International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3057

(04/2020)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for the NGN – Network signalling and control functional architecture

Signalling requirements and architecture for interconnection between trustable network entities

Recommendation ITU-T Q.3057

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
General	Q.3000–Q.3029
Network signalling and control functional architecture	**Q.3030–Q.3099**
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
VoLTE/ViLTE network signalling	Q.3640–Q.3655
NGN applications	Q.3700–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3057

Signalling requirements and architecture for interconnection between trustable network entities

Summary

Recommendation ITU-T Q.3057 specifies the signalling architecture and requirements for interconnection between trustable network entities in support of existing and emerging networks. Based on the architecture, it specifies the interfaces and signalling requirements between the functional entities and signalling procedures to be applied.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3057	2020-04-29	11	11.1002/1000/14242

Keywords

Architecture, procedure, requirement, signalling security, trusted network.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.3057

Signalling requirements and architecture for interconnection between trustable network entities

1 Scope

This Recommendation presents the signalling architecture and requirements for interconnection between trustable network entities in support of existing and emerging networks. Based on the architecture, it specifies the interfaces and signalling requirements between the functional entities. It also describes procedures to be applied for the signalling, security consideration, etc.

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 X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:1993, *Information technology – Open Systems Interconnection –The Directory: Public-key and attribute certificate frameworks.*

[IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3.*

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

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 security domain: A set of objects or entities of whose security policy can be administered by one organization.

3.2.2 signalling security gateway (SSGW): 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.

3.2.3 trusted signalling certification authority (TSCA): The root of trust for verifying digital signatures using the root certification authority (CA) model.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AKA Authentication and Key Agreement

CA Certificate Authority

CLI Calling Line Identification

CSP Communications Service Providers

DEA Diameter Edge Agent

DRA Diameter Routing Agent

DSA Digital Signature Algorithm

ECDSA Elliptic Curve Digital Signature Algorithm

HSS Home Subscriber Server

IAM Initial Address Message

IE Information Element

IMSI International Mobile Subscriber Identity

ISUP ISDN User Part

LS Local Switch

MAP Mobile Application Part

MME Mobility Management Entity

NE Network Entity

NNI Network-Network Interface

PKI Public Key Infrastructures

PLMN Public Land Mobile Network

PMI Privilege Management Infrastructure

PSTN Public Switched Telephone Network

RSA Rivest–Shamir–Adleman

SP Signalling Point

SIP Session Initiation Protocol

SMS Short Message Service

SS7 Signalling System No.7

SSGW Signalling Security Gateway

STP Signalling Transit Point

TM Tandem switch

TLS Transport Layer Security

TSCA Trusted Signalling Certificate Authority

UE User Equipment

UNI User-Network Interface

5 Conventions

None.

6 Overview of interconnection between trustable network entities

Communications service providers (CSPs) have traditionally owned network infrastructure, including access networks, core networks and service networks. User equipment (UE) are connected though a user-network interface (UNI) which is regarded as untrusted party by network. Many security requirements have been considered and satisfied on the UNI, such as an authentication and key agreement (AKA) mechanism which provides authentication and authorization. The internal network entities of the CSPs are connected through a network-network interface (NNI) and the relations between the network entities are regarded as trusted based on the closeness and isolation of the network. Connection between network entities of different CSPs is also trusted based on the commercial contracts or agreements rather than security technologies. Security measures and policies on NNI are usually not implemented due to this trusted relationship. Nowadays, telecommunication networks are more and more open. Customer's entities are accessed to the network through various interfaces and protocols which are used for NNI, e.g., session initiation protocol (SIP), signalling system No. 7 (SS7) and Diameter. Under such circumstances, signalling for controlling and management may be abused, resulting in theft or fraud of sensitive information related to the user, such as calling line identification (CLI), international mobile subscriber identity (IMSI) and location information, etc. Furthermore, short message service (SMS) and calls of users will be under surveillance illegally.

Thus, trust relationships should be built between network entities based on an appropriate mechanism. The behaviour and results between entities should be predictable, traceable, and controllable.

6.1 Introduction of public key infrastructures

Public key cryptography is a cryptographic technique that enables entities to securely communicate on an insecure public network, and reliably verify the identity of an entity via digital signatures. A public key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. PKIs help to establish the identity of devices, network entities and services – enabling controlled access to systems and resources, protection of data, and accountability in transactions.

PKI management of public-keys is usually based on the certificate standard [ITU-T X.509] which provides verification of ownership of a private-key by some external entity (certificate authority). The [ITU-T X.509] certificate is defined as a data structure that binds public-key values to subjects (e.g., domain names). The binding is asserted by trusted certificate authorities (CA) digitally signing each certificate. The CA may base this assertion by profoundly validating the identification of the private certificate holder.

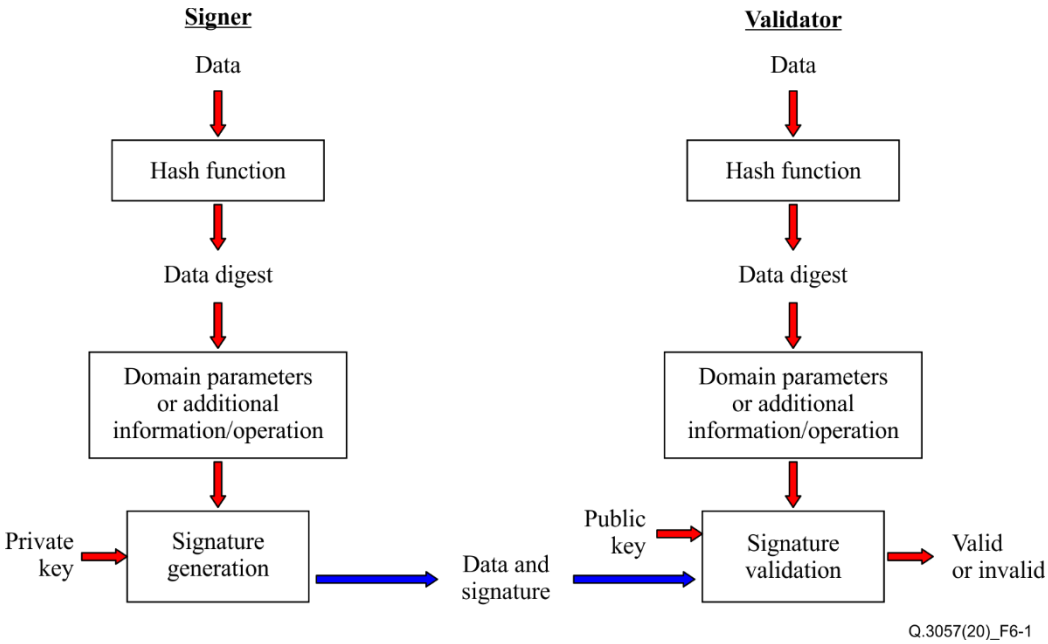


Figure 6-1 – PKI digital signature verification process [ITU-T X.509]

