ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Q.3063 (09/2022)

SERIES Q: Switching and signalling, and associated measurements and tests

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

Signalling procedures of calling line identification authentication

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
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100–Q.4139
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.3063

Signalling procedures of calling line identification authentication

Summary

Signalling system No. 7 (SS7) was originally designed for operator management on the assumption that anyone connected to the SS7 network was trustable. In the current network environment however, more and more untrusted devices (including the private automatic branch exchange (PABX), call centre and voice over Internet protocol (VoIP) access system,) are appearing that interconnect to a public land mobile network/public switched telephone network or PLMN/PSTN. As a result, calling line identification spoofing is particularly effective at defeating call blockers, thus leading to a variety of scams that work by avoiding identification.

The goal of Recommendation ITU-T Q.3063 is to identify the signalling requirements of calling line identification authentication including codes and signalling procedures based on the mechanism defined in Recommendation ITU-T Q.3057.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3063	2022-09-29	11	11.1002/1000/15043

Keywords

Authentication, calling line identification, signalling procedures.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.3063

Signalling procedures of calling line identification authentication

1 Scope

This Recommendation presents the architecture and signalling procedures of calling line identification authentication in support of existing networks. Based on the architecture of the calling line identification authentication, it specifies the procedures of calling line identification authentication.

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 E.164] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan.*

[ITU-T Q.731.3] Recommendation ITU-T Q.731.3 (2019), *Stage 3 description for number identification supplementary services using Signalling System No.7 – Calling line identification presentation.*

[ITU-T Q.763] Recommendation ITU-T Q.763 (1999), *Signalling System No. 7 – ISDN User Part formats and codes.*

[ITU-T Q.764] Recommendation ITU-T Q.764 (1999), *Signalling system No. 7 – ISDN User Part signalling procedures.*

[ITU-T Q.1902.3] Recommendation ITU-T Q.1902.3 (2001), *Bearer Independent Call Control protocol (Capability Set 2) and Signalling System No. 7 ISDN User Part: Formats and codes.*

[ITU-T Q.1902.4] Recommendation ITU-T Q.1902.4 (2001), *Bearer independent call control protocol (Capability Set 2): Basic call procedures.*

[ITU-T Q.3057] Recommendation ITU-T Q.3057 (2020), *Signalling requirements and architecture for interconnection between trustable network entities.*

[ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 calling line identification certificate (CLIC): A public certificate issued by certification authorities (CAs) that is used to prove that the originating local exchange owns the calling party number.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASN.1 Abstract Syntax Notation One

BICC Bearer Independent Call Control

CA Certification Authority

CLI Calling Line Identification

CLIC Calling Line Identification Certificate

CLIP Calling Line Identification Presentation

DSS1 Digital subscriber Signalling System No. 1

IAM Initial Address Message

ISDN Integrated Services Digital Network

ISUP ISDN User Part

PABX Private Automatic Branch Exchange

PKI Public Key Infrastructure

PLMN Public Land Mobile Network

PSTN Public Switched Telephone Network

SS7 Signalling System No. 7

SSGW Signalling Security Gateway

TM Tandem exchange

VoIP Voice over Internet Protocol

5 Conventions

None.

6 Architecture of calling line identification authentication

This clause describes the architecture, functional entities and interfaces of calling line identification authentication.

6.1 Reference architecture

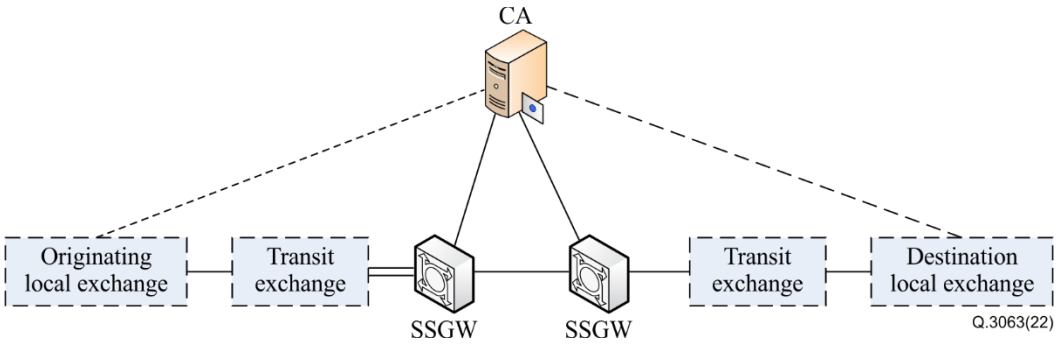

Figure 6-1 – Reference architecture of calling line identification authentication

