Smart Speaker / Voice Assistant Profile (SESIP)

Document number:	JSADEN015
Version:	0.93
Release Number:	01
Author:	PSA JSA Members: Applus+, S.L Arm Limited CAICT ECSEC Laboratory Inc Prove & Run S.A.S. Riscure B.V. SGS Brightsight B.V. TrustCB B.V. UL TS B.V.
Authorized by:	PSA JSA Members
Date of Issue:	30/05/2022

© Copyright Arm Limited 2017-2022. All rights reserved.

Licensed under the Creative Commons Attribution 4.0 International Licence

Abstract

Many connected devices are integrating voice based services where the consumer can use verbal commands to control functionality such as asking for music to be played or to turn on lights. This document is provided to OEMs and service providers as a reference Protection Profile (PP) that looks at the security problem for these devices including assets and threats to establish a baseline set of security requirements. The document has been written following the GlobalPlatform SESIP (Security Evaluation Standard for IoT Platforms) methodology and therefore could be used as the basis for a Security Target and lab based evaluation. It is provided under a permissive licence to encourage developers to adapt this threat model to their own security needs.

Innovative aspects of this PP include:
Mappings of security requirements to a chip's hardware Root of Trust e.g. a chip that has achieved PSA Certified Level 2
Encouraging Privacy by design by considering the privacy and confidentiality of voice recordings which have not triggered a "wake word"
Addressing the security needs of AI deployed in IoT edge devices
Writing the profile for use with the SESIP evaluation methodology
Compatibility with the high level security requirements of AVS

Keywords

Smart Speaker, Voice Assistant, AI, ML, Privacy, Platform Security Architecture, SESIP, Protection Profile, PSA Certified, AVS

License

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Copyright © 2022 Arm Limited (or its affiliates). All rights reserved.

Contents

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Release 01

1.2 Release Information

The change history table lists the changes that have been made to this document.

Date	Version	Confidentiality	Change
20/05/2022	0.92	Non-confidential	Additional SFR for authentication
16/02/2022	0.8	Non-confidential	Comments from Wouter
12/01/2022	0.7	Non-confidential	Generalize to voice assistants
14/12/2021	0.6	Non-confidential	Fix typos
08/12/2021	0.5	Non-confidential	Alignment with AVS requirements
17/11/2021	0.4	Non-confidential	Modifications after review
30/09/2021	0.3	Non-confidential	First draft version

1.3 References

This document refers to the following informative documents.

Ref	Doc No	Author(s)	Title
[SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP), Version 1.1, June 2021
[PSAL2PP]	JSADEN012	PSA JSA	SESIP Profile for PSA Certified Level 2
[AVS]	https://developer.amazon.com/en-US/docs/alexa/alexa-voice-service/avs-security-reqs.html	Amazon	AVS Security Requirements, last updated on October 18, 2021.
[ioXt]	C-03-25-01	ioXT Alliance	ioXt 2020 Smart Speaker Profile, Version 2.00, 25 March 2021

1.4 Terms and Abbreviations

This document uses the following terms and abbreviations

Term	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
CPU	Central Processing Unit

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

DRM	Digital Rights Management
LED	Light Emitting Diode
HTTPS	HyperText Transfer Protocol Secure
IPSec	Internet Protocol Security
NLP	Natural Language Processing
NTP	Network Time Protocol
NSPE	Non-Secure Processing Environment
OEM	Original Equipment Manufacturer
OS	Operating System
OTP	One-Time-Programmable
RAM	Random Access Memory
REE	Rich Execution Environment
ROM	Read Only Memory
RoT	Root of Trust
SFR	Security Functional Requirement
SPE	Secure Processing Environment
SoC	System-on-Chip
ST	Security Target
TEE	Trusted Execution Environment
TLS	Transport Layer Security

1.5 Feedback

The PSA JSA Members welcome feedback on its documentation.

If you have comments on the content of this documentation, send an e-mail to psacertified@arm.com. Give:

- The title (Smart Speaker and Voice Assistant SESIP Profile).
- The number (JSADEN-015) and version.
- The page numbers to which your comments apply.
- The rule identifiers to which your comments apply, if applicable.
- A concise explanation of your comments.

PSA JSA Members also welcome general suggestions for additions and improvements.

Note: PDFs are tested only in Adobe Acrobat and Acrobat Reader and cannot guarantee the appearance or behavior of any document when viewed with any other PDF reader.

2 Introduction

1. This SESIP Profile targets smart speakers and voice assistants, a type of wireless (Wi-Fi, Bluetooth or 4G) speaker and voice commanded device with an integrated virtual assistant that offers interactive actions and handsfree activation. Smart speakers and voice assistants allow users to easily obtain entertainment information and to conveniently interact with the smart devices.

