GSMA Key Management
Version 7.0
19 September 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA 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 GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

This document outlines procedures for GSMA members and eligible non-members[1] ('Participants') to exchange certificates and key material to facilitate use cases that rely on public key cryptographic algorithms. The procedures will be referred to as 'key management' in the entire document.

The key management procedures have evolved over time and can be grouped into two stages:

- Stage 1: Manual exchange of certificates (FS.34 version 6 and lower). These procedures were developed as a first approach to facilitate early adoption.
- Stage 2: Key management with enhanced scalability/automation (FS.34 version 7.x and higher). These procedures, as described in this document, are designed to enable efficient and automated key management, and are intended for widespread deployment at scale. Stage 2 makes use of the GSMA RAEX Certificate Database, which serves as a repository for all root certificates.

1.2 Scope

This document specifies key management procedures for the use cases outlined in Annex A to Annex C. Key management for additional use cases may be added to this document in the future. Other (non-documented) use cases agreed on a bilateral basis between entities are not excluded but ensuring compatibility of each use case is the responsibility of the entities involved.

This document describes key management stage 2 procedures. Stage 1 procedures, described in previous versions of this document, are available from the GSMA but are no longer maintained.

1.3 Definitions

Term	Description
Certificate Authority (CA)	An entity that verifies the identity of a Participant and issues a certificate that confirms the identity of this Participant by binding its public key to a unique identifier. Cryptographic algorithms are used by the CA to perform its tasks and to allow recipients of the certificates to verify the certificates' validity. There is a hierarchy of CAs.
Intermediate Certificate	A certificate that is in the middle of a chain of trust. The certificate is signed by a Root CA or by an Intermediate CA.
CA Certificate	A Root CA certificate or an intermediate CA certificate.
Leaf Certificate	An individual certificate for network equipment. Examples of such certificates are individual certificates for SEPP, Diameter Edge Agent (DEA)/signalling firewall (SigFW), IPX providers' network equipment, etc. Also known as an end-entity certificate.
Participant	A party that has uploaded a root certificate into the RAEX Certificate Database

[1] Eligibility criteria are described in section 2.2.4.

Term	Description
Root CA	A CA at the topmost position of a hierarchy of CAs.
Intermediate CA	A CA at one or more levels below the Root CA in the hierarchy of CAs. Also known as a subCA. An Intermediate CA signs Leaf Certificates or other Intermediate Certificates.
Trust Anchor	A list of trusted root certificates and an associated list of PLMN-IDs configured at a SEPP PLMN IDs and root certificates are related by virtue of belonging to the same Trust Anchor. Any given PLMN ID can appear in at most one Trust Anchor, while any given root certificate can appear in multiple Trust Anchors.

1.4 Abbreviations

Term	Description
5GMRR	5G Mobile Roaming Revisited (GSMA cross-working group activity)
AVP	Attribute Value Pair
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DESS	Diameter End-to-end Security Subgroup
DEA	Diameter Edge Agent
DNS	Domain Name System
DRA	Diameter Routing Agent
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
IPX	IP eXchange
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
NDS	Network Domain Security
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PMN / PLMN	Public Mobile Network. Note that references to 3GPP specifications or their contents may use the abbreviation “PLMN” representing “Public Land Mobile Network” (e.g. PLMN-ID).
PRD	Permanent Reference Document
RAEX	Roaming Agreement eXchange
SAN	Subject Alternative Name
SEG	Security Gateway
SEPP	Security Edge Protection Proxy
SigFW	Signalling Firewall

Term	Description
SubCA	Subordinate Certification Authority
TLS	Transport Layer Security
UPF	User Plane Function

1.5 References

Ref	Doc Number	Title
[1]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[2]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[3]	Handbook of Applied Cryptography	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography, http://cacr.uwaterloo.ca/hac/
[4]	BSI TR 03145	Secure Certification Authority operation
[5]	BSI TR-02102-1	Cryptographic Mechanisms https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html
[6]	PRD IR.67	DNS Guidelines for Service Providers and GRX and IPX Providers
[7]	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[8]	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[9]	3GPP TS 23.003	Numbering, addressing and identification, https://www.3gpp.org/DynaReport/23003.htm
[10]	3GPP TS 33.310	Network Domain Security (NDS); Authentication Framework (AF) https://www.3gpp.org/DynaReport/33310.htm
[11]	3GPP TS 33.501	Security architecture and procedures for 5G System https://www.3gpp.org/dynareport/33501.htm
[12]	PRD FS.19	Diameter Interconnect Security
[13]	-	RAEX Certificate Database User Manual. Available via the GSMA Roaming Gateway. https://www.raextools.com/raextools/

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 [1] and clarified by RFC8174 [2], when, and only when, they appear in all capitals, as shown here.

