ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

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	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
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/.

Table of Contents

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,

maintains the mapping relationship between the integrity verification parameters and the network account statuses of the UEs and provides the data integrity verification service.

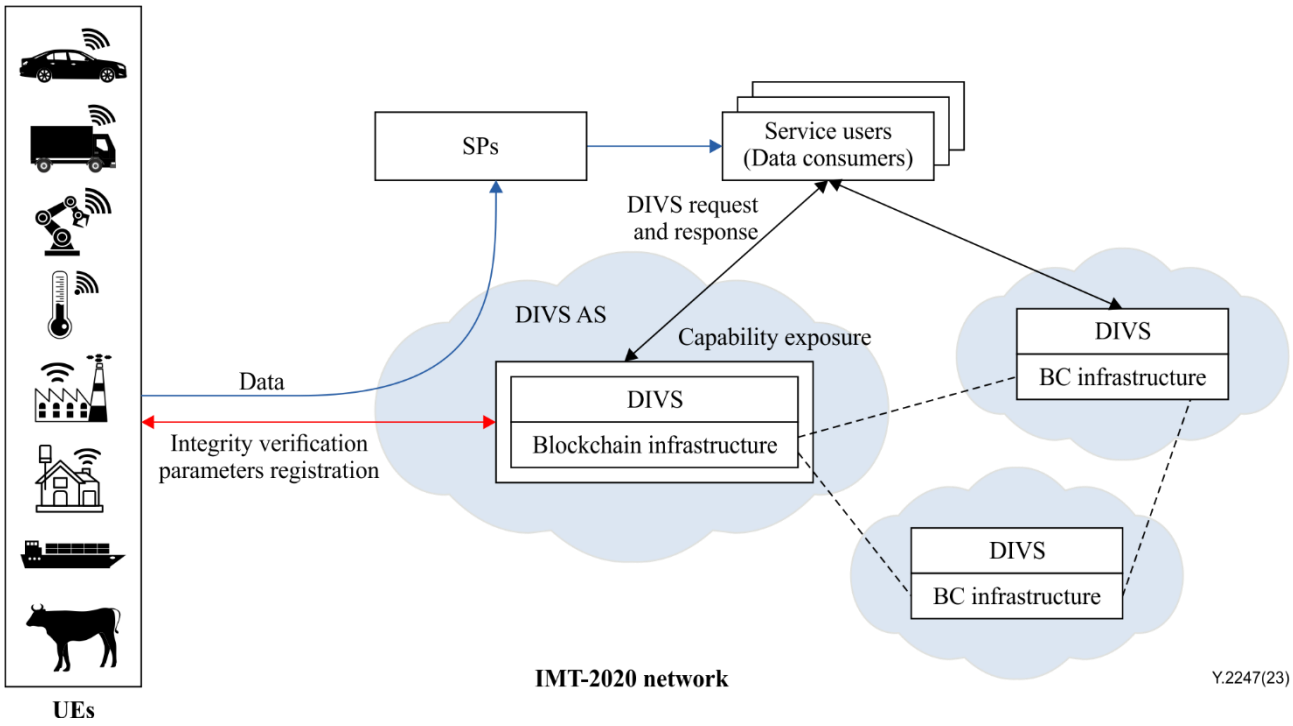


Figure 6-1 – Conceptual diagram of network-oriented DIVS

7 Service requirements of network-oriented DIVS

7.1 General requirements of network-oriented DIVS

Considering service principles with respect to the privacy protection, scalability and diversity of the UEs and the data consumers, it is required to support general requirements for network-oriented DIVS as follows:

It is recommended that the network-oriented DIVS AS should not receive and store the raw application data collected by the UEs.

It is required that the integrity of the raw application data collected by the UEs can be validated through its whole life cycle by using the network-oriented DIVS.

It is required that the UEs for the network-oriented DIVS support generation of the data integrity verification parameters and store them in trusted environment locally.

It is required that the network-oriented DIVS AS supports endorsement of the data integrity verification parameters and associates them with the network account contract information of the UEs.

It is required that the data integrity verification data stored in the network-oriented DIVS AS is tamper-proof.

It is required that the updates of the endorsed data integrity verification data can only be appended.

It is required that the network-oriented DIVS supports crossing of multiple IMT-2020 networks, e.g., industry private networks and mobile operators' networks.

It is required that the network-oriented DIVS is scalable so as to adapt diverse types of the UEs and data consumers.

7.2 Service requirements of network-oriented DIVS

According to the concept of the network-oriented DIVS, there are three roles which are:

– data collectors, such as UEs

– data recipients, such as SPs (data aggregators) and data consumers

– DIVS application servers (AS)

The service requirements of network-oriented DIVS mainly involve service capabilities, data integrity verification data management and service interaction between the three roles.

7.2.1 Service requirements of integrity verification parameters registration

Before sending the raw application data collected to the data recipients, the data collectors shall register the integrity verification parameters to the DIVS AS for endorsement. The integrity verification parameters include the public key, signature algorithms supported and UE information of the data collector.

The data collector is required to have a capability to generate the public-private key pair based on the asymmetric key generation algorithm locally, e.g., elliptic curve cryptography (ECC). The private key could be stored in the trusted environments of the UE, e.g., the trusted execution environment (TEE) or applet residing inside the universal subscriber identity module (USIM) or embedded SIM (eSIM), and utilized to generate the signature of the raw application data collected.

