Secured Applications for Mobile - Requirements

Version 1.0

08 June 2021

This Industry Specification is a Non-Binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

1.2 Scope

The Secured Applications for Mobile specification defines a capability allowing cellular connected Devices to use a wide range of secured applets within an eUICC. Such applets can be managed by a service provider, and may be paired with applications running in the Device itself. The work will focus on the eUICC where the secured applets will operate independently and outside of any eUICC Profile.

The use cases are documented in the Annex A.

1.3 Abbreviations

Abbreviation	Definition
AID	Application Identifier (as defined in ISO 7816)
ASP	Application Service Provider
CASD	Controlling Authority Security Domain (as defined in GlobalPlatform Card Specification 2.2 Amendment A)
CI	Certificate Issuer
DASMO	Device Application SAM Management Operations interface
ECASD	eUICC Controlling Authority Security Domain
EID	eUICC Identifier
FFS	For Further Study
ISD-P	Issuer Security Domain Profile (as defined in SGP.22 or SGP.02)
ISD-R	Issuer Security Domain Root (as defined in SGP.22 or SGP.02)
LAA	Local Applet Assistant
LASSMO	Local ASP SAM Service Management Operations
LPA	Local Profile Assistant (as defined in SGP.21)
mDL	mobile Driving License
NFC	Near Field Communication
PKI	Public Key Infrastructure
RID	Registered application provider Identifier (as defined in ISO 7816)
SAM	Secured Applications for Mobile
SAM SM	SAM Service Manager
SCP11	Secure Channel Protocol 11 (as defined in GlobalPlatform Card Specification 2.2. Amendment F)
SD	Security Domain
UWB	Ultra Wideband

1.4 Definitions

Definitions	Meaning
Application Service Provider	An entity that manages its SAM Applet(s) in an ASP SD to provide eUICC-based services, possibly through its Device Application(s).
ASP SD	An Application Service Provider Security Domain dedicated to SAM Applets hosted in a SAM SD.
Asynchronous Mode	A mode where the SAM Commands for a SAM SD are precomputed to be later executed.
Certificate	A certificate that can be defined using X.509 or GlobalPlatform format.
Device	Electronic equipment used in conjunction with a SAM eUICC to support SAM functionalities e.g. smartphones, wearables.
Device Application	A third party application installed in a Device and that provides functionality which relies on SAM Service(s).
Device Application SAM Management Operations Interface	An interface offered by the LAA to Device Application to manage ASP SD and SAM Applets of SAM Services.
eIDAS	Electronic Identification, Authentication and Trust Services (eIDAS) is an EU regulation on electronic identification and trust services for electronic transactions. European Parliament, Council of the European Union: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
End User	The person using the Device.
eUICC	An eUICC as defined in SGP.01 [01] or SGP.21 [02]. Note: the eUICC can be removable, embedded or integrated.
IoT SAFE	Developed by the mobile industry, IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications.
Local Applet Assistant	A functional element in the Device that provides the capability to manage SAM Services.
Local ASP SAM Service Management Operations	Operations offered to the End User by the LAA to manage ASP SDs and SAM Applets of SAM Services.
mDL	The ISO/IEC 18013-5 mDL standard defines an mDL as a driver license which resides on a mobile device or requires a mobile device as part of the process to gain access to the driving license. It is being developed by the members of the mDL International Organization for Standardization (ISO/IEC JTC1/SC17/WG10).
Profile	Profile as defined by SGP.01 [01] or SGP.21 [02]
SAM Applet	An applet installed in an ASP SD.

Definitions	Meaning
SAM CI	A trusted third party in charge of the issuance, verification and revocation of SAM Certificates to SAM SMs and/or to SAM SD issuer.
SAM Command	Command to manage the lifecycle of a SAM Applet and ASP SD.
SAM Eligibility Check	Procedure to validate the eligibility of a eUICC and the Device for the installation and execution of a SAM Applet.
SAM eUICC	eUICC with a SAM SD and other SAM specific OS functions enabling the capabilities defined in this specification.
SAM Service	A secured service provided by an ASP. A SAM Service is composed of one or more SAM Applets and their associated data.
SAM SD	A Security Domain dedicated to ASP SD and their SAM Applets that is hosted in a SAM eUICC.
SAM SD Applet	An applet directly installed in a SAM SD.
SAM SM	An entity which, on behalf of the Application Service Provider, is in charge of managing SAM Applets through SAM Commands.
Security Domain	As defined by GlobalPlatform Card Specification [04].
Strong Confirmation	A mechanism to guarantee a high level of intent by which the End User will confirm some specific LASSMO or DASMO to proceed. Note: This can be achieved by dual confirmation (e.g. “Are you really sure you want to delete”), by use of some of the Device security mechanism (device lock, Fingerprint, etc.) - Implementation is OEM specific.
Synchronous Mode	A mode where the SAM Commands for a SAM SD are generated by a SAM SM and executed in the same connection session.
Trusted Service Manager (TSM).	As defined by GlobalPlatform Messaging Specification for Management of Mobile-NFC Services [3]