As shown in Figure 6-1, according to [ITU-T X.509], the digital signature signer goes through the following procedure:

1) The signer creates a hash digest over the PKI/PMI data using a secure hashing algorithm.

2) The hash digest is then supplemented by additional information in preparation for generation of the digital signature for improved security and for padding the hash digest to a length required by the asymmetric cryptographic function. For the Rivest–Shamir–Adleman (RSA) algorithms, that supplementation can be the addition of some information to the hash digest and in some cases, to perform yet another hashing operation. For the digital signature algorithm (DSA) and the elliptic curve digital signature algorithm (ECDSA), additional domain parameters are added.

3) The result from step 2) above together with the private key of the signer and the use of a specific algorithm result in a bit string that together with the used algorithm constitute the digital signature.

4) The signature is appended to data to be signed.

Having received the data, the recipient (validator) goes through a similar procedure:

5) The validator goes through the same procedure as in steps 1) and 2) above, and if the received data is unmodified, the result will be the same as for the signer. If not, the next step will fail.

6) From the result from step 5) together with the public key of the signer, the bit string of the signature and the use of an associated algorithm, the digital signature is evaluated as either valid or invalid.

If the digital signature proves valid, the validator has ensured that the data has not been modified and that the signer is in the position of the private key that corresponds to the public key used by the validator, i.e., the digital signature provides insurance of data integrity and authentication of the signer.

If the digital signature proves invalid, either the data has been modified or the signing private key does not correspond to the public key used by the validator.

6.2 Cross-certification

When two independent CA hierarchies need to be connected or a sub-CA needs to be created, cross-certification is involved. Cross-certification allows entities from the different hierarchically-certified organizations to access entities in the other organization, and to verify the digital signature of entities from another organization. Different models can be applied to the cross-certification.

6.2.1 Peer to peer model

Figure 6-2 shows the peer to peer model. In this cross-certifications mode, authorities directly recognise each other. Peer-to-peer cross-certification must occur between CAs. Each CA needs to create an initial trust matrix from its certificate store and save it locally. When an authority A chooses to trust an authority B, the authority A signs the certificate of the authority B and distributes the new certificate (B's certificate signed by A) locally.

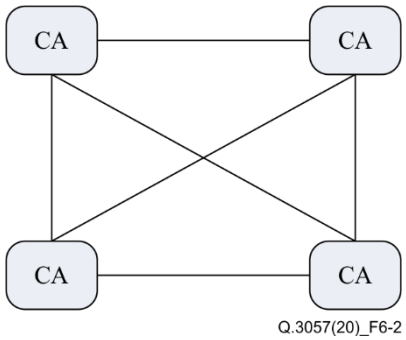


Figure 6-2 – Peer to peer model

6.2.2 Root CA model

Figure 6-3 shows the root CA model. In a strict hierarchy, the CA at the top of the hierarchy is the root CA. The trusted root CA will issue a certificate to subordinate CAs. Depending on the relevant policy, those CAs may certify other CAs. CAs trust each other because the higher CA that certifies it is trusted. Only the root CA must be trusted on its own.

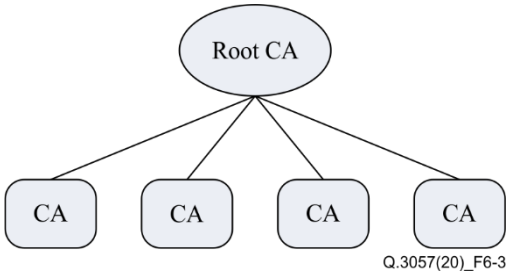


Figure 6-3 – Root CA model

In this model each CA presents the root CA's signature on their own public key with a reference to the root CA.

An additional layer of intermediate CAs can be added (optional) if the volume of traffic to the trusted signalling certificate authority (TSCA) is too high and load balancing is needed. Figure 6-4 describes the signing and referencing model of the intermediate CA model:

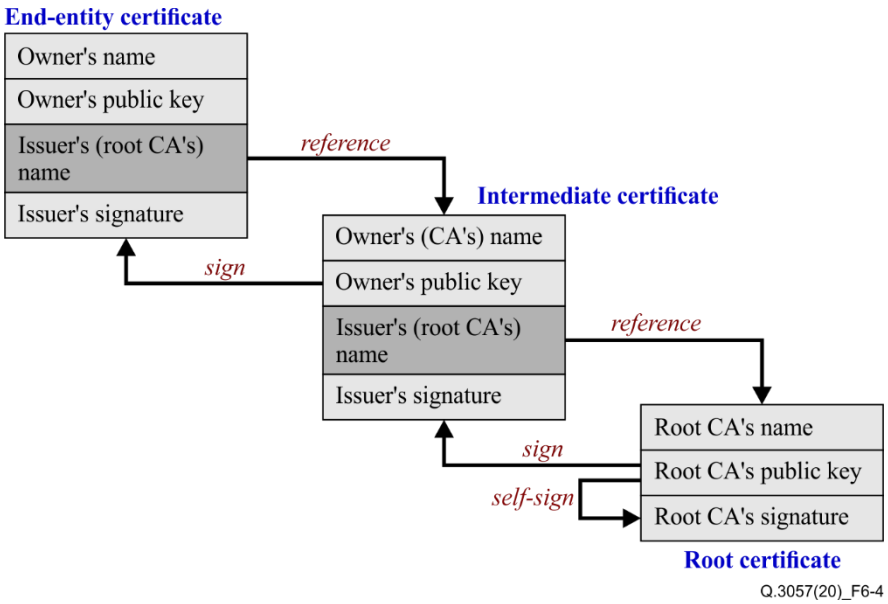


Figure 6-4 – Intermediate CA model

6.2.3 Bridge CA model

Figure 6-5 shows the bridge CA model. The bridge CA model is based around a central (bridging) CA which cross-certifies with each CA. It functions as a communication channel between each of the CAs.

