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

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.

5.9 Make systems resilient to outages

No modifications to the provisions from ETSI TS 103 645 [1], clause 5.9 are defined in the present document.

5.10 Examine system telemetry data

No modifications to the provisions from ETSI TS 103 645 [1], clause 5.10 are defined in the present document.

5.11 Make it easy for users to delete user data

Provision SVD 5.11-1 (information):

EXAMPLE: The SVD asks the user for permission to request the removal of user data including user account data from connected devices or associated services when unpairing or logging out is initiated.

Provision SVD 5.11-2 (extended): The user shall be provided with a functionality such that the erasure of user data from connected devices and associated services can be requested in a simple manner.

5.12 Make installation and maintenance of devices easy

Provision SVD 5.12-1(information):

NOTE: For SVDs, methods such as scanning QR codes, scanning dynamic graphics, inputting device identities, and NFC transactions can be provided to allow users to complete initialization with a minimum of steps.

5.13 Validate input data

No modifications to the provisions from ETSI TS 103 645 [1], clause 5.13 are defined in the present document.

6 Adapted data protection provisions for Smart Voice-controlled Device

Existing provisions from ETSI TS 103 645 [1], clause 6 are modified as follows:

Provision SVD 6-1 (information):

NOTE: It should be noted that the most common personal data collected by SVDs is the user's voice. Manufacturers should inform users in the privacy policies under what circumstances the user's voices will be collected, how and for what purpose and by whom their voices will be processed.

Provision SVD 6-4 (extended): If SVD collects log data remotely, the logs shall not contain any data pointed to the user as a natural person.

7 Additional cyber security provisions for Smart Voice-controlled Device

7.1 No universal default passwords

Provision SVD 7.1-1 (added): SVDs shall not use passwords or simple pairing codes for initial pairing.

7.2 Implement a means to manage reports of vulnerabilities

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

7.3 Keep software updated

Provision SVD 7.3-1 (added): Manufacturers of SVDs should package and release functional updates and security updates separately.

NOTE 1: This recommendation supports consumers in choosing specific feature versions according to their preferences while still enjoy the latest security fixes.

Provision SVD 7.3-2 (added): At the time the SVD is placed on the market, the operating system and pre-installed software of the SVD shall not contain unmitigated vulnerabilities that were disclosed by CVE or NVD more than 6 months ago.

NOTE 2: Providing an update that removes the vulnerabilities is a mitigation.

7.4 Securely store sensitive security parameters

No additions to the provisions from ETSI TS 103 645 [1], clause 5.4 are defined in the present document.

7.5 Communicate securely

Provision SVD 7.5-1 (added): The SVD should close unused communication sessions in a timely manner.

NOTE: Keep alive signals indicate that communication sessions are still used.

Provision SVD 7.5-2 (added): SVD should keep the number of connected devices to a minimum necessary for the intended operation.

7.6 Minimize exposed attack surfaces

Provision SVD 7.6-1 (added): In the initialized state, the SVD should use packet filtering to discard and potentially log inappropriate packages on network layer.

NOTE: Typically, inappropriate network packages make use of unused or inappropriate network addresses such as unused ports or unsuitable IP addresses.

Provision SVD 7.6-2 (added): Access over static network ports should be subject to access control.

Provision SVD 7.6-3 (added): If the user wants to install custom apps using another source than the manufacturer's app store, the user shall be informed before the installation about the risks and consequences of such installation and explicitly confirm the installation.

7.7 Ensure software integrity

Provision SVD 7.7-1 (added): If the SVD uses a root key to protect the integrity of code running on the device, the root key should not be shared between different models.

7.8 Ensure that personal data is secure

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

7.9 Make systems resilient to outages

Provision SVD 7.9-1 (added): If the SVD cannot execute the user's voice command due to a network connection failure within a brief period it shall inform the user in an explicit manner.

Provision SVD 7.9-2 (added): After a user-perceivable network failure, when the network connection is restored, the SVD shall not silently send the previously unsent user command to the target device.

7.10 Collecting log data

No additions to the provisions from ETSI TS 103 645 [1], clause 5.10 are defined in the present document.

7.11 Make it easy for users to delete user data

No additions to the provisions from ETSI TS 103 645 [1], clause 5.11 are defined in the present document.