1.5 References

Ref	Document Number	Title
[1]	SGP.01	GSMA Embedded SIM Remote Provisioning Architecture
[2]	SGP.21	GSMA RSP Architecture Specification
[3]	GPS_SPE_002	GlobalPlatform Messaging Specification for Management of Mobile-NFC Services
[4]	GPC_SPE_034	GlobalPlatform Card Specification v.2.3
[5]	GSMA PRD AA.35	Procedures for Industry Specifications Product
[6]	RFC_2119	Network Working Group: Key words for use in RFCs to indicate requirement levels, BCP 14, RFC 2119, March 1997
[7]	ISO_7816-5	ISO/IEC 7816-5:2004 Identification cards — Integrated circuit cards — Part 5: Registration of application providers
[8]	ISO_18013-5	ISO/IEC 18013-5 Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application
[9]	GPD_SPE_075	GlobalPlatform Open Mobile API Specification Version 3.3
[10]	RFC_5280	Network Working Group: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008
[11]	TR-03159	BSI Technical Guideline TR-03159 Mobile Identities
[12]	ISO_23220	ISO/IEC 23220 Card and security devices for personal identification - Building blocks for identity management on mobile devices
[13]	TS 102 412	Smart Card Platform Requirements Stage 1 Release 16.0.0.

1.6 Conventions

“The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in this document are to be interpreted as described in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** [6].”

2 Requirements

2.1 Device Requirements

Req no.	Description
DEV1	Access from Device Application to SAM Applets (e.g. APDU commands) SHOULD be provided.
DEV2	If access from Device Application to SAM Applets is provided, this access SHALL be protected by an access control mechanism (e.g: GlobalPlatform SEAC)
DEV3	If access is granted, a Device Application MAY access the metadata of its SAM Services.

2.2 SAM SD Requirements

Req no.	Description
SAM_SD1	Communication between a SAM SD (or any SAM Applets within) and a SAM SM SHALL be protected in authenticity, integrity, confidentiality and against replay attacks.
SAM_SD2	A SAM SD SHALL support a secure channel protocol based on PKI for mutual authentication and secure channel messaging (e.g. SCP11)
SAM_SD3	A SAM SD MAY support Synchronous Mode (e.g. SCP11a)
SAM_SD4	A SAM SD SHOULD support Asynchronous Mode (e.g. SCP11c)
SAM_SD5	A SAM SD SHALL provide a Certificate chained up to a SAM CI recognised by a SAM SM in order to establish a secure channel.
SAM_SD6	A SAM SD SHALL be able to perform ASP SD personalization in a confidential way (e.g. CASD key agreement model)
SAM_SD7	A SAM SD SHOULD support a SAM memory reset to delete all its ASP SDs and SAM Applets.
SAM_SD8	The availability of the SAM Applet(s) to the Device SHALL be independent of any Profile state (e.g. enabled, disabled) in the eUICC.
SAM_SD9	A SAM SD SHALL provide a means for an Application Service Provider to securely isolate its SAM Applets from SAM Applets belonging to other Application Service Providers.
SAM_SD10	Any SAM Applet SHALL NOT use any identifier (e.g. AID) used by other SAM Applets.
SAM_SD11	A SAM SD SHALL allow a SAM SM managing/owning ASP SDs to delete its ASP SDs and all related data that belong to them.
SAM_SD12	A SAM SD SHALL reside on the SAM eUICC and SHALL exist outside of the ISD-R, ECASD and any ISD-P.
SAM_SD13	The SAM SD SHALL enforce that a given SAM SM is only able to manage ASP SDs and SAM Applets whose RID(s) are under the control of the ASP.
SAM_SD14	SAM SD Applet MAY be installed and personalised under the SAM SD during the personalisation of the SAM SD. Note: the management of SAM SD Applet is out of scope of this specification.
SAM SD15	A SAM SD SHALL be able to be used by several SAM SMs.
SAM_SD16	A SAM SD using a secure channel protocol based on PKI SHALL be able to be used by any SAM SM that presents a valid Certificate as defined in CERTPK3 requirement.
SAM_SD17	SAM Applet SHALL be able to read eUICC EID (e.g. read the EID)
SAM_SD18	Any SAM SD Applet SHALL NOT use any RID used by other SAM Applets.
SAM_SD19	AIDs assigned to Profile applets on an enabled Profile and AID assigned to SAM Applets SHOULD NOT conflict with each other. Note: Solutions could be implementation dependent. E.g. separated

Req no.	Description
	interfaces between SAM Applets and Profiles' applets could be considered as a solution
SAM_SD20	A SAM Applet MAY offer services for other SAM Applets belonging to different Application Service Providers via inter-application communications between both SAM Applets based on GlobalPlatform Global Services [4].

