Key Management for 4G and 5G inter-PMN Security
Version 6.0
14 November 2023

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

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

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

Table of Contents

1 Introduction

1.1 Overview

For 5G Security Edge Protection Proxy (SEPP) interconnect security and for 4G Diameter interconnect security, a key management solution is required.

Both 5G inter-PMN roaming security (as defined in 3GPP TS 33.501 [1]) and 4G roaming inter-PMN security (as defined in GSMA PRD FS.19 [2]) require cryptographic keys to achieve peer authentication, message integrity and confidential communication. These cryptographic keys need to be managed and exchanged between stakeholders involved in roaming.

Key management in the context of this document refers to the process and technology used by mobile network operators (MNOs) and IPX providers to exchange their certificates, and how the trust relations are established between interconnect partners.

A solution in two stages is proposed for the introduction of key management for interconnect security:

- Stage 1: Light solution (mainly based on a manual exchange of certificates)
- Stage 2: Key management with enhanced scalability/automation

This document describes the stage 1 solution only. The stage 2 solution is under development and will be described in a later version of this document.

The stage 1 solution is meant to be used for early 5G roaming agreements and 4G LTE roaming with Diameter end-to-end security measures as described in FS.19, Annex D and Annex E [2]. This includes:

- N32 for 5G SA roaming
- DESS Phase 1: Authentication and integrity protection by introducing digital signatures on inter-PMN Diameter signalling messages.
- N9 operator-to-operator security: inter-PMN user plane protection with NDS/IP as per 3GPP Release 16 TS 33.501 [1].

As soon as the stage 2 solution is defined, implemented and widely rolled-out, it is expected to eventually replace the stage 1 solution. Stage 1 can be seen as a preparatory step for stage 2.

Although the key management procedures strive for a uniform procedure between 5G and LTE roaming, technical limitations prescribe a slightly different procedure for DESS Phase 1.

1.2 Scope

This document describes the key management process, i.e. the exchange of certificates and key materials that are used between the interconnect parties in order to secure the inter-PMN communication.

This document does not describe the technical details of the protection of the inter-PMN communication. Related technical specifications are listed in section 1.5.

Error! Reference source not found. For 5G SA roaming the scope of the document is limited to the following use cases of 5GMRR as mentioned in NG.140 [13]:

- 1: Mono PLMN ID/ Multi PLMN ID
- 2.1: Outsourced SEPP
- 2.2: Hosted SEPP

1.3 Definitions

Term	Description
Certificate signing request	A certificate signing request (CSR) is a request sent to a CA by an entity that wishes to obtain a certificate from that CA. The CSR contains the entity's public key and unique identifier.
Certification authority	An entity that verifies the identity of another entity and issues a certificate that confirms the identity of this other entity by binding its public key to a unique identifier. Cryptographic algorithms are used by the certification authority (CA) to perform its tasks and to allow recipients of the certificates to verify the certificates' validity. There is a hierarchy of CAs. Details of the role of a certification authority are described in this document.
Intermediate certificate / Sub CA certificate	Certificate which is in the middle of a chain of trust. The certificate is typically signed by a CA or by another intermediate certificate. Intermediate certificates can be used to sign leaf certificates or other intermediate certificates.
Issuer certificate/ CA certificate	The term "issuer certificate" is used in this document to refer to a root CA certificate or an intermediate CA certificate.
Leaf certificate	End entity certificate, e.g. 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.
Root CA	A root CA is a CA at the topmost position of the hierarchy of CAs.
Sub CA/ intermediate CA	A subordinate CA (also known as Sub CA or intermediate CA) is a CA at one or more levels below the root CA in the hierarchy of CAs.
Trust anchor	A trust anchor is of a list of trusted root certificates and an associated list of PLMN-IDs. 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 givenroot certificate can appear in multiple trust anchors.

1.4 Abbreviations

Term	Description
5GMRR	5G Mobile Roaming Revisited (GSMA cross-working group activity)
5GS	5G System
AVP	Attribute Value Pair
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List

Term	Description
CSR	Certificate Signing Request
DESS	Diameter End-to-end Security Subgroup
DEA	Diameter Edge Agent
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IP	Internet Protocol
IPX	IP eXchange
iSEPP	Initiating SEPP
JSON	JavaScript Object Notation
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PMN	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
PRINS	Protocol for N32 Interconnect Security
Root CA	Root Certification Authority
rSEPP	Receiving SEPP
RVAS	Roaming Value Added Services
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAN	Subject Alternative Name
SEG	Security Gateway
SEPP	Security Edge Protection Proxy
SigFW	Signalling Firewall
Sub CA	Subordinate Certification Authority
TLS	Transport Layer Security
UPF	User Plane Function
URL	Uniform Resource Locator

1.5 References

Ref	Doc Number	Title
[1]	3GPP TS 33.501	Security architecture and procedures for 5G System,