2 GSMA Specific Key Management Principles

Cryptographic algorithms enable confidentiality and integrity protection of data. This section provides specific details about GSMA key management. For general information about public key cryptography, the reader is referred to [3].

2.1 Bilateral Trust Model

The operating model used between parties is the ‘bilateral trust model’. It is based on an establishment of trusted relationships between Participants where each Participant has its own unique CA. Following completion of the procedures in section 3, peer Participants designate the root certificate issued by that CA as trusted. These technical procedures can be referred to and required by contractual clauses for certain use cases e.g., secure 5G N32 interconnect as specified in Annex A.

In this bilateral model, there is no centrally governed and trusted CA, and no investment towards a centralised authority to become part of the ecosystem. The bilateral model will result in a larger number of CAs to manage compared to a centralised model.

2.2 PKI and CA Requirements

The Public Key Infrastructure (PKI) CAs must comply with general requirements as part of best practices and additional specific requirements as part of the GSMA key management principles described below.

2.2.1 Certificate Hierarchy

In accordance with the bilateral trust model outlined in section 2.1, each Participant SHALL maintain its own CA. To be specific, if the GSMA key management community has 500 participants, at least 500 CA certificates (one per Participant) will be stored in the RAEX Certificate Database. For security reasons, two participants shall not share the same CA certificates in RAEX, and this is technically enforced by the system.

The CA certificate stored in the RAEX Certificate Database for a Participant SHALL have been issued to a CA dedicated to that Participant. The certificate SHOULD be self-signed, or it MAY have been signed by a Root CA or an Intermediate CA.

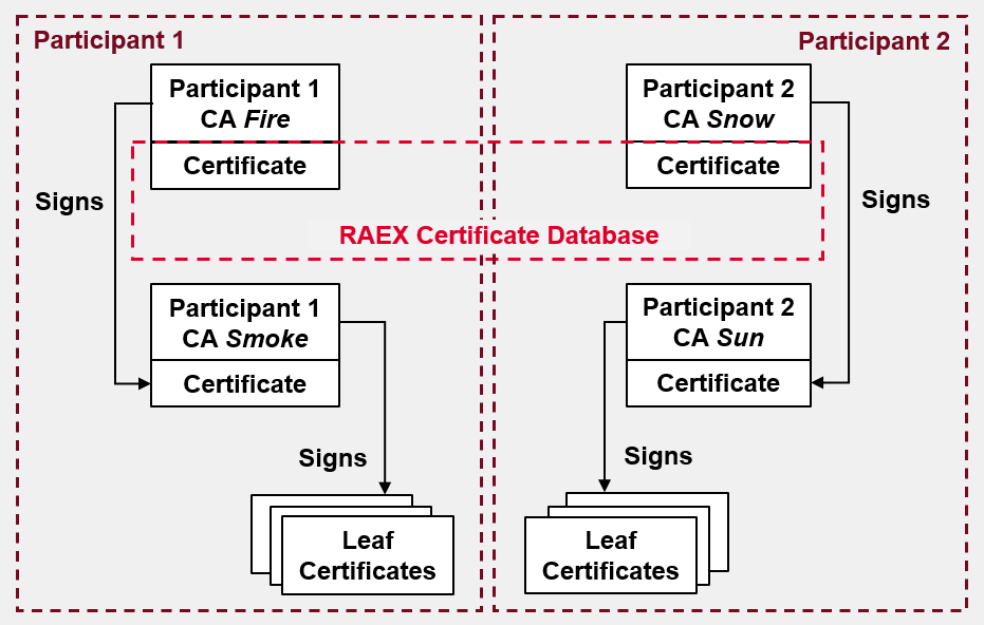

Figure 1 – Recommended Approach for Certificates Stored in RAEX Certificate Database

Figure 1 shows the recommended approach: a unique CA per Participant (*Fire* for Participant 1, *Snow* for Participant 2). In this approach, the CAs *Fire* and *Snow* each have a self-signed certificate, so each is a root CA. These certificates are stored in the RAEX Certificate Database. In this approach, Intermediate CAs (*Smoke* for Participant 1, *Sun* for Participant 2) issue the leaf certificates.

