

Recommendation

ITU-T Q.5026 (07/2023)

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

Signalling requirements and protocols for IMT-2020 –
Protocols for IMT-2020

**Signalling requirements and protocol for
providing network-oriented data integrity
verification service based on blockchain in
IMT-2020 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
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
PROTOCOLS AND SIGNALLING FOR COMPUTING POWER NETWORKS	Q.4140-Q.4159
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000-Q.5049
Signalling requirements and architecture of IMT-2020	Q.5000-Q.5019
Protocols for IMT-2020	Q.5020-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.5026

Signalling requirements and protocol for providing network-oriented data integrity verification service based on blockchain in IMT-2020 networks

Summary

Recommendation ITU-T Q.5026 specifies signalling requirements and protocol for providing network-oriented data integrity verification service (DIVS) based on blockchain in IMT-2020 networks. It includes signalling requirements, protocol procedures and message format between DIVS function with the UEs, the service users, the capability exposure function and other DIVS functions.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Q.5026	2023-07-14	11	11.1002/1000/15587

Keywords

Blockchain, IMT-2020 network, network-oriented data integrity verification service.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

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 2023

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
4 Abbreviations and acronyms	2
5 Conventions	2
6 Overview.....	3
7 Signalling requirements	3
7.1 Signalling architecture of the network-oriented DIVS.....	3
7.2 Signalling requirements.....	5
8 Signalling protocol procedures	5
8.1 Integrity verification parameter registration.....	5
8.2 Retrieve network account contract status of the UE	6
8.3 Application data integrity verification.....	7
8.4 Signalling flow of event subscription from the DIVS AS function	7
8.5 Signalling flow for event notification to DIVS AS function.....	8
8.6 Signalling flow for synchronizing the endorsed integrity verification data ...	9
9 Message format.....	9
9.1 Integrity verification parameters registration	9
9.2 Retrieve network account contract status of the UE	10
9.3 Application data integrity verification.....	13
9.4 Event subscription from DIVS AS function.....	14
9.5 Event notification to DIVS AS function	15
9.6 Event notification to DIVS AS function	16
10 Security considerations	17
Bibliography.....	18

Recommendation ITU-T Q.5026

Signalling requirements and protocol for providing network-oriented data integrity verification service based on blockchain in IMT-2020 networks

1 Scope

This Recommendation specifies the signalling requirements and protocol for providing network-oriented data integrity verification service (DIVS) based on blockchain in IMT-2020 networks.

The scope is as follows:

- Overview of the network-oriented DIVS;
- Signalling architecture and signalling requirements of the network-oriented DIVS;
- Protocol procedures and message format of the network-oriented DIVS;
- Security considerations.

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 Y.2247] Recommendation ITU-T Y.2247 (2023), *Framework and requirements of network-oriented data integrity verification service based on blockchain in future networks*.
- [ITU-T Y.2342] Recommendation ITU-T Y.2342 (2019), *Scenarios and capability requirements of blockchain in next generation network evolution*.
- [ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.
- [ITU-T Y.3104] Recommendation ITU-T Y.3104 (2018), *Architecture of the IMT-2020 network*.
- [ITU-T Y.3105] Recommendation ITU-T Y.3105 (2018), *Requirements of capability exposure in the IMT-2020 network*.
- [ITU-T Y.3108] Recommendation ITU-T Y.3108 (2019), *Capability exposure function in IMT-2020 networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 blockchain [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.2 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.3 IMT-2020 [ITU-T Y.3100]: (Based on [ITU-R M.2083-0]) Systems, system components, and related aspects that support to provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

3.1.4 network-oriented data integrity verification service (DIVS) [ITU-T Y.2247]: A network service that provides the information and verification mechanisms for the service users to verify the integrity of the raw data collected by the user equipment (UE) in IMT-2020 networks and beyond.

3.1.5 service user (SU) [b-ITU-T Q.1290]: An entity external to the network that uses its services.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Application Server
CEF	Capability Exposure Function
DIVS	Data Integrity Verification Service
ECDSA	Elliptic Curve Digital Signature Algorithm
eUICCID	embedded Universal Integrated Circuit Card Identity
IMEI	International Mobile Equipment Identity
ICCID	Integrated Circuit Card Identity
MSISDN	Mobile Subscriber International Integrated Services Digital Network/public switched telephone network Number
SP	Service Provider
UE	User Equipment
UICCID	Universal Integrated Circuit Card Identity
URL	Uniform Resource Locator
USM	Unified Subscription Management

5 Conventions

In this Recommendation:

The keywords **"is required to"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords **"can optionally"** indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.