



Question(s): 2/11

Geneva, 6-15 July 2022

TD

Source: Editors

Title: Consent – draft new Recommendation ITU-T Q.3062 (ex. Q.Pro-Trust)
“Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks” (Geneva, 6-15 July 2022)

Contact: Assaf Klinger
Vaulto Technologies Ltd.
Israel
Tel: +972502138133
E-mail: assaf.klinger@gmail.com

Contact: Minrui Shi
China Telecom
China
Tel: 021-68540571
E-mail: shimr@chinatelecom.cn

Abstract: This document contains the baseline text of draft Recommendation ITU-T Q.3062 (ex. Q.Pro-Trust) “Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks” which was finalized at Q2/11 meeting and proposed for consent at the SG11 closing plenary (15 July 2022).

This document is based on SG11-TD1833/GEN, the output of Q2/11 meeting on December 2021, and according to this meeting’s discussion and results on the following contributions and iLS:

| No. | Title | Source | Discussion |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----------------------------|
| T17-SG11-C30 | Proposal to advance the baseline text and consent on Recommendation ITU-T Q.Pro-Trust: “Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks” | Vaulto Communication Technologies Ltd. | Accepted with modifications |
| T17-SG11-C32 | This document proposes improvements of text of Q.Pro-trust according to the EDITING GUIDELINES for Consent | China Telecom | Accepted with modifications |
| T17-SG17-LS6 (TD129/GEN) | LS/i/r on draft new Recommendation ITU-T Q.Pro-Trust and Q.CIDA (SG11-LS224) | ITU-T SG17 | Accepted with modifications |

Table of Contents

| | | |
|--------|---------------------------------------------------------------------------|----|
| 1 | Scope..... | 6 |
| 2 | References..... | 6 |
| 3 | Definitions | 7 |
| 3.1 | Terms defined elsewhere | 7 |
| 3.2 | Terms defined in this Recommendation..... | 7 |
| 4 | Abbreviations and acronyms | 8 |
| 5 | Conventions | 8 |
| 6 | Architecture for interconnection between trustable network entities | 8 |
| 6.1 | Reference architecture | 9 |
| 6.2 | Functional entities | 9 |
| 6.2.1 | Certification authority | 9 |
| 6.2.2 | Trusted signalling certification authority | 9 |
| 6.2.3 | Signalling security gateway | 10 |
| 6.2.4 | Network entity | 10 |
| 6.3 | Reference points | 10 |
| 6.3.1 | Sa reference point | 10 |
| 6.3.2 | Sc reference point | 10 |
| 6.3.3 | TSa reference point | 10 |
| 7 | Security services | 10 |
| 8 | Security association attribute definition | 10 |
| 8.1 | Security association identifier (SAI) | 10 |
| 8.2 | Cryptographic parameters per Security Association | 11 |
| 9 | Structure of protected messages | 11 |
| 9.1 | Security Header | 11 |
| 9.2 | Security Payload..... | 11 |
| 9.3 | Digital Signature Algorithms (DSA)signature algorithms | 11 |
| 9.3.1 | Description of DSA-0..... | 12 |
| 9.3.2 | Description of DSA-1..... | 12 |
| 10 | Signalling procedures | 12 |
| 10.1 | TSa..... | 12 |
| 10.1.1 | Trusted signalling certification authority signalling procedures..... | 12 |
| 10.1.2 | TSa signalling procedures | 13 |
| 10.1.3 | TSa messages | 15 |
| 10.2 | Sa | 15 |
| 10.2.1 | Signalling security gateway signalling procedures..... | 15 |

| | | |
|----------------------------------------------------------------------------------------------------------------------------|--------------------------------|----|
| 10.2.2 | Sa signalling procedures..... | 16 |
| 10.2.3 | Sa messages ASN.1 format | 18 |
| 10.3 | Sc | 18 |
| 10.3.1 | Sc signalling procedures..... | 18 |
| 10.3.2 | Sc messages ASN.1 format | 19 |
| Annex A: List of verifiable CSP identifiers to be sent in the PEEC request | | 20 |
| Annex B: ASN.1 format for signaling messages | | 22 |
| Appendix I: Information validation techniques (This appendix does not form an integral part of this Recommendation.) | | 24 |
| Bibliography..... | | 25 |

List of figures

| | |
|------------------------------------------------------------------------------------------------|----|
| Figure 6-1 – Reference architecture of interconnection between trustable network entities..... | 9 |
| Figure 10-1 – Signalling procedures of a trusted signalling certification authority | 13 |
| Figure 10-2 – TSa signalling procedure..... | 14 |
| Figure 10-3 – Signalling procedures of SSGW | 15 |
| Figure 10-4 – Sa signalling procedure – Happy flow | 16 |
| Figure 10-5 – Sa signalling procedure – Unhappy flow | 17 |
| Figure 10-6 – Sc signalling procedure | 19 |

List of tables

| | |
|------------------------------------------------------------------------------------|----|
| Table 9-1 – Digital signature algorithms in this recommendation (Q.Pro-Trust)..... | 12 |
|------------------------------------------------------------------------------------|----|

Draft Recommendation ITU-T Q.3062 (ex. Q.Pro-Trust)

Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks

Summary

Signaling System No. 7 (SS7) is a stack of signaling protocols, which was initially developed by ITU (CCITT) in the 1980s. Since then, SS7 standards has become a generic stack which are widely applied in public switched telephone network (PSTN) all over the globe. With the growth of mobile telecommunications and appearance of the MAP and CAP protocols, SS7 stack has become suitable for public land mobile network (PLMN), e.g., 2G, 3G networks. Later, SS7 migrated to SIGTRAN stack developed by IETF which allows operators to setup interconnection of SS7-based networks over IP networks. Furthermore, the SS7 logic migrated to DIAMETER which is currently widely used for interconnection of IMS-based networks, including 4G (VoLTE/ViLTE).

At the development stage, SS7 was designed to be managed by operators with the understanding that anyone connected to SS7 network was considered trustworthy. With the current network environment, including interconnection over the Internet, SS7-based networks have become vulnerable and can be easily attacked. Moreover, the latest move to Diameter protocol has not solved any of the basic vulnerabilities found in SS7.

Presently, there have been multiple cases where SS7 vulnerabilities have been used for different hackers' attacks. Amongst well-known attacks on SS7 networks include telephone spam, spoofing numbers, location tracking, subscriber fraud, intercept calls and messages, DoS, infiltration attacks, routing attacks, etc.

The goal of this Recommendation is to define the signalling requirements for authentication of signalling messages, in order for operators to be able to verify the authenticity of signalling exchange based on an accepted trust anchor. This Recommendation includes codes and signalling procedures based on ITU-T Q.3057.

Keywords

Authentication, trust, signalling procedures, certification authority, digital signature, post quantum cryptography, trust anchor, data integrity, public key certificate, end entity public key certificate.