This combines aspects of both the root model and the peer to peer model. The bridge CA acts like a bridge between the authorities. It only requires one pair of cross-certifications for each CA, rather than need to know about each other in a fully meshed system.

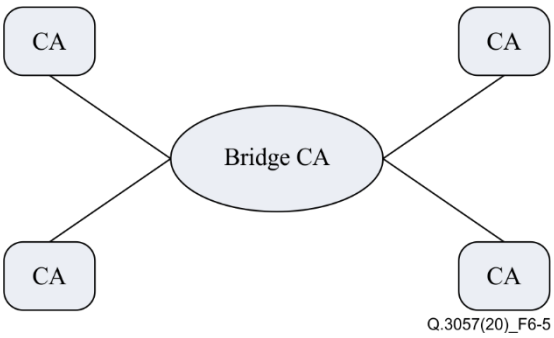


Figure 6-5 – Bridge CA model

7 Architecture for interconnection between trustable network entities

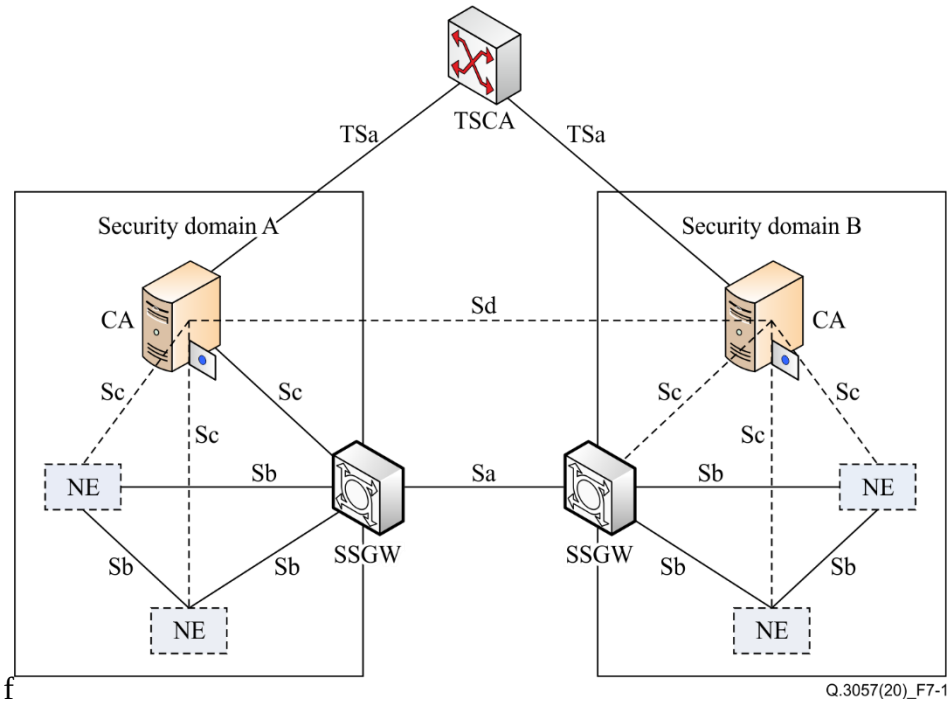
This Recommendation introduced a centralized root of trust for issuing and verifying digital signatures in signalling interconnect. In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of 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 certificate and by the party relying upon the certificate. The format of these certificates is specified by [ITU-T X.509] standard. A certificate authority can issue multiple certificates in the form of a tree structure. A root certificate is the top-most certificate of the tree, the private key of which is used to "sign" other certificates. All certificates signed by the root certificate, with the "CA" field set to true, inherit the trustworthiness of the root certificate.

Establishment of a TSCA as the root CA will assert control and traceability to the process of creating and signing digital certificates.

7.1 Reference architecture

Figure 7-1 shows the reference architecture of interconnection between trustable networks. The CA of a security domain issues certificates to the signalling security gateways (SSGWs) in the domain for communication between domains. When the SSGW of security domain A establishes a secure connection with the SSGW of domain B, they shall be able to authenticate each other by cross-certificate. Network entity (NE) is the origination or destination of signalling message. The message which should be routed or transited to the other security domain will be delivered to the SSGW. The SSGW signs the messages using the certificate issued by the CA and routes the messages to another security domain over the Sa-interface.

NOTE – Security mechanism employed is optional in the interaction between NEs within the security domain.



f

Figure 7-1 – Reference architecture of interconnection between trustable network entities

7.2 Functional entities

7.2.1 Certification authority (CA)

The CA issues digital certificates for the end entity. These digital certificates contain a public key and the identity of the owner to the SSGWs/NEs within a particular security domain. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the entity noted in the certificate. CA binds public keys with respective SSGWs/NEs, accepts requests for digital certificates and authenticates the SSGWs/NEs making the request. The binding is established through the registration and issuance process. Depending on the assurance level of the binding, this may be carried out by software at a CA or under human supervision.

7.2.2 Trusted signalling certificate authority (TSCA)

The TSCA is the root CA for the reference architecture, it functions the same as an Internet based root CA providing services to the CAs in each security domain. The TSCA provides digital

certificates to the CA which the latter can use to authenticate its identity to CAs in other security domains.

The TSCA is a system that facilitates an entity accepting certificates issued by another entity for a transaction. The TSCA serves as a hub allowing the entity to create a trust path from its security domain back to another security domain of the entity that issued the certificate. TSCA provides interoperability by managing tables including policies and procedures created by CAs.

The existence of the TSCA will greatly improve the overall security posture of the system. A centralized TSCA is recommended.

NOTE – Since the use of the TSCA is not mandatory, entities may choose other PKI methods to determine trust.