2.3 SAM Service and ASP SD Lifecycles Requirements

Req no.	Description
SAMA1	The following SAM Commands SHOULD be supported: - ASP SD creation and personalisation - ASP SD deletion - SAM Applet load - SAM Applet instantiation - SAM Applet lock - SAM Applet unlock - SAM Applet deletion
SAMA2	SAM Commands issued by a SAM SM or ASP SHALL be protected in authenticity, integrity and confidentiality.
SAMA3	Each ASP AID included in a SAM Command SHALL have an RID registered by the ASP at the ISO 7816 in order to avoid ASP AID conflicts.
SAMA4	SAM Commands issued by a SAM SM or ASP SHALL be protected against replay attacks. Note: This requirement could be covered either through the Secure Channel implementation or at application level (e.g. LAA, APDU commands limitation)
SAMA5	SAM Commands issued by a SAM SM or ASP MAY apply to multiple eUICCs.
SAMA6	SAM Commands issued by a SAM SM or ASP MAY be stored in a Device Application or remotely retrieved by the Device Application.
SAMA7	An ASP SHALL be able to send SAM Commands to their SAM Applets
SAMA8	An ASP SHALL be able to send SAM Commands to their ASP SDs.
SAMA9	SAM Applets and ASP SDs SHALL be managed via SAM Commands.
SAMA10	SAM Applets and their associated data SHALL be hosted in an ASP SD

2.4 SAM SM Requirements

Req no.	Description
SAM_SM1	A SAM SM MAY be a Trusted Service Manager (TSM).

Req no.	Description
SAM_SM2	A SAM SM SHALL provide a Certificate chained up to SAM CI recognised by SAM SD in order to establish a secure channel.
SAM_SM3	It SHALL be possible for an Application Service Provider to manage the content of its SAM Applet.
SAM_SM4	A SAM SM SHALL be able to manage its ASP SDs and SAM Applets on behalf of an Application Service Provider.
SAM_SM5	A SAM SM SHALL have a technical ability to delegate the management of the ASP SD and SAM Applets to ASP.
SAM_SM6	A SAM SM SHOULD support a secure channel protocol based on PKI for mutual authentication and secure channel messaging. For instance, a SAM SM may load and install a SAM Applet with SCP11 commands by targeting the SAM SD.
SAM_SM7	A SAM SM MAY support a secure channel protocol based on symmetric mutual authentication and secure channel messaging. For instance, a SAM SM may personalize a SAM Applet with SCP03 commands by targeting the ASP SD.
SAM_SM8	A SAM SM SHALL support a secure channel protocol based on SAM_SM6 or SAM_SM7
SAM_SM9	A SAM SM SHALL support a secure PKI and/or symmetric protocol based on mutual authentication and secure channel messaging.
SAM_SM10	SAM SM SHALL be able to collect the required information in order to ensure the eUICC/Device certification(s). Note: the information may be provided by the eUICC or/and external entity (e.g.: GP DLOA) to allow the SAM SM to read this information from an external database.

2.5 SAM Eligibility Check Requirements

The SAM Eligibility Check enables validation of the eligibility of an eUICC and a Device for the installation of a SAM Service. It relies on a set of eUICC and Device information shared with the relevant entities, which manage the installation of the SAM Service (e.g. the Device Application, the Device OS, the SAM SM and the ASP). This information is referenced herein as the SAM Eligibility Check information.

Req no.	Description
ELG0	A SAM eUICC SHALL support SAM Eligibility Check procedure to ensure the usability of SAM with a SAM SM and the LAA.
ELG1	A SAM eUICC SHALL declare for the available memory for the installation of SAM Services during the SAM Eligibility Check.
ELG2	A SAM eUICC SHALL declare the NFC services that are supported and accessible for SAM Applets during the SAM Eligibility Check.

ELG3	A SAM eUICC SHALL declare the UWB [13] services that are supported and accessible for SAM Applets during the SAM Eligibility Check.
ELG4	A SAM eUICC SHALL declare the supported SAM Commands during the SAM Eligibility Check.
ELG5	A SAM eUICC SHALL declare the Java Card version supported, if any during, the SAM Eligibility Check.
ELG6	A SAM eUICC SHALL declare if the Asynchronous or/and Synchronous Mode is supported
ELG7	If the Asynchronous Mode is supported, the SAM eUICC SHALL provide the means to perform a SAM Eligibility Check with this mode.
ELG8	If the Synchronous Mode is supported, the SAM eUICC SHALL provide the means to perform a SAM Eligibility Check with this mode.
ELG9	Relevant information collected during the SAM Eligibility Check MAY be shared with the entities which manage the installation of the SAM Service (e.g. the Device Application, the Device OS, the SAM SM and the ASP).
ELG10	If Open Mobile API [9] is supported, the Device SHALL declare the Open Mobile API version during the SAM Eligibility Check.
ELG11	A SAM eUICC SHALL provide the Certificate Issuer of the SAM SD Certificate during the SAM Eligibility Check.
ELG12	A SAM eUICC SHALL declare supported cryptographic algorithm and its configuration during the SAM Eligibility Check.
ELG13	The Device SHALL declare whether the eUICC is removable, embedded or integrated.
ELG14	All information shared during the SAM Eligibility Check to the SAM SM SHALL be protected by the SAM eUICC against manipulation: integrity and authenticity SHALL be assured by design.
ELG15	A SAM eUICC SHALL be able to declare some SAM Eligibility Check Information which is not defined in this specification in a generic way during the SAM Eligibility Check.
ELG16	A SAM eUICC SHALL be able to declare Card Recognition Data and Card Capability Data as specified in GP Card Specification [4] during the SAM Eligibility Check.
ELG17	eUICC/Device certification(s) collected during the SAM Eligibility Check MAY be shared with the entities which manage the installation of the SAM Service (e.g. the Device Application, the Device, the SAM SM and the ASP).