Draft Recommendation ITU-T Q.3062 (ex. Q.Pro-Trust)

Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks

1 Scope

This Recommendation specifies signalling procedures and protocols involved in the application of the signalling requirements and architecture, as well as reference points TSa, Sa and Sc specified in ITU-T Q.3057, for interconnection between trustable network entities (NEs) in support of existing and emerging networks.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T Q.3057] Recommendation ITU-T Q.3057 (2020) *Signalling requirements and architecture for interconnection between trustable network entities.*
- [ITU-T T.411] Recommendation ITU-T T.411 (03/1993): *Information technology - Open Document Architecture (ODA) and interchange format: Introduction and general principles*
- [ITU-T Q.1400] Recommendation ITU-T Q.1400 (03/93) *Architecture framework for the development of signalling and OA&M protocols using OSI concepts*
- [ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks.*
- [IETF RFC 4703] Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients
- [ITU-T X.510] Recommendation ITU-T X.510 (2019) *Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations*
- [ITU-T X.1163] Recommendation ITU-T X.1163 (2015) *Security requirements and mechanisms of peer-to-peer-based telecommunication networks*
- [FIPS PUB 140-2] Federal Information Processing Standards Publication FIPS PUB 140-2 (2001) + change notices (2002), *Security requirements for cryptographic modules.*
- [FIPS PUB 186-4] Federal Information Processing Standards Publication FIPS PUB 186-4 (2013), *Digital signature standard (DSS).*
- [NIST SP 800-57-3] NIST SP 800-57 Part 3 Rev.1 (2015) *Recommendation for Key Management - Part 3: Application-Specific Key Management Guidance*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authority [ITU-T X.509]: An entity, responsible for the issuance of certificates or of revocation lists.

3.1.2 certification authority (CA) [ITU-T X.509]: An authority trusted by one or more entities to create and digital sign public-key certificates. Optionally the certification authority may create the subjects' keys.

3.1.3 cross-certificate [ITU-T X.509]: A certification authority (CA) where the issuer and the subject are different CAs. CAs issue cross-certificates to other CAs as a mechanism to authorize the subject CA's existence.

3.1.4 data integrity: [b-ITU-T-T.411] The property that data has not been altered or destroyed.

3.1.5 end-entity public-key certificate [ITU-T X.509]: A public-key certificate issued to an entity, which then acts as an end entity within a public-key infrastructure.

3.1.6 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.7 global title (GT) [b-ITU-T Q.1400] This is addressing used by the SCCP, comprising dialed digits or another form of address that will not be recognized by the SS No. 7 network layer. Therefore, translation of this information to an SS No. 7 network address is necessary.

3.1.8 hash function [ITU-T X.509]: A (mathematical) function which maps data of arbitrary size into data of a fixed size called a digest.

3.1.9 security domain [ITU-T Q.3057]: A set of objects or entities of whose security policy can be administered by one organization.

3.1.10 signalling security gateway (SSGW) [ITU-T Q.3057]: An entity on the borders of the security domains that terminates and initiates secure native signalling/protocols, relays signalling traffic between security domains, configures security parameters or protocols and can perform a security policy management function.

3.1.11 trust [ITU-T X.1163]: The relationship between two entities where each one is certain that the other will behave exactly as it expects.

3.1.12 trust anchor [ITU-T X.509] An entity that is trusted by a relying party and used for validating public-key certificates.

3.1.13 trusted signalling certification authority (TSCA) [ITU-T Q.3057]: The root of trust for verifying digital signatures using the root certification authority (CA) model.

3.1.14. fully qualified domain name (FQDN) [RFC 4703]: Network entity address indicator on Internet protocol interconnect.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 local signalling security gateway: A signalling security gateway (SSGW) that sends messages on behalf of a network entity within the same security domain towards another SSGW.

3.2.2 peer signalling security gateway: A signalling security gateway (SSGW) that receives messages on behalf of a network entity within the same security domain from another SSGW.

3.2.3 provisional end entity public-key certificate: A short-term end entity public-key certificate with a 6-month validity period.

3.2.4 security association (SA): A logical connection created for security purposes. All traffic traversing an SA is provided with the same security protection. The SA specifies protection levels, algorithms to be used, lifetimes of the connection etc.

3.2.5 validated end entity public-key certificate (VEEC): A long-term end entity public-key certificate with a 2-year validity period.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|-------|----------------------------------------------------|
| CA | Certification Authority |
| CSP | Communications Service Provider |
| DS | Digital Signature |
| DSA | Digital Signature Algorithm |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EEC | End Entity public-key Certificate |
| FQDN | Fully Qualified Domain Name |
| GT | Global Title |
| IE | Information Element |
| IPX | Internet Protocol interconnect |
| NE | Network Entity |
| PEEC | Provisional End Entity Public-key certificate |
| SA | Security Association |
| SAI | Security Association Identifier |
| SCCP | Signalling Connection Control Part |
| SGC | Signalling security Gateway public-key Certificate |
| SS | Signalling System |
| SSGW | Signalling Security Gateway |
| TSCA | Trusted Signalling Certification Authority |
| TVP | Time Variant Parameter |
| UTC | Coordinated Universal Time |
| VEEC | Validated End Entity public-key Certificate |

5 Conventions

None.

6 Architecture for interconnection between trustable network entities

ITU-T Q.3057 introduced a centralized trust anchor for issuing and verifying digital signatures in signalling interconnect. In cryptography, a CA is an entity that issues digital public-key certificates. A digital public-key certificate certifies the ownership of a public key by the named subject of the

certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party – trusted both by the subject (owner) of the public-key certificate and by the party relying upon it. The format of these public-key certificates is specified in ITU-T X.509. A CA can issue end-entity public-key certificates to each operator that is signed by the root public-key certificate, which is the topmost public-key certificate of the tree. In order to create a trustable interconnection between network entities, All operator end-entity public-key certificates need to signed by the trust anchor (using the root public-key certificate). Thus inherit the trustworthiness of the trust anchor.

Establishment of a Trusted Signalling Certification Authority (TSCA) as the trust anchor asserts control and traceability to the process of creating and signing digital public-key certificates.

6.1 Reference architecture

Figure 6-1 shows the reference architecture specified in ITU-T Q.3057 for the interconnection between trustable network entities. In this NEs. This Recommendation specifies the signalling procedures for TSa, Sc and Sa interfaces.

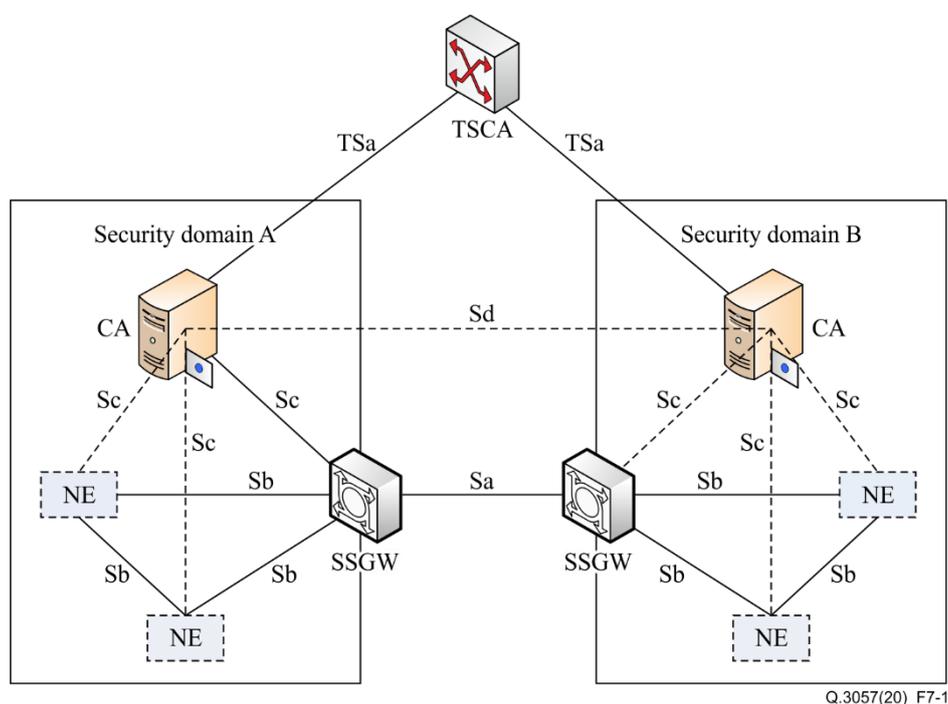


Figure 6-1 – Reference architecture of interconnection between trustable network entities

6.2 Functional entities

6.2.1 Certification authority

The CA issues digital public-key certificates for the end entity (SSGW). These digital public-key certificates contain a public key and the identity of the owner to the SSGWs/NEs within a particular security domain and are signed by the TSCA.

