ETSI TS 103 927 V1.1.1 (2024-01)

CYBER;
Cyber Security for Consumer Internet of Things;
Requirements for Smart Voice-controlled Device

Reference
DTS/CYBER-0095

Keywords
cyber security, IoT, privacy, smart voice-controlled device

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 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Symbols 7
3.3 Abbreviations 7
4 Methodology and general requirements 7
4.1 Introduction 7
4.2 Handling of provisions 7
4.3 Naming conventions 8
5 Adapted cyber security provisions for Smart Voice-controlled Device 9
5.0 Reporting implementation 9
5.1 No universal default passwords 9
5.2 Implement a means to manage reports of vulnerabilities 9
5.3 Keep software updated 9
5.4 Securely store sensitive security parameter 10
5.5 Communicate securely 10
5.6 Minimize exposed attack surfaces 10
5.7 Ensure software integrity 10
5.8 Ensure that personal data is secure 10
5.9 Make systems resilient to outages 11
5.10 Examine system telemetry data 11
5.11 Make it easy for users to delete user data 11
5.12 Make installation and maintenance of devices easy 11
5.13 Validate input data 11
6 Adapted data protection provisions for Smart Voice-controlled Device 11
7 Additional cyber security provisions for Smart Voice-controlled Device 11
7.1 No universal default passwords 11
7.2 Implement a means to manage reports of vulnerabilities 12
7.3 Keep software updated 12
7.4 Securely store sensitive security parameters 12
7.5 Communicate securely 12
7.6 Minimize exposed attack surfaces 12
7.7 Ensure software integrity 12
7.8 Ensure that personal data is secure 12
7.9 Make systems resilient to outages 13
7.10 Collecting log data 13
7.11 Make it easy for users to delete user data 13
7.12 Make installation and maintenance of devices easy 13
7.13 Validate input data 13
8 Additional data protection provisions for Smart Voice-controlled Device 13
Annex A (informative): Basic concepts, threat models, risk analysis 15
Annex B (informative): Implementation conformance statement pro forma 16
Annex C (informative): Non-cyber security aspects for Smart Voice-controlled Device 20

Annex D (informative): A typical architecture of a smart home system with SVD.....21
History 22

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 Smart Voice-controlled Device extending from the provisions for consumer IoT devices defined in ETSI TS 103 645 [1].

In terms of security concerns, SVD has a different focus than other generic IoT devices (e.g. distributed sensors, smart appliances, etc.). For example, SVD mainly interacts with users through voice assistants that can understand users' voice commands and assist users to control other devices in the IoT network. This feature actually expands the attack surface of SVD. In addition, SVD usually collects the user's voice and trains a model uniquely suitable for the current user to provide personalized service. Therefore, SVD-related privacy protection issues are particularly prominent. This vertical will focus on addressing the unique security issues of SVD.

Annex D gives an architectural diagram of a typical smart home system containing SVD to allow readers of the present document to better understand the position and purpose of SVD in a home network environment.

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 TS 103 645 (V3.1.1): "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.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 645 [1] and the following apply:

pairing: act of authentication, authorization and exchange of specific information between devices/machines and/or applications running on a device/machine resulting in a long-term trust relationship

NOTE: Pairing often involves the association of this relationship with the user's account.

Smart Voice-controlled Device (SVD): consumer IoT device with integrated voice-controlled virtual assistant logic that responds to prompts and commands from users

NOTE 1: SVD in the present document do not include SVD for industrial purposes and in-vehicle system integrated voice-controlled assistants.

NOTE 2: These devices in some cases can play music, answer questions, control smart home devices, make phone calls, and perform other tasks based on voice commands.

NOTE 3: Integrated voice-controlled virtual assistant logic can make use of associated services to interpret voice records.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 645 [1] and the following apply:

NVD	National Vulnerability Database
OTA	Over-The-Air
SVD	Smart Voice-controlled Device
SSL	Secure Sockets Layer
TLS	Transport Layer Security

4 Methodology and general requirements

4.1 Introduction

Like many Internet of Things (IoT) devices, Smart Voice-controlled Device rely on internet connectivity and may be connected to other devices within a Local Area Network (LAN), which makes them susceptible to various security risks and attacks. The voice commands processed by SVD often entail the use of personal data, such as the user's location and contacts, which further reinforces the importance of securing such devices. Additionally, the voice processing capability of SVD makes them vulnerable to eavesdropping and unauthorized access. Thus, ETSI TS 103 645 [1] serves as the security baseline, on which security requirements are promoted, refined, extended, and added to ensure the security of SVD and prevent potential security threats.

4.2 Handling of provisions

The present document adopts the provisions of ETSI TS 103 645 [1] as a baseline for the Smart Voice-controlled Device. The methodology used for the adoption is described in the present clause, which includes different operations to modify provisions from ETSI TS 103 645 [1] and add new provisions specific to Smart Voice-controlled Device.