7.2.3 Signalling security gateway (SSGW)

The SSGW is an entity on the border of the security domain and is used for communication between two security domains. The security policies are specified in the SSGW. SSGW is responsible for whether protection shall be applied and enforcing security policies towards external domain.

SSGW initials request to CA for issuing or validating certificate. All outgoing messages are protected by the SSGW belong to the domain, including signature, encryption, etc. Then, the messages are transited to the destination domain. Security of all incoming messages from another domain should be validated by the SSGW, including authentication, validate, decryption and etc. After messages are validated by a SSGW of the destination domain, the SSGW shall deliver the message to the destination NE. If the message does not comply with the security policy, it will be blocked or discarded by the SSGW.

SSGW shall not impact message routing. Therefore, SSGW are stateless at a protected level, this means no states of signalling procedure are maintained in the SSGW since the request messages and corresponding response message may be transited by different SSGWs.

SSGW may be standalone or integrated with NE.

7.2.4 Network entity (NE)

The NE is the origin or destination of the messages. It generates messages, e.g., ISDN user part (ISUP) message, mobile application part (MAP) message, and receives, interprets, and processes the received message. If NE combined with SSGW, NE would have the responsibility for enforcing security policies towards other security domains.

7.3 Reference points

7.3.1 Sa reference point

The Sa reference point is located between SSGWs, NEs or SSGW and NE. This reference point is for providing security interconnection to support protection of the domain. The Sa reference point covers all signalling between security domains, and it is mandatory for establishing trusted connections between operators. The implementation of Sa reference point between SSGW and NE or NEs is optional and depends on the operator's security policy.

7.3.2 Sb reference point

The Sb reference point is located between SSGW and NE or between NEs within the same security domain.

The Sb reference point is a legacy interface without a security connection, which means that neither the NE nor the SSGW need mutual authentication with each other.

The SSGW shall maintain explicit policy configuration for each NE allowed to communicate with when Sb reference point is implemented.

7.3.3 Sc reference point

The Sc reference point is located between the SSGW/NE and the CA. This reference point is for distribution and validation certificates for the NE and the SSGW. CA issues certificates to NEs for communication between NEs and between NE and SSGW within the responsible domain. The procedures of the Sc reference point are described in [ITU-T X.509].

7.3.4 Sd reference point

The Sd reference point is located between CAs in different security domains and is not mandatory. This reference point is used in case the TSCA is not used to cross validate signatures across different security domains. In this case the TSCA's services are not used and each individual CA will need to publish its public key to other CAs in other security domains and subscribe to other CAs publications of public keys.

7.3.5 TSa reference point

The Sa reference point is located between CAs which belong to a CSP security domain and the TSCA. This reference point is for issuing digital certificates to the CA by the TSCA.

8 Signalling requirements for interconnection between trustable network entities

8.1 General requirements

In order to build a certification path, the CA must interface with other CAs in different security domains and with the optional TSCA for cross-certification PKI and build a certification path to be used in cross-domain digital signature validation.

For signature creation/validation, the SSGW/NE must interface with the CA in order to validate the digital signature of inbound and outbound signalling messages.

For session establishment between NEs (either TCAP, ISUP or Diameter based sessions) the SSGW must communicate with other SSGWs in different security domains and establish an integrity validation process that precedes the session creation between the NEs. This integrity validation process must be transparent to the NEs and require no changes in NEs' software and/or hardware to ensure backwards compatibility while providing security.

The PKI process must comply with [ITU-T X.509].

8.2 Requirements for SSGW

The signalling between SSGWs (security domains) shall provide:

– signalling data integrity,

– data origin authentication.

Each SSGW has keys associated with the entity for signing and validation by the SSGW received. Digital signatures derived from the key and hash of data shall be included in the outgoing message to be sent to the receiver in order to validate the sender. Execution of the signalling process at the receiver's side starts when the sender is validated.

The Sa reference point allows the information exchange shown in Table 8-1.

Table 8-1 – Sa reference point related information exchange

Information element	Description	Category
Original information	The original payload should be verified by receiver	M
Digital signature	The special algorithm result from private key and data (original information) hashing	

The information elements (IEs) are sent together with other IEs received from the NEs, e.g., IE1, IE2 in the message on the Sa reference point.

Figure 8-1 shows the information flow between the SSGWs through the Sa reference point.

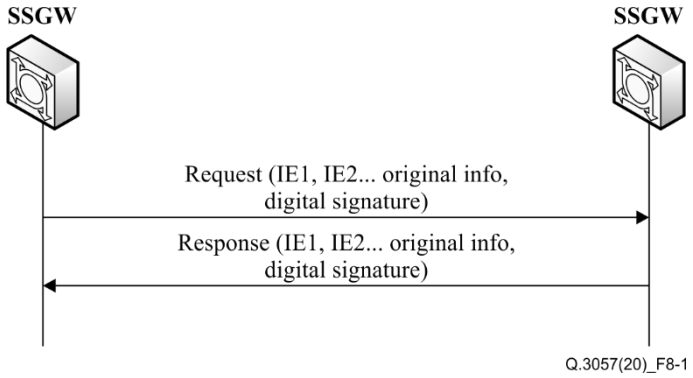


Figure 8-1 – Information flow between SSGWs in different security domains

This procedure is used to push digital signature information from the sender SSGW to other SSGWs in another security domain. This information flow is applied when SSGWs connect to each other. This connection enables the exchange of trustable signalling traffic between NEs.

8.3 Signalling requirements for TSa reference point

The following are the signalling requirements for TSa reference point:

a) In order to build a certification path, the CA must provide the reference and signature of the TSCA for cross-certification PKI.

b) For requesting a digital signature, the CA must provide the TSCA with verifiable information required by the TSCA to issue the digital certificate.

c) The digital certification process must comply with [ITU-T X.509].

9 Procedures for interconnection between trustable network entities

9.1 CA high level functions

9.1.1 CA PKI key-pair provisioning

The CA function shall create and store its own PKI key pair using a secure method. The private key will be securely stored on the CA function or another secure location local or external to the CA function. The public key will be published to other CAs via the TSCA in the certification path building function.

