Smart Camera SESIP Profile

Moderate and Substantial Protection

Document number:	JSADEN016
Version:	0.4
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:	31/05/2022

Abstract

The Platform Security Architecture approach to security combines a hardware root of trust with security by design best practice aligned with the PSA security model, NIST 8259A and the mandatory device parts of EN 303 645. Additionally, PSA Certified recommends that device manufacturers should create a threat model specific to their own device and expected use, considering the threats in scope and the assets that need protecting. The PSA JSA publishes this example protection profile (SESIP profile) under a permissive creative commons licence to assist device makers in this process.

Keywords

Smart Camera, AI, ML, Privacy, Platform Security Architecture, SESIP, Protection Profile, PSA Certified, AVS

Contents

1 About this document

1.1 Current Status and Anticipated Changes

1. Current Status: Release 01

1.2 Release Information

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

Date	Version	Confidentiality	Change
31/05/2022	0.4	Non-confidential	Align with Smart speaker profile
17/03/2022	0.3	Non-confidential	Review by Rob Smart
10/03/2022	0.2	Non-confidential	
07/02/2022	0.1	Non-confidential	First draft version

1.3 References

3. 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
[PSAL3PP]	JSADEN011	PSA JSA	SESIP Profile for PSA Certified Level 2
[ioXt-Cam]	C-20-12-15	ioXt Alliance	ioXt 2020 Residential Camera Profile, Version 1.00, March 2021

1.4 Terms and Abbreviations

4. This document uses the following terms and abbreviations

Term	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
ARoT	Application specific Root of Trust
CPU	Central Processing Unit
DRM	Digital Rights Management

HTTPS	HyperText Transfer Protocol Secure
IPSec	Internet Protocol Security
ML	Machine Learning
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

5. The PSA JSA Members welcome feedback on its documentation.
6. If you have comments on the content of this documentation, send an e-mail to psacertified@arm.com. Give:
   - The title (Smart Camera SESIP Profile).
   - The number (JSADEN-016) 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.
7. PSA JSA Members also welcome general suggestions for additions and improvements.
8. **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

9. This SESIP Profile targets network-connected cameras, such as those used in homes and offices, with some processing capabilities to connect autonomously to a network. It may also include some local analysis of the pictures.

10. The considered platform is composed of a hardware device and firmware implementing the network camera functionalities. The firmware itself may include a generic purpose operating system.

11. This SESIP Profile is proposed with two protection levels (see Section 2.4): basic and substantial protection, depending on the expected security assurance and the product architecture.

2.1 Profile Reference

12. 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 camera functionalities

2.3 Platform Functional Overview and Description

2.3.1 Usage and Major Security Features

13. Network cameras are used to stream live video for monitoring purposes. In order to reduce the required bandwidth, this usually means that the camera will have enough computing power to encode the video stream in to a compressed form.

14. The cameras considered in this Profile require a network connection. As live video streaming requires significant bandwidth, most network cameras are either connected through a cable or through Wi-Fi, typically on a local network.

15. There are many possible uses for network cameras, corresponding to very different security contexts, which can be abstracted as follows:

    - Personal use. From babyphones to security cameras, both event detection and privacy protection are essential, but the achievable level of security assurance is limited by cost constraints.
    - Enterprise, general purpose. With a traditional security camera, in a protected environment, event detection and video flow integrity are essential. Risks are limited, so the level of security assurance does not need to be maximal.

- Enterprise, high security. When a camera is highly exposed, or when it is used to protect high-value assets, the same features are essential, but the level of security assurance must be significantly higher, even if it drives up the costs.

16. Despite these differences, the security features to be included in cameras are similar enough to be described in a single Profile, as the appropriate security assurance can be personalized in a camera specific Security Target.