The scheme for calling line identification authentication is the application of [ITU-T Q.3057] which introduces a public key infrastructure (PKI) scheme for the network. The architecture of the scheme is shown in Figure 6-1. The scheme will have certification authorities (CAs) certify, issue, and revoke calling line identification certificates (CLICs) for the calling parties that have proven ownership of their respective calling party numbers. After successfully obtaining the CLIC, the calling party's originating local exchange or outgoing signalling security gateway (SSGW) can then use the calling line identification certificate to generate an authenticated call request, by extending the existing initial address message (IAM). Upon receiving an IAM call request, the incoming SSGW or destination local exchange then checks for the presence and validity of authenticated call request parameters and presents the validated calling line identification (CLI) using a security indicator during the call setup to the called party.

6.2 Functional entities

The role of each actor with regard to the calling line identification authentication scheme is as follows:

– **Certification authority (CA):** an entity in the network that verifies calling line identification (CLI) ownership and issues calling line identification certificates (CLICs) to a requester that successfully provided proof of calling line identification ownership. The CA is a trusted third party, trusted both by the calling party and by the called party relying upon the certificate. The CA is also responsible for revoking calling line identification certificates if needed.

– **Calling party:** sets up a call request with the originating exchange for the called party. Under the calling line identification authentication scheme, the originating exchange may initiate a request to obtain a calling line identification certificate from the CA.

– **Originating local exchange:** an entity initiates call setup upon a call request from the calling party. As an option functionality, the originating local exchange may obtain and store the calling line identification certificates from the CA for the calling party identification.

– **Transit exchange:** an interconnecting switch in the public switched telephone network (PSTN) that helps to route the calls from the originating exchange to the destination exchange.

– **Signalling security gateway (SSGW):** an entity obtains and stores the calling line identification certificates from the CA for the calling party's identification, generates an authenticated call setting up message on behalf of originating local exchange. The SSGW also receives the authenticated call setting up message and checks the validity and authenticity of the call request from another SSGW.

– **Destination local exchange:** an entity terminates the call and sends the call setup message to the called party. As an option functionality, destination local exchange may receive the authenticated call setting up message and check the validity and authenticity of the call request, and it sets up the call with the called party with a security indicator showing the calling line identification verification status.

7 Procedure of calling line identification authentication

The processes of the authentication scheme can be logically divided into 3 parts: certificate generating, call request initiating, and certificate verification.

In the certificate generating process, defined by [ITU-T Q.3057], the goal is for a CA to verify a SSGW's ownership and that the SSGW can be trusted in the network, afterwards the CA will issue a certificate to the SSGW. Once the CA issues a certificate to the SSGW, the SSGW will then need to generate a public-private key pair and store the private key securely. After proving to the CA that the SSGW is really the owner of the public key, the public key of the SSGW is signed by the CA with attributes indicating identification ownership information, turning it into a calling line identification certificate.

The core process is sequenced as follows:

7.1 Certification generating

The certificate generating process is sequenced as follows:

1. The SSGW setup connection with CA, generates a public-private key pair P_O and Q_O.
2. The SSGW authenticates its identity to the CA using the Sc interface defined by [ITU-T Q.3057]. SSGW sends its identity *A* encrypted with CA's public key P_C to the CA.
3. Once the CA authenticates the identity of the SSGW the CA creates an encrypted nonce EN_S by first generating a random nonce N_S and then encrypting it with the SSGW's public key *Po*. EN_S = Encrypt(P_O){ N_S }.
4. The CA creates a signature *EN-Sig*$_S$ by its private key *Qc*. *EN-Sig*$_S$*= Sign(Qc)(ENS)*.
5. The CA sends EN_S and *EN-Sig*$_S$ back to the SSGW.
6. The SSGW verifies the signature EN_S to ensure the CA's identity.
7. If *EN-Sig*$_S$ is valid, the SSGW decrypts EN_S with private key *Qo* to obtain N_S.
8. The SSGW sends decrypted N_S to CA for proving that the SSGW is really the owner of the public key.
9. The CA verifies N_S and, if valid, sets a validity time V_A and generates a certificate C_S for the SSGW by signing its identification *A*, public key *Po* and V_A using the CA's private key.
10. The CA sends C_s to the SSGW.