2. While smart speakers are dedicated devices for this purpose, voice assistants relate to devices designed for another purpose, such as a set-top-box for TV, which also embed smart speaker features. Unless specified differently, this document will use the terms 'smart speakers' as a generalization of smart speaker devices and voice assistant devices.

3. The expected operational environment of the smart speaker is a physically protected room such as office or home. Logical attacks over a distance (including from/via networks the speaker is connected to) are in scope.

2.1 Profile Reference

4. See title page.

2.2 Platform Reference

Platform name	<Platform name>
Platform version	<Platform version>
Platform identification	<Platform id details>
Platform Type	Hardware device and a firmware implementing the smart speaker functionalities

2.3 Platform Functional Overview and Description

2.3.1 Usage and Major Security Features

5. Smart speakers integrate NLP to communicate with users, this usually means that the speaker will have enough computing power to process these complex algorithms in different context.

6. The smart speakers considered in this Profile require a network connection, most of these devices are connected through Wi-Fi, typically on a local network.

7. There are many possible uses for smart speakers, corresponding to very different security contexts, that we can abstract as follows:

   - Regular personal use, general purpose. From home entertainment to virtual assistant, privacy protections are essential, but the achievable level of security assurance is limited by cost constraints.
   - Enterprise and public, general purpose. Similar like regular personal use case, privacy protections are essential, so the level of security assurance does not need to be maximal.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

- Commercial feature like online shopping, high security. When a speaker is used for purchasing, the same feature is essential, but the level of security assurance must be significantly higher, even if it drives up the costs.

8. Despite these differences, the security features to be included in speakers are similar enough to be described in a single Profile, as the appropriate security assurance can be personalized in a speaker's Security Target.

9. We consider that smart speakers include at least the following security features:

   - Security through the operational life-cycle of the smart speaker by:
     - Ensuring the smart speaker starts up securely (see "Secure Initialization of Platform") and then uniquely identifies itself (see "Verification of Platform Identity" and "Verification of Platform Instance Identity") and shows it is genuine (see "Attestation of Platform Genuineness") to the administrator.
     - Software updates. The software running on the speaker can be updated to fix vulnerabilities identified after the device's deployment. See "Secure Update of Platform" and ALC_FLR.2.
     - Protection of private data through security measures for data at rest (see "Secure Storage") and data in transit (see "Secure Communication Support") and erasure after end-of-life (see "Factory Reset of Platform").
   - Admin authentication. The administrator who performs initialization and configuration, typically the device owner, must be authenticated before connecting the device to the network or modifying its configuration or performing maintenance operations on it. See "Authenticated Access Control". Local and network authentication may rely on different methods and credentials. Smart speakers are naturally shared by people physically able to access it. As the ease of use is important to the device's utility, it is usually not necessary to authenticate the user and this profile does not consider end-user authentication.
   - Monitor audio streams from the speaker microphone to detect user commands. The speaker is typically triggered by a wake word pronounced by the user, after which the speaker interprets following commands. See "Authenticated Access Control".
   - Encryption of audio streams recorded by the speaker. The audio stream can be encrypted with a key that is only shared with intended recipients (servers or users). See "Secure Communication Support".
   - Decryption of audio streams received by the speaker. Such audio streams may be protected by DRM solutions. See "Secure Communication Support". To support the secure storage of these keys, see "Cryptographic KeyStore".
   - Secure communication. More generally, any network communication is performed using a protocol that includes integrity and confidentiality protections. See "Secure Communication Enforcement ".

2.3.2 Log of security events. Security events are logged locally on the speaker, to be made available in the forensic analysis of an attack or other suspicious event. See "Secure Communication Enforcement

10. The platform ensures that the application can only communicate with *<list of endpoints>* over the secure communication channel(s) supported by the platform using *<list of protocols and measures>*.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

11. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this. This should include the types of supported secure communication channels, the method they can be invoked, the used cryptographic material, the contexts they shall always be used.>*

12. **Note** 7: This requirement shall cover at least encryption of audio streams recorded by the speaker for intended recipients (servers or users).

    - Audit Log Generation and Storage".

2.3.3 Platform Architecture

13. *<A short introduction and description of the platform must be provided. Typically this would be taken from the datasheet.>*

14. The Platform is to be embedded in a hardware device (the speaker) that provides hardware that is used by this platform such as the microphone, the speaker, the network interface or other hardware.