7.12 Make installation and maintenance of devices easy

No additions to the provisions from ETSI TS 103 645 [1], clause 5.12 are defined in the present document.

7.13 Validate input data

Provision SVD 7.13-1 (added): The SVD shall validate the voice input to filter out hidden voice commands and only respond to the human voice input.

NOTE: Hidden voice commands are voice commands that are unintelligible to human users but are interpreted as commands by the device. Such voice commands may be either outside the range of human hearing, or within the range of human hearing but are obscured by noise and so become unintelligible. In particular, in the context of white-box attacks, the hidden voice command may be a specially created input for adversarial machine learning, which greatly increases the probability of successful attack.

Provision SVD 7.13-2 (added): The user should be able to enable and disable the recognition of the user's voice (voiceprint). If the functionality is enabled, the device should be able to recognize the user's unique voice, thus preventing any undesired users from waking up and using the device.

8 Additional data protection provisions for Smart Voice-controlled Device

Provision SVD 8-1 (added): A SVD should provide a physical switch that enables the user to turn off the microphone such that that the SVD's logic is physically inhibited to access audio signals of the microphone.

Provision SVD 8-2 (added): A SVD shall provide a functionality, that enables the user to turn off the microphone such that the SVD's logic has no access to audio signals of the microphone.

NOTE 1: Such a functionality can be activated by a software setting or a physical button.

NOTE 2: An SVD that implements SVD 8-1 (added) is also conformant to SVD 8-2 (added).

Provision SVD 8-3 (added): If the SVD is able to process prompts or commands by the user locally, the SVD shall provide a functionality, that enables the user to deny communication of audio recordings to other devices and services while the SVD still offers services based on local processing.

Provision SVD 8-4 (added): The SVD shall not retain any user voice recordings and their derivatives locally or on an associated service operated in control of the device manufacturer without explicit user's consent.

NOTE 3: A user who intends to use "voice memos/notes" functionality have explicitly agreed to allow the SVD to retain voice recordings until the user deletes the voice recording.

NOTE 4: In the case where SVD collects users' voices to improve AI models, this provision applies. Both the user's voice and the intermediate produced during the training process are considered user data.

Provision SVD 8-5 (added): If the SVD is able to access personal information on a paired device, the SVD shall provide the user with the option to choose whether to allow the SVD to access personal information on the paired device.

NOTE 5: In this context personal information can be calendars, contacts, etc.

Provision SVD 8-6 (added): The SVD should provide services with minimal or no upload of user voice and user data.

Provision SVD 8-7 (added): The confidentiality of user data communicated between the SVD and associated service operated in control of the device manufacturer shall be protected, with cryptography appropriate to the properties of the technology and usage.

Provision SVD 8-8 (added): If SVD collects the user's voice or other personal information, it shall explicitly ask the user for consent.

Provision SVD 8-9 (added): If the user refuses to provide some personal data, SVD shall explain to the user which functions and services will be affected and therefore become unavailable, and continue to provide other unaffected functions and services.

EXAMPLE: During the process of initializing an SVD, if the user refuse to grant the SVD access to his/her location, the SVD is expected to continue to complete the initialization process and provide the user with all the functions that do not need location.

Provision SVD 8-10 (added): If the SVD collects user data for model improvement or other statistical purposes, differential privacy technology should be used to protect privacy of an individual user.

Annex A (informative): Basic concepts, threat models, risk analysis

The models from ETSI TS 103 645 [1] apply.

No dedicated threat analysis documentation has been produced for this classification of devices. In lieu of such documentation, the ETSI TS 103 645 [1] threat analysis may serve as a useful reference point. It should be noted, however, that this document's treatment of threats to SVDs is singularly comprehensive in that it also accounts for vulnerabilities arising from user voice processing.

Annex B (informative): Implementation conformance statement pro forma

Table B.1 of the present document is extended from that of ETSI TS 103 645 [1] by the addition of the requirements specified in the present document for the SVDs.

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 SVDs) 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.
C	The provision is conditional. If the condition is not satisfied, the provision can be marked as N/A in an implementation conformance statement.
F	This provision applies to a feature, capability or mechanism. The existence of the feature, capability or mechanism is not determined to be mandatory/recommended by the provision. If the feature, capability or mechanism does not exist, the provision can be marked as N/A in an implementation conformance statement.