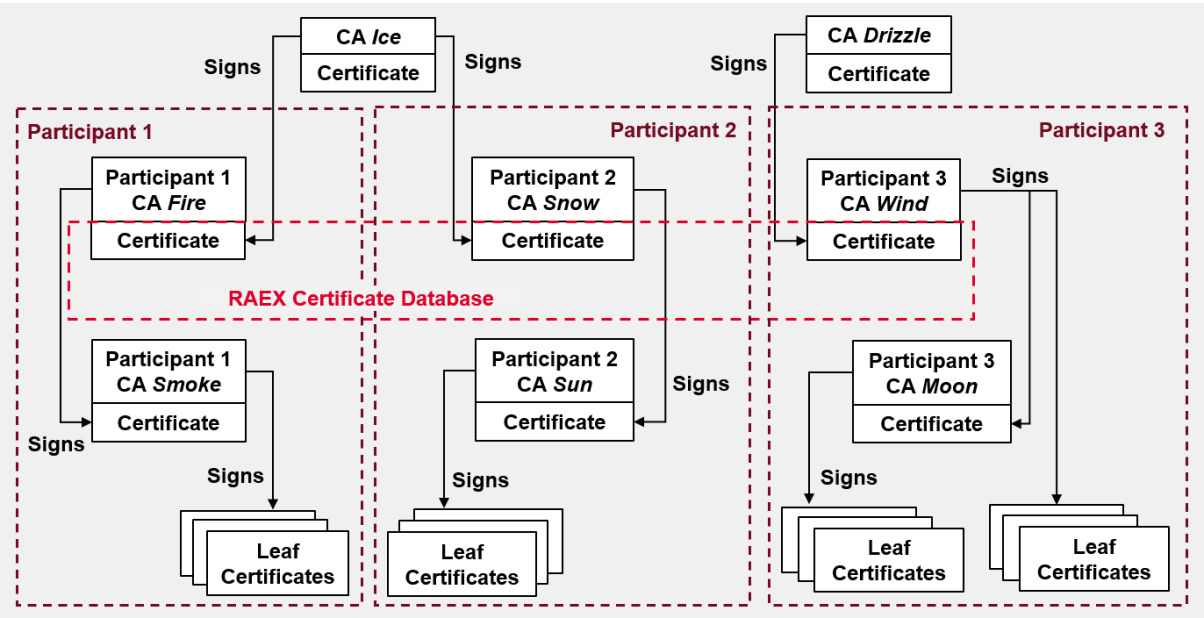

Figure 2 – Allowed Approach for Certificate Stored in RAEX Certificate Database

The approach in Figure 2 is allowed. In this case, the CA certificate stored in the RAEX Certificate Database (*Fire* for Participant 1, *Snow* for Participant 2, *Wind* for Participant 3) is not self-signed as it has been issuedby another, “higher hierarchy” CA (*Ice* for Participant 1 and 2, *Drizzle* for Participant 3). From a bilateral trust perspective, however, this “higher” CA

is relevant for signing the Participant's certificates, but plays no role in the trust establishment between participants; it may be the same for multiple participants.