15. The Figure 1 illustrates the main components for a smart speaker Platform in this Profile *<Replace this generic figure according to the Platform architecture and scope>*. It distinguishes between a Secure Processing Environment (SPE), in charge of the platform root of trust functions, such as secure boot, secure update, secure storage, and a more complex Non-Secure Processing Environment, in charge of supporting smart speaker functions. Voice assistants will typically have more software components in the Non-Secure Processing Environment as well more hardware peripherals.

16. The Secure Processing Environment can also support applications, illustrated as 'Applications Root of Trust' in Figure 1. For instance, the smart speaker can use the SPE to implement a secure wake word application. In this configuration, only the SPE would monitor surrounding sounds and conversations until it detects a user-defined wake word for the speaker and perform a handover to the NSPE for processing of user commands. This feature enhances user privacy and protects against bugs and malware in the NSPE that would allow spying on the speaker sound environment.

17. As another example of Application Root of Trust, the Secure Processing Environment can support the Neural Network / Artificial Intelligence (AI) features. The Neural Network Framework illustrated in Figure 1 in the NSPE would then be an interface to the same service in the SPE. With this configuration, AI Data and AI Model, which often expect integrity and/or confidentiality protection would benefit from the SPE isolation properties.

18. *<Add all the necessary details for the software scope: libraries, drivers, versions, …>*

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

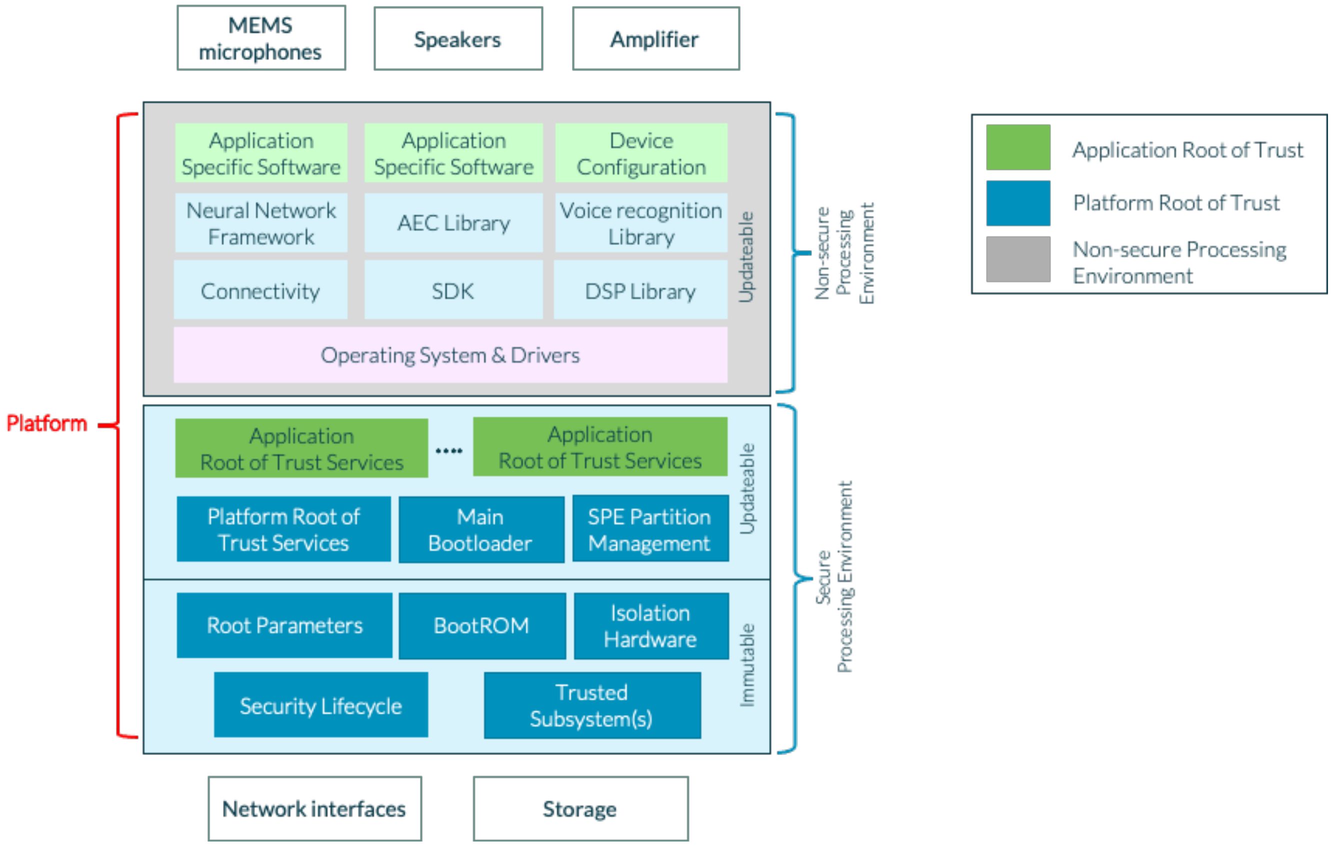
MEMS microphones
Speakers
Amplifier
Application Specific Software
Application Specific Software
Device Configuration
Neural Network Framework
AEC Library
Voice recognition Library
Connectivity
SDK
DSP Library
Operating System & Drivers
Updateable
Non-secure Processing Environment
Platform
Application Root of Trust Services
....
Application Root of Trust Services
Platform Root of Trust Services
Main Bootloader
SPE Partition Management
Updateable
Root Parameters
BootROM
Isolation Hardware
Security Lifecycle
Trusted Subsystem(s)
Immutable
Secure Processing Environment
Network interfaces
Storage
Application Root of Trust
Platform Root of Trust
Non-secure Processing Environment