Ref	Doc Number	Title
		https://www.3gpp.org/DynaReport/33501.htm
[2]	GSMA PRD FS.19	Diameter Interconnect Security
[3]	TR 02102-2	BSI Technical Guideline – Cryptographic Mechanisms: Recommendations and Key Lengths, Part 2, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html
[4]	Handbook of Applied Cryptography	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography, http://cacr.uwaterloo.ca/hac/
[5]	3GPP TS 23.003	Numbering, addressing and identification, https://www.3gpp.org/DynaReport/23003.htm
[6]	TR 03145	BSI Technical Guideline 03145 Secure Certification Authority Operation, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03145/TR03145.pdf
[7]	Introduction into Public Key Cryptography	Public key cryptography, Wikipedia, https://en.wikipedia.org/wiki/Public-key_cryptography
[8]	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[9]	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
[10]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[11]	GSMA PRD IR.67	DNS Guidelines for Service Providers and GRX and IPX Providers
[12]	GSMA PRD NG.113	5GS Roaming Guidelines
[13]	GSMA PRD NG.140	5GC SEPP Functional and Security Requirements
[14]	3GPP TS 33.310	Network Domain Security (NDS); Authentication Framework (AF) https://www.3gpp.org/DynaReport/33310.htm
[15]	RFC3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Framework

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 [9] and clarified by RFC8174 [10], when, and only when, they appear in all capitals, as shown here.

2 Key Management Principles

Cryptographic algorithms enable the protection (confidentiality and integrity protection) of data and the authentication of remote entities over an insecure network. In the context of signalling and user plane messages, both protection and authentication are required, as messages traverse networks that are subject to traffic manipulation attacks. This section provides a high-level and simplified introduction to this topic. For detailed treatment, the reader is referred to [4] or other sources.

2.1 Cryptographic Keys

Cryptographic algorithms such as those used for encryption, integrity protection and authentication of remote entities require cryptographic keys. You can generally distinguish between two types of cryptography and keys:

- Symmetric cryptography: All parties share and use the same key. This key must remain secret.
- Asymmetric cryptography: Each party has a key pair consisting of a private key and a public key. The private key is not shared with anyone and must remain secret, and the public key, which may be freely disclosed to everyone, must be distributed to all communication partners. It is crucial that partners obtain an *authentic* copy of the public key.

In the context of roaming security, a combination of symmetric and asymmetric cryptography is used. In order for the asymmetric algorithms to work, involved communication parties need to generate asymmetric key pairs and exchange their public keys.

2.2 Certificates

Certificates enable a scalable exchange and management of public keys in a setting with a large number of communication partners. The purpose of a certificate is to bind an entity's public key to its (unique) identifier. A standard public key certificate consists of at least:

- An issuer ID: The unique identifier of the entity issuing the certificate;
- A public key;
- A subject ID: At least one unique identifier of the entity to whom the public key (and corresponding private key) belongs;
- A lifetime (timestamps indicating "valid from" and "valid until");
- A unique certificate identifier that enables revocation;
- A pointer to a location where the revocation status can be retrieved; and
- A cryptographic signature of the issuer, generated by a certification authority (CA);

Given two communication partners, say "Alice" and "Bob": "Alice" has obtained "Bob's" public key and must decide whether or not that public key is authentic, i.e. whether it really belongs to Bob. If the public key is embedded in a certificate, and if Alice trusts the issuer of the certificate, then Alice can verify the signature of the certificate and obtain some assurance that the certificate is indeed authentic. If Alice trusts the issuer, she can verify the authenticity of all certificates issued by that issuer, and hence the binding of public keys to communication partners' identifiers.

For security reasons, certificates have a limited lifetime. Well before a certificate expires, a new certificate is exchanged in order to avoid interruptions and errors.

2.3 Trust relationships

Trust cannot be easily quantified. Generally speaking, the more one is exposing oneself to another entity (accepting higher levels of risk as a result), the more this other entity becomes trusted. Trust may be symmetric (i.e. mutual), but may also be asymmetric. More importantly, trust is not static and changes as information about the other entity becomes available over time. Without such information, trust cannot even be established: the foundation of trust is transparency.

This does not mean that a lot of information must be available on every single entity in given system before transactions can be made. In some situations, including a PKI, trust is transitive: if a trusted CA issues a certificate to an entity, this entity will become recognised and trusted (for a specific role) by the other participants. Nevertheless, also this trust is based on the transparency provided by the processes, procedures and governance that the CAs adhere to [15].

As a result, different and changing levels of trust may be applicable between the entities involved in the roaming relationship of interconnection partners. An MNO is likely to apply stricter filtering to messages arriving from a partner with lower trust compared to another partner.

In order to apply different policies to different entities based on different trust levels assigned to these entities, attribution is necessary. That is, as evidence that affects the trust level assigned to some entity becomes available, it must be possible to ensure that the correct entity is affected.

2.4 Certification Authorities

The issuer of a certificate is called a certification authority (CA).