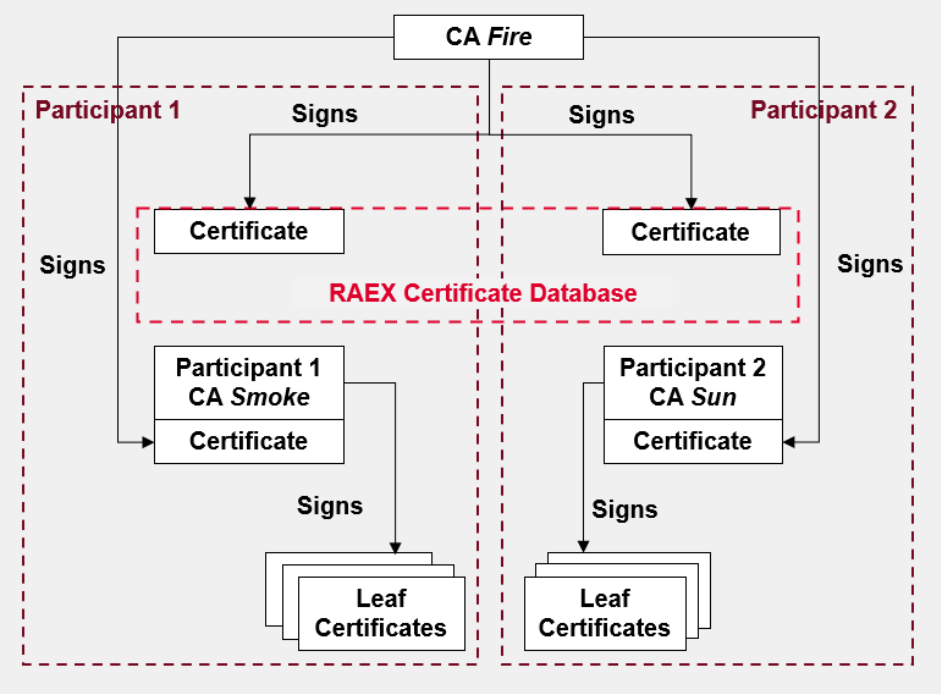

Figure 3 – Disallowed Approach for Certificate Stored in RAEX Certificate Database

Figure 3 shows the situation where the same CA (*Fire*) issues the certificates stored in the RAEX database for both Participant 1 and Participant 2. This situation is disallowed regardless of whether Participant 1 and Participant 2 publish the same certificate or different certificates in the RAEX Certificate Database.

The CA SHOULD be uniquely created for the purpose of GSMA key management. However, it MAY be an existing CA if the CA complies with the entry criteria in section 0.

A Root CA SHALL NOT issue leaf certificates, while an Intermediate CA MAY do so.

Cross-certification between CAs of different participants (a practice that facilitates trust between separate PKIs) SHALL NOT be used, as this is not considered appropriate for the bilateral trust model.

Participants have two PKI deployment options:

1. The Participant MAY use an in-house PKI for the purpose of GSMA key management. The Participant MUST use a dedicated CA for this purpose. Whether or not this CA is placed below another (Root) CA is a decision for the Participant.

2. The Participant MAY use a trusted third-party CA. The CA certificate MUST be dedicated to the Participant, i.e. is not the same as for other participants. While there MAY be a trusted third-party providing PKI services for one or more Participants, this provider SHALL offer this service exclusively on the IP Exchange (IPX) network and not exposed to the Internet. However, this requirement does not preclude publishing certificate revocation lists (CRLs) or obtaining certificate revocation information via

Online Certificate Status Protocol (OCSP) via the Internet in addition to their existence on the IPX network.

While it is possible to deploy both options simultaneously, this SHOULD be used only during a transition period from (1) to (2) or vice versa. Entry criteria for both deployment options can be found in section 0.

2.2.2 Governance

Operating a PKI in a secure manner requires a set of mechanisms and procedures to be in place, some of which are beyond the scope of this document. The guidelines in [4] SHOULD be followed by Participants. It is further recommended to consult BSI TR-02102-1 [5] to select appropriate encryption and signature algorithms as well as key lengths for operating the PKI.

Guidelines for each CA SHALL be documented and followed by at least publishing a Certificate Policy (CP) and Certification Practice Statement (CPS) for each CA in accordance with RFC 3647 [7]. Each Participant SHALL publish CP, Relying Party Agreement or other documentation, which the peer Participants can use to evaluate the trustworthiness of the Participant's CA.

It is highly recommended that CAs are certified according to ISO/IEC 27001 or an equivalent CA audit regime (e.g., WebTrust for CAs). This is due to the importance of forthcoming trust relationships between mobile networks, external functions, suppliers and roaming/ interconnect partners. Industry best practice and future regulation is trending towards having requirements for audited CAs, with robust procedures in place that enable mutual trust. This recommendation SHOULD be applied irrespective of whether CAs are operated by internal teams or outsourced, as retrofitting such requirements could be a complex activity. Special emphasis should be added that, besides being compliant with a CA audit regime or framework, the CAs implementation SHOULD follow hardening best practices. With this, shift the paradigm from "checking boxes" to be compliant, towards a more hardened deployment.

