Key Management for 4G and 5G inter-PLMN Security

Version 1.0

06 March 2020

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

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-PLMN roaming security (as defined in 3GPP TS 33.501[1]) and 4G roaming inter-PLMN 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 (e.g. DNSSec or other technical approach to be selected)

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:

- DESS Phase 1: Authentication and integrity protection by introducing digital signatures on inter-PLMN Diameter signalling messages.
- DESS Phase 2: Confidentiality measures by introducing DTLS-sessions over Diameter on inter-PLMN Diameter signalling messages.

As soon as the full stage 2 solution is defined, implemented and widely rolled-out, the stage 2 solution is expected to eventually replace the stage 1 solution. All security requirements, technical functionality and certificate handling aspects also apply to stage 2. Stage 1 is a preparatory step for stage 2. The main difference is that in stage 2, certain manual tasks will be automated.

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. DESS Phase 2 key management procedures however are similar to 5G.

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 to secure the signalling communication.

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

Although this document mentions the possibility of outsourcing or delegating the inter-PLMN security (section 3.1), the details of such an approach will be described in a later version of this document.

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.

1.4 Abbreviations

Term	Description
AVP	Attribute Value Pair
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
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

Term	Description
HSM	Hardware Security Module
IP	Internet Protocol
IPX	IP eXchange
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
PLMN	Public Land Mobile Network
PRINS	Protocol for N32 Interconnect Security
Root CA	Root Certification Authority
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAN	Subject Alternative Name
SEPP	Security Edge Protection Proxy
SigFW	Signalling Firewall
Sub CA	Subordinate Certification Authority
TLS	Transport Layer Security
URL	Uniform Resource Locator

1.5 References

Ref	Doc Number	Title
[1]	3GPP TS 33.501	Security architecture and procedures for 5G System, https://www.3gpp.org/DynaReport/33501.htm
[2]	GSMA 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

Ref	Doc Number	Title
[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

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, 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 (MNOs and IPX providers) 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 has expired, a new certificate must be exchanged for secure communication to continue. Often, a certificate has already been renewed and exchanged before it is due to expire.

2.3 IPX Trust Model

The following figure illustrates the trust relationship between interconnection partners and indicates the level of trust for every logical and physical connection.