A certification authority is an entity that verifies the identity of another entity and issues a certificate that confirms the identity of this other entity by binding its public key to a unique identifier. Its main task is to ensure that:

- only legitimate parties obtain certificates; and
- certificates contain the correct values in all fields, especially the fields that contain the unique identifier(s) of the entity (i.e. no entity can obtain a certificate issued under another entity's name).

In the context of roaming security, MNOs and other players in the IPX ecosystem will use the functionality of a CA and issue certificates to be used with signalling or user plane equipment. Afterwards, MNOs exchange issuer certificates with parties that they have a contractual relationship with.

In the model described in this document, it is assumed that every MNO is using at least one root CA. The reason for this is that there is no single globally trusted CA. A dedicated public key infrastructure (PKI) for inter-PMN security is required. It is assumed that every MNO independently operates a PKI including a root CA, or alternatively a sub CA and that it uses

this PKI to issue certificates for its own network elements and servers, as well as for the IPX providers that it has a contractual relationship with. It is further assumed that the policies and procedures governing the operation of the PKI, including the issuance and revocation of certificates, has been documented by each MNO.

As an alternative, MNOs and other players MAY use their existing root CA to sign network equipment certificates or introduce an intermediate CA instead.

More details about certification authorities, root CAs, sub CAs, PKI and certificate hierarchy are contained in section 3.

2.5 Manual Exchange of Certificates

In the stage 1 solution, issuer certificates are exchanged manually on a bilateral basis. This requires staff involvement.

As anybody could create an issuer certificate, there is a need to verify that a particular certificate actually belongs to a particular entity. This verification requires the use of a separate communication channel, i.e. not the one used to transport the issuer certificate.

3 Key Management and Processing Details

3.1 Certificate Hierarchy

The 5G N32 roaming signalling protocols are based on mTLS which relies on certificates for client and server authentication of the SEPPs. The 4G procedures also rely on certificate verification of the DIAMETER Edge Agents, although not using mTLS. Such certificates must therefore be issued to the clients and servers, and their management occurs within the context of a Public Key Infrastructure (PKI).

A PKI is a hierarchical construct where trust is derived from a special entity called the root Certification Authority (CA). In the beginning, the root CA generates an asymmetric key pair, and every entity in the system obtains an authentic copy of the public key of this pair.

The root CA then issues certificates to subordinate CAs (subCAs), and the subCAs issue certificates to the clients and servers in the system (leaf certificates). Each client and server stores its leaf certificate together with the certificate issued by the root CA to the subCA that issued this leaf certificate. They use this set of two certificates, called a certificate chain, during the setup of an mTLS connection in order to authenticate themselves to the other side. The other side checks that the presented leaf certificate was issued by the subCA, and that the presented subCA certificate was issued by the root CA, whose public key was marked as "trusted" in the beginning. If these checks succeed, the identifier in the leaf certificate is assigned to the other side.

While it is possible for a root CA to directly issue leaf certificates (i.e. skipping the subCA), such a practice is not recommended. In order to support automatic leaf certificate renewal without exposing the root CA private key to such automation, a subCA is necessary. It is also possible to extend the levels in the hierarchy with multiple levels of SubCAs. In such a case, the certificate chain of clients and servers would include three or more certificates. One could also shorten the length of certificate chains by treating one of the subCAs as a root CA. This would require adding that SubCA's public key to the set of trusted root keys.

While it is possible for a single root CA to be placed on the top of a global hierarchy, this model is not optimal in the roaming context due to the requirement in such a model for global trust. Instead it is assumed that there exists a dedicated root (or sub) CA for each MNO. It is further recommended that this CA does not directly issue leaf certificates, but that at least one subCA is placed below the root CA for this purpose.

It is further assumed that cross-certification (a practice that facilitates trust between separate PKIs) is not used.

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 [6] should be followed by MNOs. It is further recommended to consult TR 02102-1 [3] in order to select appropriate encryption and signature algorithms as well as key lengths for operating the PKI.

The following deployment options are supported.

1. The MNO may use an in-house PKI for the purposes of issuing roaming-related certificates as specified in this document. The MNO MUST use a dedicated root CA for

this purpose. Whether or not this root CA is placed below another root CA is an internal matter to the MNO.

2. The MNO may use a trusted third party CA in order to obtain certificates. This provider is required to offer this service exclusively on the IPX network and not exposed to the Internet, including downloading CRLs or obtaining certificate revocation information via OCSP. The root CA certificate MUST be dedicated to the MNO, i.e. is not the same as for other customers. The trusted 3rd party must meet a minimum set of security requirements, as specified in [6]. While there may be a trusted third party PKI provider providing PKI services for one or more MNOs, this provider is required to offer this service exclusively on the IPX network and not exposed to the Internet, including downloading CRLs or obtaining certificate revocation information via OCSP.In particular, there must be a minimum set of security requirements to be met for a 3rd party to be eligible as CA for the functionality covered by this document

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.