The data collector binds the public key with the UE identity information including the international mobile equipment identity (IMEI), UICCID/eUICCID and mobile subscriber international ISDN/PSTN number (MSISDN), etc., and generates a digital signature using the private key and specific signature algorithm. The data collector sends the integrity verification parameters with the digital signature to the DIVS AS.

7.2.2 Service requirements of integrity verification parameters endorsement

Since the data recipient makes use of the integrity verification parameters to validate the integrity of the raw application data, it is necessary for the integrity verification parameters to be endorsed by the DIVS AS to guarantee the validity and trustworthiness. The DIVS AS shall support the capabilities to endorse the integrity verification parameters.

– When receiving the registered integrity verification parameters, the DIVS AS verifies the signature making use of the public key and signature algorithm of the UE. It is to be noted that the registered integrity verification parameters include the integrity verification parameters and the signature of the public key and the UE identity information as mentioned above. The DIVS AS obtains the UE identity information in the case where the signature is valid and sends a request to the capability exposure function (CEF) in the IMT-2020 network to retrieve the data collector network account status based on the UE identity information. The CEF sends a request to the unified subscription management (USM) to fetch the data collector network account status and returns the retrieved information to the DIVS AS. The data collector network account status information could include the data collector's network contract information, UE information, the contract period, geographic restrictions, etc.

– The DIVS AS combines the registered integrity verification parameters and data collector network account status received from the CEF as the endorsing integrity verification data. The DIVS AS generates the digital signature of the endorsing integrity verification data based on its private key locally generated and signature algorithm, and records the endorsing integrity verification data, and the digital signature and certificate corresponding to the private key in the blockchain ledger. Thus the endorsed integrity verification data could be stored in the blockchain ledger for as long a time as the lifecycle of the collected raw application data and cannot be subjected to tampering.

– The DIVS AS sends the transaction ID in the blockchain ledger and the entry address of the record of the endorsed integrity verification data to the data collector. The transaction ID indicates the transaction serial number of the endorsed integrity verification data in the blockchain ledger. The entry address indicates the storage address information, e.g., the blockchain instance ID and the DIVS AS URL, which could be used to query the endorsed integrity verification data in the DIVS AS. The data recipients could retrieve the endorsed integrity verification data from DIVS AS based on the transaction ID and entry address when verifying the integrity of the raw application data.

When the network account status of a data collector changes, such as the contract termination, updates of the binding relationships between IMEI, UICCID/eUICCID and MSISDN, terminal ownership changes, etc., the DIVS AS shall have a capability to update the endorsed integrity verification data in the blockchain ledger.

– When receiving the subscribed event notification message regarding the network account status update of the data collector from the CEF and USM of the IMT-2020 network, the DIVS AS queries the blockchain ledger to obtain the registered integrity verification parameters based on the UE identity, e.g., MSISDN, UICCID/eUICCID or IMEI , in the event notification messages.
– The DIVS AS combines the registered integrity verification parameters and the updated data collector network account status as the updated endorsing integrity verification data. The DIVS AS generates the digital signature of the updated endorsing integrity verification data based on its private key and signature algorithm, and records the updated endorsing integrity verification data, the digital signature and the certificate corresponding to the private key in the blockchain ledger.
– The DIVS AS sends the updated transaction ID in the blockchain ledger and the updated entry address of the record of the endorsed integrity verification data to the data collector. The updated transaction ID indicates the transaction serial number of the updated endorsed integrity verification data in the blockchain ledger. The updated entry address indicates the storage address information, e.g., the blockchain instance ID and the DIVS AS URL, which could be used to query the updated endorsed integrity verification data.

7.2.3 Service requirements of application data integrity verification

When the data recipients receive the application data from the data collectors or other data recipients, the network-oriented DIVS shall support the data integrity verification capability to the data recipients.

– Data collectors

The data collector collects the raw application data, e.g., leveraging the sensor units in the UEs. To guarantee the integrity of the raw application data, the data collector shall generate a digital signature for the raw application data based on its private key and signature algorithm supported locally, before sending the raw application data to the data recipients. The data collector binds the raw application data collected, the corresponding digital signature and the latest transaction ID and entry address of the endorsed integrity verification data and sends them to the data recipient.

Considering confidentiality protection of the digital signature, it is required of the data collector to execute the signature algorithm in the trusted environments of the UE, e.g., the TEE or applet of USIM/eSIM.

– Data recipients

It is required that the data recipients support the capability to verify the integrity of the application data.

When receiving the application data, the data recipient sends a request with the transaction ID and entry address to the DIVS AS to query and retrieve the endorsed integrity verification data. The

data recipient verifies the integrity of the endorsed integrity verification data and gets the public key of the data collector. The data recipient verifies the digital signature of the application data based on the public key and supported signature algorithm of the endorsed integrity verification data and makes sure that the raw application data is received. In addition, the data recipient compares the timestamp of the digital signature of the application data with the network contract termination time of the data collector to make sure the valid private key for generating the digital signature is used.

– Network-oriented DIVS AS

It is required that the DIVS AS supports responding to the query requests of the data recipient for the endorsed integrity verification data.

When receiving requests of the data recipients, the DIVS AS queries the blockchain ledger based on the transaction ID and entry address and returns the endorsed integrity verification data. Depending on the indication of the request, the DIVS AS can optionally return part of the necessary data, e.g., the public key and contract termination time, to reduce the data interaction.