17. Network cameras include at least the following security features:

    - Secure operational life-cycle:
        - Ensuring the smart speaker starts up securely (see "Secure Initialization of Platform") and adminthen 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 Flaw Reporting Procedure (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 of private date after end-of-life (see "Factory Reset of Platform").
        - Secure access to debug features, if any (See “Secure Debugging”).
        - Protection against physical attacks, if needed (See “Physical Attacker Resistance”).
    - User and admin authentication. Authentication before access to the camera, and before modification of its configuration or performing any maintenance operations is required. Local and network authentication may rely on different methods and credentials. See “Authenticated Access Control”.
    - Encryption of video stream. The video stream can be encrypted with a key that is only shared with the intended recipients (servers or users). See “Secure Communication Support” and “Secure Communication Enforcement”.
    - Secure communication. More generally, any network communication is performed using a protocol that includes integrity and confidentiality protection. See “Secure Communication Support”.
    - Log of security events. Security events are logged locally on the camera, to support forensic analysis of an attack or other suspicious event. See “Audit Log Generation and Storage”.

2.3.2 Platform Architecture

18. *<A short introduction and description of the Platform, the combination of hardware and software to be evaluated, must be provided. Typically this would be taken from the datasheet.>*

19. The Platform is the combination of hardware and software that provide a runtime enviromnent and related applications for capturing and processing a video stream. It is to be embedded in a hardware device that provides the sensor, the network interface or other hardware used the smart camera but which are not part of the scope of evaluation.

20. Figure 1 illustrates the main components for a smart camera Platform in this Profile *<Replace this generic figure according to the specific 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 the Non-Secure Processing Environment, in charge of supporting smart camera functions.

21. The Secure Processing Environment can also support applications, illustrated as Applications Root of Trust (ARoT) in Figure 1. For instance, the smart camera can use the SPE to host a video payload signing ARoT, using keys protected by the SPE.

22. As another example, an Application Root of Trust can support any Neural Network / Artificial Intelligence (AI) features typically used for object detection and classification. 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.