6.2.2 Trusted signalling certification authority

The TSCA is the trust anchor for the reference architecture; it functions in the same way as an Internet-based trust anchor providing services to the CAs in each security domain.

6.2.3 Signalling security gateway

The SSGW is an entity on the border of the security domain used for communication between two security domains. SSGW is responsible for whether protection is applied and enforces security policies towards the external domain.

6.2.4 Network entity

The NE is the origin or destination of the messages. It generates messages, e.g., ISDN, those of the integrated services digital network user part or mobile application part types, and receives, interprets and processes those received.

6.3 Reference points

6.3.1 Sa reference point

The Sa reference point is located between an SSGW and a NE. This reference point provides security interconnection to support protection of the domain.

6.3.2 Sc reference point

The Sc reference point is located between an SSGW or NE and a CA. This reference point is for distribution and validation public-key certificates for the NE and SSGW.

6.3.3 TSa reference point

The Sa reference point is located between a CA that belongs to a Communications Service Providers (CSP) security domain and the TSCA. This reference point issues digital public-key certificates to the CA by the TSCA.

7 Security services

This Recommendation specifies the provision of the following security services:

- signalling data integrity.
- signalling data origin authentication.

8 Security association attribute definition

The (SA) shall contain the following data elements that are classified into two groups.

- Security association identifier (SAI) attributes.

The SSGW of each security domain creates a SA for each SSGW from other security domains it interacts with. The SA identification is based on the peer SSGW ID. The SSGW shall keep only one SA per destination SSGW.

- Assigned cryptographic parameters per SA: digital signature, key, algorithm identifiers (IDs) and SA lifetime.

8.1 Security association identifier (SAI)

Security Association Identifier = Local SSGW ID || Peer SSGW ID

where

- Peer SSGW ID is either:
 - a) the GT of the peer SSGW on the Signalling System No. 7(SS7) network.
 - b) the peer SSGW FQDN (as defined in clause 3.2.10) on the Internet protocol interconnect (IPX) network.
- Local SSGW ID is either:

- a) the GT of the local SSGW on the SS No. 7 network.
- b) the local SSGW FQDN (as defined in clause 3.2.10) on the IPX network.

8.2 Cryptographic parameters per Security Association

A **digital signature algorithm (DSA) ID** identifies the DSA. The mode of operation of an algorithm is implicitly determined by the algorithm ID. Mapping of algorithm IDs is specified in clause 9.3.

A **signalling security gateway public-key certificate (SGC)** contains the public-key certificate (public part) used to sign the signalling messages of a given SA. The host parameter of the public-key certificate is the SAI. The length of a SGC is determined according to the algorithm ID; key generation is determined according to the algorithm ID.

The **SA expiry time** determines the actual expiry time of the SA. The expiry time shall be given in Coordinated Universal Time (UTC) time with the format “YYYYMM-DDThh:mm:ssTZD” as specified in [b-W3C DTF].

9 Structure of protected messages

If a message does not require a digital signature (as indicated by the signalling procedure of the Sa reference point), then the message shall be routed unchanged to the NE by the SSGW (via the Sb reference point).

If a message requires signature, the SSGW adds a security header and security payload to the message. Both the security header and security payload are sent in cleartext.

9.1 Security Header

Security Header = SAI || TVP

where

- SAI: see clause 8.1.
- TVP: time variant parameter.

The TVP, used for replay protection of signed messages, is a 32-bit timestamp. The receiving SSGW accepts an operation only if the timestamp is within a certain time window. The resolution of the clock from which the timestamp is derived is 0.1 s. The size of the time-window at the receiving NE is not standardized.

9.2 Security Payload

Security Payload = DS || EEC

where

- DS (digital signature), bit-string of the DS, as specified in clause 6.2 of ITU-T X.509, is the result of applying the DSA onto the signalling message sent to the SSGW by the NE (via the Sb reference point);
- EEC (end entity public-key certificate) as specified in clause 7.2 of ITU-T X.509.

9.3 Digital Signature Algorithms (DSA)signature algorithms

This Recommendation specifies several DSAs that can be used to sign protected messages, each algorithm is designated as DSA-*x*, where *x* represents the ID of the DSA. Table 9-1 lists is current usable DSAs.

Table 9-1 – Digital signature algorithms in this Recommendation

| DSA Identifier DSA ID | Description | Notes |
|----------------------------------|---------------------------------------------------------------------------------|------------------|
| 0 | No signature | |
| 1 | Elliptic Curve Digital Signature Algorithm (ECDSA) p-384 curve with SHA256 hash | [FIPS PUB 186-4] |
| 2 | Not assigned yet | |
| 3 | Not assigned yet | |
| 4 | Not assigned yet | |
| 5 | Not assigned yet | |
| 6 | Not assigned yet | |
| ... | | |
| 15 | Not assigned yet | |

9.3.1 Description of DSA-0

When DSA-0 is selected, the security payload is omitted from the message.

9.3.2 Description of DSA-1

The use of ECDSA (including key-pair generations) is specified in clause 6 of [FIPS PUB 186-4]. The point of the curve selected for ECDSA is p-384 and the hash function selected is SHA256.

Note:

In preparation of post-quantum cryptography, it is recommended to use (including key-pair generations) of one of the NIST PQC third round candidates for DSA, details of on-going work by NIST and the status of each of the submitted candidates can be found in [b-NIST-PQC], current PQC DSA leaders are: [b-Crystals], [b-Falcon] and [b-Rainbow]

10 Signalling procedures

10.1 TSa

10.1.1 Trusted signalling certification authority signalling procedures

ITU-T Q.3057 specifies the signalling procedure of the TSCA, shown in Figure 10-1.