8 Framework of network-oriented DIVS

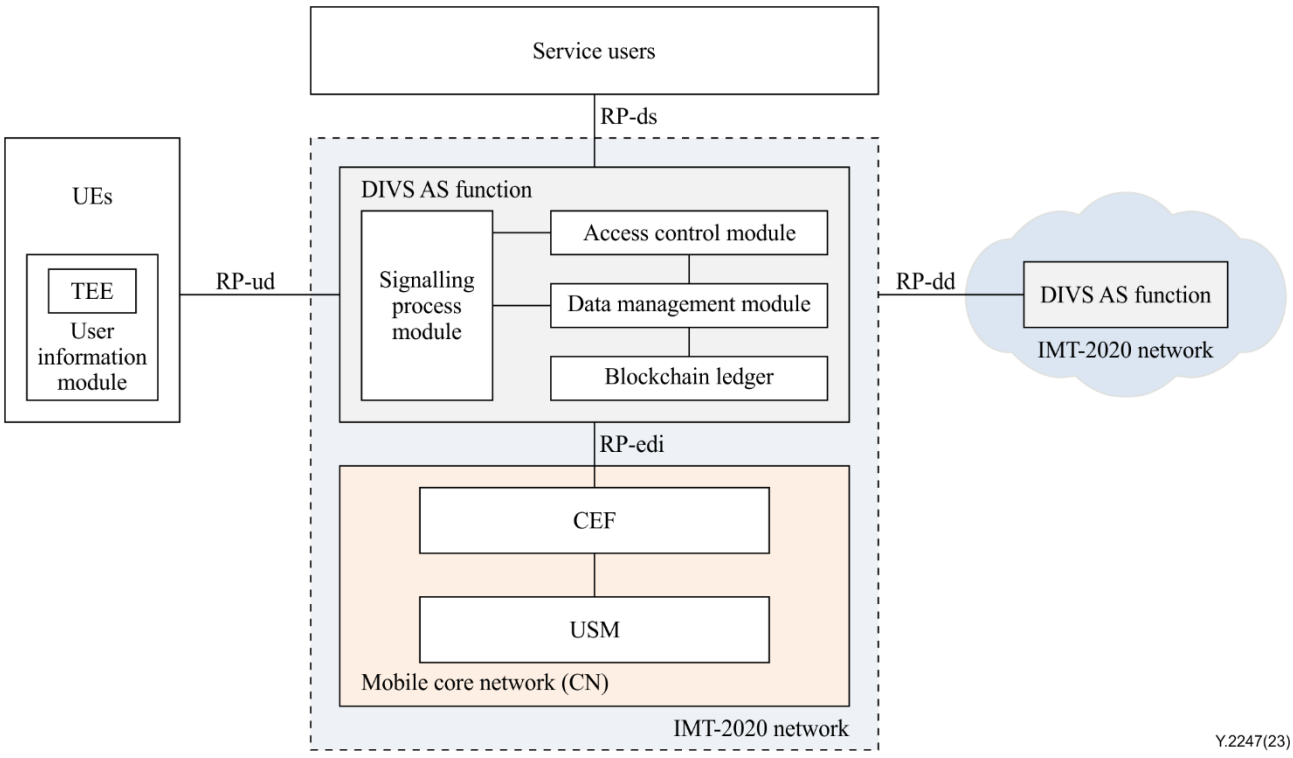


Figure 8-1 – Framework and reference architecture for network-oriented DIVS

Figure 8-1 shows the framework of the network-oriented DIVS from a functional point of view, based on the architecture of the IMT-2020 network [ITU-T Y.3104] and framework of capability exposure function [ITU-T Y.3108]. The framework of the DIVS mainly consists of the UE function, DIVS AS function and service user. The UE function is intended to collect application data and provide the integrity verification parameters to the DIVS AS function. The DIVS AS function provides the data integrity verification service to the service user (i.e., data consumer), the anti-tampering data storage of the endorsed integrity verification data, and the signalling process. The service user is the data consumer which needs to verify the integrity of the raw application data.

8.1 DIVS AS function

As illustrated in the reference architecture of the network-oriented DIVS (Figure 8-1), the DIVS AS function includes four functional modules: the signalling process module, the access control module, the data management module and the blockchain ledger module.

8.1.1 Signalling process functional module

The signalling process functional module processes the signalling from/to the UE function, CEF and service user:

– Receiving the endorsed integrity verification data request from the service users and responding based on the transaction ID;

– Receiving the integrity verification parameters from the UE, verifying the digital signature using the public key and signature algorithm of the UE, retrieving the network account status information based on the UE identity which is extracted from the integrity verification parameters, and combining the integrity verification parameters and network account status information as the endorsing integrity verification data;

– Sending the network account status information request to the CEF;

– Receiving the network account status information from the CEF based on the UE identity;

– Sending the transaction ID of the endorsed integrity verification data in the blockchain ledger and entry address to the UE function;

– Subscribing the network account status update notification event to the CEF;

– Receiving the network account status update event notification, querying the latest endorsed integrity verification data corresponding to the UE identity in the event notification, updating the endorsing integrity verification data;

– Sending the updated transaction ID of the endorsed integrity verification data in the blockchain ledger and entry address to the UE function.

8.1.2 Access control functional module

The access control functional module carries out functionalities as follows:

– Providing the authentication and authorization capability to verify the access of the service users;

– Providing the authentication and authorization capability to verify the access of the UE function.

