

Secured Applications for Mobile
Version 1.2
27 January 2025

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

Copyright © 2025 GSM Association

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.

Antitrust 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 **4**
1.1 Overview 4
1.2 Scope 4
1.3 Abbreviations 4
1.4 Definitions 5
1.5 References 9
1.5.1 1.5.1 Informative References 9
1.6 Conventions 10
2 Requirements **10**
2.1 Device Requirements 10
2.2 SAM SD Requirements 10
2.3 SAM Service and ASP SD Lifecycles Requirements 11
2.4 SAM SM Requirements 12
2.5 SAM Eligibility Check Requirements 13
2.6 ASP SD Requirements 14
2.7 LAA Requirements 14
2.8 Metadata Requirements 15
2.9 PKI Requirements 15
2.10 SAM CA Requirements 16
2.11 ASP Certificate Requirements 16
2.12 SAM SM Certificate Requirements 16
2.13 LASSMO Requirements 16
2.14 DASMO Requirements 17
2.15 User Intent and Confirmation Requirements 18
2.16 SAM SD Certification Requirements 18
3 General Architecture **19**
3.1 Architecture Overview 19
3.2 Interfaces 19
3.2.1 eUICC – LAA (SAM01) 19
3.2.2 Device Application – LAA (SAM02) 19
3.2.3 SAM SM – Device Application (SAM03) 19
3.2.4 SAM SM – LAA (SAM04) 20
3.2.5 SAM SM – SAM SD (SAM05) 20
3.2.6 Device Application – SAM applet (SAM06) 20
3.2.7 Device Application – eUICC (SAM07) 20
3.2.8 SAM SM – SAM applet (SAM08a) 20
3.2.9 SAM SM – ASP SD (SAM08b) 20
3.2.10 ASP – SAM SM (SAM09) 20
3.2.11 ASP – Device Application (SAM10) 20
3.2.12 End User LAA (SAM_{eu}) 20
3.2.13 Certificate Authority – certificate requester (SAM_{cix}) 20
Annex A Use Cases (Informative) **21**

A.1 Use Case 1 21
A.2 Use Case 2 21
A.3 Use Case 3 22
A.4 Use Case 4 22
A.5 Use Case 5 22
A.6 Use Case 6 23
A.7 **Use Case 7** 26
Annex B SAM Certificate Policy (CP) **29**
B.1 Role of the SAM CP and Other Practice Documents 29
B.1.1 SAM PKI Participants 30
B.1.2 Participants in TLS chain for Public CA 31
B.1.3 Participants in TLS chain for SAM CA 31
B.2 Certificate Authority 32
B.3 Subscribers 33
B.4 Relying Parties 33
B.5 Policy Authority 33
B.6 Other Participants 34
B.6.1 Auditors 34
B.6.2 Incident Coordinator 34
B.7 Certificate Usage 34
B.7.1 Appropriate Certificate Uses 34
B.8 Certificate Life-Cycle Operational Requirements 34
B.8.1 Certificate Application 34
B.8.2 Who Can Submit a Certificate Application 35
B.8.3 Enrolment Process and Responsibilities 35
B.8.4 Certificate Signing Request (CSR) 35
Annex C SAM Ecosystem Description (Informative) **36**
C.1 Actor-to-Role Association Models 36
C.1.1 Actor-to-Role Association Models for SAM CA 36
C.1.2 Actor-to-Role Association Models for SAM Service deployment 39
C.2 SAM Service Issuance Models 42
Annex D Document Management **46**
D.1 Document History 46
Other Information 50

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)
CA	Certificate Authority
CP	Certificate Policy
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DASMO	Device Application SAM Management Operations interface
ECASD	eUICC Controlling Authority Security Domain
ECC	Elliptic Curve Cryptography
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)
KLOC	Confidential Key Loading Off-card Certificates
KLCC	Confidential Key Loading Card Certificates
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
OID	Object Identifier
PA	Policy Authority
PKCS	Public-Key Cryptography Standard

Abbreviation	Definition
AID	Application Identifier (as defined in ISO 7816)
PKI	Public Key Infrastructure
RID	Registered application provider Identifier (as defined in ISO 7816)
SAM	Secured Applications for Mobile
SAM SM	SAM Service Manager
SCP	Secure channel protocol
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	A remote entity responsible for providing and managing its SAM Applet(s), and additionally managing their own Device Application(s).
ASP AIDs	AIDs used by an ASP for its SAM Service(s) (e.g. ASP SD AID, SAM Applet AID…).
ASP Identifier	An identifier which uniquely identifies an ASP within the allocation scheme. Note: An ASP can be assigned with multiple ASP Identifiers from different allocation schemes (e.g., RID, OID, URI, etc).
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 digital representation of information which at least: • Identifies its issuing Certificate Authority • Names or identifies the Subscriber of the Certificate • Contains the Subscriber's public key • Identifies its operational period Is digitally signed by the issuing Certificate Authority
Certificate Applicant	An individual representing the Subscriber that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorised agent of the Certificate Applicant) to a CA for the issuance of a Certificate by completing the naming document.

Definitions	Meaning
Certificate Authority	An entity authorised to issue, manage, revoke, and renew Certificates.
Certificate Revocation List	A list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Device	Electronic equipment used in conjunction with a SAM eUICC to support SAM functionalities e.g. smartphones, wearables.
Device Application	An ASP 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.
Incident Coordinator	Central point for notification and coordination in the event of a Security Incident.
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	Operations offered to the End User by the LAA to manage ASP SDs and SAM Applets of SAM Services.

Definitions	Meaning
Management Operations	
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).
Object Identifier	A globally unique numeric value that is granted by various issuing authorities to identify data elements, syntaxes, and other parts of distributed applications.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKI Participant	An individual or organisation that is one or more of the following within a PKI: either a CA, a Subscriber, or a Relying Party.
Profile	Profile as defined by SGP.01 [01] or SGP.21 [02]
Policy Authority	A Policy Authority (PA) is an organisation or administrative unit that defines and monitors policies for the management and operation of the PKI.
Public CA	A Certificate Authority, commonly used to issue Certificates for public Internet purposes, which is not subject to the SAM Certificate Policy as defined in this specification.
Public Key Infrastructure	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key Certificates.
Relying Party	Entity that receives a Certificate with a digital signature verifiable with the public key listed in the Certificate, and is in a position to assess the trust in the authentication information provided by Certificate depending on the policy governing the PKI and the Certificate verification.
SAM Applet	An applet installed in an ASP SD. NOTE: Developers of Java Card™ applets are referred to the TCA Stepping Stones [i1] document that provides important applet development guidelines, best practices and security considerations.
SAM CA	A trusted third party in charge of the issuance, verification and revocation of SAM Certificates to ASP, SAM SMs and/or to SAM SD issuer.
SAM Certificate Policy	A policy that addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of Certificates used in SAM ecosystem; see annex B.
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.

Definitions	Meaning
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. SAM SM interacts with a SAM-SD for which it has access to ASP credentials.
Security Domain	As defined by GlobalPlatform Card Specification [04].
Security Incident	The moment in time between detection of a violation of the confidentiality or integrity of a (personal) computer and the mitigation of the effects of that violation.
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.
SubCA	A CA whose Certificate is signed by another CA.
Subject	The holder of a private key corresponding to a public key. The term “Subject” can, in the case of an SAM PKI Certificate, refer to the Subscriber requesting the Certificate.
Subscriber	The entity who requests a Certificate (e.g., a manufacturer). The Subscriber is capable of using, and is authorised to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organisation acts as a Subscriber. The Subscriber Agreement contains the Certificate Application.
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.
[14]	RFC 3647	Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003. http://www.ietf.org/rfc/rfc3647.txt
[15]	RFC 2986	PKCS #10: Certification Request Syntax Specification https://datatracker.ietf.org/doc/html/rfc2986
[16]	GPC_SPE_093	GlobalPlatform Card Specification v2.2 Amendment F: Secure Channel Protocol '11' v1.4

1.5.1 1.5.1 Informative References

Ref	Document Number	Title
[i1]	TCA Stepping Stones	Stepping Stones for Java Card Applet Developers, Version 1.0

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 RFC_2119 [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 CA 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	There SHALL be a means to uniquely identify a SAM Applet.

Req no.	Description
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 their SAM Applets whose RID(s) are allowed to be used by ASP according to CERTCA1.
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	VOID
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].
SAM_SD21	A SAM SD SHALL be able to support multiple SAM CAs.

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 SHALL be protected in authenticity, integrity and confidentiality.
SAMA3	Each ASP AID included in a SAM Command SHALL have an RID registered in accordance with ISO/IEC 7816.
SAMA3a	The provisioning of AID of SAM Applets to avoid ASP AID conflicts, SHOULD be defined by the RID's owner and is out of scope of this specification.
SAMA4	SAM Commands issued by a SAM SM SHALL be protected against replay attacks.

Req no.	Description
	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 MAY apply to multiple eUICCs.
SAMA6	SAM Commands issued by a SAM SM MAY be stored in a Device Application or remotely retrieved by the Device Application.
SAMA7	An ASP represented by a SAM SM SHALL be able to send SAM Commands to manage their SAM Applets
SAMA8	An ASP represented by a SAM SM SHALL be able to send SAM Commands to manage 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).
SAM_SM2	In order to manage the ASP-SD (e.g.: creation, deletion…) and their SAM applets, an SAM SM SHALL establish an end-to end secure channel to the SAM SD using an ASP credentials recognised by SAM SD.
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 ASP SDs and SAM Applets on behalf of their Application Service Provider.
SAM_SM5	VOID
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).

Req no.	Description
	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.
SAM_SM11	SAM SM SHALL use the (D)TLS Certificate (as defined in SAM_SMCERT1) to establish a (D)TLS secured channel from the LAA to the SAM SM

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 and the SAM SM).
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 list of the Certificate Authority(s) of the SAM SD Certificate(s) 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 and the SAM SM).

2.6 ASP SD Requirements

Req no.	Description
ASP_SD1	An ASP SD SHALL have associated metadata.
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.
ASP_SD4	ASP SD associated metadata SHALL be able to include ASP Identifier(s).

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.
METADATA6	The metadata of a SAM Service MAY include one or more ASP Identifiers of the ASP.

2.9 PKI Requirements

Req no.	Description
CERTPK1	A SAM SD SHALL verify the validity of the Public Key Certificate of the ASP.
CERTPK2	A SAM CA 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 chains up a SAM CA, or a Public CA (for TLS Certificate)
	  ○ 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 CA Requirements

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

Req no.	Description
CERTCA1	A SAM CA SHALL verify that the ASP Certificate includes the RIDs that are authorised to be used for a SAM Applet.
CERTCA2	A SAM CA SHALL comply with SAM certificate policy defined in Annex B

Note: Certificates for ASP and for SAM SD Issuer can be issued by different SAM CAs

2.11 ASP Certificate Requirements

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

Req no.	Description
ASP_CERT	ASP Certificate SHALL include a list of allowed ASP RID(s).
ASP_CERT2	The ASP Certificate SHALL chain up to a SAM CA

Note: Certificates for ASP and for SAM SD Issuer can be issued by different SAM CAs

2.12 SAM SM Certificate Requirements

Req no.	Description
SAM_SMCERT1	The SAM SM Certificate for (D)TLS establishment SHALL chain up to a Public CA or SAM CA.

2.13 LASSMO Requirements

These requirements are considered in case LAA5 is performed:

Req no.	Description
LASSMO1	LASSMO SHALL be performed by the LAA.

Req no.	Description
LASSMO2	The LAA MAY manage LASSMO through SAM Commands retrieved from the corresponding 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 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.

2.14 DASMO Requirements

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

Req no.	Description
DASMO1	DASMO SHALL allow the SAM-SM on behalf of ASP to create an ASP SD and to deploy its SAM Applets via a Device Application.
DASMO2	DASMO SHALL allow the SAM-SM on behalf of ASP to delete an ASP SD and its associated SAM Applets via a Device Application.
DASMO3	DASMO SHALL allow the SAM-SM on behalf of ASP to update an ASP SD and its associated SAM Applets via a Device Application.
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 update or read the content of its SAM Applets.
DASMO6	DASMO SHALL allow the SAM-SM on behalf of ASP to lock and unlock its SAM Applets via a Device Application, as defined by GlobalPlatform Card specification.
DASMO7	DASMO SHALL allow the SAM-SM on behalf of ASP to retrieve the list of its installed SAM Services via a Device Application.
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.

2.15 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.

2.16 SAM SD Certification Requirements

Req no.	Description
CERT.01	The evaluation assurance level of the SAM SD Protection Profile (e.g.: PP-module) SHALL be (at least) EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 (EAL 4+)

3 General Architecture

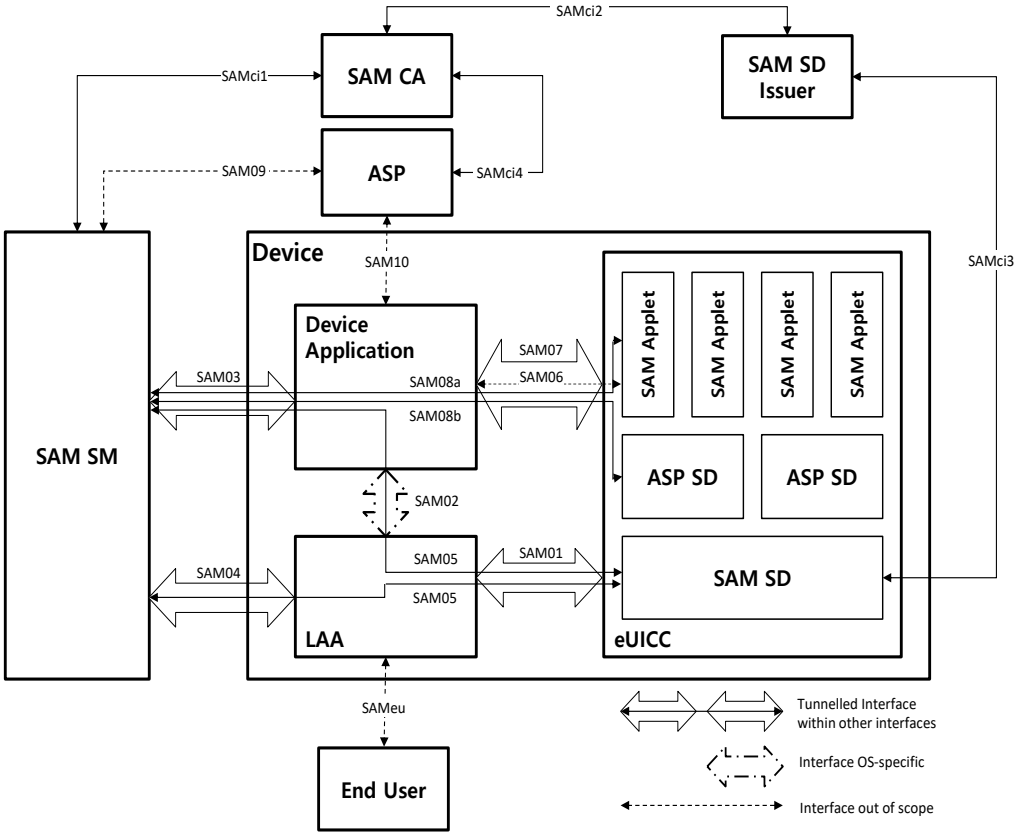


Figure 1 - General Architecture

An interface can tunnel another interface (e.g., SAM04 tunnels SAM05). Tunnelling interface (e.g., SAM04) encapsulates messages or packets of tunnelled interface (e.g., SAM05).

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 CA.

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. The same protocol is used for SAM04 and SAM03 but with different endpoints.

3.2.5 SAM SM – SAM SD (SAM05)

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

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. This interface is out of scope of this specification.

3.2.11 ASP – Device Application (SAM10)

The interface between an ASP and a Device Application. This interface is out of scope of this specification.

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 Authority – certificate requester (SAM_{cix})

SAMcix (with x being 1, 2, 3 or 4) is the interface used:

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

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.

- **Termination:** Different conditions can result in the termination of the Mobile ID application. Some of them are listed in the paragraph below. It is important to mention, that also in the termination lifecycle phase, the mobile ID applet must not leak any sensitive information or keys.

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

1. Update of End User (attestation of) attributes identity data in case of changes (e.g. address change or additional attributes)

2. Reinitialisation of end user PIN of the Mobile Identification application (in case of loss or when forgotten)

3. End user identity verification to support (1) binding of the device or data with the user, or (2) regular identity verification as mandated by the security policy

4. 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.
5. Migration to a new device, maintain the End User identity data.
6. Device Termination / Refurbishment / Factory Reset: Removal of all End User data.

A.7 Use Case 7

Secured Applications for Mobile – European Digital Identity Wallet (based on use case 6 but adapted to the revision of the eIDAS Regulation)

In June 2021, the European Commission presented a proposal for a revised version of the eIDAS Regulation. The proposal introduces the concept of European Digital Identity Wallet. Every Member State will issue a Wallet where their citizens can store their identity data. Users can request additional attributes or credentials to providers of attestation of attributes. This Wallet needs to be issued under an eID scheme at level of assurance (LoA) High.

A wide range of services will be obliged to recognise the Wallet for identification and authentication. This includes:

- Public services that require an electronic identification means;
- Private services required by national or EU law to use strong user authentication for online identification, or where strong user authentication is required by contractual obligation, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications;
- Very large online platforms.

The Wallet could leverage the eUICC present in the mobile phone to provide a high level of security (e.g. for protection of user's data), but above all meet the requirements of LoA "High" regarding authentication as required in the proposed Regulation.

Here, the Wallet would be made up with:

- **A device application;**
- **A SAM Wallet Applet,** which should be loaded and installed in an Application Service Provider SD (ASP SD) controlled by the Wallet issuer. This point is of the utmost importance as the Wallet issuer bears liability pursuant to the eIDAS Regulation with regards to the security and protection of personal data.

A typical lifecycle of the Wallet would be following:

- **Issuing Phase, Wallet Installation**: The End User downloads the Wallet application (device application) from an application store.

- **Issuing Phase, Eligibility Check**: The Wallet application performs an eligibility check of the device, including the eUICC. In case of sufficient capabilities, the installation of the SAM Wallet 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 Java Card version. In particular, the Wallet issuer needs information concerning security certification of the eUICC so that it can be sure the Wallet (device application + SAM Wallet Applet) will be secure. This includes identification of the security certificate of the eUICC hardware pursuant to the EUCC scheme or the EU 5G scheme (Cybersecurity Act), and of the eUICC.

- **Issuing Phase, SAM Security Domain registration**: In case of a positive result of the eligibility check, the Wallet issuer will register the device as customer medium and request a secure space in the SAM Security Domain.

- **Issuing Phase, SAM Wallet Applet Installation**: The Wallet issuer triggers the installation of the SAM Wallet Applet in the SAM Security Domain. Preferably this is done by using offline methods. As a result, the SAM Wallet Applet is installed within the SAM Security Domain of the eUICC and the access rights to the SAM Wallet Applet are transferred to the Wallet issuer.

- **Personalisation Phase**: The personalisation of the Wallet encompasses the following several steps (1) provisioning holder's identification data in the Wallet, (2) making sure the Wallet is in the hand of the legitimate holder at the time of provisioning (to avoid transfer of identity), and (3) registering/activating the Wallet as authentication means. This may be achieved in several ways, such as:

  - **The holder uses digital identity means (e.g.: USB token, eID application of the identity document) with a LoA "High" to demonstrate his/her identity.** The digital identity means are verified by a backend system. Upon successful holder authentication, the backend system verifies the binding between the holder and the mobile phone (e.g. through SMS OTP…), and if successful (1) loads the identification data corresponding to the holder in the Wallet and (2) registers/activates the Wallet as authentication means.
  - **The identity of the holder is verified by a duly authorised person in the course of a physical interaction (e.g. at a city hall) using a physical identity document.** Upon successful identity verification, the duly authorised person verifies the binding between the holder and the mobile phone (e.g. through SMS OTP…), and if successful (1) loads the identification data corresponding to the holder in the Wallet and (2) registers/activates the Wallet as authentication means.
  - **Remote identity proofing – using a physical identity document - is applied to verify the identity of the holder,** as described in PVID referential by ANSSI (https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/). The remote identity proofing procedure applied shall meet the applicable requirements for the LoA "High". Upon successful identity verification, the binding between the holder and the mobile phone is verified (e.g. through SMS OTP,…), and if successful (1) the identification data corresponding to the holder is loaded in the Wallet and (2) the Wallet as authentication means is registered/activated.

- **Usage Phase**: After personalisation of the Wallet, the End User can use it for various use cases as envisioned in the proposed regulation:

  - Deliver identification data and/or authenticate to relying party;
  - Query and store in the Wallet attestation of attributes pertaining to the holder;
  - Query and store in the Wallet credentials pertaining to the holder;
  - Query and store in the Wallet attributes pertaining to the holder;
  - Deliver attributes, attestation of attributes and credentials to relying party;

Besides, it shall be noted that the proposed regulation does not prohibit a holder to have several Wallets in his/her mobile phone, each of them coming from different Wallet issuer. So much so that it is already envisioned by some public authorities, to serve some specific usages (e.g. Wallet for professional use or for some specific uses case, e.g. Patient/health). In this case, the procedure described above is repeated, with a new SAM Wallet Applet being installed in a different ASP SD, as the entity that is liable for the Wallet is different.

Beyond the benefits of SAM technology, the following life cycle management procedures need to also be addressed by the Wallet issuer:

1. Discontinuation of usage, due to the following reasons:

    - End User removes the service,
    - Service provider triggers the removal of the service,
    - Wallet issuer discontinues the service availability,
    - Date of expiry (of Mobile ID or origin eID) passed,
    - An issue has arisen in the security certificate of the eUICC,
    - Device Termination,
    - Refurbishment,
    - Factory Reset: Removal of all End User data;

2. Migration to a new device.

Annex B SAM Certificate Policy (CP)

This SAM Certificate Policy comprises the policy framework for the SAM PKI and is consistent with the Internet X.509 PKI Certificate Policy and Certification Practices Framework (RFC 3647[14]). It governs the operations of the SAM PKI components by all individuals and entities within the infrastructure (collectively, “PKI Participants”). It provides the requirements that SAM PKI Participants are mandated to meet when issuing and managing Certificates and private keys. In addition, it informs potential Relying Parties about what they need to know prior to relying on issued Certificates.

This SAM CP also defines the terms and conditions under which the CAs SHALL operate in order to issue Certificates. Where “operate” includes Certificate management (i.e., approve, issue, and revoke) of issued Certificates and "issue", in this context, refers to the process of digitally signing with the private key associated with its authority Certificate a structured digital object conforming to the X.509, version 3 Certificate format, or to the GlobalPlatform Certificate format.

The SAM CP acts as an umbrella document establishing the baseline requirements and applies consistently throughout the entire SAM PKI, thereby providing a uniform level of trust throughout the applicable community. The SAM PKI accommodates a worldwide, large, public, and widely distributed community of users with diverse needs for communications and information security.

B.1 Role of the SAM CP and Other Practice Documents

The SAM CP describes the overall business, legal, and technical infrastructure of the SAM PKI. More specifically, it describes, among other things:

- the appropriate applications and the assurance levels associated with the SAM PKI Certificates
- the obligations of CAs
- the requirements for auditing of the SAM PKI
- the methods to confirm the identity of Certificate Applicants
- the operational procedures for Certificate lifecycle services: Certificate Applications, issuance, acceptance, revocation, and renewal
- the operational security procedures for audit logging, records retention, and disaster recovery
- the physical, personnel, key management, and logical security
- Certificate profile and Certificate Revocation List content

This SAM CP is completed with the following additional documents provided by the CA:

- Compromised key and recovery plan, which provides procedures for handling compromised keys and the methods of their recovery
- Disaster recovery plan, which provides procedures for handling a natural disaster or man-made disaster and procedures to retrieve off-site components to get the CA back-on-line
- Ancillary agreements, such as a Subscriber Agreement, Root CA hosting agreement, and interoperation agreements

B.1.1 SAM PKI Participants

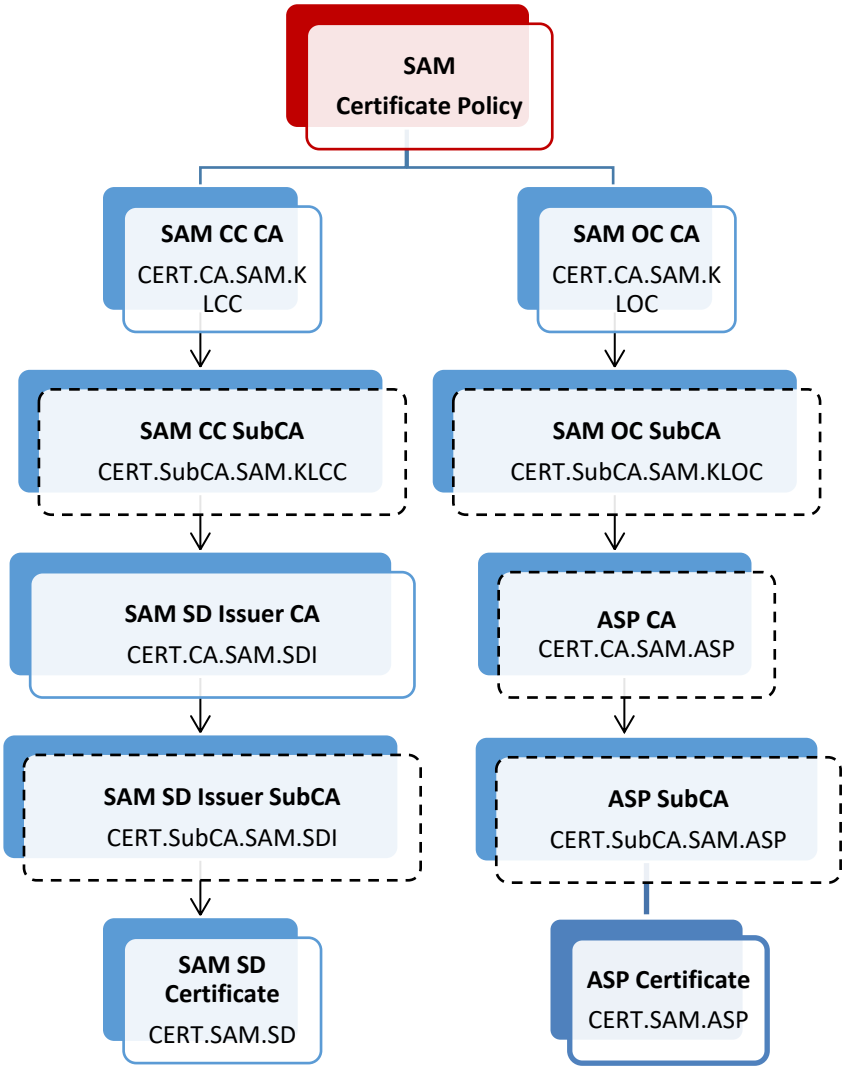


Figure 2: SAM Certificate Chains

A SAM CA is the root of trust of all the valid Certificate chains. It can be a KLOC and/or KLCC root of trust.

SubCAs and ASP CAs are optional. ASP Certificates are used to establish the secure communication based on SCP11 as defined in GlobalPlatform Amendment F [16]. A SAM SM MAY manage different ASP Certificates.

B.1.2 Participants in TLS chain for Public CA

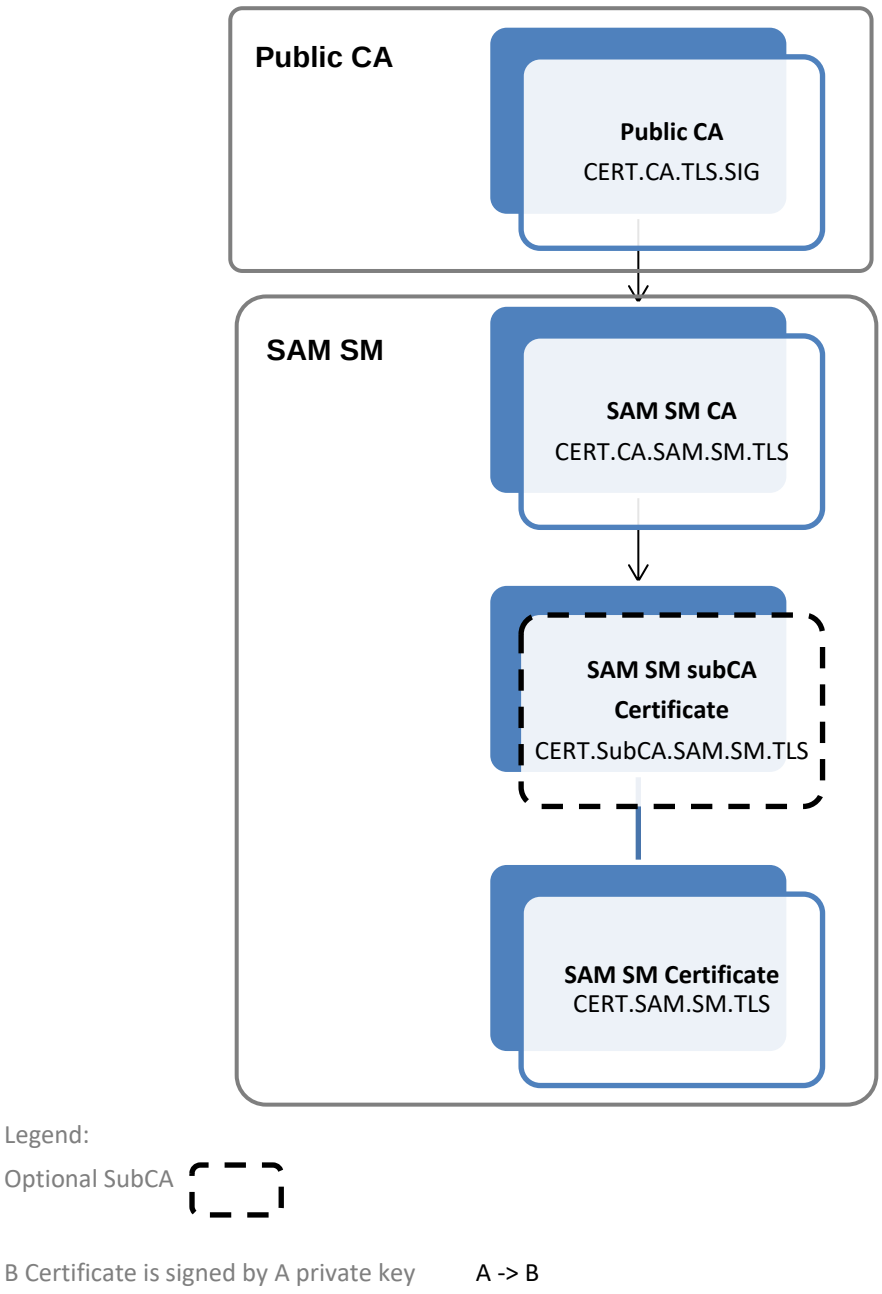


Figure 3: SAM SM TLS Certificate Chain with Public CA

B.1.3 Participants in TLS chain for SAM CA

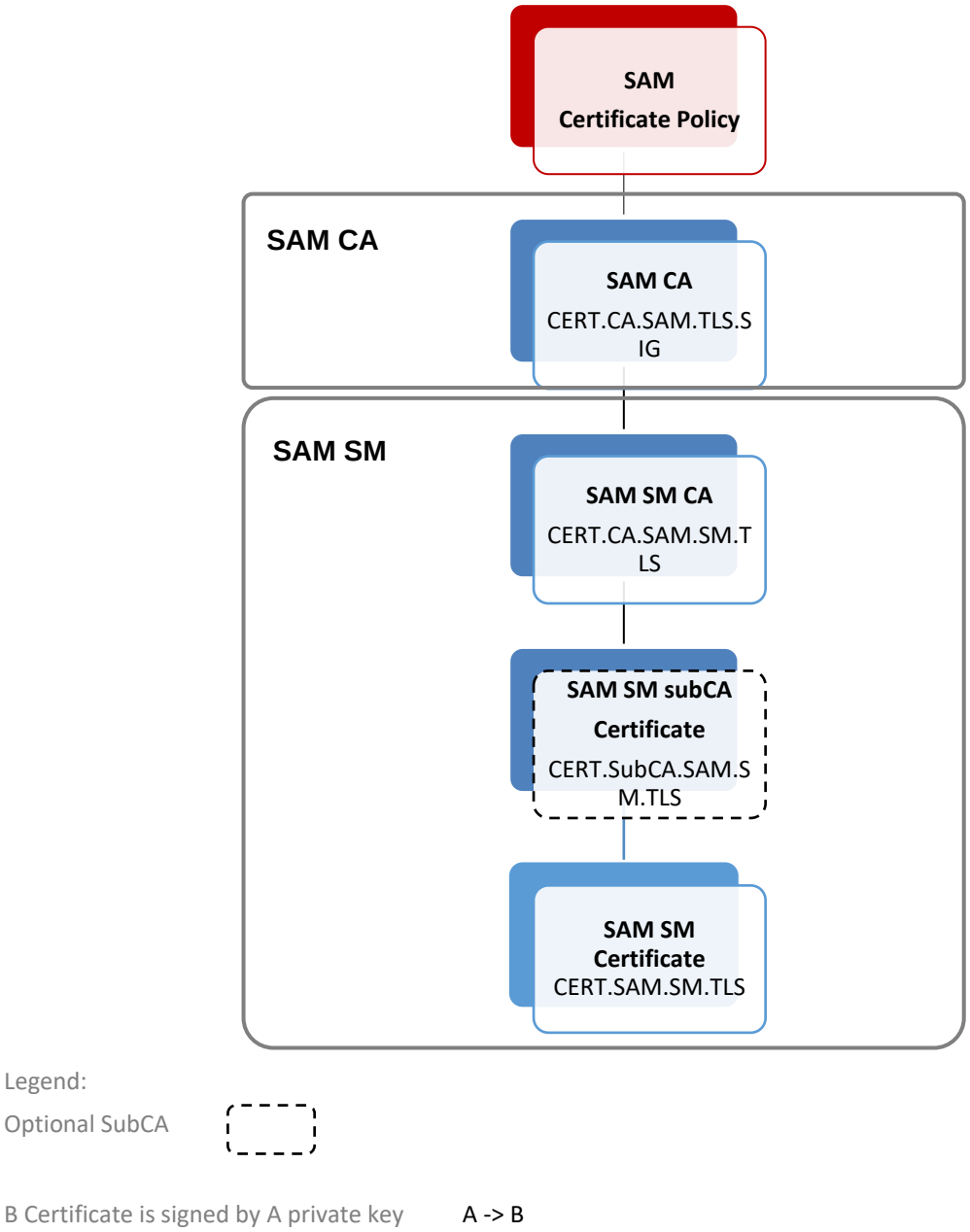


Figure 4: SAM SM TLS Certificate Chain with SAM CA

B.2 Certificate Authority

1. At the heart of a SAM PKI are entities called “Certificate Authorities” or “CAs”. CA is an umbrella term that refers to the collection of hardware, software, and operating personnel that create, sign, and issue public key Certificates under this SAM Certificate Policy. The CA is responsible for:

- issuing compliant Certificates
- the secure delivery of Certificates to its Subscribers
- the revocation of issued Certificates
- the generation, protection, operation, and destruction of CA private keys

- the Certificate lifecycle management ensuring that all aspects of the CA services, operations, and infrastructure related to Certificates issued under this document are performed in accordance with the requirements, representations, and warranties of this document
- acting as trusted party to facilitate the confirmation of the binding between a public key and the identity of the “Subject” of the Certificate.

CAs fall into several categories:

1. The SAM CA and SAM SubCAs for SAM SD Certificate chain
2. The SAM CA and SAM SubCAs for ASP Certificate chain
3. The SAM SD Issuer CAs and SAM SD Issuer SubCAs
4. The SAM SM SubCAs (only for TLS Certificate Chain)
5. The ASP CAs and ASP SubCAs

B.3 Subscribers

In the SAM PKI, the Subscriber is the entity named in the Subscriber Agreement. An authorised representative of the Subscriber, as a Certificate Applicant completes the Certificate issuance process established by the CA. In response, the CA confirms the identity of the Certificate Applicant and either approves or denies the application. If approved, the Subscriber agrees to be bound by its obligations through execution of the Subscriber Agreement.

B.4 Relying Parties

The Relying Party MAY be any entity that validates the binding of a public key to the Subscriber’s name in a Certificate. The Relying Party is responsible to check the validity of the Certificate by checking the Certificate status information. The Relying Party can use the Certificate to verify the integrity of a digitally signed message, to identify the initiator of a communication, or to establish confidential communications with the holder of the Certificate.

B.5 Policy Authority

The central role of the Policy Authority ensures that the PKI provides a trustworthy and secure environment for the management and use of digital certificates. The Policy Authority (PA) is an organisation or administrative unit that defines and monitors policies for the management and operation of the PKI. The Policy Authority plays a central role in ensuring that all parties involved in the PKI (e.g. certification authorities, registration authorities, end users) comply with the defined security and operating standards.

The tasks and responsibilities of a Policy Authority typically include:

1. Creation and maintenance of the Certificate Policy (CP): The Policy Authority defines the framework conditions and requirements for the issuance, management and use of digital certificates. These conditions are documented in the Certificate Policy. These include but are not limited to security requirements, procedures for identity verification and the handling of certificate revocation lists (CRLs).

2. Creation and/or monitoring the CP documents for each involved CA.

3. Check whether Certification Practice Statement (CPS) documents of all CAs of the PKI fulfil the requirements of the Certificate Policy (CP) before a corresponding key ceremony is carried out and the CA is set to productive.

4. Ensuring compliance with the guidelines: The Policy Authority regularly monitors and audits the PKI participants involved to ensure that they comply with the defined policies, requirements and standards in order to operate the PKI. 5. Definition of Roles and Responsibilities: The Policy Authority defines which roles and responsibilities exist within the PKI structure, such as the tasks of certification authorities, registration authorities and other parties involved.

6. Risk and Security Management: The Policy Authority is responsible for identifying potential security risks and implementing appropriate measures to minimise risks.

7. Communication and Documentation: The Policy Authority ensures that all relevant policies, procedures and changes are clearly documented and communicated to the parties involved.

B.6 Other Participants

B.6.1 Auditors

The SAM PKI Participants operating under this SAM CP MAY require the services of other authorities, such as compliance auditors.

B.6.2 Incident Coordinator

During a Security Incident, be it man-made or natural, where third parties are impacted the Incident Coordinator SHALL be in the lead together with the SAM PKI participant which it entails.

B.7 Certificate Usage

This SAM CP sets forth policies governing the use of SAM PKI Certificates. Each Certificate is generally appropriate for use with the applications set forth in this SAM CP.

B.7.1 Appropriate Certificate Uses

Certificates are suitable for authentication of devices and servers related to SAM services. The use of the Certificates permits authenticity checks of the Certificate, message integrity checks and confidentiality encryption of communications.

B.8 Certificate Life-Cycle Operational Requirements

B.8.1 Certificate Application

A SAM CA or SubCA SHALL document the processes, procedures, and requirements of their Certificate issuance process.

B.8.2 Who Can Submit a Certificate Application

The Applicant for a Certificate SHALL be the Subscriber or an authorised representative of the Subscriber.

The Application for a Certificate SHALL be submitted by the Subscriber or an authorised representative of the Subscriber.

B.8.3 Enrolment Process and Responsibilities

All communications with SAM CA SHALL be authenticated and protected from modification; any electronic transmission of shared secrets SHALL be protected. Communications MAY be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair SHALL be used. Out-of-band communications SHALL protect the confidentiality and integrity of the data.

The enrolment process for a Certificate Applicant SHALL consist of:

- Completing a Subscriber Agreement and Certificate Application
- Providing the requested information
- Responding to authentication requests in a timely manner
- Submitting required payment

B.8.4 Certificate Signing Request (CSR)

An Applicant willing to request a Certificate from a SAM CA SHALL send a Certificate Signing Request (CSR) to that SAM CA.

The CSR SHALL follow PKCS #10 format as defined in [15].

Annex C SAM Ecosystem Description (Informative)

C.1 Actor-to-Role Association Models

The following roles are described in Definition section 1.4. For the purpose of discussion of potential development models, further details are provided below:

- **SAM SD Issuer** – entity in charge of the issuance and the management of the configuration of a SAM SD.
- **Application Service Provider (ASP)** – entity in charge of providing the SAM Service components (SAM Applet and optionally the Device Application).
- **SAM Service Manager (SAM SM)** – entity in charge of managing the ASP SD creation and SAM Applet installation on behalf of an ASP.
- **SAM CAs –** set of Certification Authorities in charge of issuing certificates to the different entities of the SAM ecosystem. As an example:
    - SAM CC CA – CA in charge of issuing certificates for SAM SD Issuer CA (e.g. Device Maker or Operator).
    - SAM SD Issuer CA –CA in charge of issuing certificates for SAM SD Issuers (e.g. eUICC/UICC Manufacturer)
    - SAM OC CA – CA in charge of issuing certificates for ASP CAs
    - ASP CA – CA, representing one or more ASPs, in charge of issuing certificate for SAM SMs

C.1.1 Actor-to-Role Association Models for SAM CA

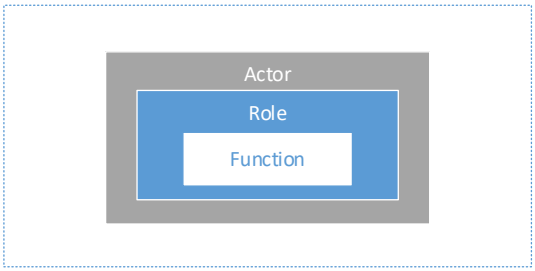
In this section we will provide some examples for SAM ecosystem configurations for Certification Authorities.

Several actors could potentially play the role of SAM CAs depending on the SAM Service security requirements and the sensitivity of the service and security requirements coming from each industry.

As an illustration, the following actors could play the role of a SAM CA:

- **An Industry Certification Organisation** – Industry-specific organisation in charge of part or the whole SAM PKI policy definition. For the payment industry, Payment Schemes could be potential candidates to play the role of one or several SAM CA(s)
- **A Government organisation** – Governmental organisation in charge of the SAM PKI policy definition. This could be done for example for digital identity (passport, national ID, mDL).
- **A (Existing) Policy Authority** – Organisation in charge of the SAM PKI policy that is already trusted by the industry and provides assurance about the security and compliance of the actors. In this context e.g:GSMA or GlobalPlatform could be potential candidates for a Policy Authority of the SAM CA. It also gives guarantees about the security and the certification of the eUICC in the telco context.
- **An Enterprise**– In case of non-sensitive services that does not follow specific security requirements, an enterprise (e.g. device manufacturer, service provider, operator) could play the role of one or several SAM CA(s).

In the rest of the annex, for diagrams describing Actors to Roles allocation model, the following graphical convention applies:



As an illustration, here are in the figures below some ecosystem configurations for CAs.

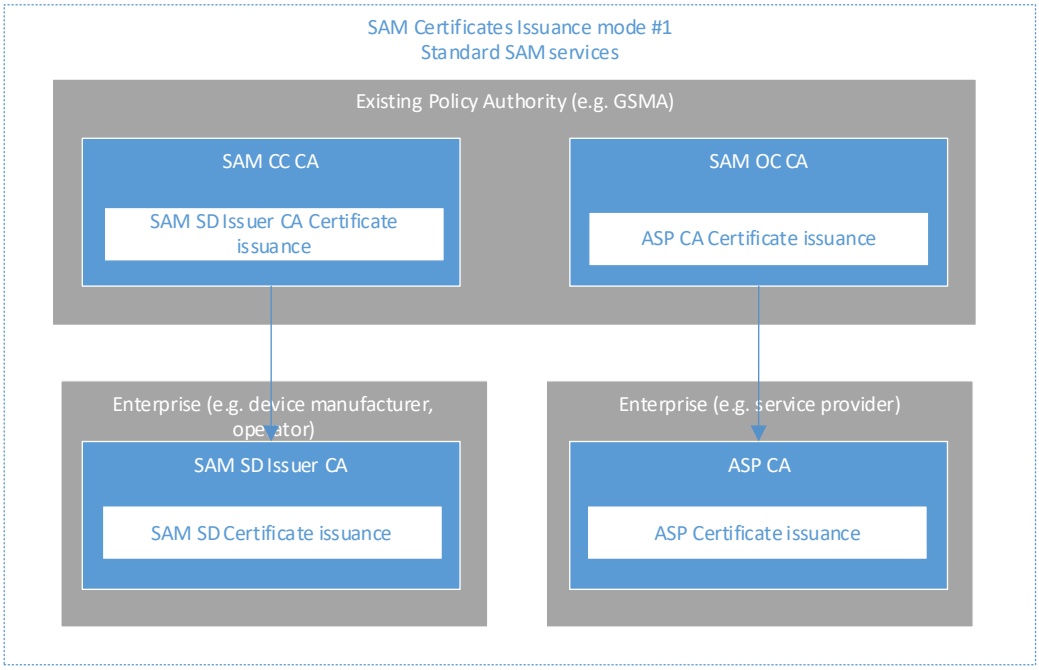


Figure 1 - Example of SAM PKI model for standard SAM services

In this model, both Root CA roles (SAM CC CA and SAM OC CA) are played by the same entity, the existing Policy Authority (e.g. GSMA) or another Policy Authority (e.g.: GlobalPlatform).

Since there is no specific requirement from the industry for the management of the targeted SAM service, an enterprise (e.g. device manufacturer) can play the role of the SAM SD Issuer CA and another enterprise (e.g. service provider) can play the role of an ASP CA.

Each Sub-CAs received its certificate from the existing Policy Authority. The SAM SD Issuer CA will issue SAM SD certificates for SAM SD Issuers while the ASP CA will issue ASP certificates (including range of RIDs associated to the SAM Applet) to the SAM SM managing, on behalf of the ASP, the SAM Service.

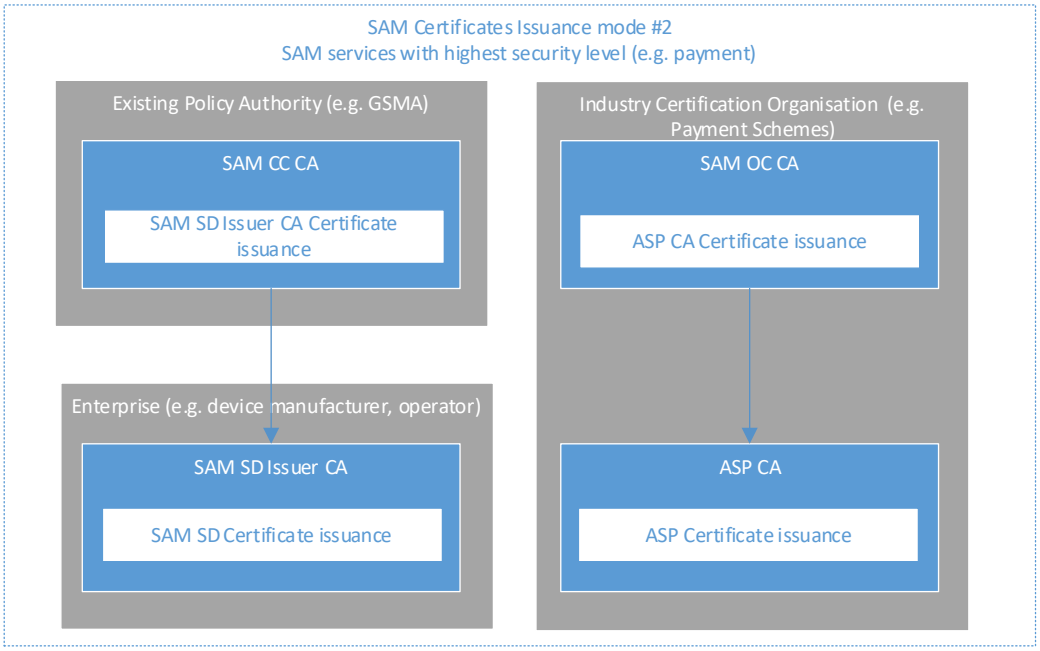


Figure 2 - Example of SAM PKI model for SAM services with highest security level

In this model, the SAM CC CA role is played by the existing Policy Authority and the SAM OC CA is played by an Industry Trusted Third Party (TTP).

The enterprise (e.g. device manufacturer) is able to play the role of SAM SD Issuer CA while the Industry TTP is also playing the role of the ASP CA.

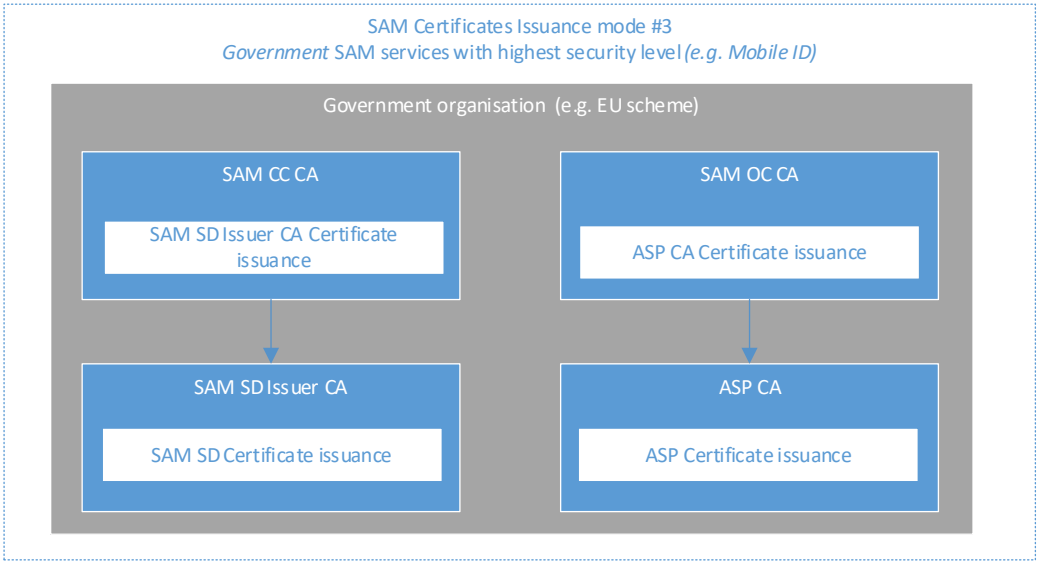


Figure 3 - Example of SAM PKI model for Government SAM services with highest security level

In this model, the government organization (e.g. EU scheme) endorses the responsibility for the whole SAM PKI scope and is playing the role of all SAM CAs.

C.1.2 Actor-to-Role Association Models for SAM Service deployment

In this section we will provide some examples of SAM ecosystem configurations for SAM Service deployment.

Two types of actors could endorse the role of SAM SM

- **A Service Provider** – in this scenario, the Service Provider manages a SAM SM platform and the deployment of its own SAM Service by itself. The Service Provider might also need a 2nd platform (ASP Back-End) to personalize its SAM applet.
- **A SAM SD Manager** – in this scenario, the Service Provider has a contract with a SAM SD Manager that will manage the deployment of a SAM Service on its behalf. The personalization of the SAM applet might be managed by the Service Provider, e.g. via its legacy SP TSM (or SDM) platform. A notification mechanism might be required to trig the personalization process, that is out of scope of this specification. A SAM SD Manager can potentially manage several SAM Services from different ASPs.

As an illustration, here are in the figures below some ecosystem configurations for SAM Service deployment.

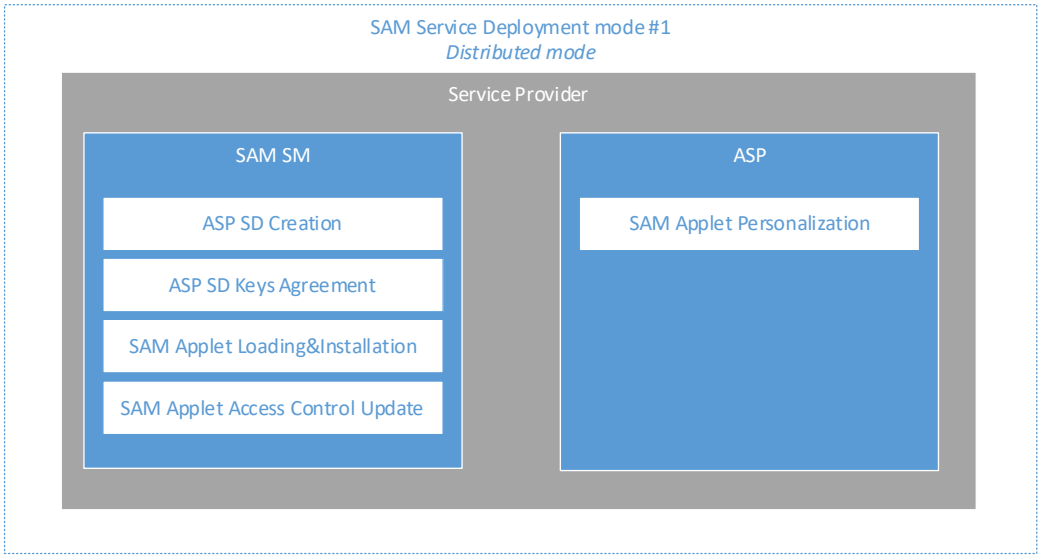


Figure 4 - Example of SAM Service deployment model in a “distributed” model

In a “distributed” model, a Service Provider plays the role of SAM SM in addition to ASP.

The Service Provider manages its own SAM SM Back-End in addition to a service-specific ASP Back-End in case the SAM Applet requires a personalization script.

In case several SAM Services coexist on the same eUICC, several SAM SMs will be sharing the management of the SAM SD.

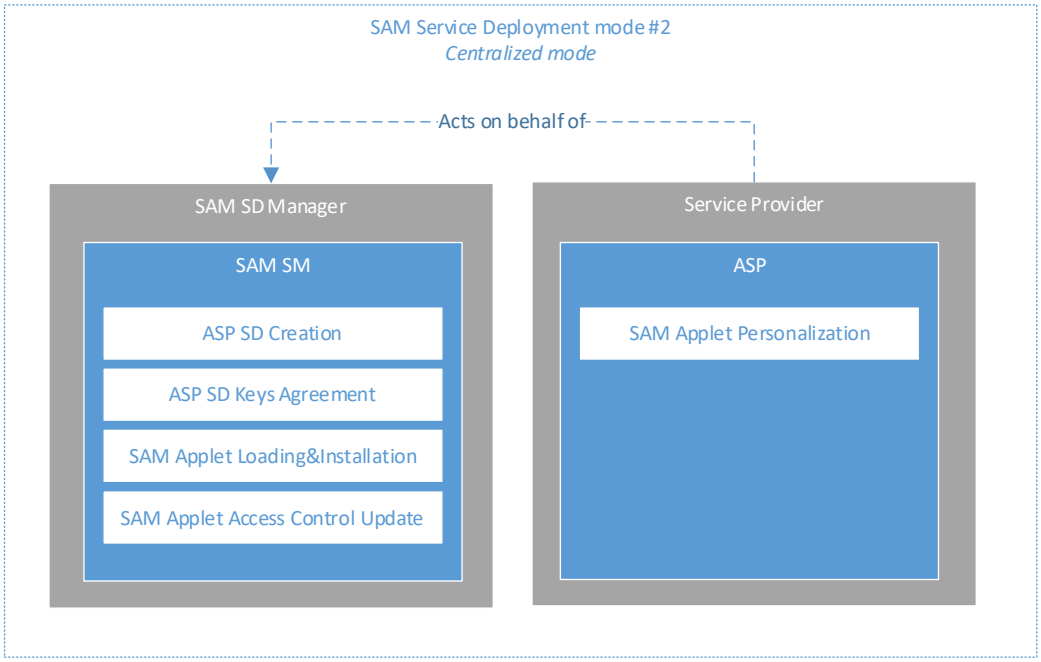


Figure 5 - Example of SAM Service deployment model in a "centralized" model

In a "centralized" model, a SAM SD Manager plays the role of a SAM SM on behalf of a Service Provider, and a Service Provider plays the role of the ASP.

The SAM SD Manager manages a "centralized" SAM SM Back-End while (a) Service Provider(s) manages (a) service-specific ASP Back-End(s) in case the SAM Applet requires a personalization script.

In case several SAM Services coexist on the same eUICC, the same SAM SM can be used for the management of all SAM Services in the SAM SD.

Alternatively, a SAM SM managed by a SAM SD Manager (potentially managing several SAM Services) could coexist with one or several SAM SM directly managed by Service Provider(s).

In that scenario, and thanks to hosted ASP Certificates, each SAM SM will handle a different range of RIDs, as depicted in the figure below.

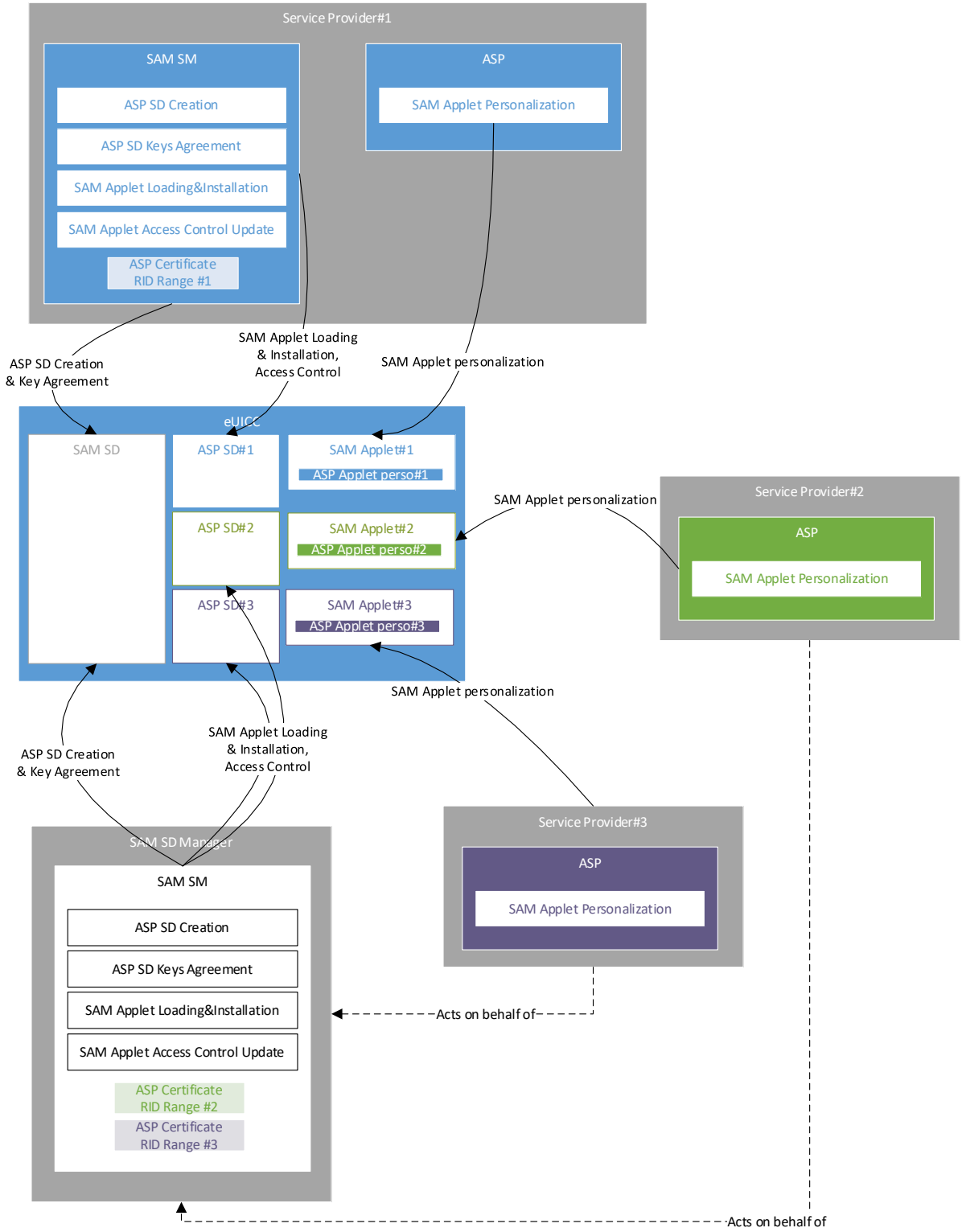


Figure 6 - Example of SAM Service deployment model in "hybrid" model

Note: in this diagram and following ones, arrows symbolizing SAM commands execution are representing both scenarios where synchronous and asynchronous model is used.

C.2 SAM Service Issuance Models

This section provides some examples of SAM Service Issuance models, focusing on Certificates and Keys exchanges.

Those models do not aim to be exhaustive, a SAM ecosystem can be built using any combination of Actors/Roles associations as defined, for example, in C.1.

The first example describes a SAM ecosystem where the Actors/Roles associations are as follows:

- The SAM SD Issuer role is endorsed by a Device Manufacturer,
- The Service Provider endorsed the role of the ASP while a SAM SD Manager offers SAM SM services to Service Providers.
- The SAM OC CA and SAM CC CA roles are endorsed by a unique Root CA entity,
- The SAM SD Issuer CA is endorsed by the Device Manufacturer,
- There is no ASP CA, leaf ASP Certificates are directly issued by the SAM OC CA

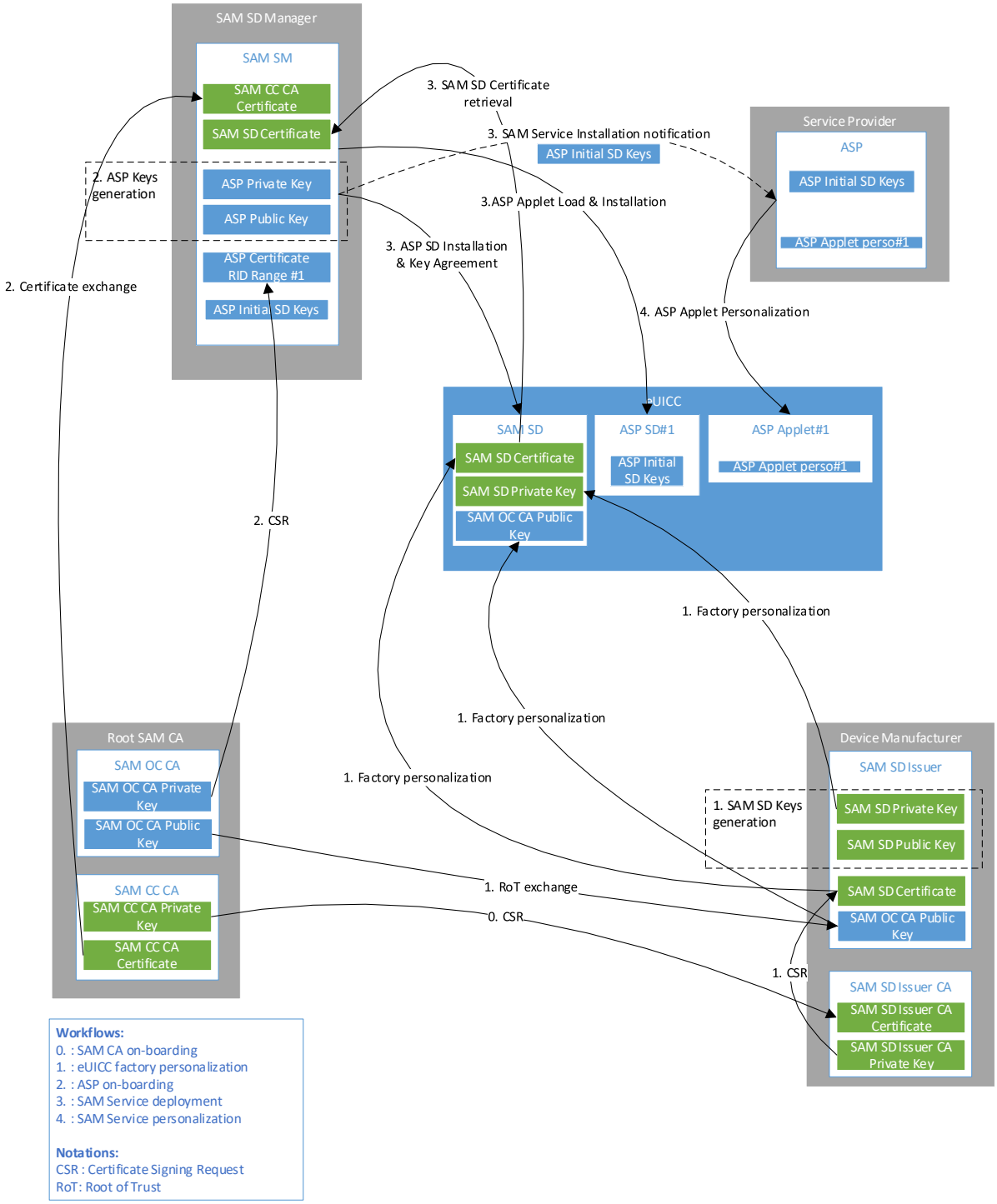


Figure 7 - SAM Service issuance model #1

The following processes are represented in the diagram above:

1. **SAM CA on-boarding** – On-boarding a new SAM SD Issuer CA; it consists in the generation by the SAM CC CA of a SAM SD Issuer CA certificate.
2. **eUICC factory personalization** – In-factory generation of a SAM SD key pair by the SAM SD Issuer, and issuing of SAM SD certificate by the SAM SD Issuer CA. The Certificate related to the generated SAM SD key pair and if required, the related private key are injected to the SD of SAM-enabled eUICCs during the eUICC personalization process.

The Root of Trust (SAM OC CA Public Key), previously generated by the SAM OC CA, shall also be injected to the SAM SD during this process.

3. **ASP on-boarding** – On-boarding of a new ASP; the SAM SM generates a new key pair for the ASP and gets an ASP Certificate from the SAM OC CA for the RIDs allocated to this ASP. The SAM CC CA certificate is also transferred to the SAM SM from the SAM CC CA.
4. **SAM Service deployment** – Creation by the SAM SM of the ASP SD, keys agreement, and loading & installation of the SAM Applet in synchronous or asynchronous model, Optionally, the ASP Initial SD Keys generated during the ASP SD Creation and Key Agreement process might be securely transferred to the ASP for the personalization of the SAM Applet. It is then up to the ASP to replace those keys with final keys if required. This process and the interface between the ASP and its SAM SD Manager are ASP-specific and out of scope of this specification.
5. **SAM Service personalization (optional)** – Sending of a personalization script to the SAM Applet via an ASP-specific mechanism.

The second example describes a SAM ecosystem where the Actors/Roles associations are as follows:

- The SAM SD Issuer role is endorsed by an EUM,
- The Service Provider endorses both roles of SAM SM and ASP
- All SAM CA roles are endorsed by a unique SAM CA entity,
- An ASP CA is present that received a certificate from the SAM OC CA to issue ASP certificates for ASPs for a set of RID ranges.

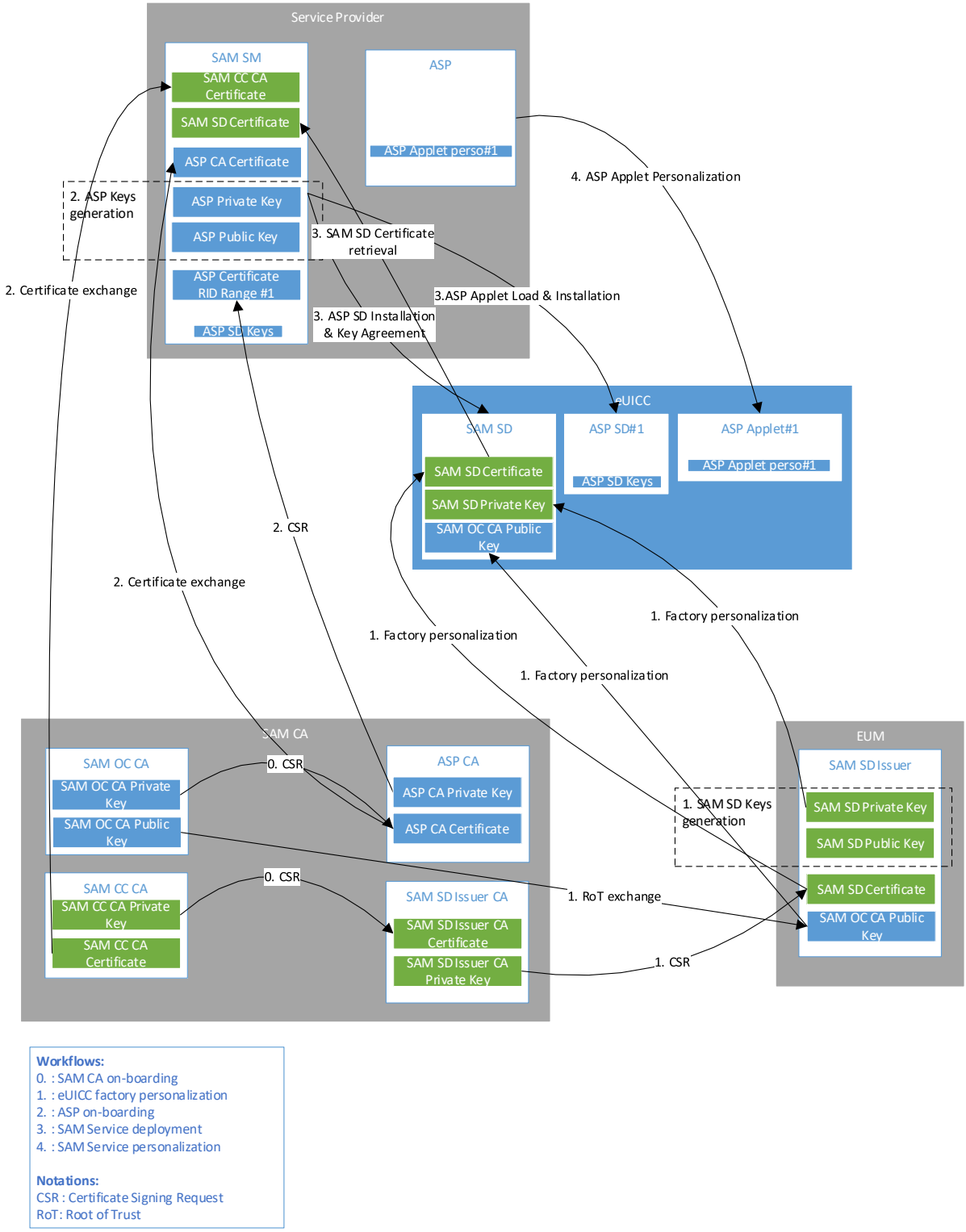


Figure 8 - SAM Service issuance model #2

The following processes are represented in the diagram above:

1. **SAM CA on-boarding** – On-boarding a new SAM SD Issuer CA and a new ASP CA; it consists in the generation by the Root CA of certificates for Sub-CAs,
2. **eUICC factory personalization –** Same as above with different actors,

3. **ASP on-boarding** – On-boarding of a new ASP; the SAM SM generates a new key pair for the ASP and gets an ASP Certificate from the ASP CA for the RIDs allocated to this ASP. The following certificates are transferred to the SAM SM:
    - The ASP CA certificate from the ASP CA,
    - The SAM CC CA certificate from the SAM CC CA
4. **SAM Service deployment** – Creation by the SAM SM of the ASP SD, keys agreement, and loading & installation of the SAM Applet in synchronous or asynchronous model,
5. **SAM Service personalization (optional)** – Same as above.

Annex D Document Management

D.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		
SAM.01 v1.1	03 November 2023	CR1001R01	eIDAS use case	ISAG	Yolanda Sanz/GSMA
		CR1002R00	Clarifying AID conflict issue		
		CR1003R01	Clarifying ELG11 as per Eurosmart comment		
		CR1005R00	Eurosmart comments Use Case A6		
		CR1006R00	EURO 5 Comment		
		CR1008R01	ASP AID rules clarification		

		CR1010R02	SAM Architecture		
		CR1004R03	Clarifying ASP Identifier		
		CR1009R01	Eurosmart-comment EURO17 Use Case A6		
		CR1011R00	Clarifying tunnelling and tunnelled interfaces		
		CR1007R07	SAM CI PKI		
		CR1008R03	ASP AID rules clarification		
		CR1012R01	ASP AID rules clarification		
		CR1013R00	Remove two Editor's notes		
		CR1014R04	Eurosmart comments		
		CR1015R02	SAM SD Certification Requirements		
		CR1016R01	Definition Clean up		
		CR1017r01	Annex B		
		CR1018R01	Certificate Chain Clarificaiton		
SAM.01 v1.2	27/10/2024	CR120001R011	Annex SAM Ecosystem	ISAG	Yolanda Sanz/GSMA
		CR120002R00	Reference to TCA JavaCard Applet guideline		
		CR120003R03	Policy Authority		

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.