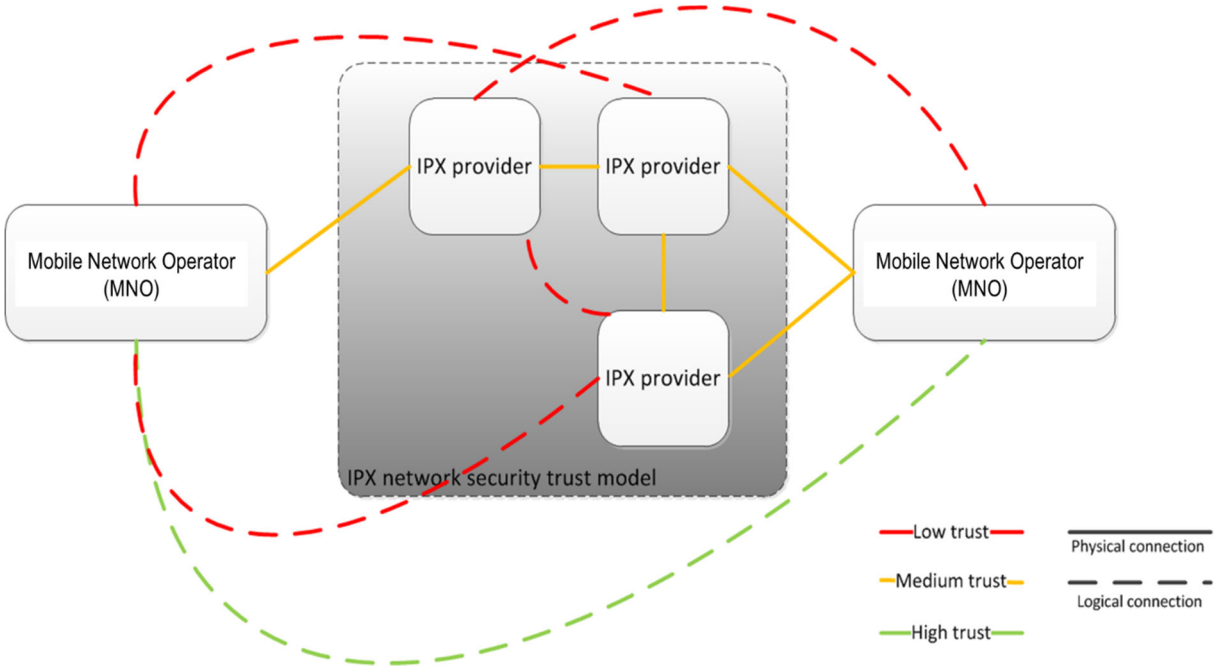

Figure 1 – IPX network security trust model relationships

The relations between stakeholders on the IPX network have various trust levels. By classifying trust into 3 levels (high trust, medium trust and low trust), the following distinctions can be made:

Relationship	Trust Level	Rationale
MNO and MNO	High trust	An MNO relationship is backed up by a roaming contract, which includes a financial relationship for roaming usage.
MNO and own IPX provider(s)	Medium trust	An MNO trusts its own IPX provider to provide the work that is agreed in their contract/agreement. Trust from a security perspective is harder however, as the assets (signalling messages) that are handled by the IPX

Relationship	Trust Level	Rationale
		provider in the exchange of signalling messages are assets of the MNO only, not of the IPX provider.
MNO and other IPX provider(s)	Low trust	An MNO has lower trust in other IPX providers than its own. While the IPX provider could be in the flow of exchanging signalling messages for assets of the MNO, there is no contract or agreement between them.
IPX provider and peer IPX provider	Medium trust	Peer IPX providers have a contractual relationship but the fact that they are competitors has an effect on the trust relationship.
IPX provider and other (unconnected) IPX provider	Low trust	IPX providers not connected to each other are competitors and do not have an agreement/contract.

Table 1 – Trust levels between IPX network stakeholders

IPX providers transport assets, i.e. signalling messages, on behalf of the MNOs. It is in the interest of the MNOs that these assets are transmitted securely. As there are third parties involved (with which the MNO has no contractual relationship), cryptographic protection is applied to protect the signalling messages when using the 4G (PRD FS.19) or 5G (3GPP TS 33.501) roaming protection schemes.

In the IPX ecosystem, it is the MNOs that have a high level of trust in each other. It is the MNOs that exchange their issuer certificates with each other. This allows them to link an identity, i.e. an MNO identifier, to a particular public key that is used by network equipment that belongs to that MNO. The high level of trust is created based on the procedures used to verify the MNO identity of the other party.

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 subject unique identifier (i.e. no entity can obtain a certificate issued under another entity's name).

In the context of roaming security, MNOs will use the functionality of a CA and issue certificates to be used with signalling 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 global CA which could be considered as trusted for all MNOs located in different geopolitical regions. A dedicated public key infrastructure (PKI) for signalling security is required. It is assumed that every MNO independently operates a PKI including a root 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.

More details about certification authorities, root CAs, sub CAs, PKI and certificate hierarchy are contained in section 5.

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 containing an identifier and a public key, 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 Exchange Procedures

The exchange of issuer certificates and DESS Phase 1 leaf certificates is a manual process. MNOs 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.

3.1 Responsibilities

This document assumes that MNOs run their own roaming operations and deploy a SEPP, DEA and/or SigFW. They are responsible for performing the procedures described in this section. Depending on the service offering of IPX providers and on the agreements between MNOs and IPX providers, some of the inter-PLMN security functionality may be operated by the IPX provider on behalf of the MNO. In such a case, responsibilities move from the MNO to the IPX provider. The IPX provider will then have to perform the steps described in this document.

As defined in 3GPP TS 33.501 [1] and in FS.19 [2], 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.

5G – Depending on the roaming relation between two MNOs, the IPX provider needs to attach the corresponding certificate to the modified 5G signalling message so that the receiving MNO can validate the modification against the root CA certificate of the sending MNO.

Diameter DESS Phase 1 – 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.

3.2 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.
- 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.

3.3 Determine Certificates to be Exchanged

Issuer certificates are required to be exchanged for:

- 5G – Transport Layer Security (TLS) + Protocol for N32 Interconnect Security (PRINS[1])
- 4G – DESS Phase 2 (Datagram Transport Layer Security (DTLS) over Diameter)

However, leaf certificates are still required to be exchanged for:

- 4G – DESS Phase 1 (authentication and integrity protection only)
    - Certificates of DEA/SigFW
    - Certificates of IPX providers

NOTE: Explanations on this special case are provided in section 3.5.