8.1.3 Data management functional module

The data management functional module carries out functionalities as follows:

– Providing the reading/writing application programming interfaces (APIs) to the blockchain ledger functional module;

– Maintaining the certificate and private key of the DIVS AS function;

– Receiving the endorsing integrity verification data, generating the digital signature based on the private key and signature algorithm of the DIVS AS function, and writing the endorsing integrity verification data, the digital signature and certificate to the blockchain ledger, and sending the transaction ID to the signalling process functional module;

– Receiving the inquiry for the endorsed integrity verification data and returning the inquiry result based on the transaction ID;

– Providing the data management regarding the access control for the service users and UEs.

8.1.4 Blockchain ledger functional module

The blockchain ledger functional module provides the anti-tampering data storage. The functionalities carried out are as follows:

– Recording the endorsed integrity verification data in the blockchain ledger;

– Synchronizing the records among blockchain ledger modules in DIVS AS functions.

8.2 UE function

The UE function carries out the following functionalities:

– Sending the collected raw application data, digital signature, transaction ID and entry address from the DIVS AS function to the service users. The entry address indicates the address information of the DIVS AS for querying the endorsed integrity verification data.

– Registering the integrity verification parameters to the DIVS AS function. The registered integrity verification parameters includes the UE identity information, the public key, signature algorithm supported and the digital signature of the public key and UE identity information. The UE identity information includes the MSISDN, IMEI, and UICCID/eUICCID, etc.

– Receiving the transaction ID in the blockchain ledger and the entry address of the endorsed integrity verification data from the DIVS AS function;

– Receiving the updated transaction ID in the blockchain ledger and the entry address of the updated endorsed integrity verification data from the DIVS AS function;

– Maintaining and generating the latest transaction ID and entry address of the endorsed integrity verification data in the DIVS AS function by comparing the updated transaction ID and entry address to the original transaction ID and entry address.

– Generating the public-private key pair based on the asymmetric key generation algorithm locally. The private key could be stored in the trusted environments of the UE.

– Generating the digital signature for the raw application data leveraging a private key and signature algorithm in a trusted environment.

8.3 Service user function

The service user function carries out the following functionalities:

– Receiving the raw application data, digital signature, transaction ID and entry address of the endorsed integrity verification data from the UE function;

– Retrieving the endorsed integrity verification data from the DIVS AS function based on the transaction ID and entry address, verifying the signature of the endorsed integrity verification data based on the certificate corresponding to the private key and signature algorithm of the DIVS AS function;

– Obtaining the public key and signature algorithm of the UE in the endorsed integrity verification data in the case the signature is valid;

– Verifying the digital signature of raw application data based on the public key and signature algorithm of the UE of the endorsed integrity verification data, and comparing the timestamp of the digital signature of the raw application data with the network contract termination time.

8.4 DIVS function reference points

The following reference points (RPs) are defined in the framework of DIVS:

– RP-edi: between the DIVS AS function and the CEF;

The reference point RP-edi is required to support retrieving of the network account contract status of the terminals, subscribe/modify/unsubscribe for event(s) related to the network account contract status update of the UE to the CEF, and deliver the event notification.

– RP-ud: between the DIVS AS function and the UEs;

The reference point RP-ud is required to provide the capability to deliver the registered integrity verification parameters to the DIVS AS function, and the transaction ID and entry address of the endorsed integrity verification data to the UEs.

– RP-ds: between the DIVS AS function and the service users.

The reference point RP- ds is required to support delivering of the integrity verification data request and response.

– RP-dd: between the DIVS AS functions.

The reference point RP-dd is required to support synchronizing of the endorsed integrity verification data between the DIVS AS functions built on the blockchain ledger.

9 Network capability requirements of network-oriented DIVS

According to the service requirements described in clause 7, the derived requirements of the network capability to support the network-oriented DIVS are as follows:

9.1 Capability requirements of the network capability exposure

The network capability exposure provides a way for the DIVS AS to retrieve the data collector's contract information and updated status.

It is required that the CEF supports the capability to retrieve the data collector's network account status information from the USM based on the UE identity information.

It is required that the DIVS AS supports the capability to retrieve the data collector's network account status information from the CEF based on the UE identity information.

It is required that the USM supports the capability to notify the updates of the data collector's network account status information to the CEF.

It is required that the CEF supports the capability to notify the updates of the data collector's network account status information to the DIVS AS.

It is required that the CEF supports the capability to subscribe the event notification of the data collector's network account status information update to the USM based on specific UE identity information.

It is required that the DIVS AS supports the capability to subscribe the event notification of the data collector's network account status information update to the CEF based on specific UE identity information.

9.2 Capability requirements of massive machine-type terminal management

The machine-type terminals included in the UEs are not only responsible for collecting the application data from the source in the vertical industry environment, but also for registering the integrity verification parameters to the DIVS AS. The massive machine-type terminal management capabilities are required to be supported in the network-oriented DIVS.

It is required to provide a capability to provision the network services for specific types of the machine-type terminals in batches.

It is required to provide a capability to issue the device and service configurations, such as the addresses of the DIVS ASs, over the air to the machine-type terminals.

It is recommended to provide a capability to issue and install the applets over the air to the USIM/eSIM in the machine-type terminals.

It is recommended to provide a capability to manage the lifecycle of the applets residing inside the USIM/eSIM.