3.2 Certificate Verification

Certificate verification logic must not be limited to checking that a valid path exists to *any* trusted CA. As described in section 4.3.1, once a CA certificate is stored in the trust anchor of a particular roaming partner, all connections from and to that roaming partner shall be validated against *that particular* trust anchor. At least the following aspects SHALL be checked as well.

- The current date/time shall lie within the validity period of all certificates in the chain
- The Issuer and Subject fields of the leaf certificate MUST follow the specified format and correspond to equipment that is eligible to send messages over the interface over which the message was received.

3.3 Certification Authority Requirements

Each MNO or other entity on the IPX network SHALL provide at least one root or sub CA and is strongly recommended to operate its own PKI. This may be an existing certificate authority or a new one dedicated to this purpose.

The policies and procedures governing the operation of the PKI MUST be documented and cover at least the topics listed in [15].

Operating a CA is security critical and involves a number of organisational and technical security measures, for example as defined in [6].

If a trusted 3rd party PKI provider operates the CA on behalf of the MNO, this trusted 3rd party must adhere to the same security requirements.

For further study: Although the compliance of CAs and trust between CAs is identified as future work for FS.34, 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 5G 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 certification authority 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.

4 Exchange Procedures

The exchange of issuer certificates and DESS Phase 1 leaf certificates is a manual process. MNOs and other players within the IPX ecosystem need to assign responsibilities for performing key management to staff. This includes key generation, certificate issuing, and certificate exchange.

During negotiation of the roaming agreement, MNOs should agree on the detailed procedure and the technical means for exchanging certificates. This document defines a high-level process that should be followed by the MNOs by default.

NOTE: Exceptions can be made and different procedures can be used if both MNOs mutually agree.

4.1 [2]Prerequisites

- Roaming partners SHALL be able to issue and distribute certificates according to [6] and to inform their peers about expiry and revocation of certificates. Staff with the relevant expertise MUST be assigned.
- Roaming partners SHALL keep contact details of responsible staff on file. Roaming partners SHALL update each other on any changes of the contact details.
- Roaming partners SHALL keep track of certificate expiry and issue a new certificate early enough before the current one expires. It is the joint responsibility of the certificate subject and the issuer to ensure that a new certificate is available well before expiry.
- For DESS Phase 1, MNOs SHALL ensure that IPX providers with which they have a contractual relationship are in the position to securely generate and store key pairs, issue certificate signing requests (CSR), and accept certificates issued by the MNO and use them in the context of signalling as specified below. MNOs SHALL further ensure that IPX providers are generating new certificate signing requests in accordance with the certificate renewal procedures defined below, and that they immediately inform the MNO if a certificate needs to be revoked. Certificate signing requests from IPX providers SHOULD be kept on file by MNOs.

4.2 Determine Certificates to be Exchanged

Issuer certificates SHALL be exchanged for:

- 5G – Transport Layer Security (TLS) + Protocol for N32 Interconnect Security (PRINS[1])
- N9 operator-to-operator security with NDS/IP

On top leaf certificates SHALL be exchanged for:

- 4G – DESS Phase 1 (authentication and integrity protection only)

NOTE: Explanations on this special case are provided in section 4.4.

4.3 Certificate Management Procedures

4.3.1 Certificate Exchange Procedure

The certificate to be exchanged as per section 4.2, SHALL be exchanged as explained below. While the section mentions MNO to improve the readability, it may also read any other entity, including a trusted third party.

Publishing MNO:

1. Install the respective certificate on the equipment (SEPP, DEA/SigFW, User Plane Function (UPF) / Security Exchange Gateway (SEG) or other) and ensure that it will be offered to peers upon establishment of a secure roaming communication.
2. Prepare an initially empty certificate revocation list and publish it under a URL (CRL URL which matches the field within the issued certificates) on the IPX network. As an optional alternative, Online Certificate Status Protocol (OCSP) stapling can be used. Note that each CA (i.e. root, intermediate) maintains its own CRL, hence there may be multiple CRLs.
3. Send the certificate by email to the roaming partner. It is suggested that the email is signed by PGP or S/MIME.
4. Prepare to receive a phone call for the purposes of verifying the certificate's fingerprint.

NOTE: The receiving MNO SHOULD initiate the phone call and not the sending MNO. This is to avoid attacks with spoofed caller IDs.

Receiving MNO:

1. On receiving an email with an issuer certificate from a roaming partner, ring up the responsible member of staff of the roaming partner and ask this person to read out the fingerprint of the certificate. In case of a mismatch, make sure that the organisation's processes and procedures are followed and that an investigation is completed to ensure this is not a malicious attack to inject a rogue certificate. In case of a match, mark the certificate as trusted and bind it to the configuration used to communicate with this particular roaming partner.

[1] PRINS is the application layer security protocol for the N32 interface described in clause 13.2 of TS 33.501 [1]. PRINS is however out of scope for 5GMRR Phase 1.