2.6 ASP Requirements

Req no.	Description
ASP_SD1	An ASP SD SHALL have associated metadata.

Req no.	Description
ASP_SD2	An ASP SD SHALL be associated to one or more SAM Services.
ASP_SD3	An ASP SD MAY host one or several SAM Applets.

2.7 LAA Requirements

Req no.	Description
LAA1	The LAA SHALL be able to select a SAM SD.
LAA2	The LAA SHALL be able to access the metadata of the installed SAM Services.
LAA3	The information available in SAM Eligibility Check information SHALL be readable by the LAA.
LAA4	The LAA SHALL be able to provide the information available in SAM Eligibility Check information to a SAM SM.
LAA5	The LAA SHOULD provide to the End User the capability to manage SAM Services through LASSMO.
LAA6	LAA Operations MAY include: - “List SAM Services” - “Lock SAM Service” - “Unlock SAM Service” - “Delete SAM Service” - “SAM SD Memory Reset“
LAA7	The LAA SHOULD provide to a Device Application the capability to deploy and manage ASP SD and SAM Applets through DASMO.

2.8 Metadata Requirements

Req no.	Description
METADATA1	The metadata of a SAM Service SHALL be able to include the name of the ASP and the name of the service. Note: The metadata extensibility and the accessibility of each field in the metadata to the LAA is FFS.
METADATA2	Some information defined in METADATA1 MAY be presented to the End User.
METADATA3	The metadata of a SAM Service SHALL include the name of the ASP.
METADATA4	The metadata of a SAM Service MAY include the name of the SAM Service.
METADATA5	The metadata of a SAM Service MAY include the URI of the associated SAM SM.

2.9 PKI Requirements

Req no.	Description
CERTPK1	A SAM SD SHALL verify the validity of the Public Key Certificate of the SAM SM.
CERTPK2	A SAM CI SHALL be able to revoke a Public Key Certificate that it signs.
CERTPK3	A Public Key Certificate SHALL be considered as valid if: • it has a valid signature • it is signed by SAM CI, or a trusted chain of Certificates up to SAM CI. ○ If used, X.509 Certificate Path validation SHALL follow the process defined in RFC 5280 ○ If used, GP certificate SHALL provide the same functionality to perform name chaining for certificate Path validation • it has not been revoked, and no Certificate in the trust chain has been revoked • it has not expired If any of these applicable verifications fail, the Public Key Certificate SHALL be considered as invalid. Note: The eUICC is not required to check the Certificate validity period or the revocation status.
CERTPK4	SAM SD issuer SHALL be able to manage remotely the public keys and certificates inside the SAM SD.

2.10 SAM CI Requirements

The following requirements apply if the secure channel protocol based on PKI is supported:

Req no.	Description
CERTCI1	A SAM CI SHALL verify that the SAM SM Certificate includes the RIDs that are authorised to be used for a SAM Applet.
CERTCI2	A SAM SD SHALL be able to support multiple SAM CIs.

Note: Certificates for SAM SM(s) and for SAM SD Issuer can be issued by different SAM CIs

2.11 SAM SM Certificate Requirements

The following requirements apply if the secure channel protocol based on PKI is supported:

Req no.	Description
SAM_SMCERT	SAM SM Certificate SHALL include a list of allowed ASP RID(s).

2.12 LASSMO Requirements

These requirements are considered in case LAA5 is performed:

Req no.	Description
LASSMO1	LASSMO SHALL be performed by the LAA.
LASSMO2	The LAA MAY manage LASSMO through SAM Commands retrieved from the corresponding ASP Device Application or retrieved dynamically from a SAM SM. Note: In the latter case, the URI of the targeted SAM SM may be retrieved from the ASP Device Application or from the SAM Service Metadata.
LASSMO3	LASSMO MAY include the LAA Operations defined in LAA6.
LASSMO4	If a SAM Service has been installed through a Device Application, then the LAA MAY notify the Device Application of execution of LASSMO relative to the SAM Service.
LASSMO5	If a SAM Service has been installed through the SAM SM, then the LAA MAY notify the SAM SM of execution of LASSMO relative to the SAM Service.
LASSMO6	The LAA MAY use some information defined in Metadata related to an installed SAM Service to provide the list of SAM Services through LASSMO, e.g. to display the Device Application name related to a SAM Service.