9.1.2 Build CA certification path

9.1.2.1 Local certification path

Every CA shall sign and validate the digital signatures of messages internal to its own security domain, in this case the certification path will be 0, i.e., the CA will validate signatures without requiring cross-validation from the TSCA/other CAs in other security domains.

9.1.2.2 Cross-domain certification path

In the case of outbound signalling messages to other security domains (i.e., other public land mobile networks (PLMNs)) the CA will build a certification path to the other security domain via the TSCA or directly via peer-CAs if there is no TSCA present. The certification path is the chaining of public keys of every peer-CA or TSCA in the path between the two security domains. Once the path is built the CA will store the chained keys and publish them to the CA in the other security domain.

9.1.3 Generation and validation of signatures in the same security domain

In the same security domain, the digital signature will be based on the domain parameters and the CA's private key. The validation of the digital signature will be performed using the security domain parameters and the CA's public key.

9.1.4 Generation of signatures cross security domains

In the cross-security domain scenario, the digital signature will be based on the same domain parameters as in the intra-security domain scenario, however, the public key will be built according to the certification path between two security domains. Validation of digital signatures will be performed using the security domain parameters and the chained public key (chained according to the CAs in the certification path).

9.2 TSCA high level functions

9.2.1 CA certificate issuance

The TSCA function shall create and store digital certificates (public/private key pair), using a secure method as warranted in the signalling requirements section above, for each CA requesting a digital signature. The issuance process has two steps:

1) Provisional certification: This is an automated process which requires machine authentifiable information from the CSP. Information provided for receiving provisional certification are IEs exchanged during the registration of the CSP's telecom license with the responsible authority. Provisional certification will have a short expiration date, and can only be obtained once, to prevent abuse.
2) Full certification: This certificate is issued to the CSP once the information provided in the provisional certificate request was duly authenticated by the responsible authority and the responsible authority is satisfied that the requesting CSP is indeed who it claims to be. Full certification has an extended validity period and must be renewed by repeating the authentication process of the CSP.

9.2.2 Signalling procedures of TSCA

TSCA generates digital certificates for CSP CAs, using the two-step process described above. The required information is transferred from the CA to the TSCA via the TSa reference point. The TSCA signalling procedure is described in Figure 9-1.

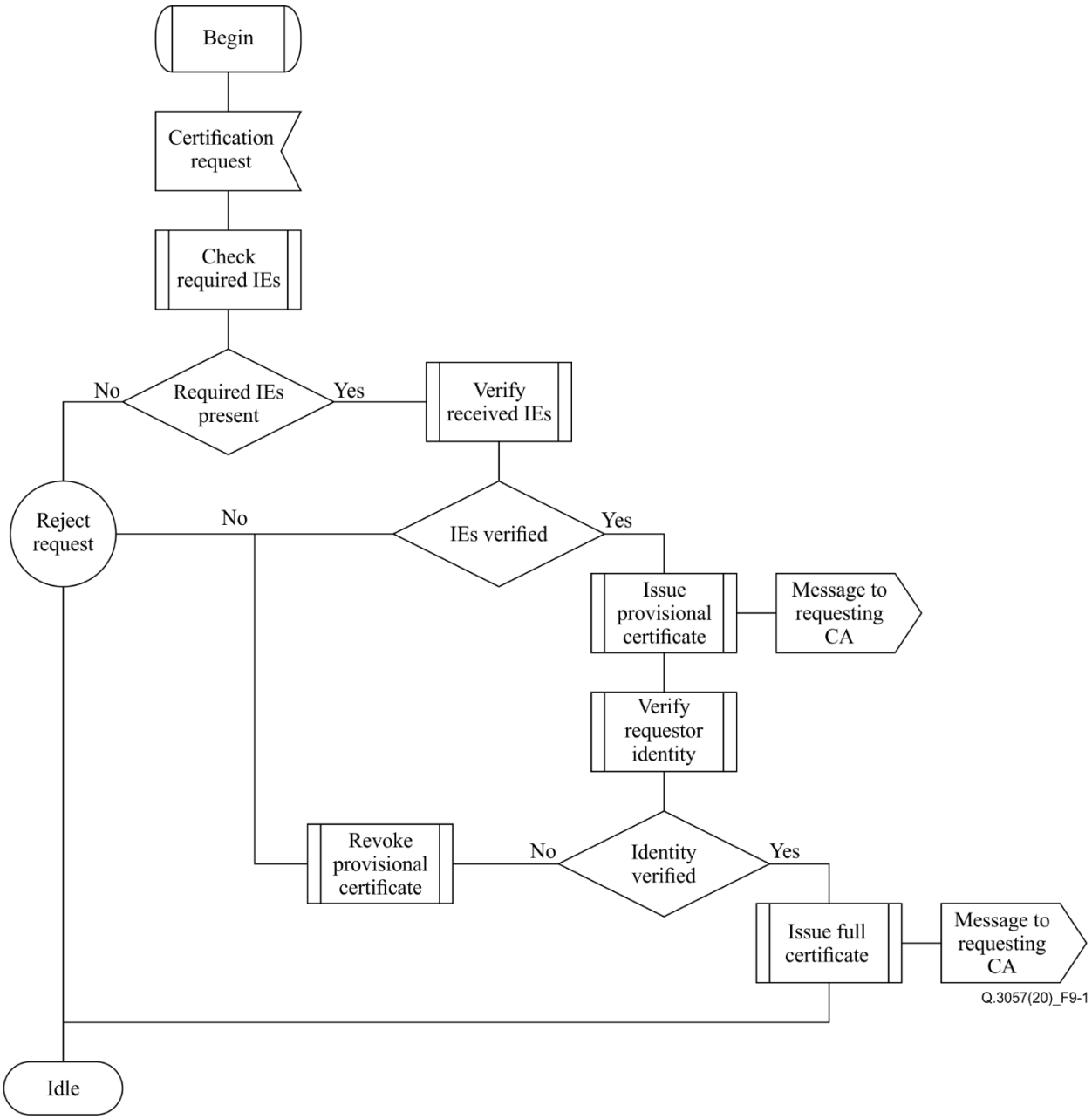


Figure 9-1 – signalling procedures of TSCA

9.3 Security policy of SSGW

Security policy shall be specified and maintained by the SSGW for a particular network. The security policy requirements are as follows:

The policy shall define whether:

– it blocks traffic without signature from another security domain or,

– the signature validation failed.