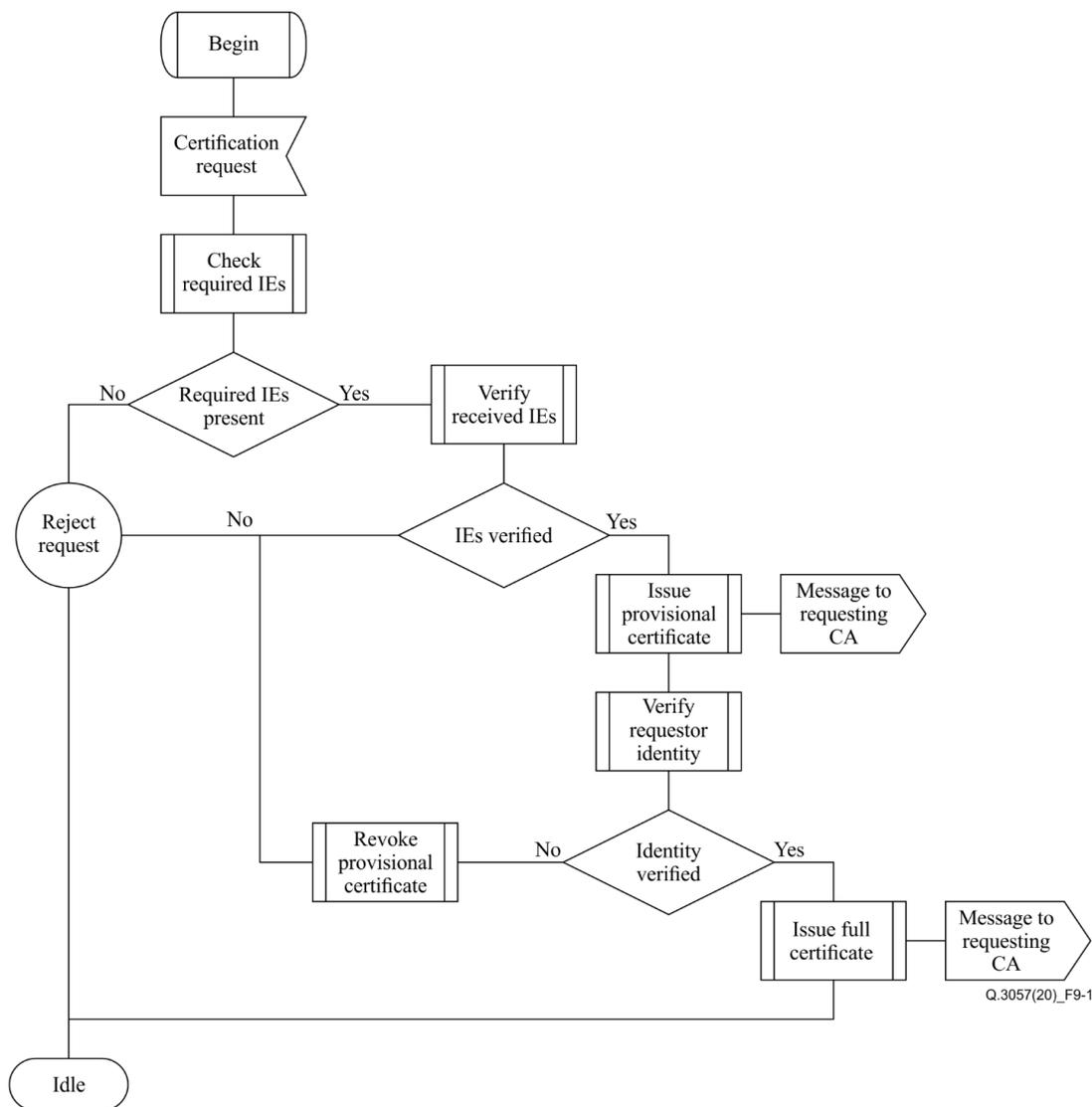


Figure 10-1 – Signalling procedures of a trusted signalling certification authority

10.1.2 TSa signalling procedures

Introduction

Figure 10-2 describes the signalling flow between a CA of a CSP and the TSCA, interacting over the TSa reference point. The TSCA component that handles the public-key certificate generation is required to be in a high security zone, such as a secure alcove or trusted execution environment, as recommended by [FIPS PUB 140-2].

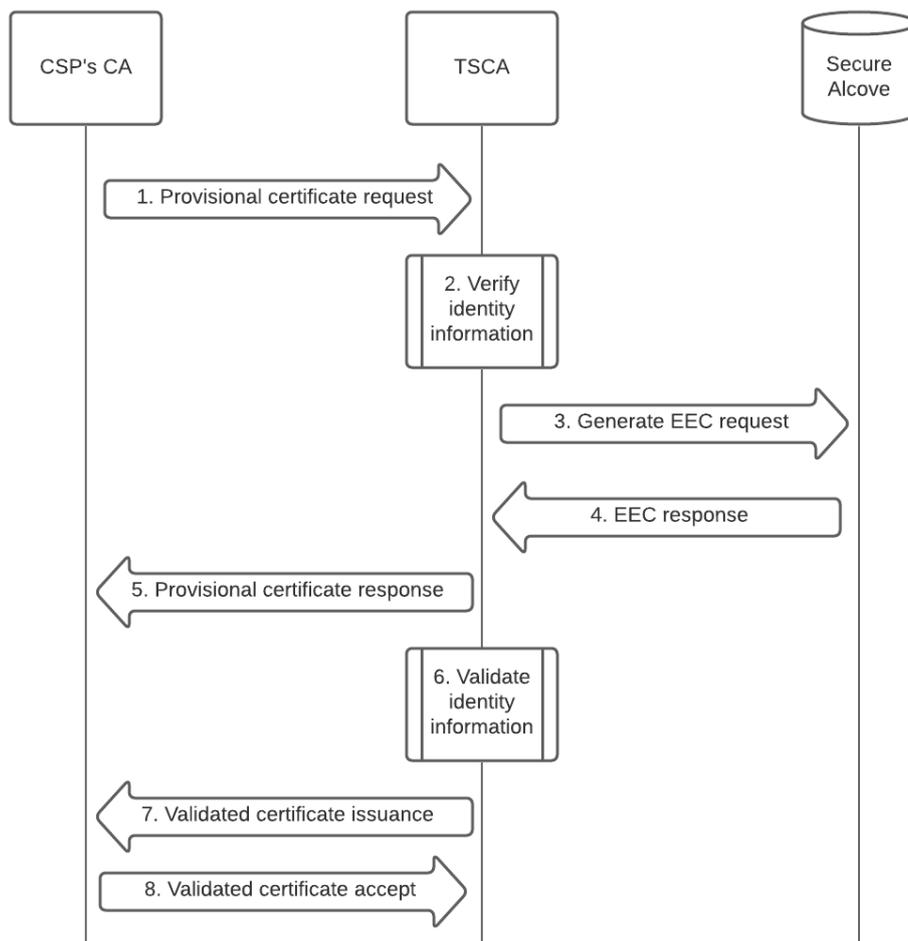


Figure 10-2 – Tsa signalling procedure

Description

The CA of each CSP holds the EEC for the security domain of an operator, an EEC can become invalid for these reasons:

- a) the validity date of the EEC has expired.
- b) the TSCA has revoked the EEC validity.
- c) the private key of the EEC is compromised or lost.

When the EEC of a CSA becomes invalid, the CA requests a new EEC from the TSCA using the following procedure.

1. The requesting CA of a CSP sends a secure provisional end entity Public-key certificate (PEEC) request to the TSCA via the relevant medium connecting the CA to the TSCA (either the IPX or the Internet). In the provisional PEEC request the CSP will include its identity information, which the TSCA will verify in order to provision the PEEC (a list of such IDs can be found in Annex A).
2. Once the TSCA receives the provisional PEEC request from the CA of a CSP, it validates the attached identity information (see Appendix I).
3. Once the identity information has been validated, the TSCA sends its secure alcove a request to generate an EEC based on the realm FQDN of the CSP. If the identity information sent by the CSP fails to verify, then steps 3 and 4 are omitted.