2.13 DASMO Requirements

The following additional requirements apply to a Device which supports DASMO:

Req no.	Description
DASMO1	DASMO SHALL allow ASP via a Device Application to create an ASP SD and to deploy its SAM Applets.
DASMO2	DASMO SHALL allow ASP via a Device Application to delete an ASP SD and its associated SAM Applets.
DASMO3	DASMO SHALL allow ASP via a Device Application to update an ASP SD and its associated SAM Applets.
DASMO4	DASMO1, DASMO2, and DASMO3 operations SHALL be performed in a secure mode (e.g. secured with SCP11).
DASMO5	DASMO SHALL allow ASP via a Device Application to exchange data with its SAM Applets.
DASMO6	DASMO SHALL allow ASP via a Device Application to lock and unlock its SAM Applets, as defined by GlobalPlatform Card specification.
DASMO7	DASMO SHALL allow ASP via a Device Application to retrieve the list of its installed SAM Services.
DASMO8	All DASMO between a Device Application and its ASP SDs or its SAM Applets SHALL be protected by an access control mechanism (e.g: GlobalPlatform SEAC).
DASMO9	Prior to performing an ASP SD creation or SAM Applet deployment through DASMO, SAM Eligibility Check SHALL be performed.

Req no.	Description
	The SAM Eligibility Check information SHALL be shared with the relevant entity which manages the installation of the SAM Applet (e.g. the Device Application, the Device OS, the SAM SM)
DASMO10	Prior to performing a SAM Applet update through DASMO, SAM Eligibility Check MAY be performed.

2.14 User Intent and Confirmation Requirements

The following requirements apply to a Device which interacts with End User via a user interface.

Req no.	Description
UIR1	The LASSMO MAY require Strong Confirmation for some operations. Note: the list of these operations is implementation specific.
UIR2	LASSMO “SAM SD Memory Reset” SHOULD require Strong Confirmation.
UIR3	The DASMO MAY require Strong Confirmation for some operations. Note: the list of these operations is implementation specific.
UIR4	The LASSMO SHALL require user intent for some operations. Note: the list of these operations is implementation specific.
UIR5	The user intent SHALL either be captured at real time or be given by the End User in advance. Note: e.g.: service agreement, or explicit device settings.

3 General Architecture

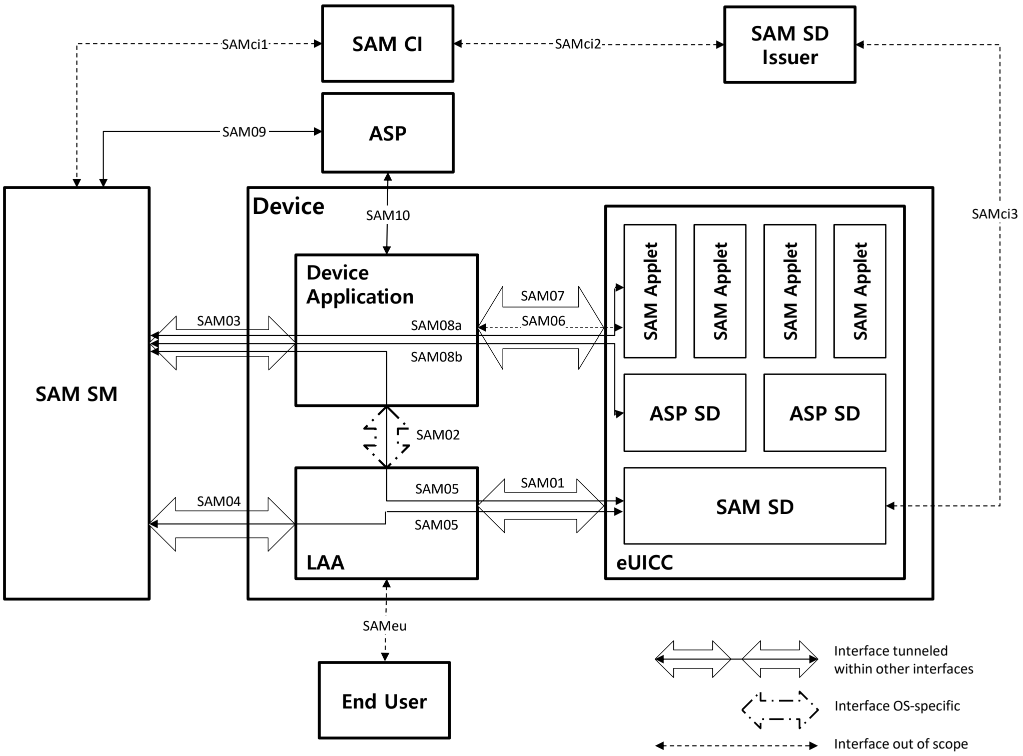

Figure 1 - General Architecture

3.1 Architecture Overview

This section contains the graphical description of the SAM architecture. The following entities are defined in section 1.5 “Definitions”:

Application Service Provider (ASP), SAM SM, Device Application, LAA (Local Applet Assistant), SAM Applet, ASP SD, SAM SD, eUICC, End-User, SAM CI.