The policy shall define actions, such as passing, block or de-signature, to be applied for each security domain that the SSGW communicate with. When "bypass-mode" is applied, signalling messages are transferred transparently.

The security policy should be defined for each security domain.

9.4 Signalling procedures of SSGW

The SSGW performs message signing, signature verify, signature remove, passing unmodified and blocking depending on the signature, the message's origin, the message's destination and the message's direction.

If the message is originated by NEs and terminated outside of the security domain, the SSGW shall decode the original received message, add a signature, re-pack and send the signed message to the corresponding SSGW according to the security policy.

If the message is originated by SSGW in another security domain and terminated at NEs in the same security domain, the SSGW shall verify the signature. If the signature is valid, the message shall be transferred to the relevant NEs with the signature removed. Otherwise, the message shall be blocked according to the security policy.

If the message is originated by another SSGW and terminated at another security domain, the SSGW shall not verify the signature and pass the message transparently according to the security policy.

Figure 9-2 shows the signalling procedure of SSGW.

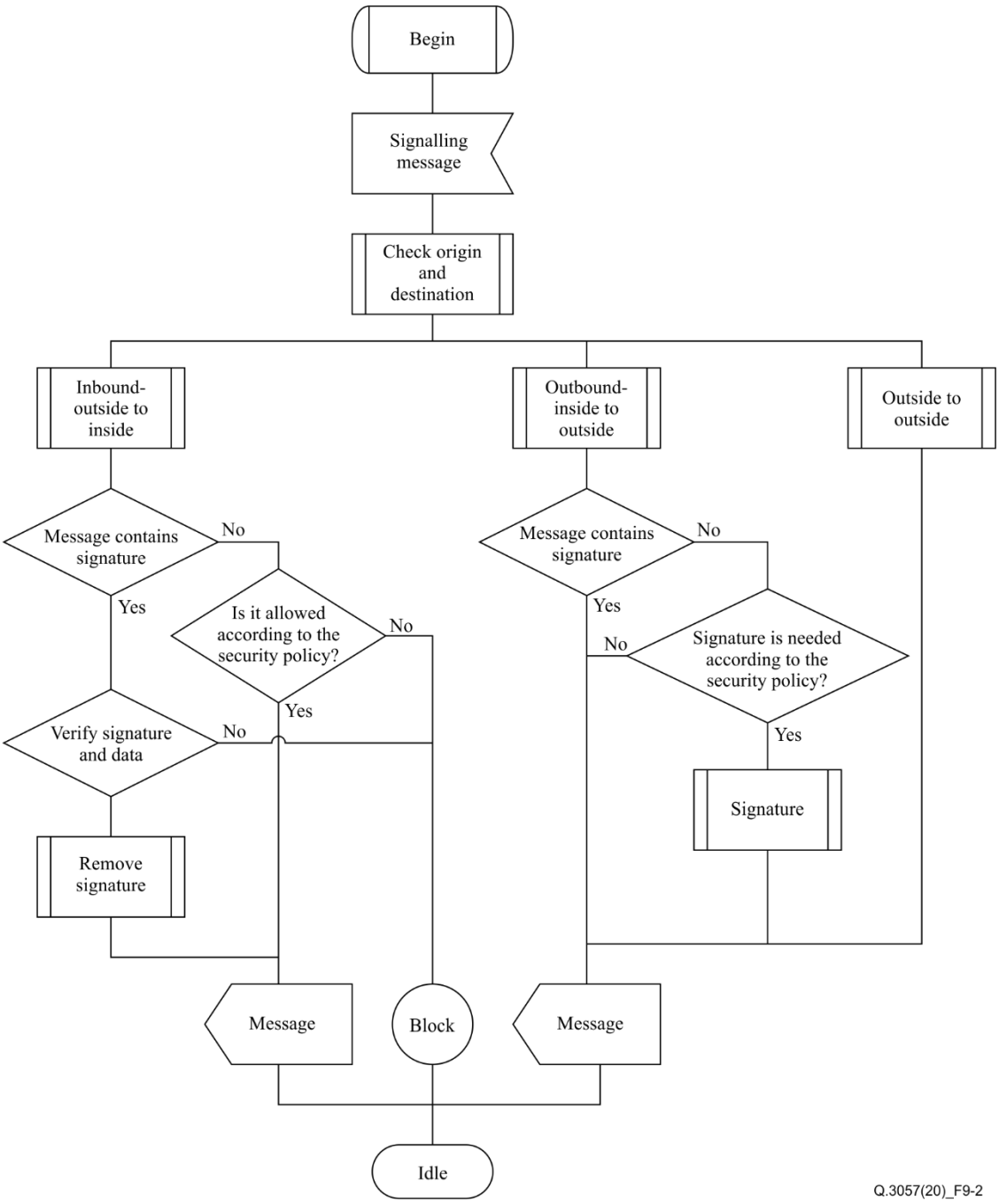


Figure 9-2 – Signalling procedures of SSGW

9.5 Message signature schemes and algorithms used in the SSGW

The algorithms used in the SSGW to sign and verify digital signatures are (in line with TLS v1.3 defined in [IETF RFC 8446]):

1) Elliptic curve digital signature algorithm (ECDSA),

2) SHA384 hash function.

10 Security considerations

In general, telecommunication service providers should treat their networks as vulnerable and other providers as un-trusted.

SSGWs are responsible for signalling security operations and shall be physically secured. Deploying multiple SSGWs will balance the traffic load and avoid single points of failure. The SSGW may also include filtering and screening functionality. If links between SSGWs are based on IP, transport layer security (TLS) is recommended to be used to ensure secure transport of signalling messages. This Recommendation is aligned with the TLS 1.3 standard defined in [IETF RFC 8446].

Appendix I

Scenarios of interconnection between trustable network entities

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

I.1 TCAP transaction between trustable network entities

Figure I.1 shows the architecture of the transaction capabilities application part (TCAP) transactions between trustable network entities. SSGWs are deployed between two public land mobile networks (PLMNs). A CA issues digital certificates for the SSGW that contain a public key and the identity of the owner. If a PLMN deploys SSGW, it has to transfer all inbound or outbound TCAP signalling messages to the corresponding PLMN's SSGW. The SSGW adds a signature for outbound messages and validates the signature of inbound messages. SSGW may be co-located with a signalling point (SP) or a signalling transit point (STP) which is located at the border of the security domain.