4. The secure alcove returns a ITU-T X.509 EEC signed by the TSCA private-key, the end-entity is denoted the realm FQDN of the CSP.
5. The TSCA sends the CA the signed EEC in the provisional public-key certificate response.
6. The TSCA validates the identity information with the validation process specified in Appendix I.
7. Once validated, the TSCA issues a VEEC to the CA.
8. The CA acknowledges the receipt of the VEEC and begins using it to sign SAs.

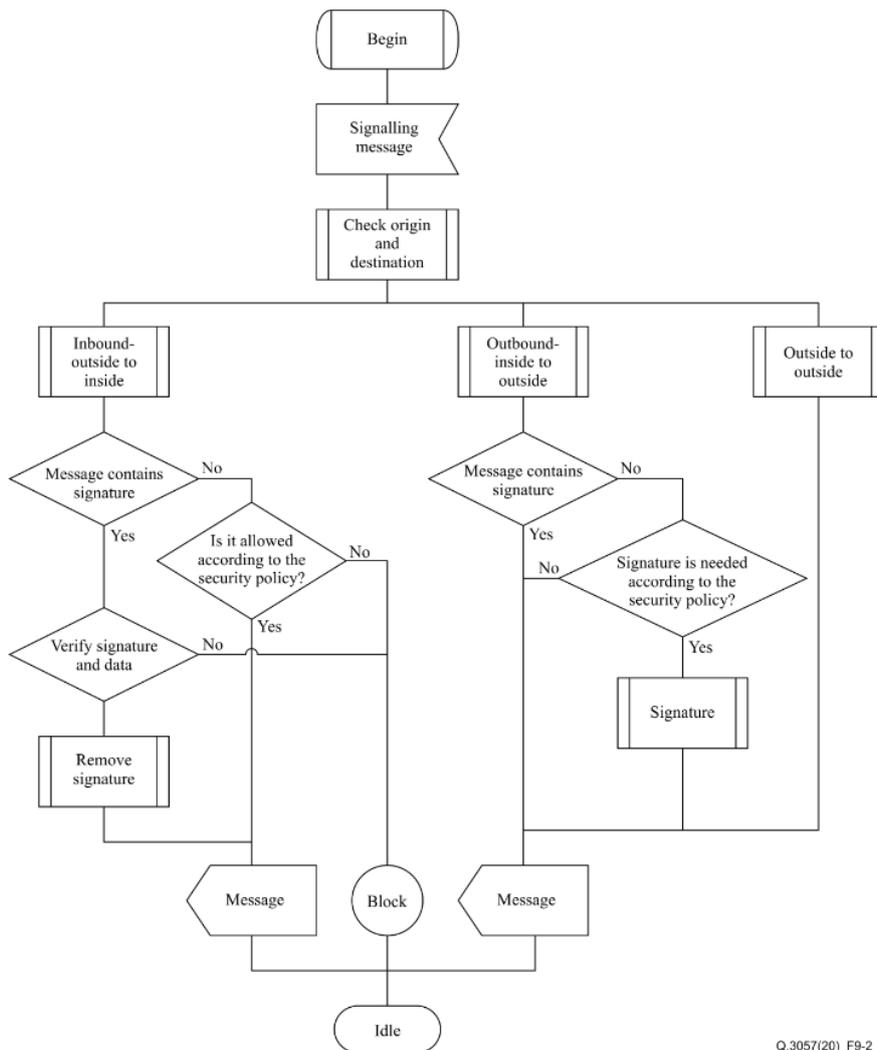
10.1.3 TSa messages

- The provisional EEC request is sent over a hypertext transfer protocol secure-based Representational State Transfer (REST) representational state transfer API and contains all information specified in Annex A as electronic documents attached to the request.
- The provisional EEC response and VEEC issuance response are sent to the requesting CSP via email with the EEC securely attached as specified in [NIST SP 800-57-3]

10.2 Sa

10.2.1 Signalling security gateway signalling procedures

ITU-T Q.3057 specifies the signalling procedure of the SSGW reference point, as shown in Figure 10-3.



Q.3057(20)_F9-2

Figure 10-3 – Signalling procedures of SSGW

10.2.2 Sa signalling procedures

10.2.2.1 Sa signalling happy flow

Introduction

Figure 10-4 describes the happy signalling flow between two SSGWs in two different security domains interacting over the Sa reference point. Happy flow is a successful signalling message traversal between SSGWs due to successful validation of the digital signature.

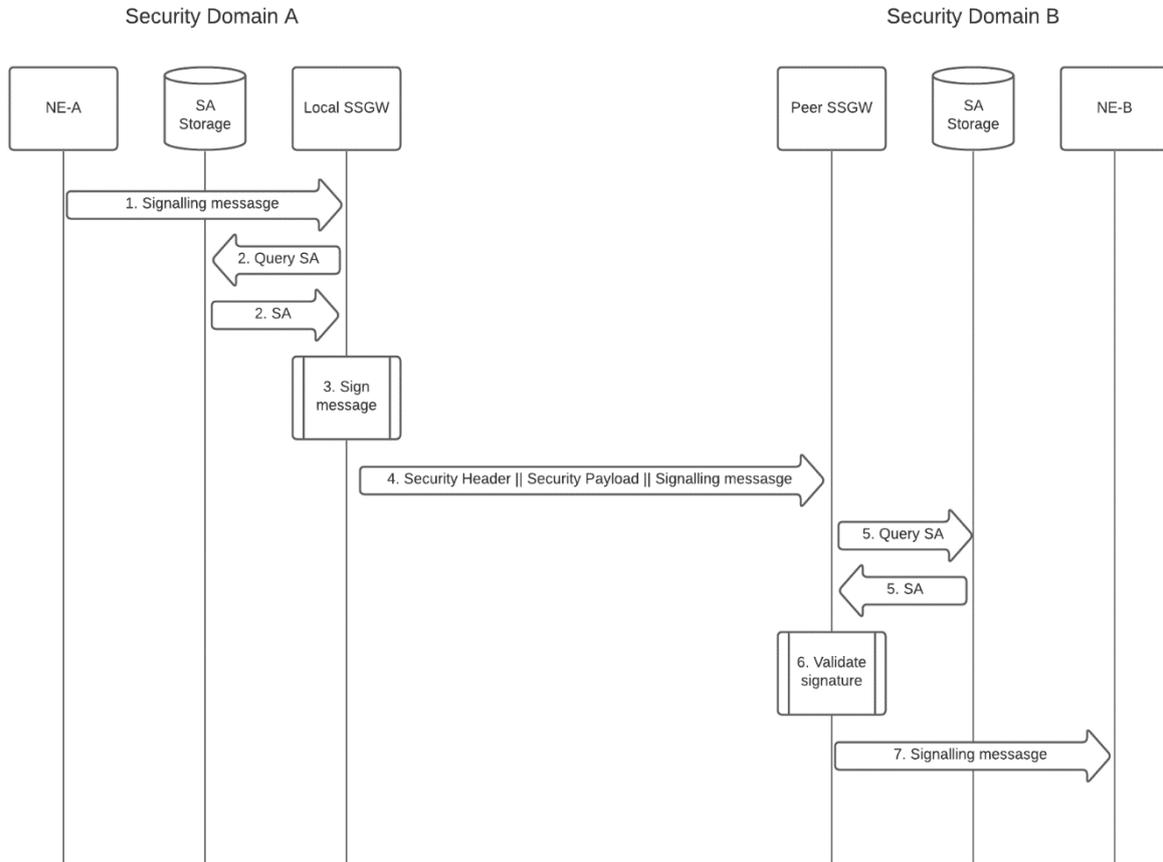


Figure 10-4 – Sa signalling procedure – Happy flow

Description

1. An originating NE in security domain A (denoted NE-A) initiates a signalling message to a terminating NE in security domain B (denoted as NE-B). NE-A sends the signalling message to the security domain A SSGW (denoted local SSGW-A).
2. Local SSGW-A (the originating SSGW) queries its internal SA storage with the SAI (derived from the destination address of the signalling message of NE-A) to retrieve the SA of the destination SSGW (denoted peer SSGW-B).
 - If there is no SA for the SSGW-B, then local SSGW-A contacts the CA to generate a new SA according to the security policy (specified in the signalling procedures of the Sc reference point)
3. SSGW-A applies the DSA to the received signalling message according to the DSA ID of the SA and attaches the security header and payload (if applicable) to the signalling message received from NE-A.
4. The SSGW sends the combined signalling message to Local The local SSGW sends the combined signalling message to the peer SSGW via the relevant medium (i.e. SS No. 7 or IPX).

