

Recommendation

ITU-T Q.3062 (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 and protocols for
enabling interconnection between trustable
network entities in support of existing and
emerging networks**

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.3062

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

Summary

Signalling system No. 7 (SS7) is a stack of signalling protocols, which was initially developed by ITU (CCITT) in the 1980s. Since then, SS7 standards have become a generic stack which is widely applied in public switched telephone networks (PSTNs) all over the world. With the growth of mobile telecommunications and the appearance of the mobile application part (MAP) and Camel application part (CAP) protocols, SS7 stack became suitable for public land mobile networks (PLMNs), e.g., 2G, 3G networks. Later, SS7 migrated to the signalling transport or SIGTRAN stack developed by the Internet Engineering Task Force (IETF) which allows operators to set up interconnection of SS7-based networks over Internet protocol (IP) networks. Furthermore, the SS7 logic migrated to Diameter signalling protocol which is currently widely used for interconnection of IP multimedia subsystem (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 the 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, denial of service (DoS), infiltration attacks, routing attacks, etc.

The goal of Recommendation ITU-T Q.3062 is to define the signalling requirements for authentication of signalling messages, in order for operators to be able to verify the authenticity of signalling exchanges based on an accepted trust anchor. This Recommendation includes codes and signalling procedures based on Recommendation ITU-T Q.3057.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3062	2022-09-29	11	11.1002/1000/15042

Keywords

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

* 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/>.

© ITU 2022

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions	3
6 Architecture for interconnection between trustable network entities	4
6.1 Reference architecture	4
6.2 Functional entities	5
6.3 Reference points	5
7 Security services	5
8 Security association attribute definition	5
8.1 Security association identifier (SAI)	6
8.2 Cryptographic parameters per security association.....	6
9 Structure of protected messages	6
9.1 Security header	6
9.2 Security payload	6
9.3 Digital signature algorithms (DSA) signature algorithms.....	7
10 Signalling procedures	7
10.1 TSa.....	7
10.2 Sa	10
10.3 Sc	14
Annex A – List of verifiable CSP identifiers to be sent in the PEEC request	16
Annex B – ASN.1 format for signalling messages	18
Appendix I – Information validation techniques	20
Bibliography.....	21

Recommendation ITU-T Q.3062

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 X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.510] Recommendation ITU-T X.510 (2020), *Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations*.
- [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)*.
- [IETF RFC 4703] IETF RFC 4703 (2006), *Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients*.
- [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 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.6 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.

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

3.1.8 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.

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

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

3.1.11 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.

3.1.12 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.

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

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

3.2 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 (PEEC): 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
CAP	Camel Application Part
CSP	Communications Service Provider
DoS	Denial of Service
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
IMS	IP Multimedia Subsystem
IPX	Internet Protocol interconnect
ISDN	Integrated Services Digital Network
MAP	Mobile Application Part
NE	Network Entity
PEEC	Provisional End Entity public-key Certificate
REST	Representational State Transfer
SA	Security Association
SAI	Security Association Identifier
SCCP	Signalling Connection Control Part
SGC	Signalling security Gateway public-key Certificate
SIP	Session Initiation Protocol
SS	Signalling System
SS7	Signalling System No. 7
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.