added): If the manufacturer deploys a software provider to host update packages, the HG should implement a mechanism for updating the software provider's public key.

Provision HG 7.3-3 (added): When using open source software, the HG should deploy Long-Term Support (LTS) versions of open source OS kernels and applications and make clear the lifetime of each LTS version.

NOTE 1: In some cases, the LTS lifetime cannot be controlled, or influenced, by any entity in the supply chain and it may be reasonable to identify a network resource that maintains the installed open source software.

Provision HG 7.3-4 (added): If the HG is an ISP administrated device, the updates shall be made available as required by the ISP-administrator and this facility shall be transparent to the served user.

Provision HG 7.3-5 (added): If the HG is not an ISP administrated device, the HG should at least once request user's consent during the first time the default configuration is changed, when doing the settings for updates.

NOTE 2: It is assumed the device starts up without further default configuration.

Provision HG 7.3-6 (added): If a HG explicitly supports third party SW installation, then it shall present a clear warning to the administrator and require consent from the administrator. By default, the installation of third-party software shall not be enabled in the configuration.

NOTE 3: The presence of such functionality can introduce additional security risks to the HG and is expected to be included only if explicitly required by the HG manufacturer.

Provision HG 7.3-7 (added): HG manufacturers and software providers shall sign update packages before releasing them to the public.

Provision HG 7.3-8 (added): If the HG software contains sensitive data, the HG manufacturer or software provider should use best-practice techniques to protect the confidentiality of updates.

NOTE 4: Best-practice techniques include using different keys for encryption and signing.

EXAMPLE 2: In common software development practice, code often includes indications of technical structure, items protected by intellectual property rights, and contains mechanisms to limit the viability of reverse engineering, all of which are considered as confidential data.

7.4 Securely store sensitive security parameters

Provision HG 7.4-1 (added): Access to the Wi-Fi® and local administrator credentials shall be restricted to the authenticated local administrator of the HG.

Provision HG 7.4-2 (added): Access to the ISP administrator credentials shall be restricted to the authenticated ISP administrator of the HG.

Provision HG 7.4-3 (added): Security critical data shall be managed independently of user data by the HG.

Provision HG 7.4-4 (added): The HG should include a Hardware-Based Root of Trust (HBRT).

Provision HG 7.4-5 (added): If the HG includes an HBRT it should support a Hardware Mediated Execution Enclave (HMEE).

Provision HG 7.4-6 (added): If enabled, data encryption and decryption using best practice cryptography should be active and confirmed from the HMEE.

NOTE 1: NVM encryption is not sufficient to protect the confidentiality of HG device software since an attacker can also retrieve the software from the HG manufacturer's download centre. This means that the HG manufacturer needs to apply a comparable level of protection to the software.

Provision HG 7.4-7 (added): If the HG does not deploy encryption and decryption of the volatile memory then it should support memory scrambling to protect data during run time.

Provision HG 7.4-8 (added): If the HG includes an HBRT it should support random number generation for cryptographic operations.

EXAMPLE 1: The random number generator is used for key generation, signature generation and in challenge-response protocols and is often termed a random bit generator but for the present document the term random number generator is used.

Provision HG 7.4-9 (added): If supported the random number generator shall provide random bits with an appropriate entropy in compliance to publicly available standard quality metrics.

EXAMPLE 2: A widely accepted quality metric can be found in NIST SP 800-90B [i.3], ETSI TS 119 312 [i.12] and in other national guidance.

Provision HG 7.4-10 (added): The HG should support hierarchical symmetric key management where each hierarchy level uses different keys.

NOTE 2: The role of a symmetric key hierarchy is to protect the root key by ensuring that it is not directly used in cryptographic process. Instead, these processes use symmetric keys that have been derived from the root key.

EXAMPLE 3: In devices using an HSM the use of a protected hierarchical key management system can allow the derived keys (i.e. those derived from the root key) to perform encryption and decryption operations outside of the HSM, with the HSM only decrypting data keys, the most sensitive, root, keys stay protected in the HSM.

Provision HG 7.4-11 (added): If the root key of a symmetric key hierarchy is not provisioned on a secure module or HSM, then this key should be generated within the HG and be unique per HG.

Provision HG 7.4-12 (added): Access to system files should be based on authorization which means proper assignment of rights to read, write and execute these files.