5. The Peer SSGW (terminating SSGW) receives a signed message from local SSGW with a security header that includes the SAI. Peer SSGW-B retrieves the SA according to the SAI from its internal storage.
 - If there is no SA for the local SSGW, then peer SSGW contacts the CA to generate a new SA according to the security policy (specified in the signalling procedures of the Sc reference point)
6. Peer SSGW validates the digital signature found in the security payload of the received message (if DSA-0 is specified as the DSA ID in the SA, then no payload is present).
7. If the signature is valid, peer SSGW then removes the security header and payload (if present) from the signalling message and forwards it to the terminating NE.

10.2.2.2 Sa signalling unhappy flow

Introduction

The following Figure 10-5 shows unhappy signalling flow between two SSGWs in two different security domains interacting over the Sa reference point. Unhappy flow is a failed signalling message traversal between the SSGWs due to failure in digital signature validation.

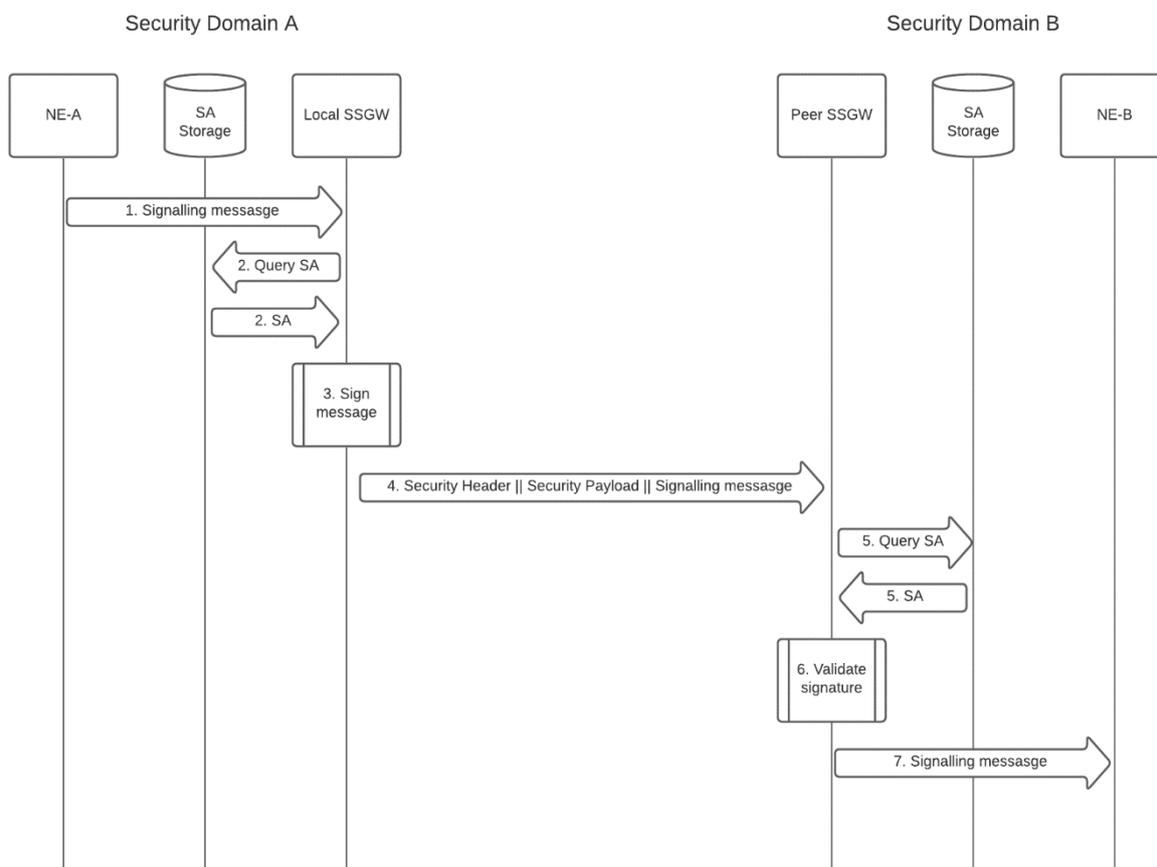


Figure 10-5 – Sa signalling procedure – Unhappy flow

Description

1. An originating NE in security domain A (denoted NE-A) initiates a signalling message to a terminating NE in security domain B (denoted NE-B). NE-A sends the signalling message to the SSGW of security domain A (denoted local SSGW).
2. Local SSGW (the originating SSGW) queries its internal SA storage with the SAI (derived from the destination address of the signalling message of NE-A) to retrieve the SA of the destination SSGW (denoted peer SSGW).

- If there is no SA for the peer SSGW, then local SSGW contacts the CA to generate a new SA according to the security policy (specified in the signalling procedures of the Sc reference point)
3. The local SSGW applies the DSA to the received signalling message according to the DSA ID of the SA and attaches the security header and payload (if applicable) to the signalling message received from NE-A and sends the signalling message to the peer SSGW via the relevant medium (i.e., SS No. 7 or IPX).
 4. The peer SSGW (terminating SSGW) receives a signed message from local SSGW with a security header that includes the SAI. Peer SSGW retrieves the SA according to the SAI from its internal storage.
 - If there is no SA for the local SSGW, then peer SSGW contacts the CA to generate a new SA according to the security policy (specified in the signalling procedures of the Sc reference point).
 5. Peer SSGW fails to validate the digital signature found in the security payload of the received message, i.e., the signature validation process fails, because it does not match the SAI.
 6. Peer SSGW (terminating) sends a signature validation failure message to the local SSGW (originating), announcing that peer SSGW has blocked the signalling message via the relevant medium (i.e., SS No. 7 or IPX).
 7. Local SSGW (originating) sends NE-A (originating) an origination failure message via Sb reference point.

10.2.3 Sa messages ASN.1 format

See Annex B for the ASN.1 schema

10.3 Sc

ITU-T Q.3057 specifies high-level functions of the CA:

- public key infrastructure key-pair provisioning.
- build CA certification path.

10.3.1 Sc signalling procedures

Introduction

Figure 10-6 describes the signalling flow between the SSGW and the CA in the same security domain, interacting over the Sc reference point. The SSGW requests a new SA from the CA if it does not have a valid SA for the inbound or outbound SAI in its internal storage.