3.2 Interfaces

3.2.1 eUICC – LAA (SAM01)

This interface is used to convey LASSMO (originated from SAM SM or End User) and DASMO commands e.g.: tunnels SAM05 messages.

3.2.2 Device Application – LAA (SAM02)

The interface between a Device Application and the LAA is OS-specific.

3.2.3 SAM SM – Device Application (SAM03)

This interface tunnels SAM08a, SAM08b and SAM05 messages between a SAM SM and a Device Application.

3.2.4 SAM SM – LAA (SAM04)

This interface tunnels SAM05 messages between a SAM SM and the LAA.

3.2.5 SAM SM – SAM SD (SAM05)

The interface between SAM SM and SAM SD e.g. to manage ASP SDs.

3.2.6 Device Application – SAM applet (SAM06)

The interface between a Device application and its corresponding SAM applet. This interface is out of scope of this specification.

3.2.7 Device Application – eUICC (SAM07)

The interface between a Device Application and the eUICC to convey SAM06, SAM08a and SAM08b messages to a SAM applet or to an ASP SD respectively.

3.2.8 SAM SM – SAM applet (SAM08a)

The interface between a SAM SM and a SAM applet.

3.2.9 SAM SM – ASP SD (SAM08b)

The interface between a SAM SM and an ASP SD.

3.2.10 ASP – SAM SM (SAM09)

The interface between an ASP and a SAM SM.

3.2.11 ASP – Device Application (SAM10)

The interface between an ASP and a Device Application.

3.2.12 End User LAA (SAM_{eu})

The interface between the End User and the LAA. This interface is out of scope of this specification.

3.2.13 Certificate Issuer – certificate requester (SAM_{cix})

SAMcix (with x being 1, 2 or 3) is the interface used:

- by the certificate requester, to send a CSR (certificate signing request) to the Certificate Issuer;
- by the Certificate Issuer, to release certificates to the requester.

The specification of the SAMcix interface is out of scope.

Annex A Use Cases (Informative)

The following section defines use cases for Secured Applications for Mobile.

A.1 Use Case 1

The End User desires to deploy a banking application (e.g. offering contactless payment and other financial services) within the Device linked with a SAM Applet.

The following steps occur:

- The End User browses a Device Application store and locates a banking Device Application, which is designed to work with its corresponding banking SAM Applet in the eUICC.
- The SAM Applet's provisioning in the eUICC could be triggered at some point in the Device Application installation, during its first use, or later (as the user signs up for related services for example) – user consent is expected to be captured. Personalization data and or the provisioning of the SAM Applet into the eUICC may be driven by an external server.
- The End User is able to use the banking Device Application in conjunction with the banking SAM Applet.
- If no longer needed, the End User deletes the banking Device Application, which may cause the banking SAM Applet to be deleted as well after user validation.
- If no longer needed, the End User can discontinue the secure service provided by the banking application, which may cause the banking SAM Applet to be deleted.
- Deletion of the banking SAM applet could also be triggered by the SP (e.g. bank).

A.2 Use Case 2

An End User manages a transport application independently of the lifecycle of their Profiles:

- An End User downloads a Profile as part of a Telecom Subscription.
- The End User downloads a transport Device Application, which has an associated transport SAM Applet.
- Once installed and configured, the End User is able to use the transport Device Application.
- The End User subsequently downloads another Profile as part of another Telecom Subscription.
- The End User disables the first Profile, then enables the second Profile.
- The End User is able to use their transport Device Application, interacting with its corresponding transport SAM Applet without problem.
- The End User disables all Profiles.
- The End User is still able to use the transport Device Application, interacting with its corresponding transport SAM Applet without problem.
- The End User deletes the two Profiles.
- The End User is still able to use their transport Device Application, interacting with its corresponding transport SAM Applet without problem.
- The End User deletes the transport Device Application, which may cause the transport SAM Applet to be deleted as well after user validation.

A.3 Use Case 3

An End User manages an identity SAM Applet without any Profiles installed.

- There are no Profiles installed on the eUICC.
- Using WiFi, the End User downloads an identity Device Application, which has an associated identity SAM Applet.
- After End User validation, both the identity Device Application and the identity SAM Applet are installed in the Device and in the eUICC respectively.
- Once configured, the End User can use the Device application associated with the identity SAM Applet without any profiles installed on the eUICC.