Figure 1: Smart Speaker Platform

19. The Physical scope for the Platform is typically composed of a digital media processor SoC which supports secure boot and isolation between SPE and NSPE. The SoC may also support OTPs to store sensitive data, such as speaker ID or secrets. *<write specific scope details, which may be a silicon chip, a PCB, … >*

20. The out of scope part comprises *<to be completed by developer>*.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.

3 Security Objectives for the Operational Environment

For the platform to fulfil its security requirements, the operational environment (technical or procedural) must fulfil the following objectives.

3.1.1 Credential Management

21. The cryptographic keys, credentials and certificates used in the Platform shall be securely generated, provisioned to the Platform.

22. *<ST writer: add the reference to the exact location in the guidance where this is described, for example: "(as described in [Manual] section "Key management rules")>*

23. Additionally, cryptographic keys shall be securely managed during the life cycle of Platform when used outside of the Platform (such as in gateways, back-end servers or maintenance devices).

24. *<ST writer: add the reference to the exact location in the guidance where this is described>*

3.1.2 Trusted Administrator

25. The Admin of the Platform is not careless, wilfully negligent or hostile.

26. *<ST writer: add the reference to the location in the guidance where this is described>*

3.1.3 Environment

27. The environment of the platform shall include all hardware components required for platform operation, such as microphone, speaker, network interface or storage.

28. *<ST writer: describe platform environment including remote services such as secure update server, NTP server.>*

3.1.4 Others

29. *<List all other mandatory objectives for the environment with reference to where in the guidance documents this objective is described*

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

4 Security Requirements and Implementation

4.1 Security Assurance Requirements

30. The claimed assurance requirements package is SESIP2 as described in Section 5.1.

4.1.1 Flaw Reporting Procedure (ALC_FLR.2)

31. In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to give generate any needed update and distribute it, the developer has defined the following procedure:

32. *<ST writer: Describe the procedure, including where flaws can be reported (website and/or email address), how the reported flaws are handled in a timely manner, and how an application developer/end-user can get informed of the update. The process to receive the reports of flaws and handling them in a timely manner needs to be described.>*

4.2 Security Functional Requirements

33. Platforms conformant to this Profile must satisfy the following security functional requirements.

4.2.1 Verification of Platform Identity

34. The platform provides a unique identification of the platform, including all its parts and their versions.
<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this.>

4.2.2 Verification of Platform Instance Identity

35. The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.
<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this.>

4.2.3 Attestation of Platform Genuineness

36. The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity”, in a way that ensures that the platform cannot be cloned or changed without detection.

37. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this.>*

4.2.4 Secure Storage

38. The platform ensures that all data stored by the application, except for *<list of data stored in plaintext>*, is protected to ensure its authenticity and integrity as specified in *<specification>* with a platform instance unique key of key length *<key length>.*

39. **Note 1:** This requirement is used to protect at least Speaker ID, Configuration and Credentials, Voice Records, as well as Speaker Logs, therefore those must not be listed in the “list of data stored in plaintext”.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

4.2.5 Secure Initialization of Platform

40. The platform ensures its authenticity and integrity during platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to *<list of controlled states>*.

41. **Note** 2: Secure initialization must cover all software part of the evaluation.

42. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this. This should include all stages of the bootchain and describe for each stage how the verification of the loaded software is performed and the cryptographic material used for that purpose.>*

4.2.6 Secure Update of Platform

43. The platform can be updated to a newer version in the field such that the integrity, authenticity, and confidentiality of the platform is maintained.

44. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this. This should include the verifications performed by the secure update mechanism, the order of these verifications, the behavior of the platform is case of a failed verification and the cryptographic material used for that purpose.>*

4.2.7 Secure Communication Support

45. The platform provides the application with one or more secure communication channel(s).

46. The secure communication channel authenticates *<list of endpoints>* and protects against *<list of attacks including disclosure, modification, replay, erasure>* of messages between the endpoints, using *<list of protocols and measures>*.

47. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this. This should include the types of supported secure communication channels, the method they can be invoked, the used cryptographic material, the contexts they shall always be used.>*

48. **Note** 3: Secure communication channels include any of IPsec, TLS or HTTPS performed by the platform. Validity of the peer certificate shall at least be determined by the certificate path, the expiration date, and the revocation status.

49. **Note** 4: Device shall use TLS 1.2 or greater. The device shall implement certificate validation for all such TLS connections and validate that connections to the device are signed using the correct certificate. Initial setup shall not include the transmission of credentials over a non-TLS session.

50. **Note** 5: When using Bluetooth BR/EDR or Bluetooth Low Energy (BLE), the device shall support Secure Connections. It shall support Security Mode 4 Level 4 when using Bluetooth Low Energy (BLE) or Bluetooth BR/EDR protocols and services; support Security Mode 1 Level 4 when using Bluetooth Low Energy (BLE) protocol and services; and use the Privacy feature when using the Bluetooth Low Energy (BLE) protocol.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

51. **Note** 6: Apart of secure communication support with remote servers and devices, this requirement for protection of audio streams by DRM solutions.

4.2.8 Secure Communication Enforcement

52. The platform ensures that the application can only communicate with *<list of endpoints>* over the secure communication channel(s) supported by the platform using *<list of protocols and measures>*.

53. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this. This should include the types of supported secure communication channels, the method they can be invoked, the used cryptographic material, the contexts they shall always be used.>*

54. **Note** 7: This requirement shall cover at least encryption of audio streams recorded by the speaker for intended recipients (servers or users).

4.2.9 Audit Log Generation and Storage

55. The platform generates and maintains an audit log of *<failed and successful authentication attempts, firmware upgrade requests and progress, integrity errors, list of other significant security events>* and allows access and analysis of these logs following a specific *<access control policy>*.

56. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this.>*

57. **Note** 8: Audit log record should mention the nature of the event, date and time of the event and the user, if any, responsible for the event.

58. **Note** 9: Significant security events include at least failed and successful authentication attempts, firmware upgrade requests and progress, integrity errors.

59. **Note** 10: The Platform should rely on a secure NTP server to provide reliable source for time stamps for the audit trail.

4.2.10 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)

60. The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

61. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this. This should include how the isolation hardware is used to enforce isolation between SPE and NSPE.>*

4.2.11 Cryptographic KeyStore

62. The platform provides the application with a way to store *<list of assets, such as cryptographic keys and passwords>* such that not even the application can compromise the *<authenticity, integrity, confidentiality>* of this data. This data can be used for the cryptographic operations *<list of operations>*.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

63. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this. This should include the storage locate of these assets and the cryptographic means and materials used to protect these assets.>*

64. **Note** 11: Cryptographic keystore is used for cryptographic assets related to secure update, secure storage, secure communication support.

4.2.12 Factory Reset of Platform

65. The platform can be reset to the state in which it exists when the composite product embedding the platform is delivered to the user, before any personal user data, user credentials, or user configuration is present on the platform.

66. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this.>*

4.2.13 Authenticated Access Control

67. The platform allows only *<list of role(s)>*, identified, authenticated and authorized as specified by *<specification>* to allow performing of *<administration operations>*.

68. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this.>*

69. **Note** 12: This SFR is not yet of part of the SFRs catalog [SESIP] but will be integrated in a future version.

4.3 Optional Security Functional Requirement

70. The following security functional requirement shall be included if the related feature, secure debugging, is supported on the platform.

4.3.1 Secure Debugging

71. The platform only provides *<list of endpoints>* authenticated as specified in *<specification>* with debug functionality.

72. The platform ensures that all data stored by the application, with the exception of *<list of exceptions>*, is made unavailable.

73. *<ST writer: add a short conformance rationale describing how this is done with a reference to the specific guidance/functional specification section describing this.>*

5 Mapping and Sufficiency Rationales

5.1 SESIP2 Sufficiency

74. SESIP2 deliverables, required to demonstrate good security practice, are contained in the Security Target itself, complemented with basic product documentation required to perform a black-box evaluation.