3.4 Certificate Management Procedures

3.4.1 Certificate Exchange Procedure

The certificate to be exchanged as per section 3.3, shall be exchanged in the following way:

Publishing MNO:

1. Install the respective certificate on the signalling equipment (SEPP or DEA/SigFW) and ensure that it will be offered to peers upon establishment of a secure roaming communication.

[1] PRINS is the application layer security protocol for the N32 interface described in clause 13.2 of TS 33.501 [1].

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. As an optional alternative, Online Certificate Status Protocol (OCSP) 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, archive the email and ask the person to send a new email with the correct certificate. In case of a match, mark the certificate as verified.
2. Install the verified CA certificate on the signalling equipment (SEPP or DEA/SigFW), 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 signalling 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.
3. Have the system periodically query the noted CRLs to verify that they can be resolved and queried.

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.

4. Record the expiry date of the received certificate and ensure to be alerted at least three months prior to its expiry, 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.

1. Ensure that the publishing and receiving MNO have the certificate in the same format. If format differs, convert the certificate into the PEM format.
2. 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`.

3.4.2 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.

3.4.2.1 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 MNO then generates a replacement certificate and puts it to use. 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.

3.4.2.2 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. Certificates for IPX providers can be issued on the basis of certificate signing requests kept on file. Reusing existing requests may avoid undue delays.
3. Perform the actions from section 3.4.1 (publishing MNO) for each roaming partner.
4. Publish the revoked certificate in the CRL and publish a new version of the CRL.

Receiving MNO:

1. When contacted by a roaming partner for the purposes of CA certificate revocation/replacement, perform the actions from section 3.4.1 (receiving MNO). Apart from verifying the fingerprint of the new CA certificate, it is crucial that the phone call is placed by the receiving MNO, and that the number dialled is the one on file for the responsible staff at the publishing MNO. This ensures that the request for CA certificate replacement is legitimate.
2. In addition to installing the new CA certificate, delete all copies of the revoked one.

3.4.3 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 3.4.1 both for the publishing and the receiving MNO.

NOTE 1: The old CA certificate shall remain valid in the signalling 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.

3.4.4 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 or SigFW not being able to verify the protected traffic, causing the traffic to be dropped or rejected.

3.5 Certificate exchange specifically for DESS Phase 1

DESS Phase 1 enhances Diameter messages on the inter-PLMN interface with additional attribute value pairs (AVPs) to support digitally signed Diameter messages. The implementation of DESS Phase 1 differs from the 5G 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.

The steps in paragraph 3.5.1 shall be executed once in preparation of the first end-to-end secured Diameter roaming relationship. The steps described in paragraph 3.5.2 and paragraph 3.5.3 shall be executed for each end-to-end secured Diameter roaming relation.

3.5.1 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 3.4.1, where its own IPX provider acts as receiving MNO
- 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.

3.5.2 Leaf Certificate exchange between MNOs

The following steps are 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 3.4.1, 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.

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

The following steps are 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 3.5) on the end-to-end secured Diameter roaming relationship it shall:

- Exchange the issuer certificate of the peer operator as described in section 3.4.1 where its own IPX provider acts as receiving MNO.
- Exchange all leaf certificates of the peer operator obtained as described in section 3.5.2 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 Naming Scheme

The naming scheme specified below follows section 28 of TS 23.003 [5].

All certificates shall:

- be X.509 v.3 certificates according to RFC 5280 with the Subject Alternative Name (SAN) extension;
- contain the structure `ca<CAID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org` in the Issuer field, where the values for MNC and MCC are each three digits long (zero prefix as necessary) and correspond to the MNO (as in section 28.2 of TS 23.003 [5]), and where `CAID` is an optional alphanumeric identifier for the CA.
- the Subject Common Name (CN) field contents shall be identical to the contents of the Subject Alternative Name field.

The contents of the Subject CN/Subject Alternative Name (SAN) field differs depending on whether or not the certificate is a self-signed root CA certificate. For self-signed root CA certificates, the contents of the Subject CN/SAN field of certificates issued by an MNO's CA shall be identical to the contents of the Issuer field.

For other certificates, the contents of the Subject CN/SAN field differ depending on whether it is issued for 5G SEPP signalling, Diameter signalling, or for an IPX provider.