7.5 Communicate securely

Provision HG 7.5-1 (added): The HG should support VPN for tunnelling data during transport.

EXAMPLE 1: A secure data transfer is realized by sending data via an established VPN tunnel.

Provision HG 7.5-2 (added): Each user should be authenticated by the HG and then assigned access rights according to their specific role.

EXAMPLE 2: Relevant roles for the HG are administrator, user, guest user, and community user.

NOTE 1: Secure authentication provides verification of a user's identity. Authorization assigns resource access rights to an authenticated user. These access rights can be based on the user's role; for example, as an administrator. Assigning role-based access rights mitigates the risk of privilege escalation attacks.

Provision HG 7.5-3 (added): The HG should support IPv4 and IPv6 packet filtering based on source and destination IP/port.

Provision HG 7.5-4 (added): Firewall techniques should be used to protect the HG from network attacks by blocking malicious packets.

Provision HG 7.5-5 (added): If a firewall is used the HG should provide ease of use for the firewall configuration with options to support all kind of users, from the IT-professional to the layman.

NOTE 2: Ease of use means that the firewall enables the user to decide which type of detail they use for configuration. It is assumed that the manufacturer's default configuration of the firewall protects the device for the case a layman is the user, meaning that all other connection possibilities and ports are blocked except the communication channel to the current layman user.

Provision HG 7.5-6 (added): If a firewall is used the default setting of the firewall configuration shall provide the most restrictive configuration to protect the layman user.

Provision HG 7.5-7 (added): If a firewall is used the firewall implemented by the HG shall not contain any port forwarding rules in the factory default state.

Provision HG 7.5-8 (added): The HG should support the use of an Access Control List (ACL) to block packets with rules based on destination and source MAC address, IP address and ports.

Provision HG 7.5-9 (added): The HG should detect and mitigate Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks using best practice techniques.

EXAMPLE 3: Annex D of ETSI TS 102 165-1 [i.7] addresses DoS/DDoS attacks in general and identifies a number of mitigation strategies.

EXAMPLE 4: ETSI TR 103 305-2 [i.6] describes approaches to recording detected DoS/DDoS events in security logs.

EXAMPLE 5: Clause D.3.4 of ETSI TS 102 165-1 [i.7] and ETSI TR 103 309 [i.5] describe measures to share knowledge of DoS/DDoS attacks with defined authorities.

NOTE 3: If the HG is supplied by the ISP, the ISP is considered responsible for identifying the entity with whom details of the attack are shared. If, however, the HG is directly supplied to the consumer by a retail outlet of the manufacturer, then the manufacturer is considered responsible for identifying the entity with whom details of the attack are shared.

Provision HG 7.5-10 (added): The HG should authenticate NMS or NTP servers prior to communication, if these are used.

Provision HG 7.5-11 (added): The HG should mitigate time-based attacks using best practice techniques.

EXAMPLE 6: Timing exploits can threaten signature and certificate verification, and allow replay attacks depending on the application. The use of NTPv4 [i.10] prevents attacks that exploit network timing.

7.6 Minimize exposed attack surfaces

Provision HG 7.6-1 (added): Any physical interfaces for debugging purpose during development shall be permanently disabled (or physically removed) from devices before delivery.

EXAMPLE 1: Debug and test physical interfaces include UART, JTAG, etc. Disable JTAG by blowing an on-chip eFuse.

Provision HG 7.6-2 (added): Any software test and debug access points during development shall be disabled, locked or removed before delivery.

EXAMPLE 2: In development of software, it is common practice to enable breakpoints or terminal access points (e.g. SSH) that allow a developer to step through the code and this kind of coding facility is removed.

Provision HG 7.6-3 (added): Where the HG supports and has enabled a guest Wi-Fi® channel and/or a community Wi-Fi® channel, each of the according Wi-Fi® account types shall be cryptographically isolated from each other.

Provision HG 7.6-4 (added): If guest Wi-Fi® or community Wi-Fi® is supported, it shall be infeasible for a guest or community user to access any asset available only to normal users.

Provision HG 7.6-5 (added): The local administrator should be able to restrict the access to assets on the local network via any access link.

EXAMPLE 3: The local administrator restricts a guest user's access to assets on the guest Wi-Fi®.