A.4 Use Case 4

An End User manages different Device Applications associated with different SAM Applets.

- The End User has installed a number of Device Applications.
- Some of the Device Applications have an associated SAM Applet.
- Whenever the End User is using a particular Device Application, the associated SAM Applet can be used, independently of the other SAM Applets associated with other Device Applications.
- The End User is able to manage the SAM Applets through a UI. For instance to delete a SAM Applet in case of insufficient SAM memory. In this case the associated Device Application may not work anymore.

A.5 Use Case 5

Secured Applications for Mobile – GSMA IoT SAFE (SIM Applet For secure End-to-End Connectivity) Use Case.

IoT SAFE (IoT **S**IM Applet For Secure End-to-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications.

In this use case, an IoT service provider wishes to leverage an eUICC as a secure, standards-based means of protecting data exchanged between a device, such as a security camera, and their remote service platform (server/cloud). The IoT service shall be available irrespective of the mobile network operator currently enabled.

When the eUICCs are securely personalised, an IoT SAFE applet is installed onto each eUICC into a SAM security domain for secure mobile applets. The IoT service provider can personalise the IoT SAFE applet with its credentials. Depending upon the device, the credentials could be a symmetric key or an asymmetric key pair and associated X.509 certificate. The applet provides security services (such as signing, key agreement, etc.) using these credentials, so that the keys themselves are never exposed outside of the eUICC.

For example, when each camera connects to the mobile network, the network and eUICC in the camera mutually authenticate each other using standard 3GPP signalling procedures. The application in the camera then establishes an internet connection to the service platform by calling APIs which interface with the IoT SAFE applet and then initiates a mutual authentication procedure to establish a secure (D)TLS connection with the remote IoT service provider platform. The device side (D)TLS mutual authentication steps are performed using the IoT SAFE applet and its stored credentials. At the end of the mutual authentication procedure, secure IP communication can take place between the camera and IoT service platform.

A.6 Use Case 6

Secured Applications for Mobile – Mobile Identification supporting eIDAS level substantial as well as mDL

The use of mobile devices for mobile services is one of the dominant global trends. Mobile applications and the mobile device as customer media substitute the home or office PC for access to online services and classical media like chipcards or paper ID as customer media for payment, ticketing etc. New applications are often only offered for mobile devices.

Overall, the mobile device is becoming the most common interface between the customer and his service providers.

For the digitalization of business process, the secure identification and authentication of end customers is a key requirement.

On one side, the eIDAS regulation of the EU is defining three levels of assurance for electronic identification. The two highest levels “high” and “substantial” are demanding the usage of secure elements (see BSI Technical Guideline TR-03159 Mobile Identities).

On the other end, mDL allows people to use a mobile phone as a form of secure digital ID. Citizens can use their ID everywhere (especially where no National ID card program is deployed) - at point of sale, for fast entry into every establishment, at the roadside, across borders. When the Driver’s License is placed on the owner device, it is called a Mobile Driver’s License or mDL. ISO 18013-5 standard details how to obtain and trust data from a mobile ID on a phone. mDL requires data encryption algorithms and communication security to combat fraud, reduce identity theft. Moreover, the mobile ID brings minimization of data as well as a selective disclosure of it to ensure privacy. ISO 18013-5 does not require a card reader for acceptance; it can interface through, at least, Bluetooth and NFC (mDL leverages all existing standards such as FIPS, ICAO and ISO).

Since the eUICC is a well-specified secure platform and gaining market share rapidly, it is the ideal platform for hosting Mobile ID applications which are offering high security.

The mobile id use case consists of the following steps (issuing phase, personalization phase, usage phase):

In the following steps description, it is assumed that the data provisioning process takes into account identity proofing, holder matching (binding to the device/data), holder authentication and checking of active status of the data. All the features therefore being possibly subject to an attestation (e.g. as currently envisioned by ISO/IEC 23220-5)

- **Issuing Phase, Application Service Provider (ASP) Installation:** The End User downloads the ASP application from an application store. The ASP application has the need of secure End User identification and integrates software components to perform this.

- **Issuing Phase, Eligibility Check**: The ASP application performs an eligibility check (EC) of the device, including the eUICC. In case of sufficient capabilities, the installation of the mobile id applet will be triggered and authorised by the End User.
- The eligibility check verifies for example the availability of sufficient free memory of the eUICC or the supported JavaCard version or libraries of the eUICC. Additionally, information concerning certification of eUICC is relevant for ASP.
- **Issuing Phase, SAM Security Domain registration**: In case of a positive result of the EC, the ASP will register the device as customer medium and request a secure space in the SAM Security Domain.
- **Issuing Phase, SAM-Applet Installation**: The ASP triggers the installation of the SAM-Applet in the SAM Security Domain. Preferably this is done by using offline methods. As a result, the mobile id applet is installed within the SAM Security Domain of the eUICC and the access rights to the SAM-Applet are transferred to the ASP.
- **Personalization Phase**: Before using the mobile id applet, it needs to get personalized with valid and trustable End User identity data. Different procedures to perform this personalization are possible. In any case, a holder binding process is required. It allows the issuing authority to express its confidence that the identity data has been provisioned to the legitimate holder and on a device under the control of the holder. Data are then bound to the holder. One solution could be to use a physical NFC ID card of the End User to retrieve the End User id data and to personalize this into the mobile id applet (derived credentials). Normally, this will involve communication with a backend system.
- **Usage Phase:** After personalization of the mobile id applet, the End User can identify and authenticate against the ASP using the End User identity data stored securely within the mobile ID applet and the authentication protocols provided by the mobile ID applet.