A sequence diagram of the certificate generating process is shown in Figure 7-1.

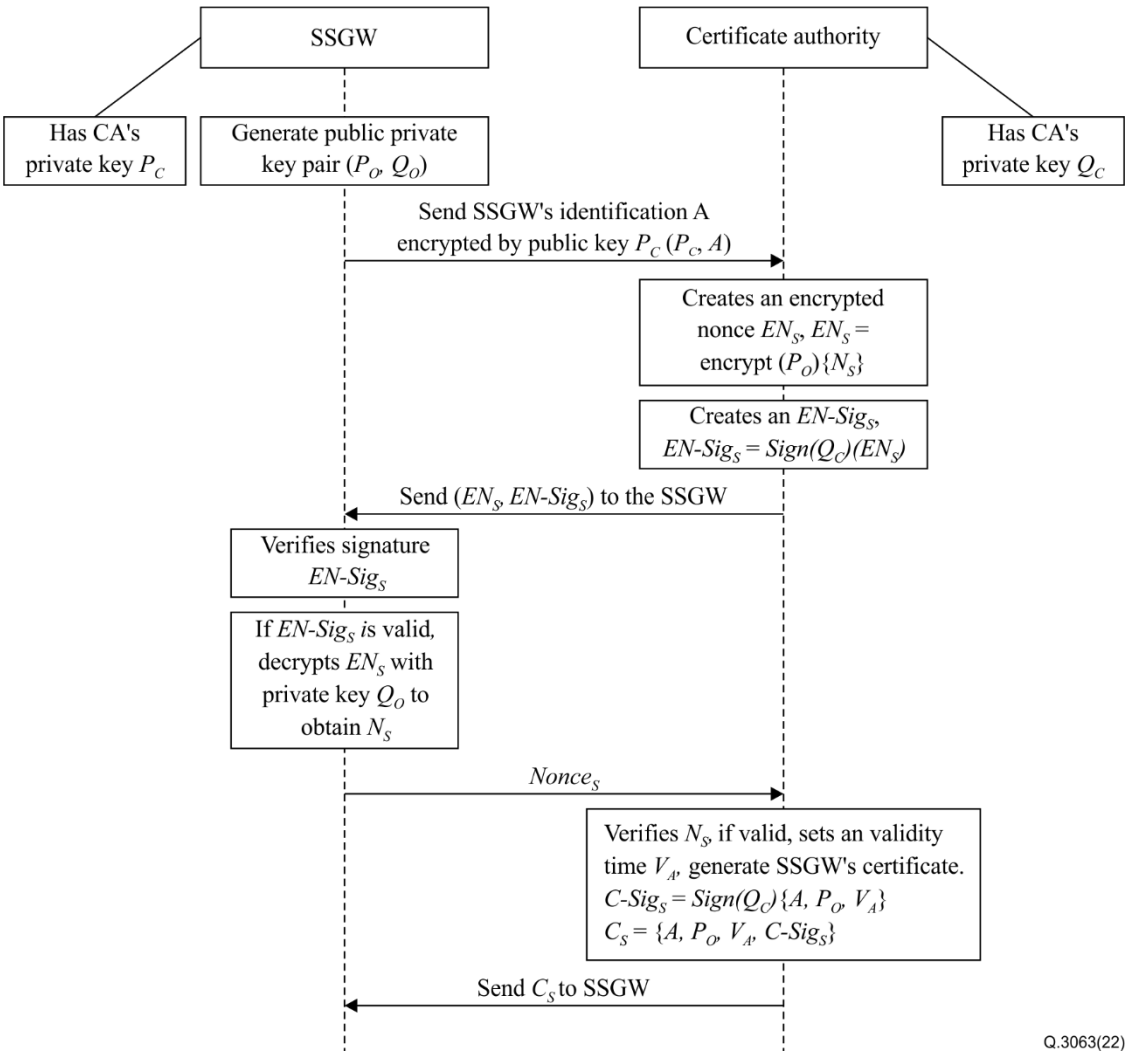

Figure 7-1 – Procedure of certificate generating

In actual deployment, there can be several CAs, allowing different users, such as those in different networks or regions, to verify with an appropriate root CA, as defined by [ITU-T Q.3057].