NOTE 1: Where the Feature (F) notation is used, the provision applies to all instances of the feature. The feature, capability or mechanisms are identified by the lettered footnotes at the bottom of the table with references provided for the relevant provisions.

NOTE 2: Where the Conditional (C) notation is used, this is conditional on the text of the provision. The conditions are provided in the numbered footnotes 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.

Table B.1: Implementation of provisions for consumer IoT security (source: ETSI TS 103 645 [1])

Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.0 Reporting implementation			
Provision 5.0-1	M		
5.1 No universal default passwords			
Provision 5.1-1	M F (a)		
Provision 5.1-2	M F (b)		
Provision 5.1-2A	R		
Provision 5.1-3	M F (c)		
Provision 5.1-4	M F (d)		
Provision 5.1-5	M C F (14, e)		
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M		
Provision 5.2-2	R		
Provision 5.2-3	R		
5.3 Keep software updated			
Provision 5.3-1	R F (f)		
Provision 5.3-2	M C (15)		
Provision 5.3-3	M F (g)		
Provision 5.3-4A	R F (g)		
Provision 5.3-4B	R F (h)		
Provision 5.3-5	R F (g)		
Provision 5.3-6A	R F (h)		
Provision 5.3-6B	R F (i)		
Provision 5.3-7	M F (g)		
Provision 5.3-8	M C (12)		
Provision 5.3-9	R F (g)		
Provision 5.3-10	M F (j)		
Provision 5.3-11	R C (12)		
Provision 5.3-12	R C (12)		
Provision 5.3-13	M		
Provision 5.3-14	R C (3)		
Provision 5.3-15A	R C (3)		
Provision 5.3-15B	R C (3)		
Provision 5.3-16	M		
5.4 Securely store sensitive security parameters			
Provision 5.4-1	M F (k)		
Provision 5.4-2	M F (l)		
Provision 5.4-3	M		
Provision 5.4-4	M F (m)		
5.5 Communicate securely			
Provision 5.5-1	M		
Provision 5.5-2	R		
Provision 5.5-3	R		
Provision 5.5-4	R		
Provision 5.5-5	M F (n)		
Provision 5.5-6	R F (o)		
Provision 5.5-7	M F (o)		
Provision 5.5-8	M C (16)		
5.6 Minimize exposed attack surfaces			
Provision 5.6-1	M F (p)		
Provision 5.6-2	M		
Provision 5.6-3	R		
Provision 5.6-4A	M F (q)		
Provision 5.6-4B	R F (r)		
Provision 5.6-5	R		
Provision 5.6-6	R		
Provision 5.6-7	R		
Provision 5.6-8	R		
Provision 5.6-9	R		

Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.7 Ensure software integrity			
Provision 5.7-1	R		
Provision 5.7-2	R F (s)		
5.8 Ensure that personal data is secure			
Provision 5.8-1	R F (t)		
Provision 5.8-2	M F (u)		
Provision 5.8-3	M F (v)		
5.9 Make systems resilient to outages			
Provision 5.9-1	R		
Provision 5.9-2	R		
Provision 5.9-3	R		
5.10 Examine system telemetry data			
Provision 5.10-1	R F (w)		
5.11 Make it easy for users to delete user data			
Provision 5.11-1	M		
Provision 5.11-2	R F (x)		
Provision 5.11-3	R		
Provision 5.11-4	R		
5.12 Make installation and maintenance of devices easy			
Provision 5.12-1	R		
Provision 5.12-2	R		
Provision 5.12-3	R		
5.13 Validate input data			
Provision 5.13-1A	M		
Provision 5.13-1B	M		
6 Data protection provisions for consumer IoT			
Provision 6.1	M		
Provision 6.2	M F (y)		
Provision 6.3A	M F (y)		
Provision 6.3B	M F (y)		
Provision 6.4	R F (w)		
Provision 6.5	M F (w)		
Provision 6.6	M F (z)		
Provision 6.7	R F (aa)		
Provision 6.8	R F (z)		

Condition:

3) software components are not updateable;
12) an update mechanism is implemented;
14) the consumer IoT device has no resource constraint determined by the use case that prevents the implementation of an mechanism which makes successful brute-force attacks on authentication mechanisms via network interfaces impracticable;
15) the consumer IoT device has no resource constraint determined by the use case that prevents the implementation of an update mechanism;
16) existence of critical security parameters that relate to the consumer IoT device.