9.3 Capability requirements of end-to-end connectivity

The UEs, service users and the DIVS ASs in the network-oriented DISV may cross multiple domains, in terms of both network and management. It is necessary to provide the end-to-end connectivity for these functions over the IMT-2020 network in the form of both public networks and dedicated networks.

It is required to provide a capability to deliver the messages between the UEs and the corresponding DIVS AS regardless of whether their home domains are different.

It is required to provide a capability to transfer the application data collected by the UEs to the data recipients regardless of whether their home domains are different.

It is required to provide a capability to interconnect the DIVS ASs for synchronizing the endorsed integrity verification data.

9.4 Capability requirements of blockchain infrastructure

The blockchain is an underlay enabling technology for the network-oriented DIVS. It is required to provide the blockchain infrastructure for the DIVS AS function. It is to be noted that the type of the blockchain for the DIVS AS function is permissioned blockchain, which includes the consortium blockchain and private blockchain [ITU-T Y.2342].

It is required to provide a capability to support multiple types of blockchain in the blockchain infrastructure.

It is required to provide a capability to support the interaction of functions over different types of blockchains in the blockchain infrastructure.

It is required to provide a capability to support the interworking between different types of blockchain in the blockchain infrastructure.

It is required to provide a capability to support off-line management in terms of the joining of the blockchain organizations and ledger nodes.

It is required to provide a capability to support the consistent API based on the smart contracts to operate the endorsed integrity verification data in the blockchain ledger.

10 Service scenarios of network-oriented DIVS

There are different factors which make the service scenarios of the network-oriented DIVS varied, such as the types of the network the terminals accesses, the different management domains of the data aggregators and data consumers, and the specific business models. However, based on which role initiates the network-oriented DIVS request, the service scenarios could be abstractly divided into two categories: the data integrity verification initiated by the data aggregator side and the data integrity verification initiated by the data consumer side.

10.1 Service scenario of the data integrity verification initiated by the data consumer side

In this service scenario, after receiving the shared data from the data aggregator, the data consumer would initiate the request to the DIVS AS to verify the integrity of the data received. The shared data between the data aggregator and data consumer could be in plaintext or ciphertext. Whether to use the data is decided by the data consumer according to the result of the data integrity verification.

Figure 10-1 shows the information flow of data integrity verification initiated by the data consumer side. The detailed workflows are as follows:

1) The UE has completed the integrity verification parameters registration and endorsement;
2) The UE collects the raw application data in different vertical industry environments, such as the manufactory, power plant, agricultural park and so on, and sends the data and signature to the data aggregator;
3) The data aggregator aggregates the raw application data gathered by the UE and shares it with the data consumer;
4) The data consumer queries the DIVS AS to retrieve the endorsed integrity verification data and verifies the data integrity;
5) The data consumer makes use of the raw application data received, such as the data analysis or the AI model training.

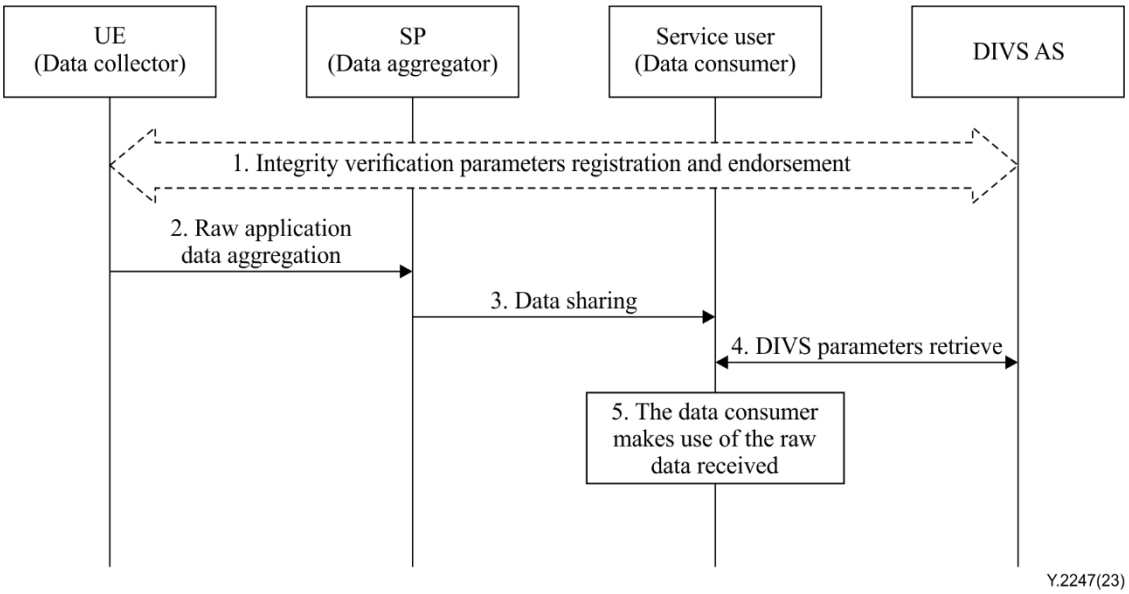


Figure 10-1 – Information flow for the data integrity verification initiated by the data consumer side

In this service scenario, the data ownership could be transferred between the data consumers. The subsequent data consumer can also inquire the DIVS AS and verify the integrity of the data shared. Thus, the data consumer is able to aggregate the data, whose integrity from the true sources could be verified, from multiple data aggregators.