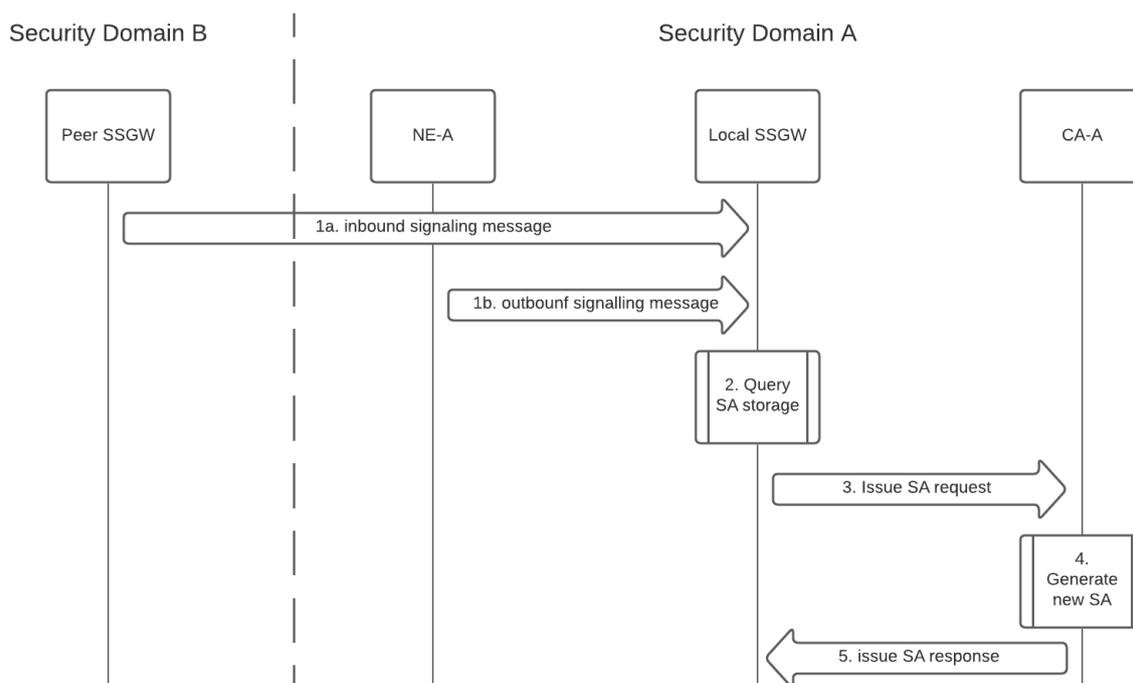


Figure 10-6 – Sc signalling procedure

Description

1. (a) A peer SSGW from another security domain sends an inbound signalling message that contains a security payload.
(b) An internal NE sends the SSGW an outbound signalling message addressed to another security domain.
2. The query of the local SSGW to its internal SA storage for the relevant SA (as described in clause 10.2.2) comes up empty, i.e., there is no valid SA for the relevant SAI, thus a new one needs to be created.
3. The local SSGW sends an issue SA request to the CA.
4. The CA uses its EEC (provisional or validated) to generate a new SA that contains an SAI specific public-key certificate, which corresponds to the security realm FQDN or SS No. 7 GT address of domain B.
5. The CA sends the generated SA back to the local SSGW to sign and verify signalling messages to or from security domain B.

10.3.2 Sc messages ASN.1 format

See Annex B for the ASN.1 schema

Annex A: List of verifiable CSP identifiers to be sent in the PEEC request

(This annex forms an integral part of this Recommendation.)

This Recommendation seeks to use already established and field proven models for its processes. Thus, reference is drawn from the extended verification certification process for SSL public-key certificates issuance ratified by the CA/Browser Forum [b-EV-Cert]. For the TSCA to issue a provisional PEEC to the requesting CSP, the following information must be sent by the SCP to the TSCA.

1. Include all information about the applicant in the EEC.
2. The applicant information shall include, but is not limited to, the following details:
 - a) Organization name. Include the formal legal organization name of the applicant in the EEC, as recorded with the incorporating or registration agency in the applicant's jurisdiction of incorporation or registration (for private organizations), or as specified in the law of the political subdivision in which the government entity operates (for government entities), or as registered with the government business registration agency (for business entities).
 - b) Assumed name (optional). Include the assumed name (e.g., "doing business as" appellation) of the applicant in the EEC, as recorded in the jurisdiction of Applicant's Place of the place of business of the applicant, if requested by the applicant.
 - c) Security domain name (FQDN). Include the domain name(s) of the applicant in the EEC.
 - d) Jurisdiction of incorporation or registration. Include the jurisdiction of incorporation or registration of the applicant in the EEC, consisting of:
 - a. city or town (if any).
 - b. state or province (if any).
 - c. country.
 - e) Incorporating or registration agency. Include the name of Applicant's the incorporating or registration agency of the applicant in the EEC.
 - f) Registration number. Include the registration number assigned to applicant by the incorporating or registration agency in the jurisdiction of incorporation or registration of the applicant in the EEC. If the incorporating or registration agency does not issue registration numbers, then the date of incorporation or registration shall be recorded.
 - g) Applicant address. Include the address of the place of business of the Applicant in the EEC, including:
 - i) building number and street.
 - ii) city or town.
 - iii) state or province (if any)
 - iv) country.
 - v) postal code (zip code).
 - vi) main telephone number.
 - h) Public-key certificate requester. Include the name and contact information of the public-key certificate requester submitting the EEC request on behalf of the applicant.
3. The applicant agreement includes the following elements.
 - a) **General.** Prior to the issuance of the EEC, the TSCA obtains the agreement of the applicant to a legally enforceable applicant agreement with the TSCA for the express benefit of relying parties and application software vendors. The applicant agreement must be signed by an authorized contract signer acting on behalf of the applicant in accordance

with local or peer SSGW law and must apply to the EEC to be issued pursuant to the EEC request. A separate Applicant agreement may be used for each EEC request, or a single applicant agreement may be used to cover multiple future EEC requests and resulting EEC(s), so long as each EEC that the TSCA issues to the applicant is clearly covered by an applicant agreement signed by an authorized contract signer acting on behalf of the applicant.

- b) **Agreement requirements.** The applicant agreement must, at a minimum, specifically name both the applicant and the individual contract signer signing the agreement on behalf of the applicant and contain provisions imposing on the applicant the following obligations and warranties.
- i) **Accuracy of information:** An obligation and warranty to provide accurate and complete information at all times to the TSCA, both in the EEC request and as otherwise requested by the TSCA in connection with the issuance of the EEC(s) to be supplied by the TSCA.
 - ii) **Protection of private key.** An obligation and warranty by the applicant or a subcontractor (e.g. hosting provider) to take all reasonable measures to maintain sole control of, keep confidential and properly protect at all times the private key that corresponds to the public key to be included in the requested EEC(s) (and any associated access information or device, e.g. password or token).
 - iii) **Acceptance of EEC.** An obligation and warranty that it will not install and use the EEC(s) until it has reviewed and verified the accuracy of the data in each EEC.
 - iv) **Use of EEC.** An obligation and warranty to install the EEC only on a SSGW accessible at the security domain name listed on the EEC and to use the EEC solely in compliance with all applicable laws, solely for signalling and solely in accordance with the Applicant Agreement
 - v) **Reporting and revocation.** Upon compromise, an obligation and warranty to promptly cease using an EEC and its associated private key, and promptly request the TSCA to revoke the EEC, if:
 - any information in the EEC is or becomes incorrect or inaccurate, or there is any actual or suspected misuse or compromise of the private key of the applicant associated with the public key listed in the EEC
 - vi) **Termination of use of EEC.** An obligation and warranty to promptly cease all use of the private key corresponding to the public key listed in an EEC upon expiration or revocation of that EEC.
 - vii) Appendix B - Information validation techniques