Feature, capability or mechanism that needs to be present for the corresponding provision to apply:

a) passwords can be used to authenticate users against the device or for machine-to-machine authentication;
b) pre-installed unique per device passwords can be used to authenticate users against the device or for machine-to-machine authentication;
c) cryptographic authentication mechanisms, including password based mechanisms, can be used to authenticate users against the consumer IoT device or for machine-to-machine authentication;
d) authentication mechanisms can be used to authenticate users against the consumer IoT device;
e) authentication mechanisms can be used for authenticating users or devices via network interfaces;
f) software components that are not immutable due to security reasons;
g) software components of the device can be updated;
h) automatic software updates are supported;
i) update notifications are provided when software updates are available;
j) software updates can be delivered over a network interface;
k) sensitive security parameters exist in persistent storage;
l) hard-coded unique per device identities are used in the consumer IoT device for security purposes;
m) critical security parameters are used for integrity or authenticity checks of software updates or for protection of communication with associated services;

Clause number and title			
Reference	**Status**	**Support**	**Detail**
n)	the consumer IoT device allows security-relevant changes in configuration via a network interface;		
o)	critical security parameters used by the device can be communicated outside of the device;		
p)	unused network or network accessible logical interfaces exist;		
q)	debug interfaces exist on the device;		
r)	debug interfaces that are physical ports exist on the device;		
s)	secure boot or other mechanism to detect unauthorized changes to IoT device software are supported by the device;		
t)	the consumer IoT device sends personal data to associated services;		
u)	the consumer IoT device sends sensitive personal data to associated services;		
v)	the consumer IoT device includes external sensing capabilities;		
w)	telemetry data can be collected from consumer IoT devices and products;		
x)	personal data can be stored by an associated service;		
y)	the consumer IoT device processes personal data on the basis of consumers' consent;		
z)	the consumer IoT device processes personal data;		
aa)	capabilities to collect data from consumer IoT devices or to processed data on the consumer IoT device, whose purpose is solely to compute an aggregate result.		

Annex C (informative): Non-cyber security aspects for Smart Voice-controlled Device

The previous text has meticulously examined the network security and data security elements of SVD and has provided comprehensive provisions accordingly. Nevertheless, it is worth noting that non-network security-related elements have a crucial impact on the secure functioning and service provision of SVD. As such, it is recommended to consider the following guidelines when designing and manufacturing an SVD:

Recommendation 1: The SVD should possess the ability to distinguish between "critical" and "non-critical" commands.

NOTE 1: Critical commands can be defined as orders that, if improperly used or abused, may result in significant consequences. For instance, executing home automation or shopping through voice commands.

Recommendation 2: The SVD should provide functionality to disable purchasing commands.

Recommendation 3: The SVD should provide feedback to the user when critical commands are executed.

NOTE 2: When critical security settings are modified or a purchase is made, SVD should notify users via email.

Recommendation 4: The SVD should be resistant to voice imitation attacks.

NOTE 3: Voice imitation attacks refer to the act of mimicking or impersonating someone's voice to gain access to their system or sensitive information. This attack can be done using various techniques such as speech synthesis, voice cloning, or deep learning algorithms to replicate the victim's voice. These attacks are becoming more sophisticated and harder to detect, and attackers can even use them to trick voice authentication systems used in banking, finance, and other industries. Multi-factor authentication is an effective protection method, but it is rarely used on SVDs. Simply using the enhanced speech recognition algorithm cannot effectively prevent well-crafted imitation speech segments, but it is still recommended that countermeasures be implemented within the algorithm in order to resist the majority of unsophisticated voice imitation attack attempts.

Recommendation 5: The wake-up word of SVD should be distinct from other common phrases or common words used in everyday conversation, so as to avoid accidental misuse / accidental waking up.

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

Figure D.1 gives a typical architecture of smart home system using Smart Voice-controlled Device. The Smart Voice-controlled Device in the figure is the target of the present document.