2.2.3 Certificate Requirements

Root or Intermediate Certificates SHALL:

- be X.509 v.3 certificates according to RFC 5280 [8];

Leaf Certificates SHALL:

- be X.509 v.3 certificates according to RFC 5280 with the Subject Alternative Name (SAN) extension.

2.2.4 Entry Criteria

Providers of a PKI for GSMA key management and its Participants SHALL:

- Maintain a CA that exclusively belongs to a particular Participant
- Offer the PKI on the IPX network including downloading CRLs or obtaining certificate revocation information via OCSP. (see sections 3.1.4 and 3.1.5)
- Publish Participant CA(s) in the RAEX Certificate Database

- Generate a CP and CPS for each CA based on RFC 3647, and to include a pointer towards the CPS in the Root CA certificate according to section 4.2.1.4 of RFC 5280.

2.2.5 Usage of the IPX Network and its Domain Names

GSMA key management is used only on the IPX network. SAN names of Leaf Certificates SHALL use the following format:

- `mnc<MNC>.mcc<MCC>.3gppnetwork.org` (strictly limited to MNOs)
- `mnc<MNC>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org` (for non-MNO participants acting under a mandate of a particular MNO)
- `<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org` (for non-MNO participants acting outside a mandate of a particular MNO.)

Refer to PRD IR.67 [6] for the procedures around obtaining and maintaining (sub) domain names on the IPX network.

Any hosts and services including certificate status checking and certificate revocation SHALL entirely occur on the IPX network.

2.2.6 Certificate Chain Verification

Due to the reliance on the bilateral trust model, the GSMA key management certificate verification logic supports multiple lists of trusted CA certificates instead of a single global one. Any given certificate chain is first mapped to a particular list of CA certificates using a mapping function. This mapping function combines information from the Leaf Certificate with locally configured data. Afterwards the certificate chain is validated with respect to the selected list. It must be possible to allocate a separate CA certificate list to each Participant in the RAEX Certificate Database.

Depending on the use case the exact implementation may vary. Refer to the use case in the annexes for further guidelines, if any.

2.3 RAEX Certificate Database

The RAEX Certificate Database acts as the repository of root and intermediate certificates. The database supports manual upload and download of certificates as well as automated certificate downloading via an API. More information on the features and use of the database can be found in the user manual [13] available to GSMA members via the RAEX application.

3 Key Management Procedures

This section describes the main GSMA key management procedures, where possible in chronological order.

3.1.1 Own Root or Intermediate Certificate Generation and Publication

Each Participant SHALL generate or reuse an existing root or intermediate certificate that shall be uploaded and published in the RAEX Certificate Database.

Among other consistency and security checks the RAEX Certificate Database will not accept certificates already published by other participants.

CRL and OCSP services for revocation SHALL be published in the certificates and SHALL have and make use of the appropriate domains as described in 3.1.4

3.1.2 Peer Root or Intermediate Certificate Downloading and Configuring

Each Participant SHALL download, either manually or automated, the root or intermediate certificates from the peer Participants. The Participant SHALL pre-configure the mapping of (the suffix of) the expected domain names of SANs in the leaf certificates to the corresponding certificate.

3.1.3 Leaf Certificate Acceptance

Upon receiving a leaf certificate of a peer participant (either in-band e.g. Transport Layer Security (TLS) or via a side channel e.g. Digital Signature Certificate) the Participant SHALL verify the SAN domain suffixes against the correct root certificate as per the procedure in 3.1.2

3.1.4 Leaf and Intermediate Certificate Revocation

Each CA SHALL maintain a list of certificates that are revoked and host such service on the IPX network. To minimise its risk, each Participant SHOULD check such listings/ and SHOULD NOT accept revoked certificates.

3.1.5 Root Certificate Revocation

If a root certificate becomes compromised, it SHALL be revoked by marking it accordingly in the RAEX Certificate Database where all peer Participants will be alerted. A new root certificate shall be uploaded to the RAEX Certificate Database as soon as possible if this has not been done already.