Provision HG 7.6-6 (added): If the HG supports simple and secure Wi-Fi® connection initialization without passwords, it should be possible for it to be disabled by the local administrator.

EXAMPLE 4: Wi-Fi Easy Connect™ [i.2] is an example of Wi-Fi® connection without password.

Provision HG 7.6-7 (added): If the HG supports simple and secure Wi-Fi® connection initialization with passwords, this should be disabled by default and only be enabled by a local administrator.

Provision HG 7.6-8 (added): The HG should support access control for the Wi-Fi® and guest Wi-Fi®, if present, based on device MAC addresses.

NOTE 1: The local administrator will not be able to control individual user access to the community Wi-Fi®. Only the ISP administrator will have the ability to enable or disable the community Wi-Fi®.

Provision HG 7.6-9 (added): If the HG supports access control for the Wi-Fi® and guest Wi-Fi®, the access control lists shall be managed by the local or remote ISP administrator.

NOTE 2: Different lists can be managed by local or by the ISP administrators.

7.7 Ensure software integrity

Provision HG 7.7-1 (added): The HG should support file integrity check feature to detect file tampering.

Provision HG 7.7-2 (added): The HG should support firmware backup to the NVM.

NOTE: The firmware is executable code and does not contain personal or other user specific data as the firmware is the same on any equal HGs.

7.8 Ensure that personal data is secure

No additions to the provisions from ETSI EN 303 645 [1], clause 5.8 are defined in the present document.

7.9 Make system resilient to outages

No additions to the provisions from ETSI EN 303 645 [1], clause 5.9 are defined in the present document.

7.10 Collecting log data

Security logs record the time and relevant data associated to system security events. To fulfil its purpose, the stored security log file contains security event data sufficient to identify the condition of the HG at the time of the event. Such data can include the IP addresses and ports of the triggering event (source and destination), the time of the event, and the HG state at the time of the event.

Any party having access to security log files need to be aware they can contain personal data and require appropriate handling.

As security log files can help to identify the attacker or the attack path, these files are themselves a target for attackers, as tampering the log files can enable to hide the attack path, camouflage attacker's identity (IP address), wrongly assign a security log entry to a victim, or even hide that there was an attack taking place. The latter could allow for undiscovered recurring revisiting and further attack path development in the worst case.

Provision HG 7.10-1 (added): The HG should record operations involving passwords, keys, access credentials and firewall settings as well as authentication failures and similar security events in a system security log.

NOTE 1: The HG needs to avoid putting passwords, keys, and access credentials in the security log files.

NOTE 2: If a single security log file is used, it is important to label entries therein in such a way that specific types of events can be easily filtered out (these are then identifiable as security logs). Similar is expected for other events such as Wi-Fi® errors or device connection events.

Provision HG 7.10-2 (added): Security logs should be backed-up to the log server regularly, and in a configurable way with respect to amount and time frame.

EXAMPLE 1: The configuration is based on the ability to trace back to the root cause of an attack, identify the adversary or even that an attack took place.

Provision HG 7.10-3 (added): Security logs should be stored encrypted with authorization-based access control. Only the administrator should be able to access, and then only for reading and copying.

Provision HG 7.10-4 (added): Security log data which could be directly identified or interpreted as personal data should be kept to the minimum necessary for the intended functionality.

Provision HG 7.10-5 (added): Security logs related to individual users should be anonymized.

EXAMPLE 2: IP address, user name and password are examples for data needing to be anonymized or generalized in the log.

Provision HG 7.10-6 (added): Security logs related to administrative operations and unsolicited incoming connections from the internet side of the HG should be kept for analysis.

7.11 Make it easy for users to delete user data

No additions to the provisions from ETSI EN 303 645 [1], clause 5.11 are defined in the present document.

7.12 Make installation and maintenance of devices easy

Provision HG 7.12-1 (added): Telnet shall be disabled by default.

7.13 Validate input data

No additions to the provisions from ETSI EN 303 645 [1], clause 5.13 are defined in the present document.

Annex A (informative): Basic concepts and models

The models from ETSI EN 303 645 [1] apply.

The threat analysis specific to HG is addressed in ETSI TR 103 743 [i.1].