10.2 Service scenario of the data integrity verification initiated by the data aggregator side

In this service scenario, the data aggregator would share the right to the use rather than the ownership of the raw data with the data consumer, which means the data computing would only be executed in the data aggregator, e.g., in a TEE enclave. The data aggregator would initiate the request to the DIVS AS to verify the integrity of the data shared according to the trigger of the data consumer.

Figure 10-2 shows the information flow of data integrity verification initiated by the data aggregator side. The detailed workflows are as follows:

1) The UE has completed the integrity verification parameters registration and endorsement;
2) The UE collects the raw application data in different vertical industry environments, such as the manufactory, power plant, agricultural park and so on, and sends the raw application data and signature to the data aggregator;

3) The data aggregator aggregates the raw application data gathered by the UE and shares with the data consumer the description information of the data, such as the data identification and UE identity;

4) The data consumer sends the data integrity verification request to the data aggregator;

5) The data aggregator queries the DIVS AS to retrieve the endorsed integrity verification data;

6) The data aggregator verifies the data integrity in the trusted environment;

7) The data aggregator returns the verification result to the data consumer;

8) The data consumer would negotiate with the data aggregator on how to make use of the data including the security connection, algorithm, and execution environment attestation; etc.

9) The data aggregator executes the algorithms of the data consumer in the local trusted environment.

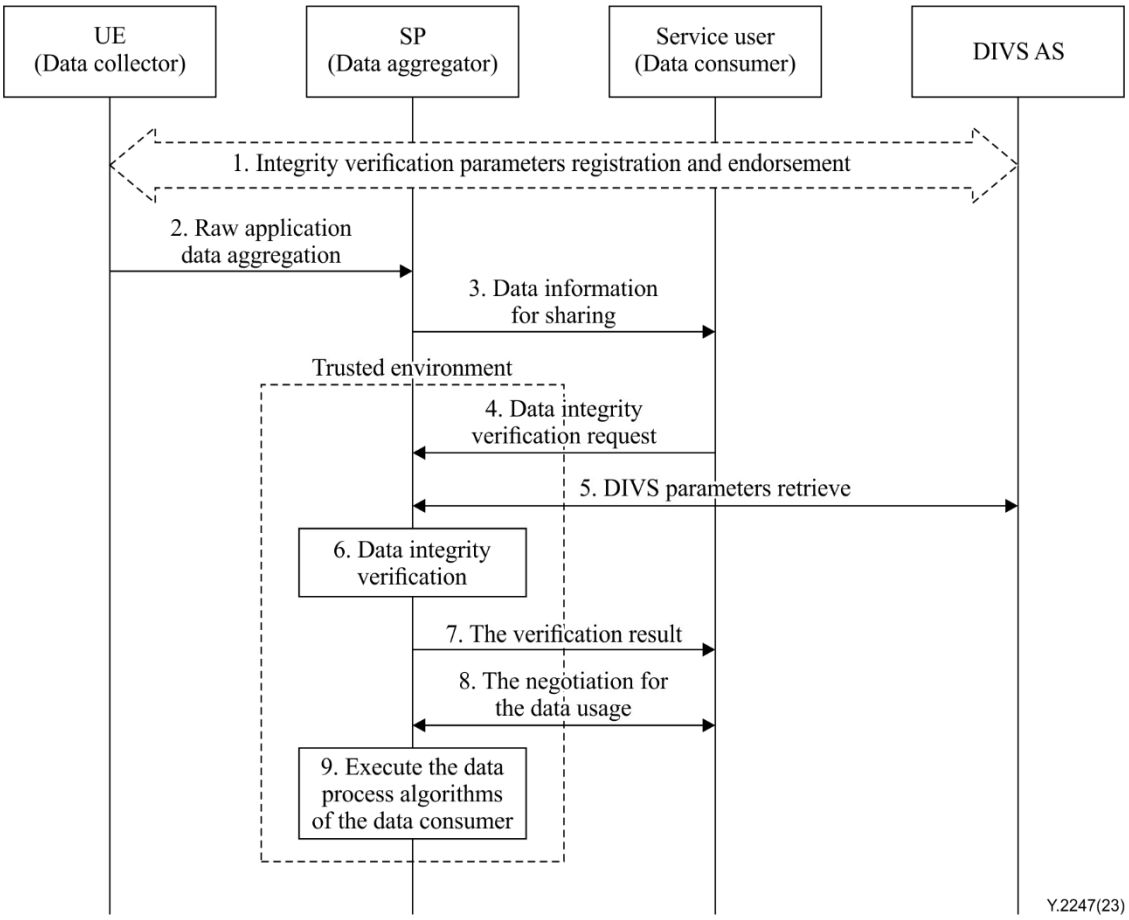


Figure 10-2 – Information flow for the data integrity verification initiated by the data aggregator side

In this service scenario, the data consumer processes the data while keeping the raw data under the management of the data aggregator. This service scenario could have multiple variants, for example, the data consumer could concurrently access multiple data aggregators for distributed training of AI and the joint modelling. The data consumer is required to make sure that the raw data collected is used leveraging the network-oriented DIVS in these specific variants.

11 Security considerations

The security and privacy considerations of network-oriented DIVS based on blockchain in future networks include the following aspects:

Data integrity verification service security, which includes the security considerations on the authentication and authorization of the service users, end-to-end communication between the UE, DIVS AS and the service user, the DIVS AS function security, and so on.