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

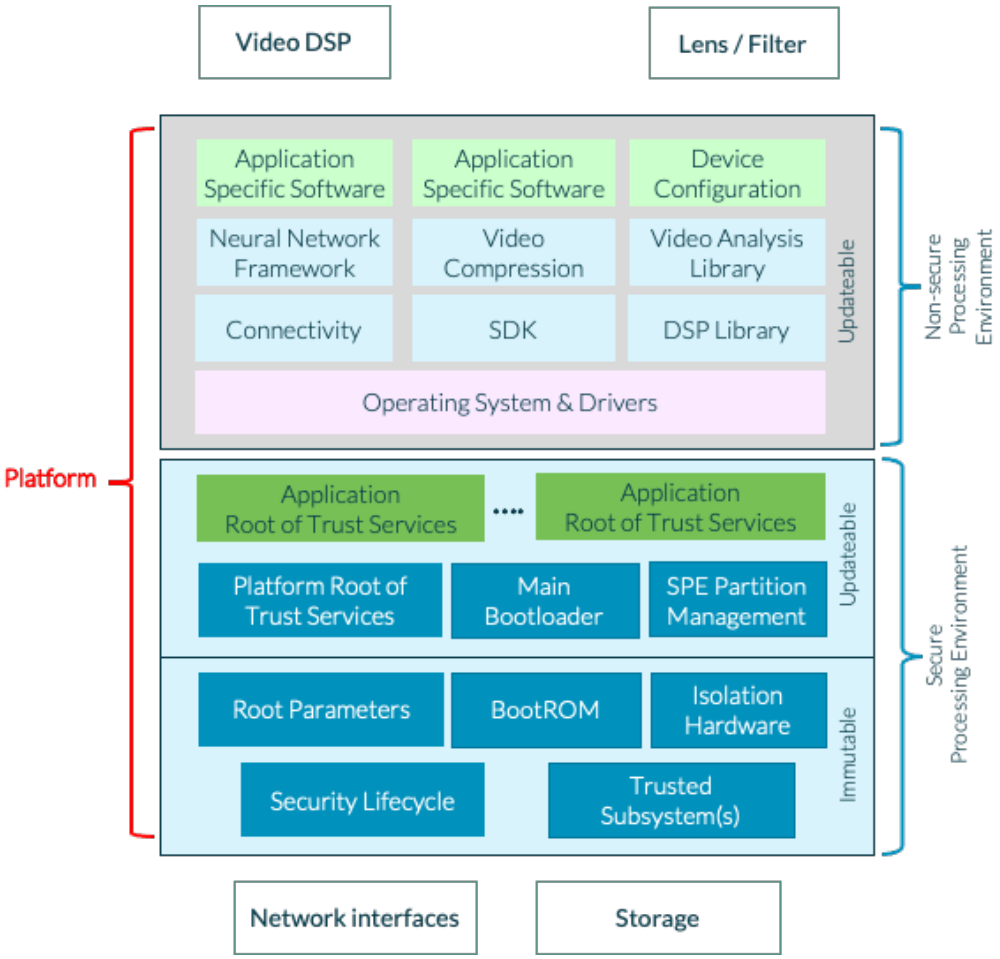

Figure 1: Smart Camera Platform

24. The Physical scope for the Platform is typically composed of a digital media processor SoC which supports hardware video encoders, 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, … >*

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

2.4 Protection Levels

26. This profile supports two protection levels depending on the expected security assurance and the product architecture:

- Moderate protection level: This level expects SESIP2 evaluation.
- Substantial protection level: This level expects SESIP3 evaluation and a platform based on a PSA Certified Level 3 chip [PSAL3PP]. It brings white-box evaluation and protection against physical attacks.

3 Security Objectives for the Operational Environment

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

3.1.1 Credential Management

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

29. Additionally, they should 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).

3.1.2 Trusted Administrator

30. The Admin of the Platform must not be careless, wilfully negligent or hostile.

3.1.3 Environment

31. The environment of the platform shall include all hardware components required for platform operation, such as any video DSP, camera, network interface or storage.

32. *<ST writer: describe the platform environment including remote services such as secure update server, NTP serve, streamed video content server.>*

3.1.4 Others

33. *<ST writer: list all other mandatory objectives for the environment with reference to where in the guidance documents this objective is described.>*

4 Security Requirements and Implementation

4.1 Security Assurance Requirements

34. According to the chosen protection level (see Section 2.4), the claimed assurance requirements package is either SESIP2 or SESIP3, as described in Section 5.1 and 5.2 respectively.

4.1.1 Flaw Reporting Procedure (ALC_FLR.2)

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

36. *<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 flaw reports and handle them in a timely manner needs to be described.>*

4.2 Security Functional Requirements

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

4.2.1 Verification of Platform Identity

38. The platform provides a unique identification of the platform, including all its parts and their versions.

39. *<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

40. The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.

41. *<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

42. 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.

43. *<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

44. 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>.*

45. **Note 1:** This requirement is used to protect at least Camera ID, Configuration and Credentials, Video Stream, Camera Logs, as well as AI Data and AI Model if used. Therefore those must not be listed in the “list of data stored in plaintext”..

4.2.5 Secure Initialization of Platform

46. 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>*.

47. **Note** 2: Secure initialization must cover all software parts of the evaluation.

48. *<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

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

50. *<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

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

52. 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>*.

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** 3: Secure communication channels may 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.

55. **Note** 4: If TLS is used then TLS 1.2 or greater must be used. 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.

4.2.8 Secure Communication Enforcement

56. 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>*.

57. *<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.>*

58. Note 7: This requirement shall cover at least encryption of video streams recorded by the smart camera for intended recipients (servers or users).

4.2.9 Audit Log Generation and Storage

59. 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>.

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

61. **Note** 5: 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.

62. **Note** 6: Significant security events include at least failed and successful authentication attempts, firmware upgrade requests and progress, integrity errors.

63. **Note** 7: 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)

64. 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.

65. *<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

66. 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>*.

67. *<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.>*

68. **Note** 8: Cryptographic keystore is used for cryptographic assets related to secure update, secure storage, secure communication support.

4.2.12 Factory Reset of Platform

69. 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.

70. *<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

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

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

73. **Note** 9: This SFR is not yet of part of the SFRs catalog [SESIP] but will be integrated in a future version.

4.3 Additional Security Functional Requirement for Substantial Level

74. The following security functional requirements shall be included according to the supported features or if Substantial Level is claimed.

4.3.1 Secure Debugging

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

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

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

78. **Note** 10: This security functional requirements shall be included if secure debugging is supported.

4.3.2 Physical Attacker Resistance

79. The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

80. *<ST writer: add a short conformance rationale describing how this is done and which types of physical attacks the platform is able to detect or prevent.>*

81. **Note** 11: This security functional requirements shall be included if Substantial Level is claimed.