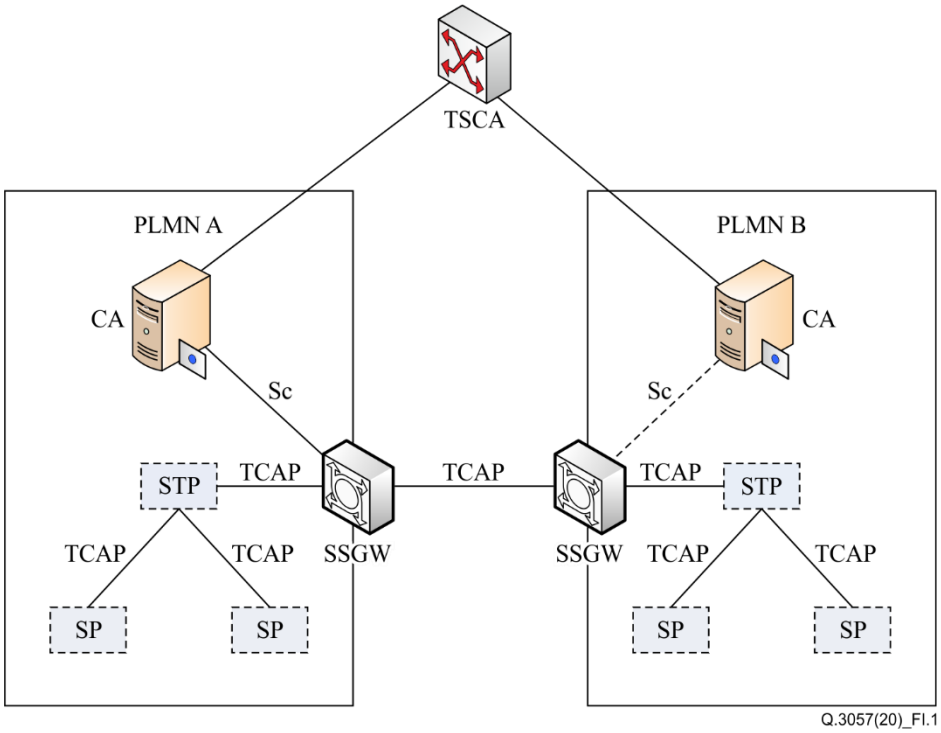


Figure I.1 – Security TCAP transaction architecture

For the outbound signalling traffic, the unprotected message is originated at a SP inside the PLMN A. It might be transferred through several STPs inside the PLMN A before it reaches SSGW A. This SSGW will analyse the routing information in the SCCP to determine the routing of the signalling. SSGW A hash original signalling data carried by TCAP and signs with the certification according to the security policy related to the route. After the messages are signed by a SSGW of the originating PLMN, this SSGW shall direct the message towards the destination SP. The message with the digital signature and hash data then is transited outside the PLMN A.

For the inbound signalling traffic, the message is originated by a SP outside the PLMN A and signed and hashed by SSGW B which belongs to the original PLMN B. It may be transited by several STPs before it reaches to the PLMN B's SSGW. Cross-certificate will be done by SSGW A. If authentication for the message is valid, the message is passed to the PLMN A inside, otherwise the message is discarded. After successful authentication, the digital signature and hash data in the message will be deleted when the message is directed to the STPs or SPs inside the PLMN A. If the

destination is outside PLMN A (PLMN A is a transit network), the message should be passed and unmodified.

I.2 CLI transition between trustable network entities

Figure I.2 shows the architecture of a calling line identification (CLI) transition between trustable network entities. SSGWs are deployed between two public switched telephone networks (PSTNs). A CA issues digital certificates for the SSGW that contain a public key and the identity of the owner. If a PSTN deploys SSGW, it has to transfer all inbound or outbound ISUP messages to the corresponding PSTN's SSGW. SSGW adds a signature for CLI for the outgoing messages and validates the signature of incoming messages. SSGW might be co-located with a tandem switch (TM) or an STP, which is located at the border of the security domain.

Certificated telephone numbers are used by the originating network to guarantee that the caller is authorized to use the ITU-T E.164 number.