2. On the 5G SEPP, store the received certificate in the dedicated trust anchor for this particular roaming partner. During the mTLS handshake used to set up the N32-c or N32-f connection the SAN records in the received leaf certificate shall be used to map to the relevant trust anchor. All SAN records within the same leaf certificate shall map to exactly one and the same trust anchor. The certificates within the trust anchor are used to verify the full certificate chain.

3. On the DEA/SigFW or UPF/SEG, install the verified CA certificate, mark it as trusted, and bind it to the configuration used to communicate with this particular roaming partner. After this binding is activated, the server MUST discard or reject all incoming messages from that particular roaming partner except those that are protected by a certificate with a certificate chain that is rooted by the bound certificate.

4. Have the system validate the noted CRLs in a timely manner and according to the organisation's policies, to verify that they can be resolved. Alternatively, using OCSP stapling is an option.

If the above steps are omitted, there is a risk that an attacker could provide a certificate that does not belong to the roaming partner and that future roaming traffic with that roaming partner could be compromised.

5. Record the expiry date of the received certificate and ensure to be alerted at least three months prior to its expiry, or earlier if specified by the organisation's policies and procedures, which allows sufficient time to be able to receive a new certificate from the roaming partner.

Obtaining the certificate fingerprint:

The following procedure is suggested for obtaining the certificate fingerprint that must be verified by phone call. It applies to both the publishing and the receiving MNO.

6. Ensure that the publishing and receiving MNO have the certificate in the same format. If format differs, convert the certificate into the PEM format.

7. Use the same tool for fingerprint verification on both sides and apply the SHA256 algorithm as the fingerprint algorithm. For example, the following command could be used.

```
Openssl x509 -nooout -fingerprint -sha256 -inform pem -in cert.crt
```

Assuming the filename of the PEM-encoded certificate is `cert.crt`.

4.3.2 Certificate Revocation

If a private key is compromised (e.g. stolen from the network equipment on which it is stored), all peers have to be informed that the corresponding certificate can no longer be used. This process is called certificate revocation.

The process differs depending on whether the certificate to be revoked is the CA certificate, or some certificate issued by the CA.

4.3.2.1 Revocation of an issued certificate

Revoking an issued (intermediate or leaf) certificate is a possibility that needs to be accounted for. First, the party suffering the compromise (MNO or IPX provider) generates a new key pair and issues a certificate signing request. The publishing entity then generates a replacement certificate and puts it to use. For DESS Phase 1 specifically it is the responsibility of IPX providers to inform MNOs about the need for certificate revocation.

The MNO MUST add the revoked certificate details to the CRL and publish the new CRL version under the previously shared URL. There is no need for further manual actions, since all peers that have correctly installed the URL in their network equipment configurations will no longer accept the revoked certificates as the systems (should) automatically check the CRL repository every 24 hours for newly revoked certificates.

4.3.2.2 Revocation of a CA certificate

Revoking the CA certificate is a relatively major incident, as this step immediately invalidates all certificates that have been issued by that CA. It is expected that CA certificate revocation is an extremely rare necessity, as the CA private key shall be protected more rigorously than other keys, as described in [6].

Publishing MNO:

1. Contact roaming partners (preferably by signed email) that the currently valid CA certificate will be exchanged with a new one shortly.
2. Issue new intermediate and leaf certificates as necessary to resume operations after CA certificate switch. Reusing existing requests may avoid undue delays.
3. Perform the actions from section 4.3.1 (publishing MNO) for each roaming partner.
4. Publish the revoked certificate in the CRL and publish a new version of the CRL. In order to minimize the delay until partner MNOs check for an updated CRL, OCSP stapling is also an option.

Receiving MNO:

5. When contacted by a roaming partner for the purposes of CA certificate revocation/replacement, perform the actions from section 4.3.1 (receiving MNO). Apart from verifying the fingerprint of the new CA certificate, it is crucial that the identity of the responsible staff at the publishing MNO is properly verified via a separate channel. If using a phone, only verifying the identity solely based on the phone number is strongly discouraged.
6. In addition to installing the new CA certificate, delete all copies of the revoked one.

4.3.3 CA certificate renewal procedure

A new issuer (CA) certificate SHOULD be issued at least six months before the current one expires. The steps to be followed are as specified in section 4.3.1 both for the publishing and the receiving MNO.

NOTE 1: The old CA certificate SHALL remain valid in the equipment of both the publishing MNO and the receiving MNO until the pre-defined time of expiry.

NOTE 2: After a CA certificate replacement (renewal or revocation), the CRL is initially empty.

4.3.4 Non-CA (Intermediate or Leaf) certificate renewal procedure

Issued certificates SHOULD be renewed three months before expiry. MNOs are responsible to issue new certificates for their servers in a timely manner, and they SHALL ensure that they receive certificate signing requests from IPX providers on time.