Assurance Class	Assurance Family	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	<Section "Introduction" and title page of the Security Target>	<TBD>
	ASE_OBJ.1 Security requirements for the operational environment	<Section "Security Objectives for the Operational Environment" of the Security Target>	<TBD>
	ASE_REQ.3 Listed Security requirements	<Section "Security Requirements and Implementation" of the Security Target>	<TBD>
	ASE_TSS.1 TOE Summary Specification	<Section "Security Requirements and Implementation" of the Security Target>	<TBD>
ADV: Development	ADV_FSP.4 Complete functional specification	<Description of which developer evidence is used to meet this requirement>	<TBD>
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	<Description of which developer evidence is used to meet this requirement>	<TBD>
	AGD_PRE.1 Preparative procedures	<Description of which developer evidence is used to meet this requirement>	<TBD>
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	<ALC_FLR section in the Security Target and description of which developer evidence is used to meet this requirement>	<TBD>
ATE: Tests	ATE_IND.1 Independent testing: conformance	<Description of which developer evidence is used to meet this requirement>	<TBD>
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities.	<TBD>

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Appendix A Security Problem Definition

75. This informational appendix provides the risks analysis elements that justify the choice of the security requirements in Section 4.

A.1 Users and External Entities

76. The external entities that are considered in this Profile are the User and the Device Owner, who also plays the role of the Admin.

77. The User is freely to user smart speaker for the basic use cases which have no authentication needs.

78. The Device Owner can pair the speaker with mobile APP for setting and configuration, after authentication.

79. The Admin can modify the speaker configuration, perform firmware update and access audit logs after authentication.

A.2 Assets

A.2.1 Platform Data

A.2.1.1 Speaker ID

80. A unique ID to identify the platform on a network, such as a MAC address or a unique device ID managed by OEM.

81. Properties: Integrity

A.2.1.2 Firmware

82. The speaker's firmware.

83. Properties: Integrity, Authenticity, Confidentiality

A.2.1.3 Firmware Certificate

84. The cryptographic certificate used to authenticate firmware and firmware updates.

85. Properties: Integrity, Authenticity

A.2.1.4 Logs

86. The event logs, that can be used to detect suspicious activities.

87. Properties: Integrity

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

A.2.2 User Data

A.2.2.1 Audio content

88. The audio stream produced by the speaker exchanged over the network, and voice recordings stored locally.

89. As input to the speaker, this includes spoken user commands to the speaker but may include also private conversation. As output from the speaker, this includes music, podcast or conversations with remote people.

90. Properties: Integrity, Confidentiality

A.2.2.2 Configuration

91. The smart speaker's configuration, split into two components:

- The speaker's software configuration, including mobile APP pairing status, wake word, voice ID configuration and other settings.
- The speaker's network configuration, such as the name of a WLAN network and security setting. Depending on the implementation, the configurations are locally and/or remotely stored.

92. Properties: Integrity

A.2.2.3 Credentials

93. The authentication credentials, used for local and remote authentication, such as:

- Network credentials, to authenticate if needed on the network, for instance a Wi-Fi pre-shared key or an 802.1x certificate, to be protected in integrity and confidentiality.
- Device authentication credentials to authenticate on remote servers, to be protected in integrity and confidentiality.
- Device authentication credentials to authenticate on local devices (thermostat, lights, outlets, door lock, …) when the device is used as a smart home hub, to be protected in integrity and confidentiality.
- Server authentication data, such as public key certificates, to be protected in integrity.
- DRM credentials, for broadcasted audio content.
- Session keys, used after establishment of a trusted communication channel with servers, to be protected in integrity and confidentiality.
- Administration credentials, to authenticate to the services provided by the smart speaker for administration, to be protected in integrity and confidentiality.
- Device Owner biometric patterns to be used in voice recognition or similar algorithms, to be protected in integrity and confidentiality.

94. Properties: Integrity, Confidentiality

A.2.2.4 Application Root of Trust Data

95. Data used by Applications Root of Trust if such applications are present in the Secure Processing Environment.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

96. This data can be for instance the wake work, when it is managed by the SPE, or AI Data and AI Model when an Articificial Intelligence framework is managed by the SPE.

97. This data is isolated from the Non-Secure Processing Environment.

98. Properties: Integrity, Confidentiality

A.2.3 Others

99. Although assets of this section are not informational assets, but rather resources available to the Platform, they may be the direct targets of attackers.

A.2.3.1 Computing Power

100. The processing capabilities of the Platform, as provided by its central and possibly graphic processing units.

A.2.3.2 Network Bandwidth

101. The network resources used by the Platform to exchange data.

A.2.3.3 Storage Space

102. The mass storage space used by the Platform to store data. As the Platform processes audio, the volume of stored data may be significant.