Annex B (informative): Implementation conformance statement pro forma

Table B.1 of the present document is extended from that of ETSI EN 303 645 [1] by the addition of the requirements specified in the present document for the HG.

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

Table B.1 can provide a mechanism for the user of the present document (who is expected to be an entity involved in the development or manufacturing of the HG) 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 1: Where the conditional notation is used, this is conditional on the text of the provision. The conditions are provided at the bottom of the table with references provided for the relevant provisions to help with clarity.

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.

NOTE 2: In table B.1, provisions highlighted in yellow are taken without alteration from ETSI EN 303 645 [1] and a conforming HG has to conform to that provision, provisions highlighted in orange are taken from ETSI EN 303 645 [1] and extended (i.e. a conforming HG implementation has to conform to both the provisions from the EN and to the extensions from the present document).

Table B.1: Implementation of provisions for HG security

Clause number and title			
Reference	**Status**	**Support**	**Detail**
4.1 Reporting implementation			
HG 4.1 (extended)	M		
5.1 No universal default passwords			
Provision 5.1-1	M C		Extended by HG 5.1-1 as below
HG 5.1-1 (extended)	M C		
Provision 5.1-2	M C		
Provision 5.1-3	M C		
Provision 5.1-4	M C		Extended by HG 5.1-4a/b/c as below
HG 5.1-4 (extended) a	M		
HG 5.1-4 (extended) b	M		
HG 5.1-4 (extended) c	M		
HG 5.1-5 (refined)	M		
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M		HG 5.2-1 (information) clarifies this for the HG
Provision 5.2-2	R		HG 5.2-2 (information) clarifies this for the HG
Provision 5.2-3	R		
5.3 Keep software updated			
Provision 5.3-1	R		Extended by HG 5.3-1a/b as below
HG 5.3-1 (extended) a	M C (1)		
HG 5.3-1 (extended) b	M (1)		
HG 5.3-2 (refined)	M (1)		
Provision 5.3-3	M C		
Provision 5.3-4	R C		
HG 5.3-5 (refined)	R (1)		
Provision 5.3-6	R C		Extended by HG 5.3-6 as below
HG 5.3-6 (extended)	M C (1)		
Provision 5.3-7	M C		
Provision 5.3-8	M C		
HG 5.3-9 (promoted) a	M (1)		
HG 5.3-9 (extended) b	M C (1)		
Provision 5.3-10	M		
HG 5.3-11 (refined)	R (1)		
Provision 5.3-12	R C		
Provision 5.3-13	M		
HG 5.3-14 (excluded)	Not applicable		
HG 5.3-15 (excluded)	Not applicable		
Provision 5.3-16	M		Extended by HG 5.3-16 as below
HG 5.3-16 (extended)	M		
5.4 Securely store sensitive security parameters			
Provision 5.4-1	M		HG 5.4-1 (information) clarifies this for the HG
Provision 5.4-2	M C		
Provision 5.4-3	M		
Provision 5.4-4	M		
5.5 Communicate securely			
Provision 5.5-1	M		HG 5.5-1 (information) clarifies this for the HG
Provision 5.5-2	R		
Provision 5.5-3	R		HG 5.5-3 (information) clarifies this for the HG
Provision 5.5-4	R		Extended by HG 5.5-4a/b as below
HG 5.5-4 (extended) a	R		
HG 5.5-4 (extended) b	R		
Provision 5.5-5	M		HG 5.5-5 (information) clarifies this for the HG
Provision 5.5-6	R		
Provision 5.5-7	M		
Provision 5.5-8	M		
5.6 Minimize exposed attack surfaces			
Provision 5.6-1	M		
HG 5.6-1 (extended)	M C (3)		
Provision 5.6-2	R		
Provision 5.6-3	R		
Provision 5.6-4	R		
HG 5.6-5 (promoted)	M		