Data integrity verification parameters security, which includes the security considerations on the private key management of the UE, network account status and contract data, integrity verification parameters privacy, and so on.

Blockchain security, which includes the security considerations on smart contract management, certificate management, private key storage and recovery, multi-vendor blockchain interoperability. The additional blockchain security consideration can be optionally aligned with the capability requirements specified in [b-ITU-T X.1402].

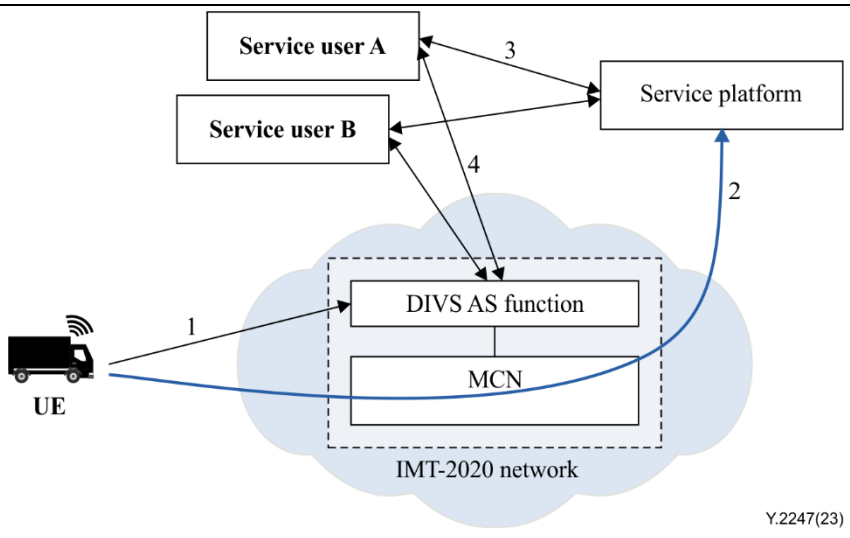
In addition, the security and privacy considerations of network-oriented DIVS based on blockchain can be optionally aligned with the security guideline requirements specified in [ITU-T Y.3101] [b-ITU-T Y.2701].

Appendix I

Use cases of network-oriented data integrity verification service

(This appendix does not form an integral part of this Recommendation.)

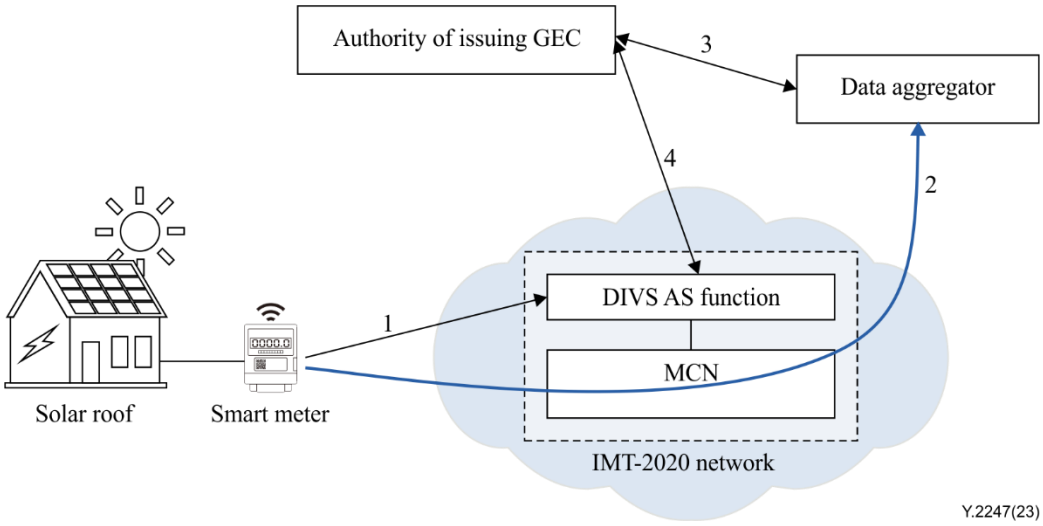
I.1 Data integrity verification of transport vehicles in logistics industry

Title	Data integrity verification of transport vehicles in logistics industry
Description	Transport vehicles in logistics industry generate masses of valuable data in different dimensions, such as the driving behaviour data, the location and route data, the running speed and distance data, etc. On the one hand, the service platform/operation platform could optimize the service operations making use of the data collected, such as vehicle dispatching, safety reminders, route optimization and so on. On the other hand, the collected data may generate derivative business, e.g., second-hand transaction and finance leasing businesses. However, the collected data may be tampered with during the circulation between the data consumers, which may lead to unnecessary economic losses and even security attacks. The network-oriented DIVS provides a trusted data integrity verification infrastructure for the data consumers in the industry chain. The data consumers could directly verify if the data provided by the service platform/operation platform is the same as that collected originally based on DIVS, in the entire lifecycle of the data.
Pre-conditions (optional)	1) The DIVS AS function has obtained the parameters for the data integrity verification, such as the public key, the signature algorithm, device ID, ICCID, MSISDN, etc. 2) The UE (transport vehicle) has sent the application data with signature and necessary identity information to the service platform/operation platform.
Post-conditions (optional)	None.
Roles	UE (transport vehicle): The UE collects the specific source data, generates the digital signature of the data and sends it to the service platform. The service platform: The service platform could be a vehicle management platform or service operation platform, which collects the application data from the UEs. The DIVS AS function: The DIVS AS function is an application function in IMT-2020 network, providing the data integrity verification service. The service user: The service user needs to verify the data integrity from the DIVS AS function and makes use of the data.
Figure and operational flows (optional)	