A.3 Threats

103. An attacker is a threat agent (a person or a process acting on his/her behalf) trying to undermine the Platform security policy defined by the current Profile. The attacker especially tries to change properties of the assets defined in Section A.2.

A.3.1 Impersonation

104. An attacker impersonates a legitimate admin user on the speaker.

105. The admin credentials may be obtained through interception, for instance in insecure communication links, or exposed through data disclosure.

106. The attacker may then access voice records, modify configuration, firmware or logs or impersonate user on remote server or local devices.

107. Assets threatened directly: Credentials
Assets threatened indirectly: Firmware, Audio content, Configuration, Logs.

A.3.2 MITM

108. An attacker performs a Man-In-The-Middle attack or impersonates a server the speaker connects to, for instance to download the voice records or the event logs.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

109. The attacker may rely on insecure communication links or prior modification of the server credentials on the speaker through insecure configuration.

110. The attacker may then access and modify Audio content, Logs, Credentials, Configuration data.

111. Assets threatened directly: Credentials (Server), Logs, Voice Records, Configuration

A.3.3 Firmware Abuse

112. An attacker exploits a flawed version of the firmware and obtains partial or total control of the speaker. The firmware may have been modified prior to the attack to include a malware or consist of an outdated version of the original firmware.

113. The attacker may for instance use data injection or modify on the device the value of the firmware certificate used to authenticate the installed firmware or firmware updates.

114. Such an attack can allow for elevation of privileges, where a regular user gains access to admin privileges.

115. This attack can also be used to take control over the Platform resources, for instance to carry a denial-of-service attack on other network devices, to store illegal files or to mine cryptocurrencies.

116. Assets threatened directly: Firmware, Firmware Certificate, Computing Power, Network Bandwidth, Storage Space.

117. Assets threatened indirectly: All.

A.3.4 Repudiation

118. A User of the smart speaker denies action performed on the Platform on its behalf.

119. This can be impersonating the remote administrator for configuration or firmware update.

120. Assets threatened directly: Logs, Audio content, Firmware.

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Appendix B Mapping with PSA Certified

121. This appendix provides a mapping between the Security Requirements of PSA Certified Level 2 SESIP Profiles for PSA-RoT [PSAL2PP] and this Profile.

122. Should the smart speaker rely on a PSA certified Level 2 or 3 PSA-RoT platform, the smart speaker Security Requirements for which the following table provides a “Same” mapping for PSA Certified Level 2 SESIP Profile SFR are already part of the certified PSA-RoT platform. The Security Requirements with an “Optional” mapping are part of the certified PSA-RoT platform only if they have been included in the Security Target for the considered PSA-RoT.

Smart Speaker Profile SFR	PSA Certified Level 2 SESIP Profile SFR
Verification of Platform Identity	Same
Verification of Platform Instance Identity	Same
Attestation of Platform Genuineness	Same
Secure Storage	Same: either Secure Encrypted Storage (internal storage) or Secure Storage (internal storage) or Secure External Storage
Secure Initialization of Platform	Same
Secure Update of Platform	Same
Secure Communication Support	Not in PSA Certified Level 2
Audit Log Generation and Storage	Optional
Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE)	Same
Cryptographic KeyStore	Same
Secure Debugging	Optional
Factory Reset of Platform	Not in PSA Certified Level 2

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Appendix C Mapping with AVS Security Requirement

123. This appendix provides a mapping between the AVS Security Requirements [AVS] and this Profile.

124. Should the smart speaker be certified according to the Smart Speaker Profile, it already fulfils most of the AVS Security Requirements. The following table provides a mapping between the latter and the Smart Speaker Profile requirements.

AVS Security Requirements	Smart Speaker Profile Requirements
1.1. Device SHALL use a secure software update distribution that uses cryptographic signing so that only authentic and authorized updates are applied to the device.	Secure Update of Platform
1.2. Device SHALL implement industry standard device hardening methods. For example, prohibiting default passwords, removing unnecessary network services and software, validating inputs before processing it in services on the device, and applying all security patches to vulnerable open source software.	AVA_VAN.2 Vulnerability analysis
1.3. Device SHALL use TLS 1.2 or greater for all communications to Alexa endpoints outside of initial setup. You SHALL have the Amazon Trust Services root CAs installed in the CA bundle. The device SHALL implement certificate validation for all such TLS connections and SHALL validate that connections to the device are signed using the correct Amazon certificate. Initial setup SHALL NOT include the transmission of credentials over a non-TLS session.	Secure Communication Support
1.4. Company SHALL have a software maintenance update strategy that specifically defines how software updates will be created and distributed within a reasonable period of discovery when vulnerabilities are identified.	ALC_FLR.2 Flaw reporting procedures
1.5. Company SHALL publish information in English and any other appropriate language on company's public website about vulnerability reporting program (VRP) and how security researchers can submit security vulnerability reports of their devices.	ALC_FLR.2 Flaw reporting procedures
1.6. Company SHALL implement and share with Amazon a security response plan that describes how company will proceed if a security incident arises, when company will	ALC_FLR.2 Flaw reporting procedures