The SVD is typically connected to a home gateway in order to establish an internet connection, and is also situated on a LAN with other smart appliances that are connected to the same home gateway. The SVD device directly interacts with the user through a voice user interface to complete the functions requested by the user. When users need to control other smart appliances through SVD devices, the instructions may be issued through an IoT cloud, or may be directly transmitted to the smart home appliances through the LAN, depending on the service platform/control protocol used by the smart appliances.

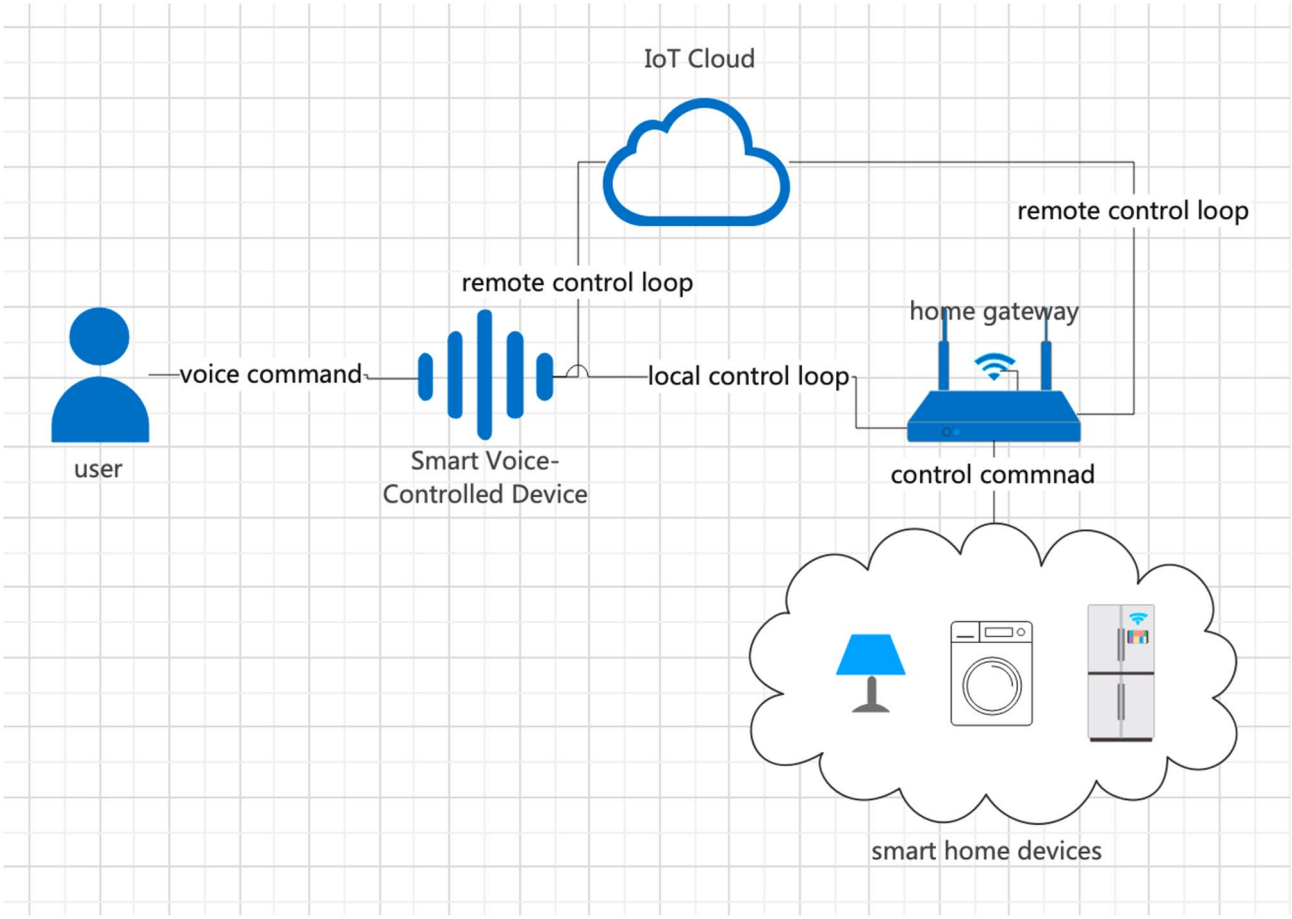

Figure D.1: A typical architecture of smart home system with SVD

History

Document history		
V1.1.1	January 2024	Publication