5 Mapping and Sufficiency Rationales

5.1 SESIP2 Sufficiency (Moderate Protection)

82. 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>

5.2 SESIP3 Sufficiency (Substantial Protection)

83. SESIP3 deliverables also add basic documentation required to perform a white-box evaluation, as well as basic evidence of the use of configuration management.

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>
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	<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_CMC.1 Labelling of the TOE	<Description of which developer evidence is used to meet this requirement>	<TBD>
	ALC_CMS.1 TOE CM Coverage	<Description of which developer evidence is used to meet this requirement>	<TBD>
	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.3 Focused Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities.	<TBD>

Appendix A Security Problem Definition

84. 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

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

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

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

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

A.2 Assets

A.2.1 Platform Data

A.2.1.1 Camera ID

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

90. Properties: Integrity

A.2.1.2 Firmware

91. The camera's firmware.

92. Properties: Integrity, Authenticity, Confidentiality

A.2.1.3 Firmware Certificate

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

94. Properties: Integrity, Authenticity

A.2.1.4 Logs

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

96. Properties: Integrity

A.2.2 User Data

A.2.2.1 Video Stream

97. The video stream produced by the camera sent over the network and possibly stored locally according to camera storage policy.

98. Properties: Integrity, Confidentiality

A.2.2.2 Configuration

99. The smart camera's configuration, split into two components:

    - Camera's dynamic configuration, including network configuration such as the name of a WLAN network, or IP and DNS addresses
    - Camera settings such as pan, tilt, and zoom, the events to be detected and notified. Depending on the implementation, the configurations are locally and/or remotely stored.

100. Properties: Integrity

A.2.2.3 Credentials

101. 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.
    - Device authentication credentials to authenticate on remote servers.
    - Server authentication data, such as public key certificates, to be protected in integrity only.
    - Session keys, used after establishment of a trusted communication channel with servers.
    - Administration and user credentials, to authenticate to the services provided by the network camera, either for administration or for regular use.
    - User biometric patterns to be used in face recognition or similar algorithms.

102. Properties: Integrity, Confidentiality

A.2.2.4 Application Root of Trust Data

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

104. This data can be for instance for AI Data and AI Model when an Articifial Intelligence framework is managed by the SPE.

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

106. Properties: Integrity, Confidentiality

A.2.3 Others

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

A.2.3.1 Computing Power

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

A.2.3.2 Network Bandwidth

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

A.2.3.3 Storage Space

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

A.3 Threats

111. 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

112. An attacker impersonates a legitimate user on the camera, either a regular user that can access the video stream or an admin user.

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

114. The attacker may then access video stream, modify configuration or try to modify firmware.

115. Assets threatened directly: Credentials
Assets threatened indirectly: Firmware, Video Stream, Configuration, Logs.

A.3.2 MITM

116. An attacker performs a Man-In-The-Middle attack or impersonates a server the camera connects to, for instance to upload the video stream or the event logs.

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

118. The attacker may then access and modify Video Stream, Logs, Credentials, Configuration data.

119. Assets threatened directly: Credentials (Server), Logs, Video Stream, Configuration

A.3.3 Firmware Abuse

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

121. 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.

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

123. 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.

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

125. Assets threatened indirectly: All.

Appendix B Mapping with PSA Certified

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

127. Should the smart camera rely on a PSA certified Level 2 or 3 PSA-RoT platform, the smart camera 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 Camera 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

Appendix C Mapping with ioXt Requirement

128. This appendix provides a mapping between the ioXt Residential Camera Profile level 1 security pledges [ioXt-Cam] and this Profile.

ioXt security pledge	ID	Features	Smart Speaker Profile Requirements
Automatically Applied 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	VDP1	Vulnerability Disclosure Program (VDP) in place	ALC_FLR.2 Flaw reporting procedures
	VDP2	Accept External Submissions	ALC_FLR.2 Flaw reporting procedures
Verified Software	VS1	Manufacturer has an update patch policy	
	VS2	Software images including plugins and apps are signed and verified	Secure Update of Platform
	VS3	Proven Cryptography	Secure Update of Platform
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
	SI1.2	Remote Attack: Unused Services are disabled	
	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