If this renewal is not done in a timely manner it will lead to roaming traffic being impacted due to the certificate not being valid and the SEPP, DEA, SigFW or other equipment not being able to verify the protected traffic, causing the traffic to be dropped or rejected.

4.4 Certificate exchange specifically for DESS Phase 1

As defined in FS.19 [2], for DESS, MNOs issue certificates for their serving IPX providers. The corresponding keys, belonging to the IPX provider, are to be used by the IPX provider when it modifies signalling messages on transit.

The IPX provider for the modified Diameter signalling messages should re-sign the message by using the DESS signature. The receiving MNO should validate the signature by using the IPX certificate which should be properly signed by the sending MNO's issuer certificate.

DESS Phase 1 enhances Diameter messages on the inter-PMN interface with additional attribute value pairs (AVPs) to support digitally signed Diameter messages. The implementation of DESS Phase 1 differs from the 5G PRINS[2] and the foreseen DESS Phase 2:

- There is no in-band exchange of MNO leaf certificates and IPX provider leaf certificates.
- IPX providers do not append the certificate (chain) to the digital signature
- IPX providers sign modified messages (as in 5G they sign JavaScript Object Notation (JSON) patches), but IPX providers also need to verify the message before they re-sign the message. In 5G IPX providers have no role in message verification.

These characteristics imply a different key management procedure:

- In addition to the issuer certificate, individual leaf certificates need to be exchanged.
- As IPX providers need to verify digitally signed messages, they need to possess the issuer certificate of their client MNO and the issuer certificate of the peer MNO, and all underlying DEA/SigFW leaf certificates. This includes the peer MNOs' IPX certificates responsible for Diameter signing.

It is foreseen that DESS Phase 1 is an intermediate step towards DESS Phase 2, where certificates will be exchanged in-band.

[2] If 5GMRR proceeds with PRINS

For DESS Phase 1 MNOs SHOULD introduce a dedicated intermediate CA for network equipment connected to the IPX provider. This intermediate CA would sign all leaf certificates of all the network equipment of the IPX provider of the serving MNO. This has two major advantages:

- MNOs can assign responsibility for the intermediate CA to a different department than the owners of the root CA. This simplifies issuing certificates for new network equipment.
- For roaming partners, it is easier to determine which network equipment they could trust for secure exchange of messages. It would be all certificates issued by this particular sub CA.

The steps in section 4.4.1 SHALL be executed once in preparation of the first end-to-end secured Diameter roaming relationship. The steps described in section 4.4.2 and section 4.4.3 shall be executed for each end-to-end secured Diameter roaming relation.

4.4.1 Certificate exchange between MNO and own IPX provider

The following steps are executed only once in preparation of the first end-to-end Diameter roaming relationship.

If an MNO anticipates that its IPX provider needs to make changes to Diameter messages as described in Annex D of [2], it SHALL:

- Exchange its own issuer certificate as described in section 4.3.1, where its own IPX provider acts as receiving MNO
- MNO CA to sign for all leaf certificates and potentially sub CAs of the IPX provider, see section **Error! Reference source not found.** for the certificate hierarchy
- Exchange all leaf certificates of the MNO relevant entities for Diameter signing (DEA/SigFW leaf certificates)

Leaf certificates are considered authentic if they are signed by the exchanged issuer certificate. The method used to manually exchange leaf certificates is left to the MNO and the IPX provider to agree.

4.4.2 Leaf Certificate exchange between MNOs

The following steps SHALL be executed for each end-to-end secured Diameter roaming relationship.

For each end-to-end secured Diameter roaming relationship, leaf certificates need to be exchanged. This means that, in addition to the procedure described in section 4.3.1, all underlying DEA/SigFW leaf certificates, including the peer MNO’s IPX certificate entities responsible for Diameter signing (if any), SHALL be manually exchanged.

Leaf certificates are considered authentic if they are signed by the exchanged issuer certificate. The method used to manually exchange leaf certificates is left to the MNO to decide.

4.4.3 Peer MNO Certificate exchange between an MNO and its own IPX provider

The following steps SHALL be executed for each end-to-end secured Diameter roaming relationship.

If an MNO anticipates that its IPX provider needs to make changes to messages (which indicate that it needs to verify Diameter messages as well, see section 4.4) on the end-to-end secured Diameter roaming relationship it shall:

- Exchange the issuer certificate of the peer operator as described in section 4.3.1 where its own IPX provider acts as receiving MNO.
- Exchange all leaf certificates of the peer operator obtained as described in section 4.4.2 that are relevant for Diameter signing entities (DEA/SigFW leaf certificates), including the peer MNO's IPX certificates responsible for Diameter signing (if any).

Leaf certificates are considered authentic if they are signed by the exchanged issuer certificate. The method used to manually exchange leaf certificates is left to the MNO and the IPX provider to agree.

4.4.4 DESS Phase 1 functionality delegation

As stated in FS.19 [2], DESS Phase 1 functionality may be delegated to the serving IPX provider of an MNO. This delegation SHALL be published in the IR.21 of the MNO.