3.1.6 Root Certificate Expiry and Replacement

Root and intermediate certificates are expected to have a lifetime of multiple years. If the certificate has to be replaced, the new certificate SHALL be uploaded to the RAEX Certificate Database at least 6 months before expiry of the current certificate.

Annex A Use case - Secure 5G N32 interconnect

A.1 SEPP Leaf Certificate Specific Formatting

The format for 5G Leaf Certificates including a Security Edge Protection Proxy (SEPP) SHALL follow section 28 of 3GPP TS 23.003 [9] and 3GPP TS 33.310 [10]. Specifically for MNOs this implies that it contains values for Mobile Network Code (MNC) and Mobile Country Code (MCC) in the SAN, each three digits long (zero prefix as necessary) and corresponding to the MNO.

A.2 PLMN ID Based Trust Anchoring

As outlined in section 3.1.2, each downloaded root CA from the RAEX Certificate Database will be associated with one or more PLMN IDs. More precisely, each Participant generates a set of Trust Anchors, where each Trust Anchor is a combination of two unordered lists:

1. A list of root CA certificates downloaded from the RAEX Certificate Database, and
2. A list of PLMN IDs.

The semantics of a Trust Anchor are: the CA(s) represented by the certificates within this Trust Anchor are designated as the root of trust for the purposes of authenticating SEPPs claiming to belong to any of the PLMNs with the PLMN IDs within this Trust Anchor.

It is important to note that any given PLMN ID cannot belong to more than a single Trust Anchor.

While it is possible to create Trust Anchors with many root certificates, and even generate single global list of all root certificates and associate this list with all PLMN IDs, doing so is strongly discouraged. It is instead recommended to create many Trust Anchors with the finest possible granularity, and this SHOULD be done. This is to prevent impersonation attacks and to limit the attack surface represented by a compromised CA.

A.3 SEPP Naming Scheme

The format for 5G leaf certificates including SEPPs SHALL follow section 28 of TS 23.003 [9] and TS 33.310 [10]. Specifically for MNOs this implies that it contains values for MNC and MCC in the SAN, each three digits long (zero prefix as necessary) and corresponding to the MNO.[2]

A.3.1 MNO SEPP

A SAN field SHALL be structured as:

`<SEPP-id>.sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

where `SEPP-id` contains at least one label/sub domain

Example domain names include:

[2] The SEPP naming scheme is still (as of May 2024) under discussion in GSMA 5GMRR. This section may be updated based on the output of those discussions.

- 1b.sepp.5gc.mnc001.mcc001.3gppnetwork.org
- Madrid.roaming.sepp.5gc.mnc001.mcc001.3gppnetwork.org
- paris1.test.sepp.5gc.mnc001.mcc001.3gppnetwork.org

The certificate for an MNO SEPP SHALL include all applicable Fully Qualified Domain Names (FQDNs) in SAN fields as Domain Name System (DNS) name. For example:

- <SEPP-id>.sepp.5gc.mnc<MNC1>.mcc<MCC>.3gppnetwork.org
- <SEPP-id>.sepp.5gc.mnc<MNC2>.mcc<MCC>.3gppnetwork.org

A.3.2 Non-MNO SEPP

When the SEPP does not belong to an MNO, e.g., a hosted SEPP belonging to a non-MNO Participant, the certificate SHALL indicate this in the SAN fields and SHALL also be published in the RAEX Certificate Database accordingly. The SAN field SHALL be structured as:

<SEPP-id>.sepp.5gc.mnc<MNC>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org

where SEPP-id contains at least one label/sub domain. An entity that operates a hosted SEPP SHALL use separate SEPP certificates for each MNO that it serves.

Non-MNO SEPP certificates SHALL include all FQDNs in SAN fields as DNS name for any host on which the non-MNO SEPP runs the N32 connection. For example:

- <SEPP-id1>.sepp.5gc.mnc<MNC>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org
- <SEPP-id2> sepp.5gc.mnc<MNC>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org

NOTE: MNO connection to non-MNO SEPP is out of scope of this document. The type of connection (e.g. TLS or Network Domain Security/Internet Protocol (NDS/IP)) and corresponding key management is left to the MNO and outsourced SEPP provider or MNO group SEPP.