Clause number and title			
Reference	**Status**	**Support**	**Detail**
Provision 5.6-6	R		
Provision 5.6-7	R		Extended by HG 5.6-7 as below
HG 5.6-7 (extended)	R C		
Provision 5.6-8	R		
Provision 5.6-9	R		HG 5.5-5 (information) clarifies this for the HG
HG 5.6-9 (extended) b	R		
5.7 Ensure software integrity			
Provision 5.7-1	R		Extended by HG 5.7-1 as below
HG 5.7-1 (extended)	R		
Provision 5.7-2	R		Extended by HG 5.7-2 as below
HG 5.7-2 (extended)	R		
5.8 Ensure that personal data is secure			
Provision 5.8-1	R		
Provision 5.8-2	M		
Provision 5.8-3	M		
5.9 Make systems resilient to outages			
Provision 5.9-1	R		
HG 5.9-2 (promoted)(refined)	M C (5)		
Provision 5.9-3	R		Extended by HG 5.9-3 as below
HG 5.9-3 (extended)	R C (5)		
5.10 Examine system telemetry data			
Provision 5.10-1	R C		
5.11 Make it easy for users to delete user data			
Provision 5.11-1	M		
Provision 5.11-2	R		
Provision 5.11-3	R		
Provision 5.11-4	R		
5.12 Make installation and maintenance of devices easy			
Provision 5.12-1	R		Extended by HG 5.12-1 as below
HG 5.12-1 (extended)	R		
Provision 5.12-2	R		
Provision 5.12-3	R		
5.13 Validate input data			
Provision 5.13-1	M		
6 Adapted Data protection provisions for the HGs			
Provision 6.1	M		
Provision 6.2	M C		
Provision 6.3	M		
Provision 6.4	R C		
Provision 6.5	M C		
7.1 No universal default passwords			
HG 7.1-1 (added)	R		
7.2 Implement a means to manage reports of vulnerabilities			
7.3 Keep software updated			
HG 7.3-1 (added)	M		
HG 7.3-2 (added)	R C		
HG 7.3-3 (added)	R C (4)		
HG 7.3-4 (added)	M		
HG 7.3-5 (added)	R C		
HG 7.3-6 (added)	M C		
HG 7.3-7 (added)	M		
HG 7.3-8 (added)	M C		
7.4 Securely store sensitive security parameters			
HG 7.4-1 (added)	M		
HG 7.4-2 (added)	M		
HG 7.4-3 (added)	M		
HG 7.4-4 (added)	R		
HG 7.4-5 (added)	R C		
HG 7.4-6 (added)	R C		
HG 7.4-7 (added)	R C		
HG 7.4-8 (added)	R		
HG 7.4-9 (added)	M		
HG 7.4-10 (added)	R		

Clause number and title			
Reference	**Status**	**Support**	**Detail**
HG 7.4-11 (added)	R C		
HG 7.4-12 (added)	R		
7.5 Communicate securely			
HG 7.5-1 (added)	R		
HG 7.5-2 (added)	R		
HG 7.5-3 (added)	R		
HG 7.5-4 (added)	R		
HG 7.5-5 (added)	R C		
HG 7.5-6 (added)	M C		
HG 7.5-7 (added)	M C		
HG 7.5-8 (added)	R		
HG 7.5-9 (added)	R		
HG 7.5-10 (added)	R		
HG 7.5-11 (added)	R		
7.6 Minimize exposed attack surfaces			
HG 7.6-1 (added)	M		
HG 7.6-2 (added)	M		
HG 7.6-3 (added)	M C (3)		
HG 7.6-4 (added)	M C (3)		
HG 7.6-5 (added)	R (4)		
HG 7.6-6 (added)	R C		
HG 7.6-7 (added)	R C		
HG 7.6-8 (added)	R		
HG 7.6-9 (added)	M C		
7.7 Ensure software integrity			
HG 7.7-1 (added)	R		
HG 7.7-2 (added)	R		
7.8 Ensure that personal data is secure			
7.9 Make system resilient to outages			
7.10 Collecting log data			
HG 7.10-1 (added)	R		
HG 7.10-2 (added)	R		
HG 7.10-3 (added)	R		
HG 7.10-4 (added)	R		
HG 7.10-5 (added)	R		
HG 7.10-6 (added)	R		
7.11 Make it easy for users to delete user data			
7.12 Make installation and maintenance of devices easy			
HG 7.12-1 (added)	M		
7.13 Validate input data			
Conditions: 1) An update mechanism is implemented. 2) Open source software or 3rd party software is used. 3) A guest or community Wi-Fi® channel is enabled. 4) The programming language contains unsecure functions that have been superseded by secure counterparts. 5) The HG device fails in its function due to power loss or similar failure.			

History

Document history		
V1.1.1	March 2022	Publication