With regards to the certificate format, it could be based on [ITU-T X.509] format, and the calling line identification in the certificate is based on international E.164 format.

A CA issues a public-key certificate of the SSGW by digital signing identification of information, including its distinguished name, the identification of the SSGW, a validity period, and the value of a public-key algorithm and public key. The following ASN.1 data type specifies the syntax of public-key certificates:

```
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]]

}

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 ::= {...}
```

7.2 Call request initiating

The call request initiating process is sequenced as follows:

Prerequisites: (1) the SSGW has CA's public key P_C, and (2) the SSGW has certificate C_S and its private key Q_O.

a) When the originating exchange receives a call request from the user A, an IAM with the calling party number is generated for the call request as usual. The IAM may be succeeded by several tandem exchanges (TMs) before reaching the outgoing SSGW.

b) The outgoing SSGW analyses the routing information to determine the routing of the call, The SSGW analyses the bearer independent call control/ ISDN user part or BICC/ISUP parameter and gets the CLI information. The SSGW creates the hash H_A of the CLI parameter.

c) The outgoing SSGW generates an IAM signature $IAM\text{-}Sig_A$ by signing H_A. $IAM\text{-}Sig_A = Sign(Qo)\{H_A,\}$.

d) The outgoing SSGW attaches the IAM signature $IAM\text{-}Sig_A$ and certificate C_S in the optional parameters (refer to clauses 7.1 and 7.2) of the IAM and sends the extended IAM to the SSGW act as incoming exchange.

A sequence diagram of the call request initiating process is shown in Figure 7-2:

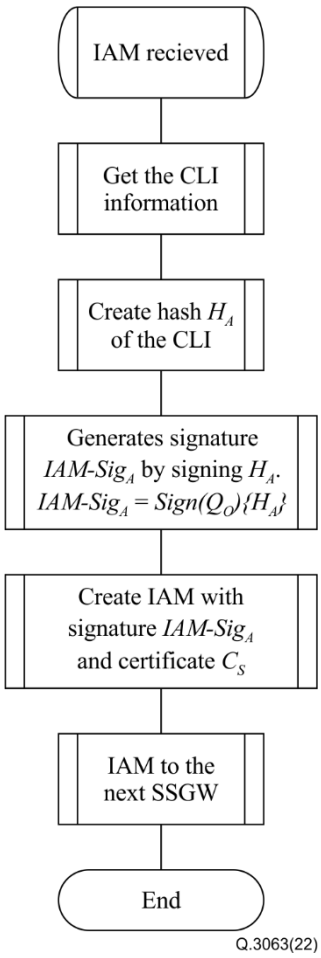

Figure 7-2 – Procedure of call request initiating at the SSGW

7.3 Certification verification

The verification process is sequenced as follows:

a) The incoming SSGW obtains the extended IAM and checks if the certificate C_S is valid, expired or revoked.

b) If the C_S is valid, the IAM signature is verified against the CLI.

c) If the IAM signature is valid and the called party number is correct, the SSGW removes the optional parameters $IAM\text{-}Sig_A$, hashed *CLI* H_A and certificate C_S.

d) The SSGW sends the IAM to the destination exchange.

e) If the IAM signature is not valid or the called party number is not correct, the SSGW sends the IAM to the destination exchange without the calling party number parameter when the call is allowed to pass the call according to the policy.