MNOs with an existing root CA may reuse existing root CA certificates if there are reasons for not operating a separate CA for the purposes of 5G/Diameter signalling security. In this case, the root CA certificate will not necessarily follow the naming scheme defined above, which is acceptable in this case. However all other certificates (intermediate CA and leaf) shall follow the naming scheme described here.

4.1 SEPP

The Subject CN/SAN field shall be structured as

`sepp<SEPPID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

where `SEPPID` is the SEPP ID as specified in Section 13.2.2.4.2 of TS 33.501 [1].

NOTE: The certificate is used by the SEPP to establish N32-c connections with other SEPPs. This is not to be confused with the wildcard certificate used by the SEPP in the context of N32-f as described in Section 13.1 of TS 33.501 [1].

4.2 Diameter

The Subject CN/SAN field shall be structured as:

`diameter<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.

4.3 IPX Provider

The Subject CN/SAN field shall be structured as

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

Where `UNIQUE-IPX-PROVIDER-ID` 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. The FQDN shall also be resolved by a DNS server on the IPX network.

The DESS-Signing-Identity AVP shall indicate the signer in the exact format of the Subject/SAN field outlined above.

5 Key Management and Processing Details

5.1 Certificate Hierarchy

Certificates are typically issued by an authority that is part of a hierarchy. On the top, there is a single issuer certificate, the so-called root certificate. The root certificate is used by the root CA to generate certificates for other entities, typically (non-root) CAs. These CAs are called subordinate CAs (sub-CAs) or intermediary CAs. Entities that request and receive certificates in their role of communication partners, and that do not issue certificates themselves, are the main reason for which the system is set-up. Their certificates are called leaf certificates. The entire certification hierarchy and surrounding procedures is called a public key infrastructure (PKI).

MNOs tend to operate their own their certification authorities (CAs) and are able to issue certificates for network equipment. In some cases, it is useful to introduce a hierarchy of CAs. An organisation has one root CA and multiple intermediate CAs. The root CA signs all the intermediate certificates. The intermediate CAs sign certificates of network equipment (leaf certificates) for certain domains. All the CAs, their hierarchy, creation and management of certificates are collectively referred to by the term public key infrastructure.

The CA (root CA or intermediate CA) shall be used to sign every individual certificate in certain MNO networks. By using this principle, it is sufficient for certain protection models just to exchange the root CA certificate between the roaming partners. Every MNO receiving signalling messages shall use the chain of trust to verify the root CA, the intermediate CA and the individual certificates of DEA, SEPP or further network equipment, and to validate that they all have been correctly signed by a proper CA.

Figure 2 illustrates an example of three MNOs having a root CA each and some also having intermediate CAs. These MNOs shall exchange the certificates of their root CAs.

