

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/>.

© ITU 2020

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	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	3
6	Overview of interconnection between trustable network entities.....	3
	6.1 Introduction of public key infrastructures	3
	6.2 Cross-certification	5
7	Architecture for interconnection between trustable network entities	6
	7.1 Reference architecture	7
	7.2 Functional entities	7
	7.3 Reference points	8
8	Signalling requirements for interconnection between trustable network entities.....	9
	8.1 General requirements.....	9
	8.2 Requirements for SSGW	9
	8.3 Signalling requirements for TSa reference point.....	10
9	Procedures for interconnection between trustable network entities	10
	9.1 CA high level functions.....	10
	9.2 TSCA high level functions	11
	9.3 Security policy of SSGW	12
	9.4 Signalling procedures of SSGW.....	13
	9.5 Message signature schemes and algorithms used in the SSGW.....	14
10	Security considerations.....	14
	Appendix I – Scenarios of interconnection between trustable network entities	16
	I.1 TCAP transaction between trustable network entities.....	16
	I.2 CLI transition between trustable network entities.....	17
	I.3 Diameter transaction between trustable network entities	18
	Bibliography.....	19

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 through 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.