Additionally, the following life cycle management procedures needs to be addressed:

1. Update of End User identity data in case of changes (e.g. address change or additional attributes)
2. Discontinuation of usage, due to the following reasons: End User removes the service, service provider triggers the removal of the service, identity service provider discontinues the id service availability, date of expiry (of Mobile ID or origin eID) passed.
3. Migration to a new device, maintain the End User identity data.
4. Device Termination / Refurbishment / Factory Reset: Removal of all End User data.

Annex B Document Management

B.1 Document History

Version	Date	CR Number	Brief Description of Change	Approval Authority	Editor / Company
V1.0	8 June 2021	CR0001R05	SAM.01 scope	ISAG	Yolanda Sanz, GSMA
		CR0002R06	SAM Use Cases		
		CR0004R03	IoT SAFE Use Case		
		CR0005R01	Add clarification on the scope		
		CR007R02	Mobile ID Use case		
		CR008R01	SAM eUICC Definition		
		CR009R04	Mobile ID Use Case missing a reference to mDL		
		CR010R01	SAM SD requirements		
		CR017R01	SAM Definitions and abbreviations		
			To revert the changes made in CR017R01		
		CR017R02	SAM Definitions and abbreviation		
		CR019R01	SAM Revision of SAM SD requirements		
		CR012R01	SAM SD requirements		
		CR013R01	SAM Application Lifecycle requirements		
		CR018R02	SAM applet and Editorial CR		
		CR0021R01	Device access control requirement		
		CR0022R02	Additional SAM SD requirements		
		CR023R01	Definition of Application Service Provider		
		CR024R01	SAM SD Requirements		
		CR925R01	SAM Application Lifecycle requirements		
		CR020R02	SAM definitions		
		CR026R01	Additional set of requirements on secure commands		
		CR027R03	Introducing multiple ASP Applets per ASP SD		
		CR028R01	PKI Requirements		
		CR014R03	SAM SM Requirements		
		CR015R03	PKI Requirements		
		CR029R04	LAA requirements		
		CR0030R01	SAM Eligibility Check Requirements		
		CR0031R02	SAM LASMO Requirement		

		CR0032R01	Device Application SAM Management Operations Interface requirements		
		CR0033R02	SAM Additional Eligibility Check Requirements		
		CR0035R01	DASMO Update functionality		
		CR0036R02	Additional set of requirements for SAM Eligibility Check		
		CR0037R01	Device Application Definition		
		CR0038R01	SAM-DASMO4		
		CR0039R02	SAM REQ without LAA		
		CR016R06	SAM Architecture		
		CR042R01	SAM UX Requirement		
		CR043R01	Definition updates		
		CR044R01	ASP Service Update		
		CR040R01	Further requirement regarding Eligibility Check		
		CR046R01	SAM DASMO Updates V2		
		NA	To fix some issues		
		CR047R01	Device and LAA requirements updates		
		CR048R01	Eligibility requirements updates		
		CR045R03	UX requirements		
		CR049R01	LASMO Updates and additional requirements		
		CR053R00	SAMA Requirements		
		CR050R01	Requirement SAMA6		
		CR051R02	Device Application access to Applet		
		CR056R03	Generic Applets		
		CR057R01	Multiple SAM SM		
		CR0058R00	SAM Service updated		
		CR0060R00	eUICC identification by SAM Applet		
		CR0062R01	Further Multiple SAM SM requirements		
		CR0054R03	Additional ELG requirements		
		CR0061R00	SAM Generic Applet		
		CR0064R01	Definition of term “Device”		
		CR0065R01	Additional ELG requirement		
		CR0066R01	Reference		

		CR0070R01	Editorial Changes		
		CR0068R01	Inconsistencies fixed		
		CR0071R01	Editor’s note review		
		CR0069R03	Internal SAM Applet communication		
		CR0072R02	CI Definition		
		CR0073R01	Clarification on User Interaction		
		CR0074R07	Support of existing Root CIs form SGP.21		
		CR0076R01	UIR requirements clarification		
		CR0077R01	SAM SD Certificate Management		
		CR0075R04	Description of SAM General Architecture		

Other Information

Type	Description
Document Owner	Yolanda Sanz
Editor / Company	GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.