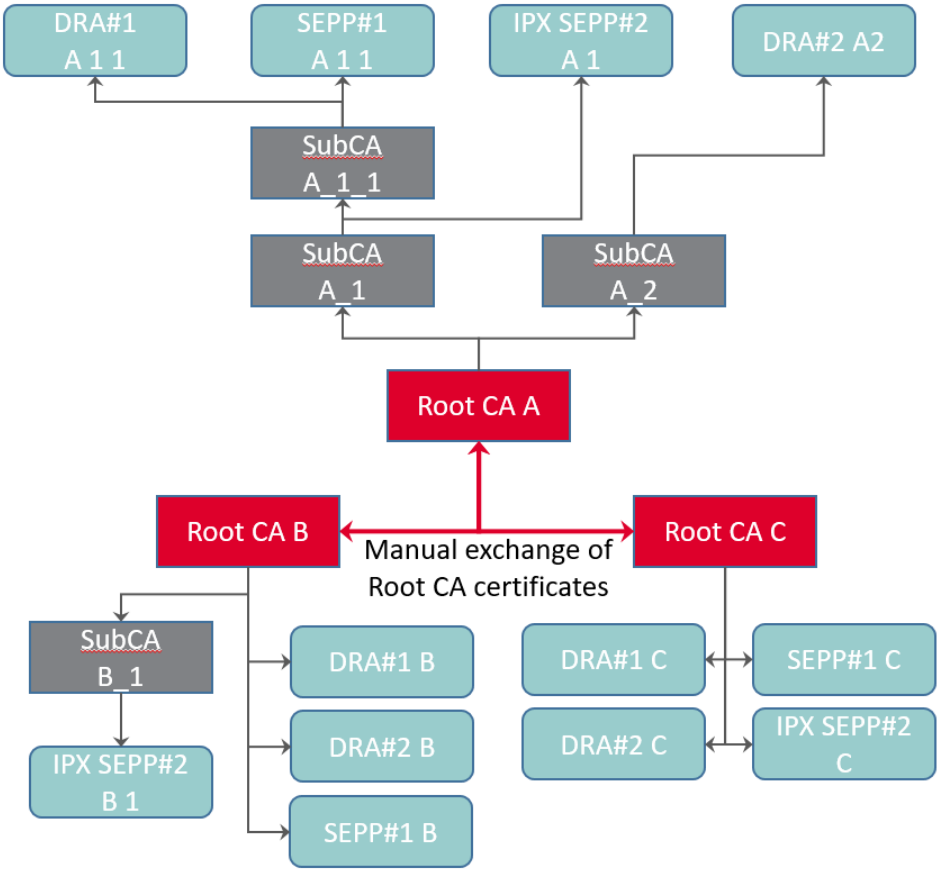

Figure 2 – Example MNO PKIs

All CAs are issuers, as they issue certificates for entities below them in the chain of trust. An issuer certificate is the one that was issued for the issuer. It contains the public key of the issuer.

The root CA issues a certificate for itself. In this exceptional case, the issuer equals the subject, i.e. the entity for which the certificate is issued. For all other certificates, the issuer is the entity one step further up in the certificate chain. In the example in Figure 2, the issuer of SubCA B_1 is Root CA B and the issuer of IPX SEPP#2 B1 is SubCA B_1.

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.

5.2 Outsourcing of Certification Authorities

An adversary could render signalling security ineffective either by compromising the MNO's CA private key, by compromising the private key of any certificate issued by the MNO's CA, or by illegitimately obtaining certificates from the MNO's PKI. It is therefore important to note that signalling security relies on the security of the MNO's PKI procedures, in particular around certificate issuing, and on ensuring that private keys corresponding to issued certificates are sufficiently well-protected.

Since an MNO has no control over the private CA key of third-party certificate providers, MNOs are strongly recommended to have and operate their own root CA. It is also not allowed to use PKI providers on the Internet.

5.3 Certificate Verification

Certificate verification logic must not be limited to checking that a valid path exists to *any* trusted CA and that the current date lies within the validity period of all certificates in the chain. As described in section 3.4.1, once a CA certificate is bound to a particular roaming partner, all signalling from that roaming partner must be rooted *in that particular* CA certificate, and this must be checked.

The following aspects should be checked as well.

- The Issuer and Subject fields of the leaf certificate must follow the specified format and correspond to signalling equipment that is eligible to send messages over the interface over which the signalling message was received.
- For all certificates in the chain: The issuer of the certificate must match the subject, i.e. they must both correspond to the same MNO. In the case of SEPP this means that the MNC and MCC fields are identical for all certificates in the certificate chain. In the case of Diameter, this means checking that the Diameter Identity belongs to the same MNO as indicated by the MNC and MCC in the CA certificate. In case of IPX providers, this means that the MNO (as identified by MCC and MNC tuple) is indeed known to have a contractual relationship with the IPX provider whose FQDN appears in the subject alternative name field.

5.4 MNO Certification Authority requirements

A dedicated public key infrastructure (PKI) for signalling security is required.

Each MNO should use at least one root CA, and it is strongly recommended to operate its own PKI. It should always be the MNO that is issuing certificates for its own network elements and servers, as well as for the IPX providers that the MNO has a contractual relationship with.

It is further required that the policies and procedures governing the operation of the PKI are documented by the MNO.

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

MNOs are recommended to introduce a dedicated intermediate CA for network equipment connected to the IPX. This intermediate CA would sign all leaf certificates of all the network equipment that can communicate on the IPX. 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 should trust for secure signalling. It would be all certificates issued by this particular sub CA.

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, it is possible that an MNO already has an internal certification authority. If so, MNOs are strongly advised to use this existing infrastructure due to the costs required to create a secure PKI infrastructure.

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 organization 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)

B.2 Other Information

Type	Description
Document Owner	DESS
Editor / Company	Martin Kacer / P1 Security

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.