

Recommendation

ITU-T Y.2247 (01/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Next Generation Networks – Service aspects: Service capabilities and service architecture

Framework and requirements of network-oriented data integrity verification service based on blockchain in future networks

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199

Service aspects: Service capabilities and service architecture **Y.2200–Y.2249**

Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

FUTURE NETWORKS

CLOUD COMPUTING

BIG DATA

QUANTUM KEY DISTRIBUTION NETWORKS

INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES

General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.2247

Framework and requirements of network-oriented data integrity verification service based on blockchain in future networks

Summary

Recommendation ITU-T Y.2247 specifies the network-oriented data integrity verification service (DIVS) based on blockchain in future networks. It provides the service requirements, framework and service scenarios of the network-oriented data integrity verification service based on blockchain and specifies the network capability requirements accordingly in the context of future networks including IMT-2020 network and beyond. Detailed descriptions of the use cases are listed in the appendix.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2247	2023-01-13	13	11.1002/1000/15247

Keywords

Blockchain, data integrity verification service, framework, future networks, IMT-2020 network and beyond, network capability exposure, network-oriented.

* 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 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
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	Overview and concept of network-oriented DIVS	3
	6.1 Background and motivation	3
	6.2 Concept of network-oriented DIVS.....	3
7	Service requirements of network-oriented DIVS	4
	7.1 General requirements of network-oriented DIVS	4
	7.2 Service requirements of network-oriented DIVS	5
8	Framework of network-oriented DIVS.....	7
	8.1 DIVS AS function	8
	8.2 UE function	9
	8.3 Service user function	9
	8.4 DIVS function reference points.....	9
9	Network capability requirements of network-oriented DIVS	10
	9.1 Capability requirements of the network capability exposure	10
	9.2 Capability requirements of massive machine-type terminal management.....	10
	9.3 Capability requirements of end-to-end connectivity	11
	9.4 Capability requirements of blockchain infrastructure	11
10	Service scenarios of network-oriented DIVS	11
	10.1 Service scenario of the data integrity verification initiated by the data consumer side	11
	10.2 Service scenario of the data integrity verification initiated by the data aggregator side.....	12
11	Security considerations	14
	Appendix I – Use cases of network-oriented data integrity verification service	15
	I.1 Data integrity verification of transport vehicles in logistics industry	15
	I.2 Data integrity verification of the capacity record of distributed renewable power generation	16
	I.3 Trustworthy source verification of industry digital twin.....	18
	Bibliography.....	20

Recommendation ITU-T Y.2247

Framework and requirements of network-oriented data integrity verification service based on blockchain in future networks

1 Scope

This Recommendation specifies the framework and requirements of a network-oriented data integrity verification service (DIVS) based on blockchain in future networks including IMT-2020 networks and beyond. The scope is as follows:

- Service requirements and framework
- Network capability requirements
- Service scenarios

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.2342] Recommendation ITU-T Y.2342 (2019), *Scenarios and capability requirements of blockchain in next generation network evolution*.
- [ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.
- [ITU-T Y.3104] Recommendation ITU-T Y.3104 (2018), *Architecture of 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 [b-ITU-T Y.3100]: Systems, system components, and related technologies that provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

NOTE – [b-ITU-R M.1645] defines the framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000 for the radio access network.

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

3.1.5 third party (3rd party) [b-ITU-T Y.3100]: In the context of IMT-2020, with respect to a given network operator and network end-users, an entity which consumes network capabilities and/or provides applications and/or services.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 network-oriented data integrity verification service (DIVS): 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
API	Application Programming Interface
AS	Application Server
BC	Blockchain
CEF	Capability Exposure Function
DIVS	Data Integrity Verification Service
ECC	Elliptic Curve Cryptography
eSIM	embedded SIM
eUICCID	embedded Universal Integrated Circuit Card Identity
GEC	Green Electricity Certificate
IMEI	International Mobile Equipment Identity
MCN	Mobile Core Network
MSISDN	Mobile Subscriber International ISDN/PSTN number
SP	Service Provider
TEE	Trusted Execution Environment
UE	User Equipment
UICCID	Universal Integrated Circuit Card Identity
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
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 "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

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.

In the body of this document and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted respectively as, is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview and concept of network-oriented DIVS

6.1 Background and motivation

As the IMT-2020 networks are deployed, massive machine-type terminals, especially in vertical industries, collect massive data which accelerates industry digital transformation in industries such as agriculture, logistics, transportation, healthcare, environment, supply chain finance, etc. This is not only valuable directly for the service provider (SPs) who collect, aggregate and analyse the data, but also for the data consumers who exchange and reuse the data for derivative businesses, such as environmental data (e.g., air temperature and wind speed) for the agricultural insurance sector, driving behaviour data of vehicles for second-hand vehicle sales businesses, and transportation traffic data for artificial intelligence (AI) model training. The importance of the data collected by IMT-2020 networks raises concerns about the integrity of the raw data.

Usually the data integrity is validated by the data consumers leveraging the digital signature of the data provider [b-IETF RFC 4880] [b-ITU-T X.509]. However, it is difficult for the data consumers to examine it to know if the exchanged data is the same as it was collected originally. Furthermore, when the data is shared and reused by data consumers, there is no way for the data consumers to validate the integrity of the original data either. The data consumers have to trust the data provider unconditionally, while specific third-party services derived from the (vertical industry devices) data, such as the agricultural insurance and distributed AI applications, are sensitive to the data integrity and trustworthiness. Tampered data, intentionally or unintentionally, may lead to unnecessary economic losses and even security risks. Thus, the data integrity verification service (DIVS) oriented network is necessary for the services of data consumers.

6.2 Concept of network-oriented DIVS

The network-oriented data integrity verification service (DIVS) provides the information and verification mechanisms for service users to verify the integrity of the original application data collected by UEs in IMT-2020 networks and beyond based on specified network parameters. Leveraging network-oriented DIVS, the service users could retrieve the public key, hash algorithm, timestamp and other metadata to validate the integrity in the whole life cycle of the data shared by the SPs. The network-oriented DIVS provides a trust anchor taking advantage of the IMT-2020 network for the service users and reduces the cost of trust transfer in industry digital transformation.

A conceptual diagram of network-oriented DIVS is shown as Figure 6-1. The UEs send the collected raw application data to the SPs. The UEs include machine-type terminals, vertical industry terminals and industry sensors which can access the IMT-2020 networks directly. The SPs are responsible for aggregating the collected data from the UEs and share the data with the data consumers. The data consumers receive the aggregated data, analyse the data, mine data values and develop derivative services. The data consumers are the service users of the network-oriented DIVS, thus the terms 'data consumer' and 'service user' are used equally in this text. The DIVS application server (AS) in IMT-2020 network endorses the integrity verification parameters,