Annex B 5G User Plane

The 5G inter-PMN user plane SHALL be secured with IPsec ESP and IKEv2 certificate-based authentication unless security is provided by other means as described in section 9.9 of 3GPP TS 33.501 [11]. A Security Gateway (SEG) may be used to terminate the IPSec tunnels. Naming conventions for securing at User Plane Function (UPF) or SEG are outlined below.

B.1 Naming conventions

When an FQDN is used, the Subject SAN field SHALL be structured as either:

a) `<UPF-id>.upf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

or

b) `<SEG-id>.seg.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

NOTE: Outsourcing or delegating N9 operator-to-operator security is to be studied in a later stage in collaboration with the GSMA 5G Mobile Roaming Revisited (5GMRR) group.

Annex C Use case - DESS Phase 1

DESS Phase 1 entails signing and verifying Diameter messages on the interconnect and is described in more detail in PRD FS.19 [12].

C.1 DESS Phase 1 Leaf Exchange Procedure

As DESS Phase 1 makes use of digital signature certificates that are not exchanged in-band, the certificates have to be exchanged manually. This procedure is envisioned to be automated at a later stage by introducing a central or distributed certificate repository.

C.2 DESS Phase 1 Naming Scheme

DESS Phase 1 related entities such as a signalling firewall (SigFW), Diameter Routing Agent (DRA) or DEA have a different naming convention depending on whether they belong to the MNO or to the serving IPX provider. In all cases the DESS-Signing-Identity attribute value pair (AVP) shall indicate the signee in the exact format of the Subject/SAN field outlined in sections C.2.1 and C.2.2.

C.2.1 MNO DESS Equipment

The Subject SAN field SHALL be structured as:

`diameteridentity.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

where `diameteridentity` is the Diameter host to which the certificate is issued.

C.2.2 Non-MNO DESS Equipment, DESS Phase 1 Delegation from MNO to IPX Provider

For security delegation, not to be confused with intermediate signing as per C.2.3, as described in FS.19 [12] the Subject SAN field SHALL be structured as:

`diameteridentity.epc.mnc<MNC>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org`

C.2.3 Non-MNO DESS Equipment, Intermediate Changes

For intermediate signing as described in FS.19 [12] the Subject SAN field SHALL be structured as:

`diameteridentity.epc.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org`

where `diameteridentity` is the Diameter host to which the certificate is issued.

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	6 Mar 2020	First version describing key management stage 1 solution for early 5G roaming agreements and 4G LTE roaming with Diameter end-to-end security measures as described in FS.19.	TG	DESS members including Martin Kacer (P1 Security), Ewout Pronk (NetNumber), Pieter Veenstra (NetNumber), Sven Lachmund (Deutsche Telekom), Andreas Pashalidis (BSI), Anja Jerichow (Nokia), Daan Planqué (KPN)
2.0	30 Jun 2021	Added requirements related to N9 operator-to-operator security. Updates to naming scheme section. Addition and application of key word conventions	ISAG	Ewout Pronk (NetNumber), Martin Kacer (Mobileum), Andreas Pashalidis (BSI), Ahmad Muhanna (Mavenir), David Maxwell (GSMA)
3.0	16 Dec 2021	Added 5GMRR Phase 1 scope definitions and clarifications. Further refinements on the entire document	ISAG	Ewout Pronk (NetNumber), Roger Piqueras Jover (Google)
4.0	18 May 2022	Simplification of the addressing structure for SEPPs.	ISAG	Ewout Pronk (NetNumber)
5.0	19 Oct 2022	Added certificate hierarchy when 3rd party runs CA.	ISAG	Nataliya Stanetsky & Roger Piqueras Jover, (Google), Ewout Pronk (Titan.ium Platform LLC)
5.1	21 Apr 2023	Updated GSMA logo.	N/A	David Maxwell (GSMA)
6.0	14 Nov 2023	CR1006: Stage 1 full review and updates prior to Stage 2 development.	ISAG	Ewout Pronk (Titan.ium Platform), Andreas Pashalidis (BSI), Stefan Kiebooms (BICS).
7.0	19 Sep 2024	CR1007: Rewritten to specify key management stage 2.	ISAG	DESS members

D.2 Other Information

Type	Description
Document Owner	Fraud and Security Group (FASG) DESS
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.