See section **Error! Reference source not found.** for the certificate hierarchy for DESS 1 delegation.

5 Naming Scheme

The naming scheme specified below follows section 28 of TS 23.003 [5]and TS 33.310 [14]

Error! Reference source not found. Root or intermediate certificates SHALL:

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

Leaf certificates SHALL:

- be X.509 v.3 certificates according to RFC 5280 with the Subject Alternative Name (SAN) extension
- contain values for MNC and MCC in both the common name and the subject alternative name, each three digits long (zero prefix as necessary) and correspond to the MNO (as in section 28.2 of TS 23.003 [5]) reflecting the main PLMN ID of the MNO
- comply with the naming schemes described in this section5.15.3
- repeat the Common Name (CN) in the Subject Alternative Name (SAN) field
- Specifically for SEPP certificates: contain all PLMN IDs that the SEPP represents on a given N32 connection. Refer to section 5.1

The `UNIQUE-IPX-PROVIDER-ID` in root, intermediate and leaf certificates can be any valid alphanumeric host ID that can be put into a Fully Qualified Domain Name (FQDN). It must be unique across all IPX providers worldwide. GSMA PRD IR.67 [11] describes the

procedure for how the alphanumeric host ID can be reserved and handed out. The FQDN shall also be resolved by a DNS server on the IPX network.

5.1 SEPP

The naming scheme of the SEPPs differs depending on whether the SEPP is operated by the MNO, or operated by another entity (e.g. hosted SEPP)

5.1.1 MNO SEPP

The Subject CN 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[1]

Example domain names include:

`1b.sepp.5gc.mnc001.mcc001.3gppnetwork.org`

`madrid.roaming.sepp.5gc.mnc001.mcc001.3gppnetwork.org`

`paris1.test.sepp.5gc.mnc001.mcc001.3gppnetwork.org`

MNO SEPP certificates SHALL include all PLMN IDs in SAN fields as DNS name for where it runs the N32 connection e.g.:

`<SEPP-id>.sepp.5gc.mnc<PLMN ID 1>.mcc<MCC>.3gppnetwork.org`

`<SEPP-id>.sepp.5gc.mnc<PLMN ID 2>.mcc<MCC>.3gppnetwork.org`

Signalling traffic containing other PLMNs IDs SHALL NOT be accepted.

The well-known SEPP FQDN `sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org` as described in GSMA PRD NG.113 [12] is only a stepping stone to trigger SEPP discovery via DNS.

5.1.2 Non-MNO SEPP

When the SEPP does not belong to an MNO, e.g. a hosted SEPP , the certificate SHALL clearly indicate this in the CN/SAN fields and SHALL also be published in the IR.21 accordingly. The CN field SHALL be structured as:

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

[1]where `SEPP-id` contains at least one label/sub domain. Entities that operate an hosted SEPP SHALL use separate SEPP certificates for each MNO that it serves.

Non-MNO SEPP certificates SHALL include all PLMN IDs in SAN fields as DNS name from the MNO for where it runs the N32 connection e.g.:

`<SEPP-id>.sepp.5gc.mnc<PLMN ID 1>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org`

`<SEPP-id> sepp.5gc.mnc<PLMN ID 2>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org`

Signalling traffic containing other PLMNs IDs SHALL NOT be accepted.

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

In order to enable multi-tenancy, the initiating SEPP (iSEPP) SHALL always include the SEPP FQDN of the MNO in the TLS SNI-parameter. Also, the receiving SEPP (rSEPP) SHALL not duplicate FQDNs in CN/SAN in different certificates.

5.2 DESS Phase 1 related entities

DESS Phase 1 related entities such as SigFW,DRA or DEA have a different naming convention whether the below to the MNO or to the serving IPX provide.

5.2.1 MNO DESS Phase 1 equipment

The Subject CN/SAN field SHALL be structured as:

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

where `diameteridentity` is the Diameter node (host) to which the certificate is issued. If all Diameter nodes use the same certificate the Subject/SAN field shall be structured as:

`diameter.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

For DESS Phase 1 the DESS-Signing-Identity AVP shall indicate the signee in the exact format of the Subject/SAN field outlined above.

5.2.2 IPX provider intermediate signing DESS Phase 1 equipment

For intermediate signing as described in FS.19 [2] the Subject CN/SAN field SHALL be structured as:

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

where `diameteridentity` is the Diameter node (host) to which the certificate is issued. If all Diameter nodes use the same certificate the Subject/SAN field shall be structured as:

`diameter.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org`

For DESS Phase 1 the DESS-Signing-Identity AVP shall indicate the signee in the exact format of the Subject/SAN field outlined above.