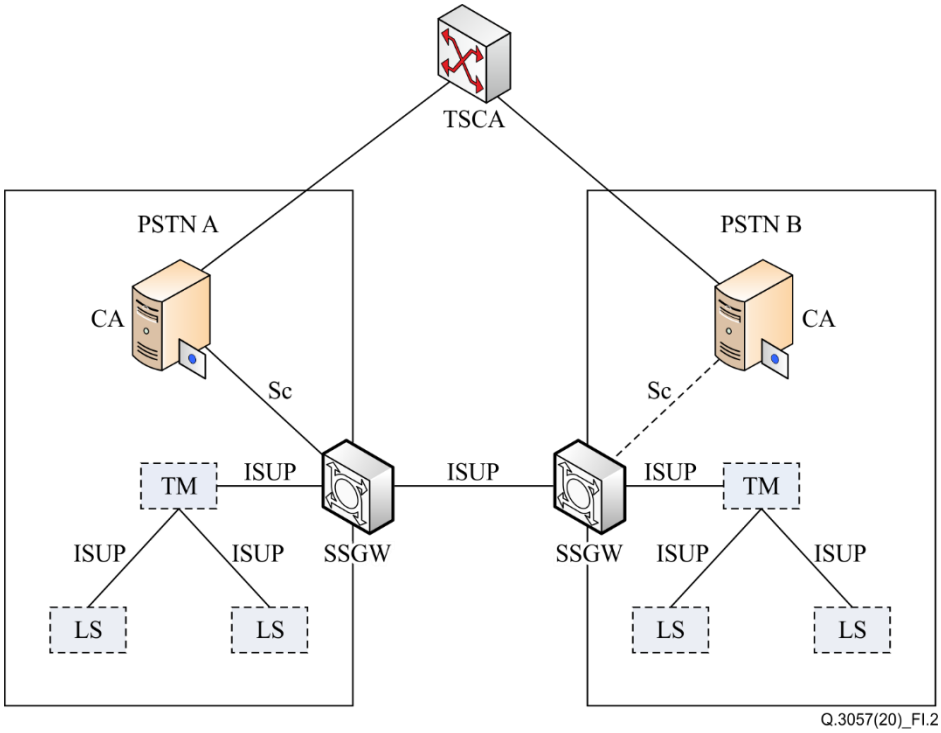


Figure I.2 – CLI transit architecture

For the outbound call traffic, the ISUP message (IAM) with unprotected CLI is originated at a local switch (LS) inside the PSTN A. It might be succeeded by several TMs inside the PSTN A before it reaches the SSGW A. This SSGW will analyze the routing information to determine the routing of the call, hash original CLI and signs with the certification according to the relevant security policy. After CLI is signed by a SSGW of the originating PSTN, this SSGW shall successfully transmit the message towards the destination PSTN. Then a suitable free inter exchange circuit is seized and an Initial Address Message (IAM) with the digital signature and hash data is sent to the SSGW that belongs to PSTN B.

For the inbound call traffic, the CLI within an IAM is originated by a LS outside PSTN A and signed and hashed by SSGW B that belongs to the original PSTN B. IAM may be forwarded by several TMs before it reaches to the PSTN A's SSGW. Cross-certificate will be done by SSGW A. If authentication for the CLI is valid, IAM is forwarded to the PSTN A inside, otherwise the CLI is discarded or the call is released. After successful authentication, the digital signature and hash data in the message will be deleted when IAM is sent to the TMs or LSs inside the PSTN. If the

destination is outside PLMN A (PLMN A is a transit network), the message should be passed and unmodified.

I.3 Diameter transaction between trustable network entities

Figure I.3 shows the architecture of Diameter transactions between trustable network entities. SSGWs are deployed between two PLMNs (4G). A CA issues digital certificates for the SSGW that contain a public key and the identity of the owner. If a PLMN deploys SSGW, it has to transfer all inbound or outbound Diameter messages to a corresponding PLMN's SSGW. SSGW adds a signature for outbound messages and validates the signature of inbound messages. SSGW might be co-located with a diameter routing agent (DRA) or diameter edge agent (DEA), which is located at the border of the security domain.

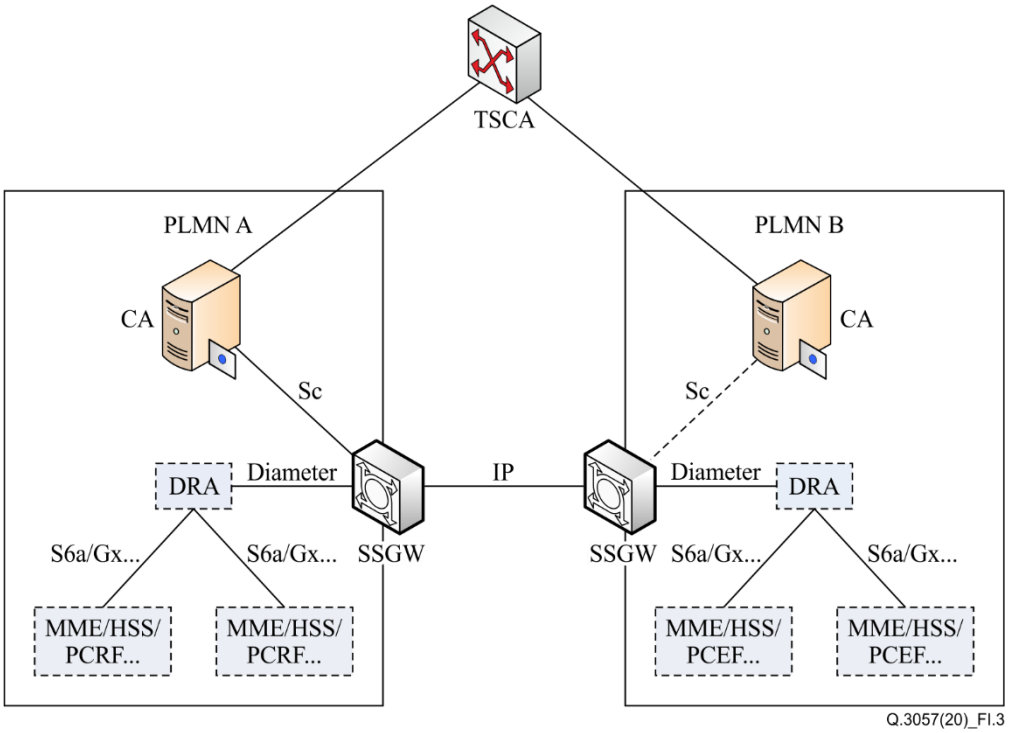


Figure I.3 – Security Diameter transaction architecture

For the outbound signalling traffic, the unprotected message is originated at an entity, e.g., mobility management entity (MME), home subscriber server (HSS), inside the PLMN A. It may be transferred by several DRAs inside the PLMN A before it reaches the SSGW. This SSGW will analyze the routing information to determine the routing of the signalling. SSGW A hash original signalling data and signs with the certification according to the security policy related to the route. After the messages are signed by a SSGW of the originating PLMN, this SSGW shall direct the message towards the destination entity. The message with the digital signature and hash data then is transited outside the PLMN A.

For the inbound signalling traffic, the message is originated by an entity outside the PLMN A and signed and hashed by SSGW B that belongs to the original PLMN B. It may be transferred by several DRAs before it reaches to the PLMN A's SSGW. Cross-certificate will be done by SSGW A. If authentication for the message is valid, the message is passed to the PLMN A inside, otherwise the message is discarded. After successful authentication, the digital signature and hash data in the message will be deleted when the message is directed to the DRAs or entities inside the PLMN A. If the destination is outside PLMN A (PLMN A is transit network), the message should be passed and unmodified.

Bibliography

[b-ITU-T X.1163] Recommendation ITU-T X.1163 (2015), *Security requirements and mechanisms of peer-to-peer-based telecommunication networks.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020