Annex B: ASN.1 format for signaling messages

(This annex forms an integral part of this Recommendation)

```
Pro_Trust_Schema DEFINITIONS AUTOMATIC TAGS ::= BEGIN
Sa_Signalling_Message ::= SEQUENCE {
  security_header SEQUENCE {
    sai SEQUENCE {
      local_ssgw_id UTF8String,
      peer_ssgw_id UTF8String,
      tvp UTF8String
    },
    security_payload SEQUENCE {
      digital_signature SIGNATURE,
      eec UTF8String
    }
  }
}
Sc_IssueCAreqs ::= SEQUENCE {
  sai SEQUENCE {
    local_ssgw_id UTF8String,
    peer_ssgw_id UTF8String,
    tvp UTF8String
  }
}
Sc_IssueCAresponds ::= SEQUENCE {
  security_association_identifier SEQUENCE {
    dsa INTEGER (0..15),
    sgc Certificate,
    expiry_time UTCTime
  }
}
/* The digital signature of a data item may expressed by the following ASN.1 data type
which is defined in 6.2.1 of [ITU-T X.509], where the signature component is a bit string
resulting from using the appropriate digital signature algorithm. */

SIGNATURE ::= SEQUENCE {
  algorithmIdentifier AlgorithmIdentifier{{SupportedAlgorithms}},
  signature BIT STRING,
  ... }
/* If one or two signatures are to be appended to the data, the following ASN.1, which is
defined in 6.2.1 of [ITU-T X.509], may be used to define the data type resulting from
applying one or two signatures to the given data type. */

SIGNED{ToBeSigned} ::= SEQUENCE {
  toBeSigned ToBeSigned,
  COMPONENTS OF SIGNATURE,
  ... }
[[4:
altAlgorithmIdentifier AlgorithmIdentifier{{SupportedAltAlgorithms}} OPTIONAL,
altSignature BIT STRING OPTIONAL]]
] (WITH COMPONENTS {..., altAlgorithmIdentifier PRESENT, altSignature PRESENT } |
WITH COMPONENTS {..., altAlgorithmIdentifier ABSENT, altSignature ABSENT } )

/* The following ASN.1 information object class is used for specifying cryptographic
algorithms which is defined in 6.2.2 of [ITU-T X.509]. */

ALGORITHM ::= CLASS {
  &Type OPTIONAL,
  &id OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
  [PARMS &Type]
  IDENTIFIED BY &id }
/* The following general parameterized data type specifies the syntax of an algorithm
specification which is defined in 6.2.2 of [ITU-T X.509]. */

AlgorithmIdentifier{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {
  algorithm ALGORITHM.&id({SupportedAlgorithms}),
  parameters ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  ... }

```

```
/* The algorithm component shall be an object identifier that uniquely identifies the
cryptographic algorithm being defined.
The parameters component, when present, shall specify the parameters associated with the
algorithm. Some, but not all algorithms require associated parameters. */
```

```
/* The definitions of the following information object sets are deferred to referencing
specifications having a requirement for specific information object sets.*/
```

```
SupportedAlgorithms ALGORITHM ::= {...}
SupportedAltAlgorithms ALGORITHM ::= {...}
```

```
UniqueIdentifier ::= SEQUENCE {
algorithm ALGORITHM.&id({SupportedAlgorithms})
... }
```

```
/* The following ASN.1 data type specifies the syntax of public-key certificates which is
defined in 7.2.1 of [ITU-T X.509]. */
Certificate ::= SIGNED{TBSCertificate}
```

```
TBSCertificate ::= SEQUENCE {
version [0] Version DEFAULT v1,
serialNumber CertificateSerialNumber,
signature AlgorithmIdentifier({SupportedAlgorithms}),
issuer Name,
validity Validity,
subject Name,
subjectPublicKeyInfo SubjectPublicKeyInfo,
issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,
...,
[[2: -- if present, version shall be v2 or v3
subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL]],
[[3: -- if present, version shall be v2 or v3
extensions [3] Extensions OPTIONAL]]
-- If present, version shall be v3]]
}
```

```
Version ::= INTEGER {v1(0), v2(1), v3(2)}
```

```
CertificateSerialNumber ::= INTEGER
```

```
Validity ::= SEQUENCE {
notBefore Time,
notAfter Time,
... }
```

```
SubjectPublicKeyInfo ::= SEQUENCE {
algorithm AlgorithmIdentifier({SupportedAlgorithms}),
subjectPublicKey BIT STRING,
... }
```

```
Time ::= CHOICE {
utcTime UTCTime,
generalizedTime GeneralizedTime }
```

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
```

```
Extension ::= SEQUENCE {
extnId EXTENSION.&id({ExtensionSet}),
critical BOOLEAN DEFAULT FALSE,
extnValue OCTET STRING
(CONTAINING EXTENSION.&ExtnType({ExtensionSet}){@extnId})
ENCODED BY der,
... }
```

```
der OBJECT IDENTIFIER ::=
{joint-iso-itu-t asn1(1) ber-derived(2) distinguished-encoding(1)}
```

```
ExtensionSet EXTENSION ::= {...}
```

```
Name ::= UTF8String
END
```

Appendix I: Information validation techniques

(This appendix does not form an integral part of this Recommendation.)

Information validation techniques are listed in Section F, pp. 16-39 of [b-EV-Cert]

Bibliography

- [b-ITU-T Q.1400] Recommendation ITU-T Q.1400 (1993), *Architecture framework for the development of signalling and OA&M protocols using OSI concepts*.
- [b-ITU-T T.411] Recommendation ITU-T T.411 (1993): *Information technology – Open document architecture (ODA) and interchange format: Introduction and general principles*.
- [b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [b-ITU-T X.1163] Recommendation ITU-T X.1163 (2015), *Security requirements and mechanisms of peer-to-peer-based telecommunication networks*.
- [b-NIST-PQC] Computer Security Resource Center (Internet), *Post-quantum cryptography – PQC – Round 3 submissions*. Gaithersburg, MD: National Institute of Standards and Technology. Available [2022-06-04] at: <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions>
- [b-Crystals] Crystals Team (2022), *Crystals: Cryptographic suite for algebraic lattices*. Available [2022-06-04] at: <https://pq-crystals.org/>
- [b-Falcon] Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z. (2017), *Falcon: Fast-Fourier lattice-based compact signatures over NTRU*. Available [2022-06-04] at: <https://falcon-sign.info/>
- [b-Rainbow] Rainbow Team (Internet), *PQCRainbow: Rainbow signature: One of the three post-quantum signature NIST finalists*. Available [2022-06-04] at: <https://www.pqcraibow.org/>
- [b-EV-Cert] CA/Browser Forum (2007), *Guidelines for the issuance and management of extended validation public-key certificates*, version 1.0. 78 pp. Available [viewed 2022-06-03] at: https://cabforum.org/wp-content/uploads/EV_Certificate_Guidelines.pdf
- [b-W3C DTF] W3C (1998), *Date and time formats*. Boston, MA: World Wide Web Consortium. Available [2022-06-04] at: <http://www.w3.org/TR/1998/NOTE-datetime-19980827>
-