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

communicate with Amazon on an incident, and the estimated timelines for remediation of an incident.	
1.7. Company SHALL provide a report from an independent security expert or a certified security specialist who has conducted an in-depth security review of the device.	SESIP certification report
1.8. Company SHALL submit reports of known exploitable security vulnerabilities that exist on the device, along with a plan to fix the vulnerabilities.	SESIP certification report ALC_FLR.2 Flaw reporting procedures
1.9. Device SHALL support Secure Connections when using Bluetooth BR/EDR or Bluetooth Low Energy (BLE).	Secure Communication Support
1.10. Device SHALL support Security Mode 4 Level 4 when using Bluetooth Low Energy (BLE) or Bluetooth BR/EDR protocols and services.	Secure Communication Support
1.11. Device SHALL support Security Mode 1 Level 4 when using Bluetooth Low Energy (BLE) protocol and services.	Secure Communication Support
1.12. Device SHALL use the Privacy feature when using the Bluetooth Low Energy (BLE) protocol.	Secure Communication Support
1.13. Company SHALL submit an un-encrypted file system image (full firmware) of the device for scanning vulnerabilities in operating system and open source software components. This requirement applies to a new device or an existing device upgrading SDK versions.	*Can be addressed by upgrading the assurance level in the product security target to SESIP3 or SESIP2 with white-box*
1.14. Device SHALL protect local Amazon software from unauthorized access. For example, on-device MiTM attack or display hijacking.	Partial contribution from: Secure Communication Support, Isolation of Platform
1.15. Device SHALL implement a hardware based on/off control mechanism for any microphones and cameras. This control must remove power from the microphones/camera and include a dedicated microphone/camera status indicator to inform users of the on/off status.	*Hardware design choice not in scope of SESIP certification*
1.16. Device SHALL use a chipset that relies on hardware-based security capabilities and meets PSA certified Level 1 or similar.	*Hardware design choice not in scope of SESIP certification, but a certification according to the Smart Speaker already fulfil most of PSA certified Level 2 requirements (see Appendix B).*
1.17. Company SHALL confirm that device software components and use of Amazon SDKs must not violate the license terms of the SDKs.	*Process not in scope of SESIP certification*
1.18. Device SHOULD use a fleet management solution, such	*Process not in scope of SESIP*

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

AWS IoT Device Management or similar.	*certification*

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Appendix D Mapping with ioXt Requirements

125. This appendix provides a mapping between the ioXt Smart Speaker Profile level 1 security pledges [ioXt] and this Profile.

ioXt security pledge	Id	Features	Smart Speaker Profile Requirements
Automatic Security Updates	AA1	Software Updates Supported	Secure Update of Platform ATE_IND.1 Independent testing: conformance
	AA2	Software is Maintained and Updated	ALC_FLR.2 Flaw reporting procedures
	AA3	Software updates are made available to impacted parties	ALC_FLR.2 Flaw reporting procedures
Security Expiration Date	SE1	End of life notification policy is published OR Expiration Date is published	
Vulnerability Reporting Program	VP1	VDP in place	ALC_FLR.2 Flaw reporting procedures
	VP1	Accept External Submissions	ALC_FLR.2 Flaw reporting procedures
Verified Software	VS1	Manufacturer has an update patch policy	
	VS2	Software images including plug-ins and apps are signed and verified	Secure Update of Platform
	VS3	Proven Cryptography	Secure Update of Platform
No Universal Passwords	UP1	Must have user authentication, and must not use common and predictable passwords, or require user to change at initial use.	Can be covered by Authenticated Access Control SFR if the variable part <*specification*> includes this security measure
Proven Cryptography	PC1	Standard Cryptography	Secure Update of Platform Secure Communication Support Authenticated Access Control
Secured Interfaces	SI1.1	Remote Attack: All certifiable protocols used on the interfaces contained in the device shall be Certified	Secure Communication Support
	SI1.2	Remote Attack: Unused Services are disabled	

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

	SI1.3	Remote Attack: Authentication	Authenticated Access Control
	SI1.4	Remote Attack: Secured Communications	Secure Communication Enforcement

Acknowledgements

This document was written for Arm by ProvenRun
http://www.provenrun.com

Copyright © 2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential