GSMA eUICC PKI Certificate Policy
Version 2.0
24 October 2019

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice (Test)

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

Security and trust are an integral part of the GSMA's Specification for remote provisioning connections. The ability to provision operator subscription data securely "over the air" to change from one operator to another requires secure connections, as well as data confidentiality and integrity, and system availability. Paramount to the achievement of these objectives is the establishment and maintenance of an efficient and effective end-to-end trust infrastructure within the ecosystem. For the eUICC and Servers defined by GSMA for remote provisioning an eUICC Public Key Infrastructure (PKI) to support the use of Certificate for authentication has been defined.

Mobile Network Operators relying on the eUICC PKI need to be able to determine the degree of trust which can be placed in the authenticity and integrity of the Certificates issued by a Certificate Authority (CA). Information upon which such determination can be made is documented here in the eUICC PKI Certificate Policy.

1.2 Scope

This document defines the policies by which the eUICC PKI will be governed by the eUICC PKI Policy Authority.

1.3 Definitions

Term	Description
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.
Certificate Authority	An entity authorised to issue, manage, revoke, and renew Certificates.
Certificate Chain	An ordered list of Certificates containing a Subscriber Certificate and one or more CA Certificates, which terminates in a Root Certificate.
Certificate Policy	A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, Compromise, recovery and administration of Certificates.
Certificate Revocation List	A periodically (or exigently) issued 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.

Term	Description
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Compliance Audit	A periodic audit that a CA system undergoes to determine its conformance with eUICC PKI requirements that apply to it.
Compromise	A violation of a Security Policy, in which an unauthorised disclosure of, or loss of control over, sensitive information has occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorised use, or other Compromise of the security of such private key.
Elliptic Curve Cryptography (ECC)	A public-key cryptography system based on the algebraic structure of elliptic curves over finite fields.
GSMA Certificate Issuer	A Certificate Authority accredited by GSMA. Also referred as “GSMA CI” in SGP.22 [11].
Incident Coordinator	Central point for notification and coordination within GSMA in the event of a Security Incident.
Incident Owner	Central point of contact for security related matters, including Security Incidents, in the organisation.
Intellectual Property Rights	Rights under one or more of the following: copyright, patent, trade secret, trademark, or any other Intellectual Property Rights.
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 the eUICC PKI: GSMA, a CA, a Subscriber, or a Relying Party.
Public Key Infrastructure (PKI)	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.
Pseudonymity	A word derived from pseudonym**,** meaning 'false name', is a state of disguised identity
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 Certificate Policy governing the PKI and the Certificate verification.
RSA (Algorithm)	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Public CA	A Certificate Authority, commonly used to issue Certificates for public Internet purposes, which is not subject to the GSMA Policy Authority as defined in this specification.
Secret Share	A portion of the activation data needed to operate the private key, held by individuals called “Shareholders.” Some threshold number of Secret Shares (n) out of the total number of Secret Shares (m) SHALL be required to operate the private key.

Term	Description
Security Policy	The highest-level document describing GSMA security policies.
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.
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 eUICC 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.
Validity Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.

1.4 Abbreviations

Term	Description
CA	Certificate Authority
CP	Certificate Policy
CRL	Certificate Revocation List
CSR	Certificate Signing Request
ECC	Elliptic Curve Cryptography
EUM	eUICC Manufacturer
id-ce	Object Identifier for Version 3 Certificate extensions. (OID value: 2.5.29)
IETF	Internet Engineering Task Force
OID	Object Identifier
PA	Policy Authority
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RFC	Request for Comment
RSA	Rivest, Shamir, Adelman
SAS	Security Accreditation Scheme
SM-DS	Subscription Management – Discovery Service
SM-DP	Subscription Management – Data Preparation
SM-DP+	Subscription Management – Data Preparation for Consumer Devices
SM-SR	Subscription Management – Secure Routing

1.5 References

Ref	Doc Number	Title
[1]	RFC 2119	Key Words for use in RFCs to Indicate Requirement Level, IETF (Bradner), March 1997. http://www.ietf.org/rfc/rfc2119.txt
[2]	RFC 5280	Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008. http://www.ietf.org/rfc/rfc5280.txt
[3]	RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 1999. http://www.ietf.org/rfc/rfc2560.txt
[4]	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
[5]	RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, Hurst), September 2007. http://www.ietf.org/rfc/rfc5019.txt
[6]	FS.04	GSMA SAS-UP Standard, latest version available at www.gsma.com/sas
[7]	FS.05	GSMA SAS-UP Methodology, latest version available at www.gsma.com/sas
[8]	FS.17	GSMA Security Accreditation Scheme - Consolidated Security Requirements, latest version available at www.gsma.com/sas
[9]	SGP.02	GSMA Remote Provisioning Architecture for embedded UICC: Technical Specification
[10]	Void	Void
[11]	SGP.22	RSP Technical Specification
[12]	Void	Void
[13]	RFC 2986	PKCS #10: Certification Request Syntax Specification
[14]	FS.08	GSMA SAS-SM Standard for Subscription Manager Roles, latest version available at www.gsma.com/sas
[15]	FS.09	GSMA SAS-SM Methodology for Subscription Manager Roles, latest version available at www.gsma.com/sas
[16]	FS.18	Security Accreditation Scheme - Consolidated Security Guidelines, latest version available on request to sas@gsma.com
[17]	WeBTRUST	WEBTRUST® for certification authorities webtrust principles and criteria for certification authorities
[18]	SGP.21	RSP Architecture
[19]	SGP.24	RSP Compliance Process
[20]	SGP.16	M2M compliance process
[21]	SGP.01	Embedded SIM Remote Provisioning Architecture
[22]	SGP.28	eSIM GSMA Recognised CI Accreditation
[23]	EN 319 411	Policy and security requirements for Trust Service Providers (aka CI) issuing certificates;

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 RFC2119 [1]."

2 Certificate Policy (CP)

This Certificate Policy comprises the policy framework for the eUICC PKI and is consistent with the Internet X.509 PKI Certificate Policy and Certification Practices Framework (RFC 3647 [4]). It governs the operations of the PKI components by all individuals and entities within the infrastructure (collectively, "PKI Participants"). It provides the requirements that PKI Participants are required 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 CP also defines the terms and conditions under which the CAs SHALL operate 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 CP acts as an umbrella document establishing baseline requirements and applies consistently throughout the entire eUICC PKI, thereby providing a uniform level of trust throughout the applicable community. The eUICC PKI accommodates a worldwide, large, public, and widely distributed community of users with diverse needs for communications and information security.

2.1 Role of the CP and Other Practice Documents

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

- Appropriate applications for, and the assurance levels associated with the PKI Certificates
- Obligations of CAs
- Requirements for audit of the PKI
- Methods to confirm the identity of Certificate Applicants
- Operational procedures for Certificate lifecycle services: Certificate Applications, issuance, acceptance, revocation, and renewal
- Operational security procedures for audit logging, records retention, and disaster recovery
- Physical, personnel, key management, and logical security
- Certificate profile and Certificate Revocation List content

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

- Compromise Key and Recovery Plan, which provides procedures for handling a Compromised key and the methods of 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

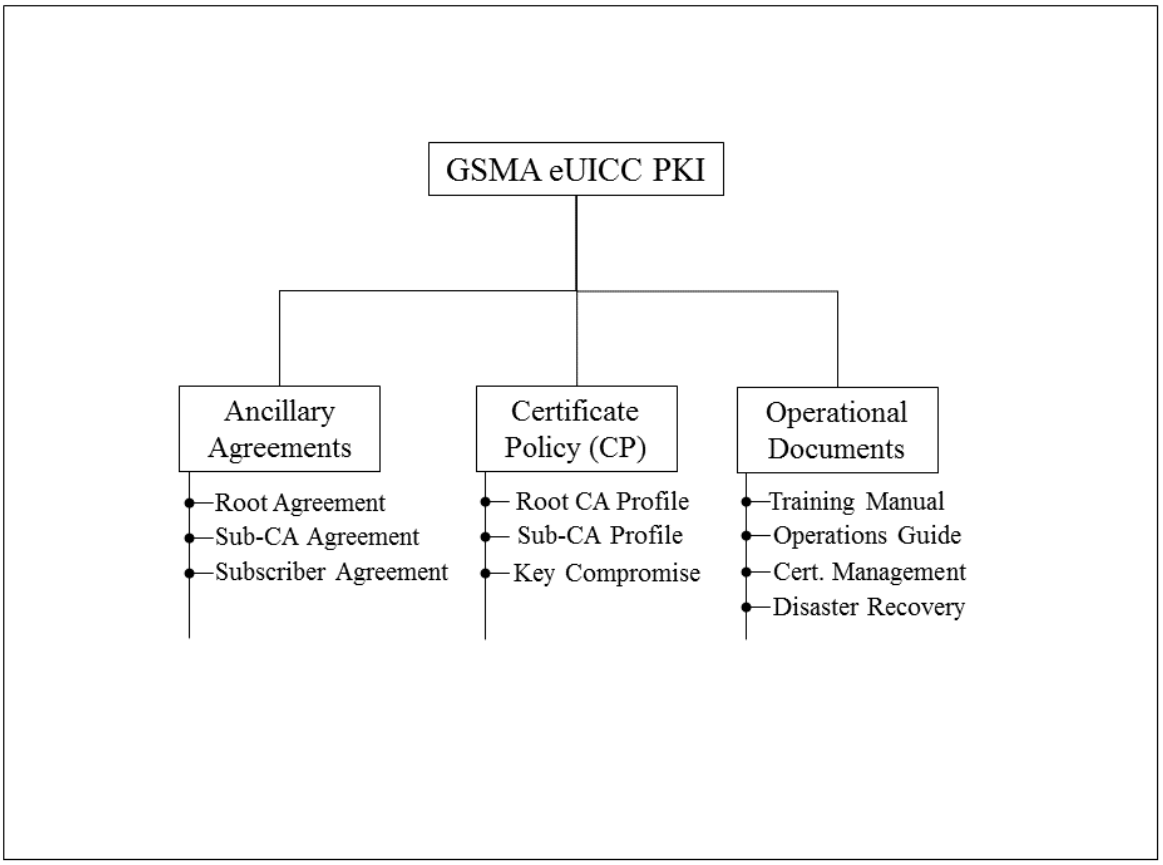

Figure 1: eUICC PKI Document Architecture

As shown in Figure 1 the CP is an integral part of the eUICC PKI document architecture and sets the minimum standards for governing, administrating and operating the PKI. Ancillary security and operational documents, developed by the CA operator, supplement the CP in setting more detailed requirements.

Table 1 is a matrix of the various eUICC PKI practice documents, whether they are publicly available, and their locations. The list is not intended to be exhaustive, nor will each document listed be applicable to every CA. Note that documents not expressly made public are confidential to preserve the security of the eUICC PKI.

Documents	Availability	Available From:
GSMA Certificate Policy (CP)	Public	GSMA
Ancillary Agreements	Public	GSMA
Compromise Key and Recovery Plan	Confidential	CA
Disaster Recovery Plan	Confidential	CA

Table 1: Availability of Practice Documents

2.2 Document Name and Identification

This document is the GSMA Certificate Policy. GSMA, acting as a policy-defining authority, in the future, MAY assign a policy Object Identifier value extension for this CP.

2.3 PKI Participants

The eUICC PKI shown in figure 1 and 2 represent the different Certificate chains that are allowed for SGP.02 [9] and SGP.22 [11].

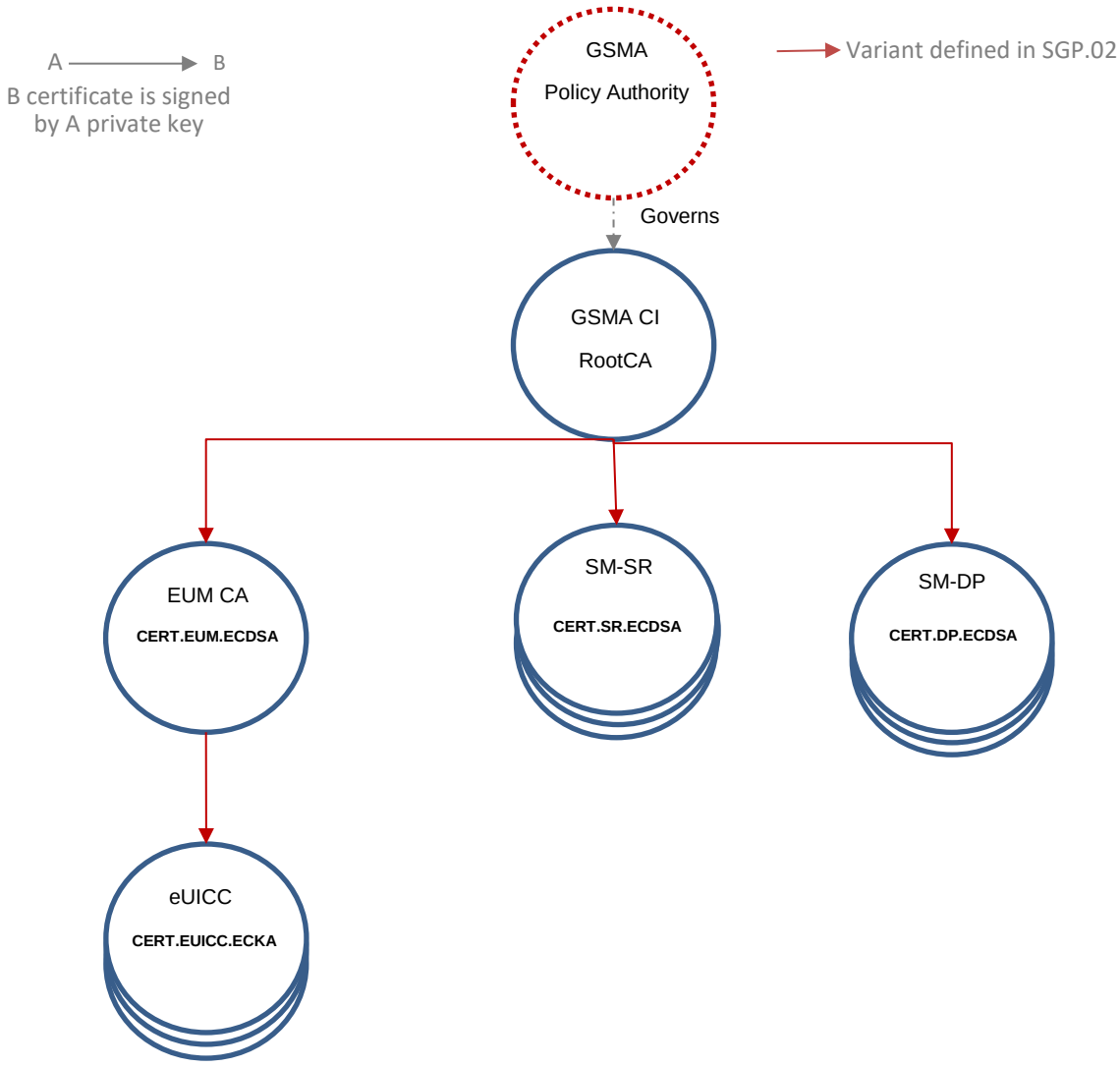

Figure 1 Certificate chain for SGP.02 [9]

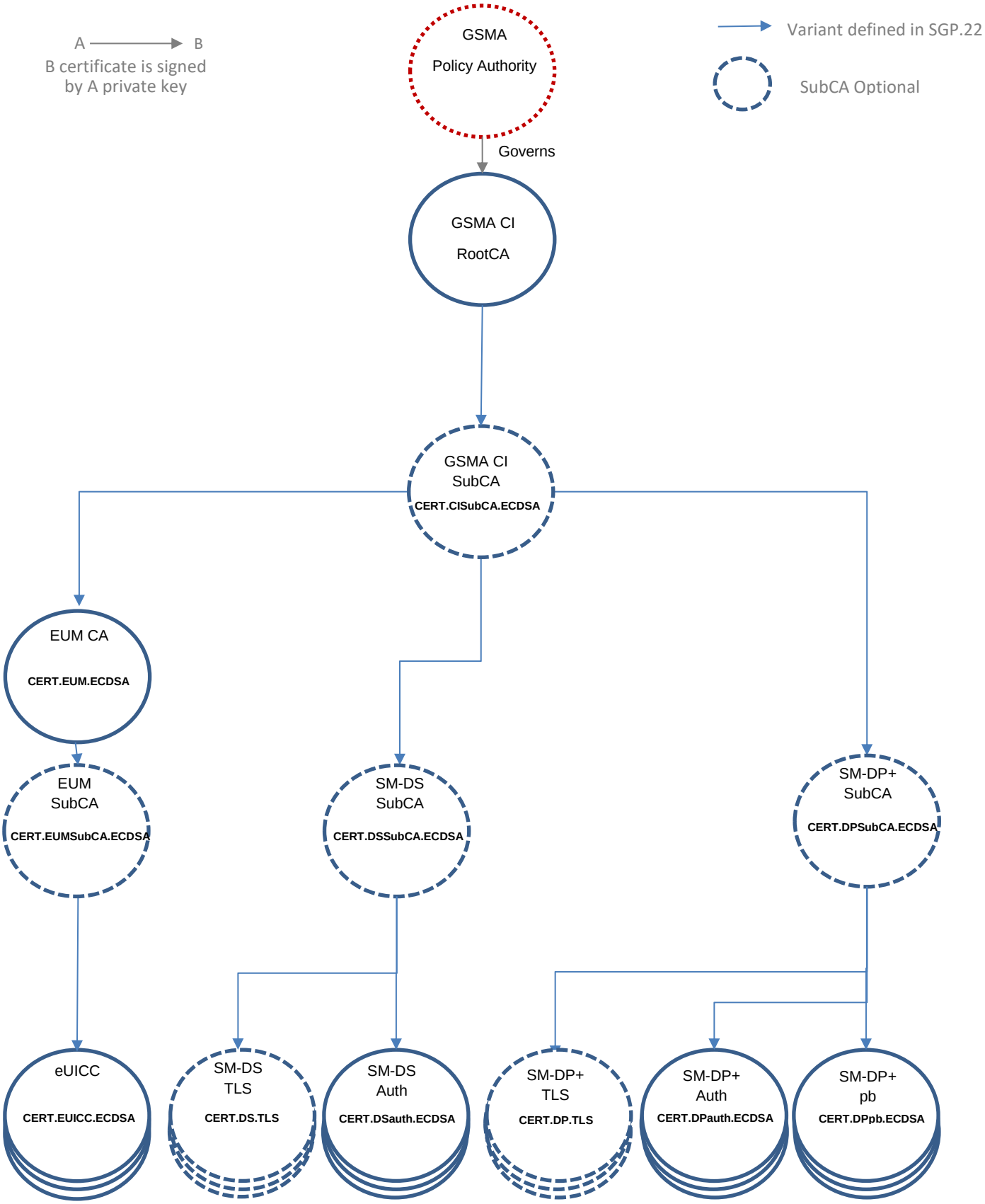
A → B
B certificate is signed by A private key
GSMA
Policy Authority
Variant defined in SGP.22
SubCA Optional
Governs
GSMA CI
RootCA
GSMA CI
SubCA
CERT.CISubCA.ECDSA
EUM CA
CERT.EUM.ECDSA
EUM
SubCA
CERT.EUMSubCA.ECDSA
SM-DS
SubCA
CERT.DSSubCA.ECDSA
SM-DP+
SubCA
CERT.DPSubCA.ECDSA
eUICC
CERT.EUICC.ECDSA
SM-DS
TLS
CERT.DS.TLS
SM-DS
Auth
CERT.DSauth.ECDSA
SM-DP+
TLS
CERT.DP.TLS
SM-DP+
Auth
CERT.DPauth.ECDSA
SM-DP+
pb
CERT.DPpb.ECDSA

Figure 2 Certificate chain for SGP.22 [11]

The conditions for the CA to deliver a Certificate is described in section 5.

The GSMA CI RootCA is the root of trust of all the valid Certificate chains except for the TLS Certificates that MAY be issued by a Public CA. The following describes the relevant participant roles in the eUICC PKI.

2.3.1 Policy Authority

GSMA is the eUICC PKI Policy Authority (PKI-PA). It owns this policy and represents the interest of its members in developing the policies that govern the eUICC PKI. The PKI-PA is responsible for:

- Maintaining this CP, ancillary agreements, security, and operational documents
- Governing and operating the PKI according to this CP
- Approving the Compliance Audit report for each CA operating under this policy and the continued conformance of each CA that issues Certificates under this policy with applicable requirements as a condition for allowing continued participation

2.3.2 Certificate Authority

At the heart of a 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 policy. The CA is responsible for:

- Issuing compliant Certificates
- Secure delivery of Certificates to its Subscribers
- Revocation of Certificates
- Generation, protection, operation, and destruction of CA private keys
- 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
- CAs act as trusted parties 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:

- For SGP.02 [9]: CAs fall into two categories (1) The GSMA CI RootCA, which is operated by a PKI-PA designated CA and (2) the EUM CAs.

- For SGP.22 [11]: CAs fall into several categories:

    - (1) The GSMA CI RootCA and GSMA CI RootCA SubCAs which are operated by a PKI-PA designated CA

    - (2) the EUM CAs and EUM SubCAs

- (3) the SM-DP+ SubCA
- (4) the SM-DS SubCA

2.3.3 Subscribers

In the eUICC 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.

References to “Subscribers” in this CP apply only to the eUICC and the SM-SR/SM-DP/SM-DP+/SM-DS servers.

2.3.4 Relying Parties

The Relying Party MAY be any entity that validates the binding of a public key to the Subscriber’s name in a GSMA 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. For instance, a SM-SR can use the eUICC Certificate embedded in a client device to authenticate the device receiving services from the server.

2.3.5 Other Participants

2.3.5.1 Auditors

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

2.3.5.2 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 PKI participant which it entails.

2.4 Certificate Usage

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

2.4.1 Appropriate Certificate Uses

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

2.4.2 VOID

2.5 Policy Administration

2.5.1 Organisation Administering the Document

The PKI-PA is responsible for all aspects of this CP.

2.5.2 Contact Person

Inquiries regarding this CP SHALL be directed to the PKI-PA:

eUICC PKI Policy Authority
GSMA Head Office
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
UK
Tel: +44 (0)207 356 0600
Web: www.gsma.com
Email: RootCA@gsma.com

3 Publications

3.1 Repositories

CAs SHALL ensure the integrity, authenticity and availability for their repository and posting Certificate revocation status in a repository that is publicly accessible to the Relying Parties of the PKI.

For the SM SubCA Certificates, the SM Server MAY choose not to manage revocation status of its leaf Certificates. In that case the SM Server SHALL limit the validity period of these Certificates as described in section 8.2 in order to mitigate the risk of a compromised Certificate being used (i.e. limit their validity periods).

3.2 Publication of Certification Information

The CP, GSMA CI RootCA(s) Certificates and their Certificate revocation status SHALL be publicly available on the GSMA website (see www.gsma.com).

GSMA CI RootCA(s) and their SubCA(s) Certificates SHALL be made publicly available within three (3) business days after issuance.

3.3 Void

3.4 Access Controls on Repositories

The CAs SHALL implement controls to prevent unauthorised addition, deletion, or modification of repository entries.

4 Identification and Authentication

4.1 Naming

4.1.1 Types of Names

CAs SHALL assign X.501 distinguished names for Certificates issued under this CP. CAs SHALL populate the Subject and Issuer fields in Certificates with a non-empty X.500 distinguished name as specified in section 5.1.3

4.1.2 Need for Names to be Meaningful

The Certificates issued pursuant to this CP are meaningful if the names that appear in the Certificates can be understood by the Relying Parties. Names used in the Certificates SHALL identify the object to which they are assigned in a meaningful way.

Subscriber Certificates SHALL contain meaningful names that represent the Subscriber in a way that is easily understandable for humans. For devices, this MAY be a model number and serial number, or an application process.

The Issuer name of any Certificate SHALL match the Subject name of the issuing CA Certificate, as required by RFC 5280 [2].

4.1.3 Anonymity or Pseudonymity of Subscribers

CA SHALL NOT issue anonymous or pseudonymous Certificates.

4.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting Distinguished Name forms are specified in X.501.

4.1.5 Uniqueness of Names

Name uniqueness for Certificates issued by CAs SHALL be enforced. Each CA SHALL enforce name uniqueness within the X.500 name space within its domain. Name uniqueness is not violated when multiple Certificates are issued to the same Subscriber (e.g.: Certificates for different curves). Name uniqueness is enforced for the entire Subject Distinguished Name of the Certificate rather than a particular attribute (e.g., the common name field). The CA SHALL identify the method for checking uniqueness of Subject Distinguished Names within its domain.

4.1.6 Recognition, Authentication, and Role of Trademarks

CAs operating under this policy SHALL NOT issue a Certificate knowing that it infringes the trademark of another party. Certificate Applicants SHALL NOT use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Neither the PKI-PA, nor any CA SHALL be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any Intellectual Property Rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark. The PKI-PA, and any CA SHALL be entitled, without liability to any Certificate Applicant, to reject or suspend any Subscriber Agreement because of such dispute.

4.2 Initial Identity Validation

4.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a Certificate generates its own keys, that party SHALL be required to prove possession of the private key, which corresponds to the public key in the Certificate request. The GSMA CI SHALL prove that the Subscriber possesses the private key by verifying the Subscriber's digital signature on the PKCS #10 [13] Certificate Signing Request (CSR) with the public key in the CSR.

When the key pair is generated by the CA on behalf of a Subscriber; then in this case proof of possession of the private key by the Subscriber is not required.

4.2.2 Authentication of Organisation Identity

The GSMA CI's Certificate issuance process SHALL authenticate the identity of the organisation named in the Subscriber Agreement by confirming that the organisation:

- Exists in a business database (e.g., Dun and Bradstreet), or alternatively, has organisational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organisation, such as articles of incorporation, Certificate of Formation, Charter Documents, or a business license that allow it to conduct business
- Conducts business at the address listed in the agreement

4.2.3 Authentication and Authorisation of the Subscriber

This CP allows a Certificate to be issued only to Subscriber representing a single entity (e.g. an eUICC) or a SubCA. CAs SHALL NOT issue Certificates that contain a public key whose associated private key is shared. The GSMA CI SHALL validate the requestor's authorisation to act in the name of the Subscriber prior to issuing a Certificate. The GSMA CI SHALL obtain the PKI-PA's approval prior to issuing Certificates. In the case of an SM server, SM Server subCA or EUM CA, the criteria for the Certificate issuance SHALL be based on the certification process defined in SGP.24 [19] or SGP.16 [20] for Consumer or M2M respectively.

The GSMA CI's Certificate issuance process SHALL verify that :

- The representative submitting the Subscriber Agreement and Certificate Application, is a duly authorised representative of the organisation as an employee, partner, member, agent, etc. and is authorised to act on behalf of the organisation
- The corporate Contact listed in the Subscriber Agreement is an officer in the organisation and can act on behalf of the organisation
- The administrator listed in the Subscriber Agreement and Certificate Application, is a duly authorised representative of the organisation as an employee, partner, member, agent, etc. and is authorised to act on behalf of the organisation.
- The contacts listed on the Subscriber Agreement are authorised to act on behalf of the organisation
-

4.2.4 Non-verified Subscriber Information

Non-verifiable information MAY be included in eUICC PKI Certificates, such as:

- Organisation Unit (OU)
- Any other information designated as non-verified in the Certificate

4.2.5 VOID

4.2.6 Criteria for Interoperation

The PKI-PA SHALL determine the interoperability criteria for CAs operating under this policy.

4.3 Identification and Authentication for Re-key Requests

Re-keying a Certificate consists of creating a new Certificate with a different public and private key pair (and serial number) while retaining the remaining contents of the old Certificate.

The new Certificate MAY be assigned a different Validity Period, key identifiers, specify a different CRL distribution point, and/or be signed with a different issuing CA key.

After Certificate rekey, the issuing CA MAY or MAY NOT revoke the old Certificate, but SHALL NOT rekey, renew, or modify it further.

4.3.1 Identification and Authentication for Routine re-key

CA Certificate re-key SHALL follow the same procedures as initial Certificate issuance.

For SM-DP, SM-SR, SM-DP+ (SubCA) and SM-DS (SubCA) server Certificates, re-key SHALL follow the same procedures as initial Certificate issuance.

For eUICC end-entity Certificates, no stipulation.

4.3.2 Identification and Authentication for Re-key After Revocation

Once a Certificate has been revoked, a re-key request SHALL require issuance of a new Certificate. The Subscriber SHALL go through the initial identity validation process per CP section 4.2.

4.4 Identification and Authentication for Revocation Request

After a Certificate has been revoked other than during a renewal or update action, the Subscriber is required to go through the initial registration process described per CP section 4.2 to obtain a new Certificate.

Revocation requests SHALL be authenticated and MAY be authenticated using that Certificate's public key, regardless of whether or not the associated private key has been Compromised.

5 Certificate Life-Cycle Operational Requirements

5.1 Certificate Application

A GSMA CI RootCA or SubCA SHALL document the processes, procedures, and requirements of their Certificate issuance process.

5.1.1 Who Can Submit a Certificate Application

An applicant for a Certificate SHALL be the Subscriber or an authorised representative of the Subscriber.

An application for a Certificate SHALL be submitted by the Subscriber or an authorised representative of the Subscriber.

Note: prior to request a Certificate, the applicant SHOULD be compliant with SGP.24 and SGP.16

5.1.2 Enrolment Process and Responsibilities

All communications with GSMA CI 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 (see section 5.1.3)
- Responding to authentication requests in a timely manner
- Submitting required payment

5.1.3 Certificate Signing Request (CSR)

An Applicant willing to request a Certificate from a GSMA CI SHALL send a Certificate Signing Request (CSR) to that GSMA CI. This section describes the format of the CSR.

The CSR SHALL follow PKCS #10 format as defined in [13], with the specific coding given in this section.

All CSRs defined in this section SHALL be signed using the Subject entity's private key which public part is included in the CSR, as defined in [13]. The algorithm identifier and parameters set in the `CertificationRequest.CertificationRequestInfo.subjectPKInfo` and in `CertificationRequest.signatureAlgorithm` SHALL be identical. The algorithm identifier and parameters related to the issuing GSMA CI RootCA or GSMA CI SubCAkey pair SHALL also be identical.

Additional attributes MAY be present in the `CertificationRequestInformation`, but their usage is out of scope of this specification.

The generated Certificate following an accepted CSR SHALL have its Validity Period set according to its nature as defined in section 8.2.

NOTE: CSR are described using table representation for easiness, but conform to the ASN.1 format given in RFC 2986 [13].

5.1.3.1 CSR for EUM CA Certificate

This CSR is applicable for EUM Certificates defined in SGP.02 [9] and SGP.22 [11]. The EUM Certificate (denoted as CERT.EUM.ECDSA in SGP.22 [11] and simply denoted as EUM Certificate in SGP.02 [9]) SHALL be returned in X.509 format.

This CSR SHALL have its `CertificationRequestInformation` fields set as described in the following table.

Field	Value Description
`version`	V1(0)
`subject`	Distinguished Name of the EUM (Certificate subject) as defined in SGP.22 [11].
`subjectPKInfo`	`subjectPublicKey`= public key generated by the EUM. `algorithm.algorithm` and `algorithm.parameters` SHALL identify one of the curve defined SGP.22 [11] or SGP.02 [9] which SHALL also be supported by the CA.
`Attributes (list of)`	

`(ExtensionRequest)`	Extension request for Certificate Policies indicated an EUM CA Certificate.
	`extnID = id-ce-certificatePolicies`
	`extnValue = id-rspRole-eum or id-rspRole-eum-v2 (value defined in SGP.22 [11])`

`(ExtensionRequest)`	Extension request for subjectAltName
	`extnID = id-ce-subjectAltName`
	`extnValue = { registeredID (8) = EUM OID }`

`(ExtensionRequest)`	Extension request for Name Constraints
	`extnID = id-ce-nameConstraints`
	`extnValue NameConstraints ::= <as defined in SGP.22[11]>`

Table 2: CSR for EUM Certificate fields

By verifying that the CSR is related to an EUM Certificate request (e.g. based on Certificate Policy value), and in addition to extensions specified in the CSR, the GSMA CI RootCA or GSMA CI SubCA SHALL automatically include the other extensions defined in SGP.22 [11]:

- Authority Key Identifier (id-ce-authorityKeyIdentifier)
- Subject Key Identifier (id-ce-subjectKeyIdentifier)
- Key usage (id-ce-keyUsage) with values as defined in SGP.22 [11]

- Basic Constraints (id-ce-basicConstraints) with values as defined in SGP.22 [11]. The value of the pathLenConstraint SHALL be set according to the provided Certificate Policy.
- CRL Distribution Point (id-ce-cRLDistributionPoints) with values as defined in SGP.22 [11]

5.1.3.2 CSRs for SM-DP+ Certificates (CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, CERT.DPSubCA.ECDSA or CERT.DP.TLS)

This CSR is applicable for SM-DP+ Certificates (CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, CERT.DPSubCA.ECDSA or CERT.DPauth.TLS) defined in SGP.22 [11]. The Certificate resulting of this CSR SHALL be returned in X.509 format as defined in SGP.22 [11].

A CSR for one of these four Certificates SHALL have its `CertificationRequestInformation` fields set as described in the following table.

A distinct CSR SHALL be sent for each of these three Certificates.

Field	Value Description
`version`	V1(0)
`subject`	Distinguished Name of the SM-DP+ (Certificate subject) as defined in SGP.22 [11].
`subjectPKInfo`	`subjectPublicKey`= public key generated by the SM-DP+. `algorithm.algorithm` and `algorithm.parameters` SHALL identify one of the curve defined SGP.22 [11] which SHALL also be supported by the CA.
`Attributes (list of)`	

`(ExtensionRequest)`	Extension request for Certificate Policies indicated an SM-DP+ Certificate.
	`extnID = id-ce-certificatePolicies`
	`extnValue = id-rspRole-dp-auth,` or `id-rspRole-dp-pb,` or `id-rspRole-dp-tls,` or id-rspRole-dpSubCa
	or
	`extnValue = id-rspRole-dp-auth-v2,` or `id-rspRole-dp-pb-v2,` or `id-rspRole-dp-tls-v2`
	Each of these OIDs are defined in SGP.22 [11]

`(ExtensionRequest)`	Extension request for subjectAltName
	`extnID = id-ce-subjectAltName`
	`extnValue = { registeredID (8) = SM-DP+ OID }`
	for CERT.DPauth.ECDSA, CERT.DPpb.ECDSA and CERT.SubCA.ECDSA.
	`extnValue = { dNSName(2), registeredID (8) = SM-DP+ OID }`
	for CERT.DP.TLS

Table 3: CSRs for SM-DP+ Certificate fields

By verifying that the CSR is related to an SM-DP+ Certificate for authentication, binding, SubCA or TLS request (e.g. based on Certificate Policy value), and in addition to extensions specified in the CSR, the GSMA CI RootCA or GSMA CI SubCA SHALL automatically include the other extensions defined in SGP.22 [11]:

- Authority Key Identifier (id-ce-authorityKeyIdentifier)
- Subject Key Identifier (id-ce- subjectKeyIdentifier)
- Key usage (id-ce-keyUsage)
- CRL Distribution Point (id-ce-cRLDistributionPoints)
- (only for CERT.DP.TLS) Extended Key usage (id-ce-extKeyUsage)
- (only for CERT.DPSubCA.ECDSA) Basic Constraints (id-ce-basicConstraints)

5.1.3.3 CSRs for SM-DS Certificates (CERT.DSauth.ECDSA, CERT.DSSubCA. or CERT.DS.TLS)

This CSR is applicable for SM-DS Certificates (CERT.DSauth.ECDSA, CERT.DSSubCA.ECDSA or CERT.DS.TLS) defined in SGP.22 [11]. The Certificate resulting of this CSR SHALL be returned in X.509 format as defined in SGP.22 [11].

A CSR for one of these three Certificates SHALL have its `CertificationRequestInformation` fields set as described in the following table.

A distinct CSR SHALL be sent for each of these two Certificates.

Field	Value Description
`version`	V1(0)
`subject`	Distinguished Name of the SM-DS (Certificate subject) as defined in SGP.22 [11].
`subjectPKInfo`	`subjectPublicKey`= public key generated by the SM-DS. `algorithm.algorithm` and `algorithm.parameters` SHALL identify one of the curve defined SGP.22 [11] which SHALL also be supported by the CA.
`Attributes (list of)`	

`(ExtensionRequest)`	Extension request for Certificate Policies indicated an SM-DS Certificate.
	`extnID = id-ce-certificatePolicies`
	`extnValue = id-rspRole-ds-auth,` or `id-rspRole-ds-tls,` or id-rspRole-dpSubCa
	or
	`extnValue = id-rspRole-ds-auth-v2,` or `id-rspRole-ds-tls-v2`
	Each of these OIDs are defined in SGP.22 [11]

(ExtensionRequest)	Extension request for subjectAltName extnID = id-ce-subjectAltName extnValue = { registeredID (8) = SM-DS OID } for CERT.DSauth.ECDSA and CERT.DSSubCA.ECDSA extnValue = { dNSName(2), registeredID (8) = SM-DS OID } for CERT.DS.TLS

Table 4: CSRs for SM-DS Certificate fields

By verifying that the CSR is related to an SM-DS Certificate for authentication, SubCA or TLS request (e.g. based on Certificate Policy value), and in addition to extensions specified in the CSR, the GSMA CI RootCA or GSMA CI SubCA SHALL automatically include the other extensions defined in SGP.22 [11]:

- Authority Key Identifier (id-ce-authorityKeyIdentifier)
- Subject Key Identifier (id-ce-subjectKeyIdentifier)
- Key usage (id-ce-keyUsage)
- CRL Distribution Point (id-ce-cRLDistributionPoints)
- (only for CERT.DS.TLS) Extended Key usage (id-ce-extKeyUsage)
- (only for CERT.DSSubCA.ECDSA) Basic Constraints (id-ce-basicConstraints)

5.1.3.4 CSRs for SM-DP Certificate (CERT.DP.ECDSA)

This CSR is applicable for SM-DP Certificate (CERT.DP.ECDSA) defined in SGP.02 [9]. The Certificate resulting of this CSR SHALL be returned in GlobalPlatform format as defined in SGP.02 [9].

This CSR SHALL have its `CertificationRequestInformation` fields set as described in the following table.

Field	Value Description
version	V1(0)
subject	Distinguished Name of the SM-DP (Certificate subject). Note: This information is not set in the generated Certificate.
subjectPKInfo	subjectPublicKey= public key generated by the SM-DP. algorithm.algorithm and algorithm.parameters SHALL identify one of the curve defined in SGP.02 [9] which SHALL also be supported by the CA. This information SHALL be used to build the Public Key Data Object (tag '7F49')
Attributes (list of)	
(ExtensionRequest)	Extension request for subjectAltName extnID = id-ce-subjectAltName extnValue = { registeredID (8) = SM-DP OID } This value SHALL is set in the subject identifier field (tag '5F20')

Table 5: CSRs for SM-DP Certificate fields

By verifying that the CSR is related to a CERT.DP.ECDSA, the GSMA CI RootCA or GSMA CI SubCA SHALL automatically include in the generated CERT.DP.ECDSA the other values according to SGP.02 [9].

5.1.3.5 CSRs for SM-SR Certificate (CERT.SR.ECDSA)

This CSR is applicable for SM-SR Certificate (CERT.SR.ECDSA) defined in SGP.02 [9]. The Certificate resulting of this CSR SHALL be returned in GlobalPlatform format as defined in SGP.02 [9].

This CSR SHALL have its `CertificationRequestInformation` fields set as described in the following table.

Field	Value Description
`version`	V1(0)
`subject`	Distinguished Name of the SM-SR (Certificate subject). Note: This information is not set in the generated Certificate.
`subjectPKInfo`	`subjectPublicKey`= public key generated by the SM-SR. `algorithm.algorithm` and `algorithm.parameters` SHALL identify one of the curve defined in SGP.02 [9] which SHALL also be supported by the CA. This information SHALL be used to build the Public Key Data Object (tag '7F49')
`Attributes (list of)`	

`(ExtensionRequest)`	Extension request for subjectAltName
	`extnID = id-ce-subjectAltName`
	`extnValue = { registeredID (8) = SM-SR OID }`
	This value SHALL is set in the subject identifier field (tag '5F20')

Table 6: CSRs for SM-SR Certificate fields

By verifying that the CSR is related to a CERT.SR.ECDSA, the GSMA CI RootCA or GSMA CI SubCA SHALL automatically include in the generated CERT.SR.ECDSA the other values according to SGP.02 [9].

5.2 Certificate Application Processing

It is the responsibility of the GSMA CI to verify that the information in Certificate Applications is accurate.

5.2.1 Performing Identification and Authentication Functions

The identification and authentication functions SHALL meet the requirements described in CP subsections 4.2 and 4.3.

Prior to Certificate issuance, a Subscriber SHALL be required to sign an agreement detailing Subscriber responsibility, which SHALL include the requirement that the Subscriber SHALL protect the private key and use the Certificate and private key for authorised purposes only.

5.2.2 Approval or Rejection of Certificate Applications

A GSMA CI SHALL approve a Certificate Application if all of the following criteria are met:

- For Consumer, the EUM and SM Server Providers have demonstrated and declared compliance with SGP.21 [18] and SGP.22 [11] as defined in SGP.24 [19].
- For M2M, the EUM and SM Server Providers have demonstrated and declared compliance with SGP.01 [21] and SGP.02 [9] as defined in SGP.16 [20].
  - A fully executed Subscriber Agreement
  - A signed Certificate Application
  - Successful identification and authentication of all required information
  - Receipt of all requested supporting documentation
  - Payment (if applicable) has been received
  - The Subcriber respond to notice within a specific time.

  A GSMA CI SHALL reject a Certificate Application if any of the above criteria failed or a Security Incident has taken place at Subscriber level but the findings have not yet been mitigated and approved by the Incident Coordinator

The PKI-PA MAY approve or reject a Certificate Application.

5.2.3 Time to Process Certificate Applications

GSMA CI SHALL begin processing Certificate Applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement.

5.3 Certificate Issuance

Upon receiving a request for a Certificate, the GSMA CI SHALL respond in accordance with the requirements set forth in the CP.

While the Subscriber MAY do most of the data entry for a Certificate request and profile, the GSMA CI SHALL verify that the information is correct and accurate.

5.3.1 CA Actions During Certificate Issuance

Upon receiving the request, the GSMA CI SHALL:

- verify the identity of the requester.
- verify the authority of the requester and the integrity of the information in the Certificate request.
- build and sign a Certificate if all Certificate requirements have been met.
- make the Certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged their obligations as described in section 11.6.3.

All authorisation and other attribute information received from a prospective Subscriber SHALL be verified before inclusion in a Certificate.

5.3.2 Notification to Subscriber by the CA of Issuance of Certificate

GSMA CI SHALL notify Subscribers that it has created the requested Certificate(s), and provides Subscribers with access to the Certificates by notifying them that their Certificates are available and the means for obtaining them. Certificates SHALL be made available to

Subscribers, either via download from a web site or via a message sent to the Subscriber containing the Certificate.

5.4 Certificate Acceptance

The Subscriber Agreement SHALL be executed setting forth the responsibilities of all parties before the PKI-PA authorises issuance of a Certificate by the issuing GSMA CI. Once a Certificate has been issued, its acceptance by the Subscriber SHALL commence interoperability with the eUICC PKI and triggers the Subscriber's obligations under the Subscriber Agreement and this CP.

5.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes Certificate acceptance by the Subscriber:

- Downloading a Certificate
- Failure to object to the Certificate or its content

5.4.2 Publication of the Certificate by the CA

GSMA CI RootCA or GSMA CI SubCA Certificates SHALL be published in a publicly available repository as specified in CP section 3.1.

This policy makes no stipulation regarding publication of Subscriber Certificates.

5.4.3 Notification of Certificate Issuance by the CA to Other Entities

The PKI-PA SHALL be notified whenever a GSMA CI operating under this policy issues a CA Certificate.

5.5 Key Pair and Certificate Usage

5.5.1 Subscriber Private Key and Certificate Usage

Subscriber private key usage SHALL be specified through Certificate extensions, including the key usage and extended key usage extensions, in the associated Certificate. Subscribers SHALL protect their private keys from unauthorised use and SHALL discontinue use of the private key following expiration or revocation of the Certificate.

Certificate use SHALL be consistent with the KeyUsage field extensions included in the Certificate.

5.5.2 Relying Party Public Key and Certificate Usage

Relying Parties SHOULD assess:

- The restrictions on key and Certificate usage specified in this CP and which are specified in critical Certificate extensions, including the basic constraints and key usage extensions.
- The status of the Certificate and all the CA Certificates in the Certificate Chain. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to determine whether reliance on a Certificate prior to revocation of a Certificate in the Certificate Chain is reasonable. Any such reliance is made solely at the risk of the Relying Party.

5.6 Certificate Renewal

Certificate renewal is the issuance of a new Certificate for an existing key pair without changing any information in the Certificate except the Validity Period and serial number.

5.6.1 Circumstance for Certificate Renewal

A Certificate MAY be renewed if the public key has not reached the end of its Validity Period, the associated private key has not been Compromised, and the Subscriber name and attributes are unchanged. Certificates MAY be renewed:

- To maintain continuity of Certificate usage

A Certificate MAY be renewed after expiration. The original Certificate MAY or MAY NOT be revoked, but SHALL NOT be further re-keyed, renewed, or modified.

Certificates SHALL never be renewed if deemed to be compromised. Instead a new key pair SHALL be generated and a new Certificate issued based on these keys.

5.6.2 Who MAY Request Renewal

The following MAY request a Certificate renewal:

- The Subscriber of the Certificate or an authorised representative of the Subscriber
- The GSMA CI MAY request a renewal on behalf of a Subscriber
- The GSMA CI MAY request a renewal of its own Certificate(s)
- The PKI-PA MAY request renewal of GSMA CI RootCA or GSMA CI SubCA Certificates
- The Incident Coordinator MAY request renewal of all Certificates during a Security Incident, if a Certificate has been deemed to be Compromised. In such a situation this is not allowed by any other party.

5.6.3 Processing Certificate Renewal Requests

For a Certificate renewal request, the GSMA CI SHALL confirm the identity of the Subscriber in accordance with the requirements specified in CP section 4.2.

GSMA CI RootCA or GSMA CI SubCA Certificate renewal SHALL be approved by the PKI-PA following the criteria defined in SGP.28 [22].

5.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of Certificate renewal to the Subscriber SHALL be in accordance with CP section 5.3.2.

5.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a renewed Certificate SHALL be in accordance with CP section 5.4.1.

5.6.6 Publication of the Renewal Certificate by the CA

Publication of a renewed Certificate SHALL be published in a publicly available repository as specified in CP section 3.1.

5.6.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of Certificates SHALL be in accordance with CP section 5.4.3.

5.7 Certificate Re-key

Certificate re-key consists of creating a new Certificate for a different key pair (and serial number) but can retain the contents of the original Certificate's Subject Name. Certificate re-key does not violate the requirement for name uniqueness. The new Certificate MAY be assigned a different Validity Period, and/or be signed with a different key.

5.7.1 Circumstance for Certificate Re-key

Certificates SHALL be re-keyed:

- To maintain continuity of Certificate usage
- For loss or Compromise of original Certificate's private key
- By a CA during recovery from key Compromise

A Certificate SHALL be re-keyed after expiration. The original Certificate SHALL NOT be further re-keyed, renewed, or modified.

5.7.2 Who May Request Certification of a New Public Key

The following MAY request a Certificate re-key:

- The Subscriber of the Certificate or an authorised representative of the Subscriber
- The GSMA CI MAY request a re-key on behalf of a Subscriber
- The CA MAY request a re-key of its own Certificate(s)
- The CA MAY re-key its issued Certificates during recovery from a CA key Compromise
- The PKI-PA MAY request re-key of GSMA CI RootCA or GSMA CI SubCA Certificates
- The Incident Coordinator MAY request a re-key of any Certificate if deemed necessary during a Security Incident.

5.7.3 Processing Certificate Re-keying Requests

For Certificate re-key, the GSMA CI or GSMA CI SubCA SHALL confirm the identity of the Subscriber in accordance with the requirements specified in this CP for the authentication of an original Certificate Application. GSMA CI RootCA and GSMA CI SubCA Certificate(s) re-key SHALL be approved by the PKI-PA.

5.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed Certificate to the Subscriber SHALL be in accordance with CP section 5.3.2.

5.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting Acceptance of a re-keyed Certificate SHALL be in accordance with CP section 5.4.1.

5.7.6 Publication of the Re-keyed Certificate by the CA

Publication of a re-keyed Certificate SHALL be published in a publicly available repository as specified in CP section 3.1.

5.7.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of Certificates SHALL be in accordance with CP section 5.4.3.

5.8 Certificate Modification

Modifying a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old Certificate. The old Certificate MAY or MAY NOT be revoked, but SHALL NOT be further re-keyed, renewed, or modified.

5.8.1 Circumstance for Certificate Modification

Certificates MAY be modified:

- For a Subscriber organisation name change or other Subscriber characteristic change
- For Validity Period

A Certificate MAY be modified after expiration.

The original Certificate MAY NOT be revoked, but SHALL NOT be further re-keyed, renewed, or modified. If revoked, the CA SHALL publish the revocation status.

5.8.2 Who May Request Certificate Modification

The following MAY request a Certificate modification:

- The Subscriber of the Certificate or an authorised representative of the Subscriber
- The GSMA CI MAY request a Certificate modification on behalf of a Subscriber
- The CA MAY request a Certificate modification of its own Certificate
- The CA MAY modify its issued Certificates during recovery from a CA key Compromise
- The PKI-PA MAY request modification of GSMA CI RootCA or GSMA CI SubCA Certificates
- The Incident Coordinator MAY request modification of any Certificate if deemed necessary during a Security Incident.

5.8.3 Processing Certificate Modification Requests

For Certificate modification requests, the GSMA CI SHALL confirm the identity of the Subscriber in accordance with the requirements specified in this CP for the authentication of an initial Certificate Application.

GSMA CI RootCA and GSMA CI SubCA Certificate modification SHALL be approved by the PKI-PA.

5.8.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a new Certificate to the Subscriber SHALL be in accordance with CP section 5.3.2.

5.8.5 Conduct Constituting Acceptance of Modified Certificate

Conduct constituting Acceptance of a modified Certificate SHALL be in accordance with CP section 5.4.1.

5.8.6 Publication of the Modified Certificate by the CA

Publication of a modified Certificate SHALL be published in a publicly available repository as specified in CP section 3.1.

5.8.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of Certificates SHALL be in accordance with CP section 5.4.3.

5.9 Certificate Revocation and Suspension

The following Certificates MAY be revoked and suspended:

- GSMA Root CI Certificate (CERT.CI.ECDSA)
- GSMA CI SubCA Certificate (CERT.CISubCA.ECDSA)
- EUM Certificate (CERT.EUM.ECDSA)
- EUM SubCA Certificate (CERT.EUMSubCA.ECDSA)
- SM-DP+ Certificates (CERT.DPauth.ECDSA, CERT.DPpb.ECDSA)
- SM-DP+ SubCA Certificate (CERT.DPSubCA.ECDSA)SM-DP+ TLS Certificate (CERT.DP.TLS)
- SM-DS Certificate (CERT.DSauth.ECDSA)
- SM-DS SubCA Certificate (CERT.DSSubCA.ECDSA)
- SM-DS TLS Certificate (CERT.DS.TLS)

Because of their potential number, eUICC Certificates CERT.ECASD.ECDSA [11] are not revoked individually. When a eUICC is Compromised, all similar products MAY be affected. In this case, the EUM Certificate used to issue this eUICC Certificate MAY be revoked instead of individual eUICC Certificates.

With the exception of CAs that issue Certificates with a short validity period (see section 8.2), CAs SHALL issue CRLs. CRL SHALL cover all unexpired Certificates issued under this policy except for OCSP responder Certificates that include the id-pkix-ocsp-nocheck extension. CAs MAY provide additional means for publishing the revocation status.

GSMA CI RootCA or GSMA CI SubCA SHALL make public a description of how to obtain revocation information for the Certificates they publish, and an explanation of the consequences of using dated revocation information. This information SHALL be given to Subscribers during Certificate request or issuance, and SHALL be readily available to any potential Relying Party.

Revocation requests SHALL be authenticated. Requests to revoke a Certificate MAY be authenticated using that Certificate's associated private key, regardless of whether or not the private key has been Compromised.

5.9.1 Circumstances for Revocation

A Certificate SHALL be revoked when the binding between the Subject and the Subject's public key defined within the Certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- The confidentiality or integrity of the private key corresponding to the Certificate has been Compromised due to:
    - Disclosure or theft
    - Natural or man-made disasters
    - Physical Compromise where the key is stored and/or used
    - Equipment failure or production fault
    - Abuse of the key or Certificate(s) (other than the description in SGP.22 [11])
- After fixing critical bugs in hardware or software of the system storing and/or using the key
- The Subscriber or an authorised representative of the Subscriber asks for the Certificate to be revoked for any reason whatsoever
- The Subscriber can be shown to have violated the stipulations of its Subscriber Agreement (including, for example, a failure to maintain SAS certification)
- The Subscriber Agreement with the Subscriber has been terminated
- There is an improper or faulty issuance of a Certificate
- A prerequisite to the issuance of the Certificate can be shown to be incorrect;
    - Information in the Certificate is known, or reasonably believed, to be false.
    - Any other circumstance that MAY reasonably be expected to affect the reliability, security, integrity or trustworthiness of the Certificate or the cryptographic key pair associated with the Certificate.
    - The Subscriber has not submitted payment when due
- Identifying information of the Subscriber in the Certificate becomes invalid (e.g.: invalid Fully-QualifiedDomain Name)
- Attributes asserted in the Subscriber's Certificate are incorrect
- The Certificate was issued:
    - In a manner not in accordance with the procedures required by the CP
    - To a person other than the one named as the Subject of the Certificate
    - Without the authorisation of the entity named as the Subject of such Certificate
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading
- The continued use of that Certificate is harmful to GSMA ecosystem
- A CA has issued a Certificate they are not authorised to issue

Whenever any of the above circumstances occur, the associated Certificate SHALL be revoked and placed on the CRL. Revoked Certificates SHALL be included on all new publications of the Certificate status information until the Certificates expire.

In addition, if it is determined subsequent to issuance of the new Certificates that a private key used to sign requests for one or more additional Certificates MAY have been Compromised at the time the requests for additional Certificates were made, all Certificates authorised by directly or indirectly chaining back to that Compromised key SHALL be revoked.

5.9.2 Who can Request Revocation

Within the eUICC PKI, revocation requests MAY be made by:

- The Subscriber of the Certificate or any authorised representative of the Subscriber
- The CA for Certificates within its domain
- The PKI-PA
- The Incident Coordinator if deemed necessary during a Security Incident

A GSMA CI SHALL NOT revoke any Certificate that it has issued without the approval of the PKI-PA.

Other (third) parties MAY submit Certificate problem reports informing the issuing CA of reasonable cause to revoke the Certificate.

5.9.3 Procedure for Revocation Request

A request to revoke a Certificate SHALL identify the date of the request, the Certificate to be revoked, the reason for revocation, and allow the requestor to be authenticated.

Prior to the revocation of a Subscriber Certificate, the GSMA CI SHALL authenticate the request.

GSMA CI is entitled to request the revocation of its Subscriber Certificates. GSMA CI SHALL obtain approval from the PKI-PA prior to performing the revocation functions. The GSMA CI SHALL send a written notice and brief explanation for the revocation to the Subscriber.

The requests from GSMA CI to revoke a Certificate SHALL be authenticated by the PKI-PA. PKI-PA SHALL provide a final decision of a Certificate revocation request within five (5) business days of receipt upon the circumstances defined in section 5.9.1. If revocation is required the GSMA CI SHALL be notified within this period.

Upon revocation of a Certificate, the CA that issued the Certificate SHALL publish its revocation status.

5.9.4 Revocation Request Grace Period

Revocation requests SHOULD be submitted as promptly as possible within a reasonable time of becoming aware of a revocation circumstance listed in CP section 5.9.1.

5.9.5 Time Within Which CA Must Process the Revocation Request

If a Certificate has been declared to be Compromised during a Security Incident it SHALL be revoked within 24 hour of the revocation request being received.

5.9.6 Time to Process Certificate Application after Recovery from Disaster

If an already identified Subscriber Certificate is revoked due to a Security Incident, and the root cause of the revocation is verifiably mitigated, the GSMA CI SHALL begin processing the new Certificate Application. There is no time stipulation to complete the processing of a Certificate Application unless otherwise indicated in the relevant Subscriber Agreement.

5.9.7 Revocation Checking Requirement for Relying Parties

Relying Parties SHOULD check the status of Certificates on which they wish to rely using the means provided by the CA (e.g.: CRL).

Each Certificate in the eUICC PKI SHALL include an indication of the means by which its revocation status is available.

5.9.8 CRL Issuance Frequency

CRLs SHALL be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information MAY be issued more frequently than the issuance frequency described below. A CA SHALL ensure that superseded Certificate status information is removed from the PKI Repository upon posting of the latest Certificate status information. The GSMA CI RootCA or SubCA SHALL issue the CRLs at least every week. Other CAs SHALL issue CRLs at least once every (1) month. All CAs SHALL issue CRLs within 24 hours after revoking a Certificate, with the value of the nextUpdate field not later than their required frequency.

Certificate status information SHALL be published not later than the next scheduled update. This facilitates the local caching of Certificate status information for off-line or remote operation. CAs SHALL coordinate with the PKI Repositories to which they post Certificate status information to reduce latency between creation and availability.

If Certificates have to be revoked due to a Security Incident where the Certificates were compromised, the CA SHALL reissue a CRL immediately after revoking the Certificates.

5.9.9 VOID

5.9.10 VOID

5.9.11 VOID

5.9.12 Other Forms of Revocation Advertisements Available

A CA MAY use other methods to publicise the revocation status of the Certificates it has issued in combination with the public CRL repository. Any alternative method SHALL meet the following requirements:

- The alternative method SHALL be described by the CA
- The alternative method SHALL provide authentication and integrity services commensurate with the assurance level of the Certificate being verified

- The alternative method SHALL meet the issuance and latency requirements for CRLs stated in section 5.9.8.

5.9.13 Special Requirements Regarding Key Compromise

The PKI-PA SHALL notify eUICC PKI Participants of a GSMA CI RootCA Certificate revocation using commercially reasonable efforts.

5.9.14 Circumstances for Suspension

The eUICC PKI does not offer suspension services for its Certificates.

5.10 Certificate Status Services

5.10.1 Operational Characteristics

No stipulation.

5.10.2 Service Availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the Certificate status service.

5.10.3 Optional Features

No stipulation.

5.11 VOID

5.12 Key Escrow and Recovery

No stipulation.

6 Security Controls

Every systems or party that is part of the PKI infrastructure has a responsibility to sustain the trust of the RSP solution, the confidentiality of mobile communication, and the availability of global remote SIM provisioning. The controls that follow are designed to guarantee this and SHALL be followed.

6.1 Disaster Recovery

All stakeholder that take part within the PKI infrastructure SHALL follow the following matrix during a Security Incident.

Role	Activities	Responsible	Approver	Consulted	Informed
Incident Owner	Manages all security processes and requirements within the company and communicates with the Incident Coordinator.	X	X		

Incident Coordinator	Coordinates Security Incidents and validates the mitigation plan from the Incident Owner.		X		
SAS Certification Body	Considers impact of security incident on SAS accreditation of affected site				X
GSMA Communications	Manages external communications in the event of a Security Incident			X	
Relying Parties	Information Collection				X

Table 7: Stakeholder Security Incident Matrix

All stakeholders SHALL inform the Incident Coordinator as soon as possible that a Security Incident has taken place. At this time the Incident Coordinator SHALL document this fact and determine, together with the Incident Owner, the possible impact of the Security Incident. If the Security Incident impacts Relying Parties or their data then the Incident Coordinator coordinate the Security Incident and validate the mitigation plan as proposed by the Incident Owner. The criteria whereupon this is decided SHALL be described by the Incident Coordinator.

7 Operational security controls

The GSMA CI requires that all audits of Certification Authorities be performed by qualified auditors in accordance with an eligible audit scheme, such as the WebTrust® Program for Certification Authorities [17] or ETSI [23]. or SM-SM PKI Certificate [15].

All other CAs SHALL conform to the requirements of the GSMA PRD FS.17 SAS Consolidated Security Requirements [8] document, specifically addressing the requirements for:

- Policy, strategy and documentation (including business continuity planning)
- Organisation and responsibility
- Information
- Personnel security
- Physical security
- Key and Certificate management
- Computer and network management
- Audit as FS.05 SAS-UP Methodology [7] for EUM CA and FS.09 SAS-SM Methodology for Subscription Manager Role [15].

8 Cryptographic Keys

8.1 Algorithms and Key Sizes

Keys in the eUICC PKI SHALL satisfy the requirements for algorithm type and key size defined in SGP.22 [11] or SGP.02 [9].

8.2 Certificate Validity Periods

The Certificate validity period SHALL be set to the time limits set forth as follows:

- GSMA CI RootCA and GSMA CI SubCA Certificates SHALL have a validity period of up to 35 years
- EUM Sub-CA and EUM CA Certificates SHALL have a validity period of up to 20 years.
- eUICC Certificates SHALL have an infinite validity period.
- SM-DP, SM-SR, SM-DP+, SM-DP+ SubCA, SM-DS SubCA and SM-DS Certificate SHALL have a validity period of up to 3 years; however, if the Certificate is directly signed by the GSMA CI RootCA, it SHALL have a validity period of up to 10 years.

As described in RFC 5280[2], a Certificate is considered invalid if one of the Certificates in its Certificate chain is invalid. eUICC PKI Participants SHALL cease all use of their Certificates after their validity periods have expired.

SM-DS and SM-DP+ SubCAs MAY use short validity periods for the issuance of their end entity Certifcates (TLS and ECDSA Certificates) to avoid the management of Certificate revocation. In this case, the maximum validity period SHALL be no more than 15 days.

9 Certificate, CRL AND OCSP Profiles

9.1 Certificate Profile

eUICC PKI Certificate SHALL follow the format defined in their respective specifications, i.e. SGP.22 [11] or SGP.02 [9].

9.2 VOID

9.3 VOID

9.4 CRL Profile

The CRL Profile is defined in SGP.22 [11].

9.5 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular Certificate. If this option is supported by a CA, OCSP Responses SHALL conform to RFC 5019 [5] and SHALL either be:

- Signed by the CA that issued the Certificates whose revocation status is being checked, or

- Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. Such OCSP Responder signing Certificate SHALL contain the extension id-pkix-ocsp-nocheck as defined by RFC 2560 [3].

10 Compliance Audits

CAs under this policy are subjected to be audit as defined in section 7.

11 Other Business and Legal Matters

11.1 Fees

11.1.1 Certificate Issuance or Renewal Fees

GSMA CI RootCA or SubCA MAY charge a fee for the issuance, management, and renewal of Certificates.

11.1.2 CA Certificate Access Fees

CAs SHALL NOT charge a fee as a condition of making a CA Certificate available in a repository or otherwise making CA Certificates available to Relying Parties.

11.1.3 Revocation or Status Information Access Fees

CAs SHALL NOT charge a fee as a condition of making Certificate revocation status available in a repository or otherwise available to Relying Parties.

11.1.4 Fees for Other Services

No stipulation.

11.1.5 Refund Policy

CAs stipulate refund policies in the appropriate agreement (e.g., Subscriber Agreement).

11.2 Financial Responsibility

11.2.1 Insurance Coverage

CAs SHOULD maintain a commercially reasonable level of insurance coverage for errors and omissions.

11.2.2 Other Assets

CAs SHALL have sufficient financial resources to maintain their operations and perform their duties.

11.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

11.3 Confidentiality of Business Information

11.3.1 Scope of Confidential Information

CAs SHALL keep the following information confidential and private:

- Certificate Application records, whether approved or disapproved
- Transactional records (both full records and the audit trail of transactions)
- Audit trail records
- Audit reports
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of CA hardware and software

11.3.2 Information not Within the Scope of Confidential Information

eUICC PKI Participants acknowledge that Certificates, Certificate revocation status information, CA Certificate and Certificate revocation status repositories, and information contained within them are not considered Confidential Information.

11.3.3 Responsibility to Protect Confidential Information

CAs SHALL secure confidential information from Compromise and disclosure to unauthorised third parties as specified in section 3 of the FS.17 *SAS Consolidated Security Requirements* [8].

11.4 Privacy of Personal Information

11.4.1 Privacy Plan

CAs SHALL have a privacy plan to protect personally identifying information from unauthorised disclosure. The privacy plan SHALL comply with the requirements specified in section 3 of FS.17 “SAS Consolidated Security Requirements” [8].

11.4.2 Information Treated as Private

CAs SHALL protect Subscribers’ personally identifying information from unauthorised disclosure. Records of individual transactions MAY be released upon request of any Subscribers involved in the transaction or their legally recognised agents. The contents of the archives maintained by CAs operating under this CP SHALL NOT be released unless authorised by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

11.4.3 Information not Deemed Private

CAs SHALL deem all Information included in the Certificates they issue as pubic information.

11.4.4 Responsibility to Protect Private Information

CAs SHALL store private information securely, and SHALL NOT release private information unless authorised by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

11.4.5 Notice and Consent to Use Private Information

The PKI-PA or CAs SHALL NOT be required to provide any notice or obtain the consent of the Subscriber in order to release private information when authorised by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

11.4.6 Disclosure Pursuant to Judicial or Administrative Process

The PKI-PA or CAs SHALL NOT disclose private information to any third party unless authorised by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

11.4.7 Other Information Disclosure Circumstances

No stipulations.

11.5 Intellectual Property Rights

The PKI-PA retains all Intellectual Property Rights in and to this CP.

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue.

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Subscribers are the property of the CAs and Subscribers that are the respective Subjects of these Certificates. Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares.

Without limiting the generality of the foregoing, GSMA's root public keys and Certificates containing them, including all CA and Subscriber public keys and Certificates containing them, are the property of GSMA. GSMA licenses software and hardware manufacturers to reproduce such public key Certificates to place copies in GSMA compliant devices or software.

11.6 Representations and Warranties

The PKI-PA SHALL:

- Review periodic SAS Compliance Audits to ensure that CAs are operating in compliance with the CP
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all Certificates issued under this CP
- Revise this CP to maintain the level of assurance and operational practicality
- Publicly distribute this CP
- Coordinate modifications to this CP to ensure continued compliance by CAs

11.6.1 CA Representations and Warranties

CAs operating under this CP SHALL warrant that:

- The CA procedures are implemented in accordance with this CP
- Any Certificate issued is in accordance with this CP
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
- Their Certificates meet all material requirements of this CP
- The revocation of Certificates in accordance with this CP
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP

11.6.2 Subscriber representations and warranties

Subscribers SHALL sign an agreement containing the requirements the Subscriber SHALL meet including protection of their private keys and use of the Certificates before being issued the Certificates. In addition, Subscribers SHALL warrant that:

- The Subscriber SHALL abide by all the terms, conditions, and restrictions levied on the use of their private keys and Certificates.
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created
- Subscriber's private keys are protected from unauthorised use or disclosure
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true
- All information supplied by the Subscriber and contained in the Certificate is true
- The Certificate is being used exclusively for authorised and legal purposes, consistent with all material requirements of this CP
- The Subscriber SHALL promptly notify the appropriate CA upon suspicion of loss or Compromise of their private key(s)
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise

Subscriber Agreements MAY include additional representations and warranties.

11.6.3 Relying Party Representations and Warranties

This CP does not specify the steps a Relying Party SHOULD take to determine whether to rely upon a Certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., Certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the Relying Party MAY wish to employ in its determination. Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such

information, and that they SHALL bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

11.6.4 Representations and Warranties of Other Participants

No stipulations.

11.7 Disclaimers of Warranties

To the extent permitted by applicable law, Subscriber Agreements SHALL disclaim GSMA's and the applicable Affiliate's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

11.8 Limitations of Liability

The liability (and/or limitation thereof) of Subscribers SHALL be as set forth in the applicable Subscriber Agreements.

11.9 Indemnities

To the extent permitted by applicable law, Subscribers are required to indemnify CAs for:

- Falsehood or misrepresentation of fact by the Subscriber on the Certificate Application
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party
- The Subscriber's failure to take the precautions necessary to prevent the Compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's private key(s)
- The Subscriber's use of a name (including that which infringes upon the Intellectual Property Rights of a third party)

11.10 Term and Termination

11.10.1 Term

The CP becomes effective when approved by the PKI-PA. Amendments to this CP become effective upon publication. This CP has no specified term.

11.10.2 Termination

This CP as amended from time to time SHALL remain in force until it is replaced by a new version. Termination of this CP is at the discretion of the PKI-PA.

11.10.3 Effect of termination and survival

Upon termination of this CP, eUICC PKI Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the Validity Periods of such Certificates.

11.11 Individual Notices and Communications with Participants

eUICC PKI Participants SHALL use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

11.12 Amendments

11.12.1 Procedure for Amendment

The PKI-PA SHALL review this CP at least once every year. Corrections, updates, or changes to this CP SHALL be made available to eUICC PKI Participants, such communication SHOULD include a description of the change and a change justification.

11.12.2 Notification Mechanism and Period

The PKI-PA reserves the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PKI-PA's decision to designate amendments as material or non-material SHALL be within the PKI-PA's sole discretion.

Change notices to this CP SHALL be distributed electronically to eUICC PKI Participants and observers in accordance with the PKI-PA document change procedures.

11.12.3 Circumstances Under Which OID Must be Changed

Object Identifiers (OIDs) SHALL be changed if the PKI-PA determines that a change in the CP reduces the level of assurance provided. If the PKI-PA determines that a change is necessary in the OID corresponding to a Certificate Policy, the amendment SHALL contain new Object Identifiers for the Certificate Policies corresponding to each Class of Certificate. Otherwise, amendments SHALL NOT require a change in Certificate Policy Object Identifier.

11.13 Dispute Resolution Provisions

The PKI-PA SHALL facilitate the resolution between entities when conflicts arise as a result of the use of Certificates issued under this CP.

11.14 Governing Law

This CP is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders. This governing law SHALL govern the enforceability, construction, interpretation, and validity of this CP. This choice of law is made to ensure uniform procedures and interpretation for all GSMA Participants, no matter where they are located.

Agreements incorporating the CP by reference MAY have their own governing law provisions.

11.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. All CAs operating under this CP SHALL comply with applicable law.

11.16 Miscellaneous provisions

11.16.1 Entire Agreement

No Stipulation

11.16.2 Assignment

No stipulation

11.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP SHALL remain in effect until the CP is updated. In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP SHALL remain valid.

11.16.4 Enforcement (Attorneys' fees and waiver of rights)

No Stipulation

11.16.5 Force Majeure

To the extent permitted by applicable law, eUICC PKI agreement (e.g., Subscriber Agreements) SHALL include a force majeure clause protecting GSMA and the applicable Affiliate.

11.17 Other Provisions

No Stipulation.

12 Multiple CA support

12.1 On Servers

To allow the support of multiple CAs where different CAs are operating in different regions or within the same region, a GSMA SAS-SM certified Server (SM-SR, SM-DP, SM-DP+, and SM-DS) can get a Certificate from the CA operating in the targeted region. The Server SHALL use different key pairs (public and private keys) for each of its Certificates whether they are issued by the same or different CA. The same GSMA SAS-SM certified Server OID SHALL be used in all the Certificates of this specific GSMA SAS-SM certified Server.

In figure below, we give an example of a SM-DP+ under CA2 willing to target eUICC1 under CA1.

The SM-DP+2 has the ability to manage eUICC from region 1 and eUICC from region 2. SM-DP+1 can only manage eUICC from region 1.

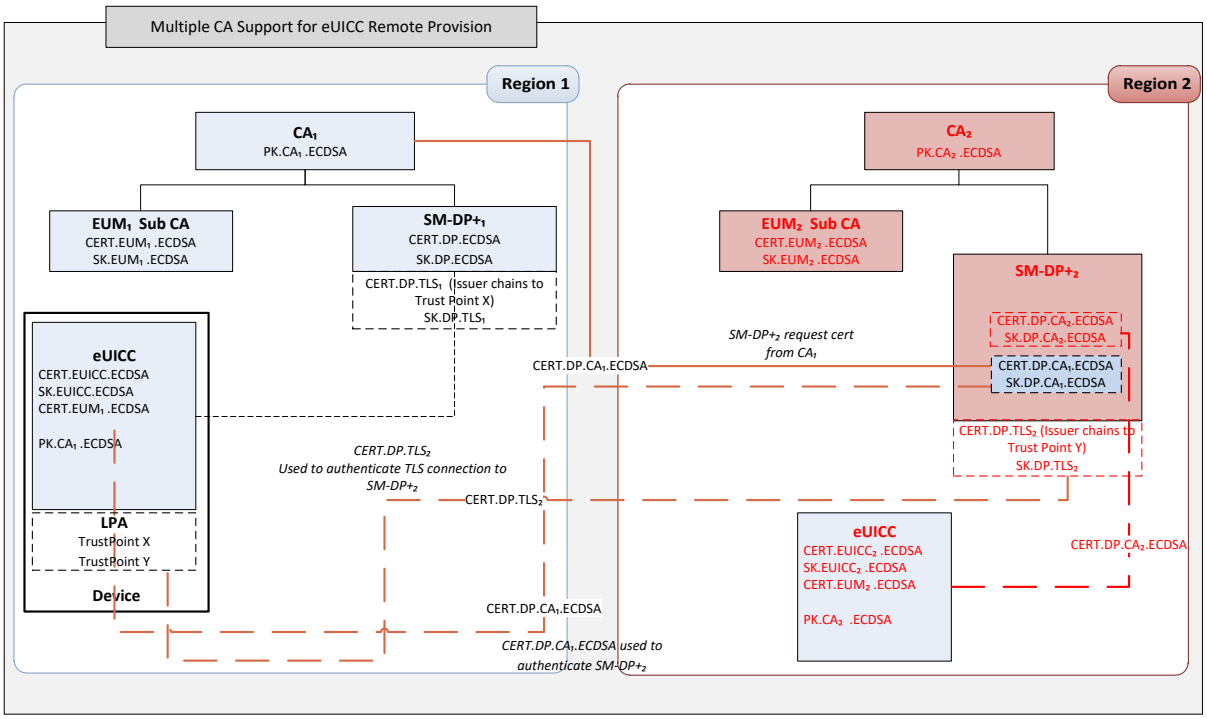

Figure 2: Multiple CAs support

12.2 On eUICCs as defined in SGP.22 [11]

To allow an eUICC to be managed from different regions where different CAs are operating, an eUICC MAY be configured with:

- Several keys for signature verification from different CAs (PK.CI.ECDSA)
- Several keys for signature generation (SK.EUICC.ECDSA), where each key is associated with a Certificate (CERT.EUICC.ECDSA) which chain of trust can lead to different CAs. The eUICC SHALL use different key pairs (public and private keys) for each of its Certificates whether they are issued by the same or different CA. Similarly, the EUM SHALL use different key pairs for each of its Certificates.

12.3 On eUICCs as defined in SGP.02 [9]

Support for Multiple CAs is for further study.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	13 June 2016	Output from ESIMWI5#06	N/A – draft	Gloria Trujillo, GSMA
1.0	14 July 2016	Quality changes	SIM Group	D Goodstein, GSMA
1.1	03 March 2017	ESIMWI5 minor changes on multi-CI, Security Incident, revocation, validity period and alignment with SGP.02 and SGP.22.	SIM Group	D Goodstein, GSMA
2.0	15 July 2019	Output to align the specification with the latest version of SGP.22 and SGP.02	eSIM Group	Yolanda Sanz, GSMA

A.2 Other Information

Type	Description
Document Owner	eSIM Group
Editor / Company	Yolanda Sanz, 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.