All provisions from ETSI TS 103 645 [1] shall apply in the present document, unchanged, to the Smart Voice-controlled Device, unless otherwise noted in the present document.

Consumer IoT devices in the vertical domain of a SVD are not constrained devices. Consequently, all provisions from ETSI TS 103 645 [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 TS 103 645 [1]:

- **Information:** Providing additional information (in the form of informative text) to an unmodified provision. The original provision in ETSI TS 103 645 [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 TS 103 645 [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 TS 103 645 [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 TS 103 645 [1] is still valid.

- **Substitution:** Replacing a recommendation that is not applicable for the Smart Voice-controlled Device 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 TS 103 645 [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 Smart Voice-controlled Device. The original provision in ETSI TS 103 645 [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 TS 103 645 [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 Smart Voice-controlled Device that cannot be linked to any provision in ETSI TS 103 645 [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 Smart Voice-controlled Device. The acronym for the Smart Voice-controlled Device is set to SVD.

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 "SVD" 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 TS 103 645 [1] additional informative information is provided for. The suffix is "(information)".

- **Promotion:** The id is the id of the original provision in ETSI TS 103 645 [1] that is promoted. The suffix is "(promoted)".

- **Refinement:** The id is the id of the original provision in ETSI TS 103 645 [1] that is refined. The suffix is "(refined)".

- **Extension:** The id is the id of the original provision in ETSI TS 103 645 [1] that is extended. The suffix is "(extended)".
- **Substitution:** The id is the id of the original provision in ETSI TS 103 645 [1] that is substituted. The suffix is "(substituted)".
- **Exclusion:** The id is the id of the original provision in ETSI TS 103 645 [1] that is excluded. The suffix is "(excluded)".
- **Addition:** The id is a new and unique id added in clause 7 or 8 that reflects the clause in which it is defined. The suffix is "(added)".

5 Adapted cyber security provisions for Smart Voice-controlled Device

5.0 Reporting implementation

Provision SVD 5.0-1 (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.

5.1 No universal default passwords

Existing provisions from ETSI TS 103 645 [1], clause 5.1 are modified as follows.

Provision SVD 5.1-1, Provision SVD 5.1-2 (information):

NOTE: Credentials that are commonly used by SVD for initial pairing, such as pairing codes and QR codes, are also be considered as "passwords" in these provisions. Best practice is to ensure that credentials for pairing are either unique per device or dynamically generated, to reduce the probability of random guessing.

Provision SVD 5.1-5 (refined): The SVD 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

No modifications to the provisions from ETSI TS 103 645 [1], clause 5.2 are defined in the present document.

5.3 Keep software updated

Existing provisions from ETSI TS 103 645 [1], clause 5.3 are modified as follows:

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

Provision SVD 5.3-4A (promoted): One secure update mechanism shall be configurable to be automated.

Provision SVD 5.3-7 (extended): If the SVD is updated OTA, a secure channel where the communication partner is authenticated via a trusted certificate should be used to transmit the update.

EXAMPLE 1: A secure channel might be the latest version of TLS/SSL tunnel.

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

Provision SVD 5.3-11 (information):

NOTE: Given the limited user interface of some SVD devices, details such as information on risks mitigated by the update may be provided to users separately.

EXAMPLE 2: For SVD without a screen, the paired phone/APP can be used to notify the user about security updates, to obtain user consent, and to display update-related information.

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

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

5.4 Securely store sensitive security parameter

Provision SVD 5.4-1 (information):

NOTE 1: Possible sensitive security parameters in SVD include but are not limited to: cryptographic parameters used for initialization or pairing, such as pre-installed certificates in the device or immutable unique identity of the device or unique symmetric/asymmetric root keys of the device; encryption keys used to transmit user commands or user voice or other data

Provision SVD 5.4-2 (information):

NOTE 2: If the SVD uses a hard-coded device unique identity, tampering protection can be implemented by one of the following methods:

a) store the identity in a secure element;

b) write the identity in chip fuse;

c) use software methods to protect the identity, such as integrity checking, white-box cryptography, obfuscation, etc.

5.5 Communicate securely

Provision SVD 5.5-4 (promoted): Access to device functionality via a network interface in the initialized state shall only be possible after authentication on that interface.

Provision SVD 5.5-5 (information):

NOTE: The pairing of new devices or apps is such a security-relevant change.

5.6 Minimize exposed attack surfaces

Provision SVD 5.6-1 (information):

NOTE: Some SVDs provide network and/or logical interfaces to transport voice commands e.g. via external microphones.

Provision SVD 5.6-4B (refined): Debug interfaces that are physical ports shall be physically disabled.

Provision SVD 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.

5.7 Ensure software integrity

No modifications to the provisions from ETSI TS 103 645 [1], clause 5.7 are defined in the present document.

5.8 Ensure that personal data is secure

No modifications to the provisions from ETSI TS 103 645 [1], clause 5.8 are defined in the present document.