A sequence diagram of the verification process is shown in Figure 7-3:

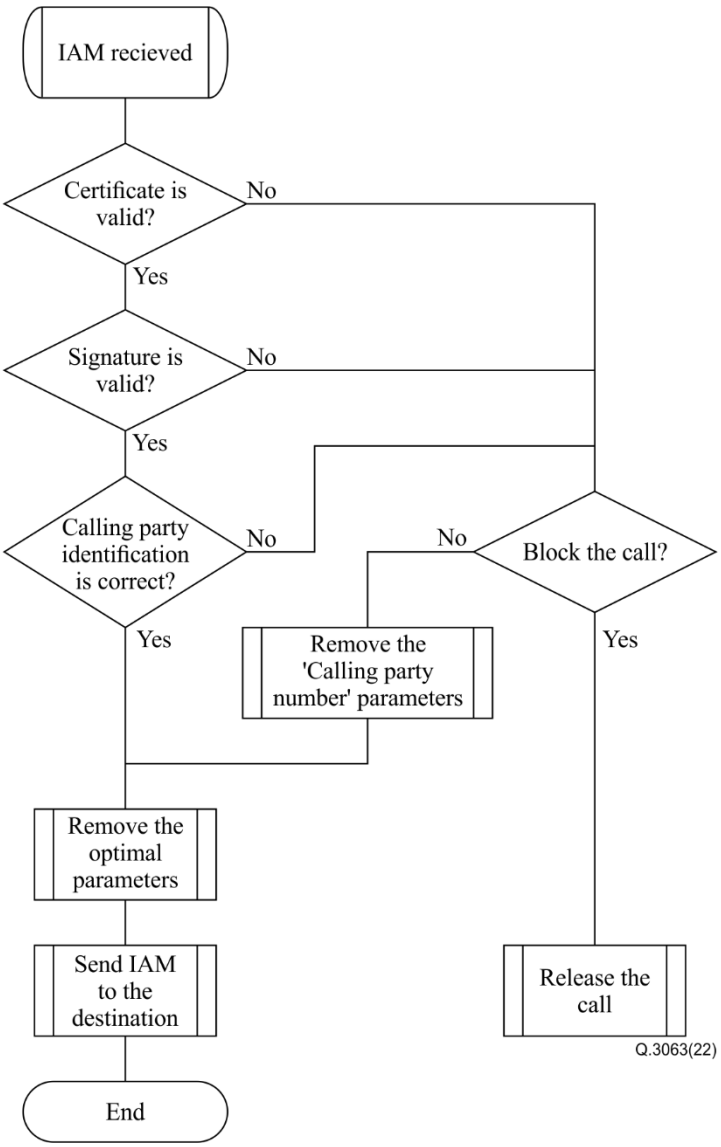

Figure 7-3 – Procedure of verification at the SSGW

8 Procedure of calling line identification presentation

This clause was produced to meet the need for the implementation of the calling line identification authentication. It should be read in conjunction with [ITU-T Q.731.3].

8.1 Actions at the outgoing SSGW/international gateway exchange

The procedure of calling line identification presentation (CLIP) for outgoing SSGW/ international gateway exchange is defined in clause 6.4.2.3 of [ITU-T Q.731.3]. The extended parameters which include authentication information should be included in IAM for calling line identification authentication.

To ensure transit compatibility, the extended IAM should include a "parameter compatibility information" parameter to instruct the existing transit exchanges to transfer the extended IAM parameters transparently to the next exchange. The format of the parameter compatibility information parameter field is shown in clause 3.41 of [ITU-T Q.763] and clause 6.71 of [ITU-T Q.1902.3].

8.2 Actions at the transit exchange

On receipt of unrecognized signalling information parameters, the specified compatibility signalling procedures which can be found in clause 2.9.5.3.2 of [ITU-T Q.764] and clause 13.4.4.2 of [ITU-T Q.1902.4] should be performed by the transit exchange between the outgoing and incoming international exchange.

8.3 Actions at the incoming SSGW/ international gateway exchange

If the calling party number is valid, the procedure of calling line identification presentation for incoming SSGW/ international gateway exchange is defined in clause 6.4.2.4 of [ITU-T Q.731.3]. Extended parameter for calling line identification authentication should be included in the IAM.

If the calling party number is not valid and the call may not be blocked according to the policy. If the call can be processed the calling party number parameter should be removed.

8.4 Action at the destination local exchange (optional)

If the called user is provided with the CLIP supplementary service and the extended parameter for calling line identification authentication is available, the extended information should be included in SETUP message sending to the called user.

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

Published in Switzerland
Geneva, 2022