5.2.3 IPX provider security delegation DESS Phase 1 equipment

For security delegation, not be to confused with intermediate signing, as described in FS.19 [2] the Subject CN/SAN field SHALL be structured as:

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

where `diameteridentity` is the Diameter node (host) to which the certificate is issued. If all Diameter nodes use the same certificate the Subject/SAN field shall be structured as:

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

For DESS Phase 1 the DESS-Signing-Identity AVP shall indicate the signee in the exact format of the Subject/SAN field outlined above.

5.3 N9 operator-to-operator security

The Subject CN/SAN field SHALL be structured as either:

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

or

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

(a) may indicate a UPF or a UPF cluster providing the secure tunnel.

(b) may indicate a or a Security Gateway (SEG) providing the secure tunnel.

NOTE: Outsourcing or delegating N9 operator-to-operator security is to be studied in a later stage in collaboration with 5GMRR

Annex A Public Key Infrastructure (PKI)

A.1 Introduction to PKI

PKI, or public key infrastructure, is a summarizing term for the infrastructure and processes that facilitate the use of certificates. In their essence certificates allow two parties to share their identity via a standardized format, often X.509, and have a centrally trusted third party verify that what both parties have sent is indeed true. Combine this service with the assurance of provably strong asymmetric cryptography and you have a service that can provide a very high level of trust between two parties.

In more technical terms, this infrastructure starts with a central entity called a root CA, or root certification authority. This party is, within this PKI infrastructure, at the top of a pyramid and trusted by all parties that use its services. If two parties want to create trust between each other using certificates they start with creating a pair of keys – a public and a private part. With this keypair they generate a certificate signing request (CSR) which in essence is their certificate which they ask the root CA to sign. The root CA verifies the identity of the requesting party according to specific procedures and, if OK, will sign the certificate with its own keypair. Now, both parties can exchange these signed certificates, in combination a signature from their key pair, and have a certain amount of verifiable proof that both parties are who they say they are.

This methodology is also what provides the initial setup of a TLS transaction, or in the case of Diameter DTLS, to setup a secure connection (HTTPS between two SEPPs) or provide integrity and confidentiality protection of Diameter traffic. For more details a good start is the Wikipedia page on this subject [7].

A.2 Example PKI using EJBCA

There are multiple ways of operating a PKI. In this annex we have chosen to provide an example of using EJBCA to run a PKI infrastructure, as it provides all aspects needed to do this technically and procedurally, and has an unlimited free version that can be extended with paid for support for those companies whose internal policies require it. However, the certification authority required for a PKI infrastructure must be operated securely as it is key to maintaining the trust between all the organisations participating in the infrastructure. There are a number of global references that define how multi-organisation PKI infrastructures can be secured, this includes [6]. Due to the costs required to create a secure PKI infrastructure MNOs are strongly advised to use existing PKI Infrastructure capabilities, either internal or external to maintain inter-organisation trust.

EBJCA can be installed in two ways – standalone using JBOSS, or in a docker container. Please follow the respective installation guide which can be found here – https://www.ejbca.org/download/.

To setup the root CA, a keypair first needs to be created. It is advised, due to the importance of these keys, to create and store these keys in a hardware security module (HSM). EJBCA supports multiple solutions – https://download.primekey.com/docs/EJBCA-Enterprise/6_15_2/Hardware_Security_Modules_(HSM).html. It is advised to be critical in the evaluation when choosing an HSM – however, even a simple variant such as a Nitrokey HSM or Yubikey HSM is better than storage on disk or in a SoftHSM.

With these keys ready, a root CA can be created using the certification authority selector, and then selecting ‘create new’ at the bottom. Information on how to fill in these fields can be found in the EJBCA documentation as well as in RFC 5280 [8]. If a root CA is already present in an MNO organisation one should create a separate sub (or leaf) CA for signing certificates used for mobile roaming traffic. This to reduce the impact of compromised key material, clarify the scope a certificate is allowed to be used in, not share company internal information, and keep a better overview of where certificates are used and for which purpose.

When the root (or sub) CA is created it is advised to create a certificate profile. This is to prevent differences between certificates within your infrastructure and reduce the burden on employees. The details on defining the profile can be found in the EJBCA documentation or RFC 5280 [8].

When these steps have been concluded, the employee responsible for the SEPP, DEA or SigFW can start the process for receiving a signed certificate from the root or sub CA. The specific procedure will be vendor specific but the steps are always as follows:

1. Generate an asymmetric key pair on the system in question using the approach specified in [1]
2. Generate the certificate signing request (CSR) and have this signed by the root/sub CA. If needed ONLY export the CSR to EJBCA. NEVER export the private key off the system as this compromises its confidentiality and all traffic protected by it.
3. Import the signed certificate back onto the platform and configure your platform to use only that certificate for all specific communication.

If the platform supports OpenSSL, the following website provides a short introduction on how that might be used to create a CSR: https://support.rackspace.com/how-to/generate-a-csr/.

Annex B Document Management

B.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).

B.2 Other Information

Type	Description
Document Owner	DESS
Editor / Company	Ewout Pronk / Titan.ium Platform LLC

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.