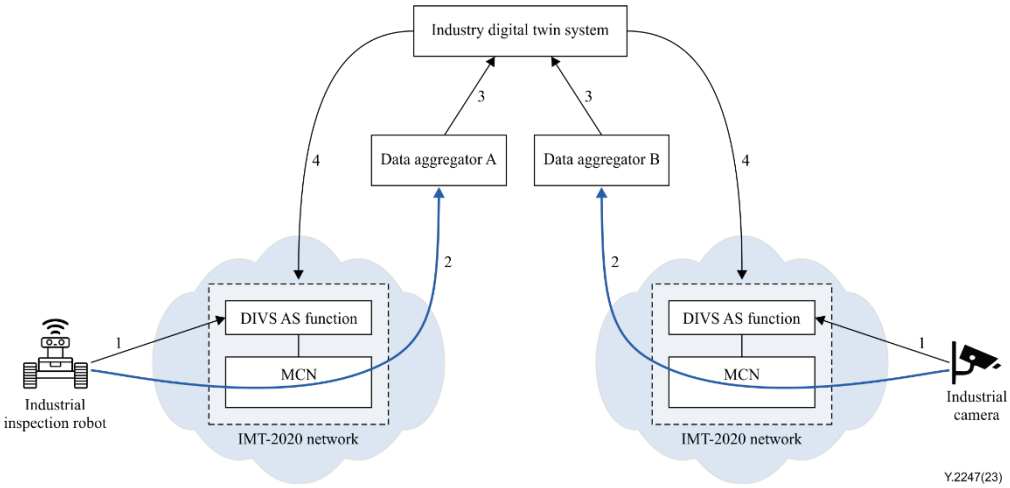
	Operational flows: 1) The DIVS AS function obtains and stores the data integrity verification parameter from the UE (transport vehicle) and MCN if necessary. 2) The UE (transport vehicle) generates and collects the data specified by the service platform, generates the digital signature of the data and sends it to the service platform through the data plane of the IMT-2020 network. The data could include driving behaviour data, the location and route, the running speed and distance, the timestamp, etc. 3) The service user A applies for the data or the data signature related parameters to the service platform. 4) The service user A requests to get the data integrity verification metadata from the DIVS AS function and verifies the data integrity. 5) The service user A makes use of the data. For the sake of privacy protection, the service platform may only exchange the data integrity signature related information but not original data with the service user A.
Derived requirements	Based on the operational flows: The DIVS AS function provides data integrity verification service to the service users. The service includes returning the data signature verification metadata. The DIVS AS function obtains and stores the data integrity verification parameter once the network service of the UE provisioning. The DIVS AS function provides anti-tamper storage of the data integrity verification metadata.

I.2 Data integrity verification of the capacity record of distributed renewable power generation

Title	Data integrity verification of the capacity record of distributed renewable power generation
Description	Distributed renewable power generation systems, e.g., a solar-panel roof, are often installed by private owners in their homes or by enterprises in their parks. The electricity generated could be used by the individuals and enterprises themselves to reduce costs and achieve carbon neutrality. The distributed renewable power generation systems can also connect to the electricity grid to obtain benefits by selling overcapacity. A smart meter connected to the IMT-2020 network records the electricity consumption and the electricity supplied to the grid. Since the green electricity from distributed power generation could be used for applying the subsidies from the governments and carbon trading, it is important to guarantee that the number recorded by the smart meter is untampered and that the integrity of the data collected by the smart meter could be verified throughout its lifecycle. The DIVS AS provides the network-oriented DIVS for applying the green electricity certificate or the subsidies.
Pre-conditions (optional)	1) The UE (smart meter) has completed the network service provisioning and is able to access the IMT-2020 network, either the slice of public network or dedicated network. The smart meter has registered the data integrity verification parameters to the DIVS AS function. 2) The DIVS AS function has endorsed the data integrity verification parameters. 3) The UE has sent the recorded data of the electricity consumption with the signature and necessary identity information to the data aggregation platform.
Post-conditions (optional)	The owner of the distributed renewable power generation system receives the green electricity certificate based on the smart meter record of the electricity consumption.

Roles	UE (smart meter): The UE records the data of the electricity consumption and sends it to the data aggregator. The data aggregator: The data aggregator could be a vendor management platform for the distributed renewable power generation systems, or a third party service platform for applying the green electricity certificate. The data aggregator receives and stores the data from UEs. The DIVS AS function: The DIVS AS function is an application function in IMT-2020 network, which is providing the data integrity verification service. Authority for issuing green electricity certificate: The authority for issuing the green electricity certificate needs to verify the data integrity from the data aggregator and then issues the green electricity certificate.
Figure and operational flows (optional)	 Operational flows: 1) The DIVS AS function obtains and stores the data integrity verification parameter from the UE (smart meter) and MCN if necessary. 2) The UE (smart meter) gathers the data of the electricity capacity, generates the digital signature of the data and sends it to the data aggregator through the data plane of the IMT-2020 network. The data could include the electricity consumption, electricity supplied to the grid, the timestamp, etc. 3) The data aggregator applies the green electricity certificate to the authority for issuing the green electricity certificate according to the accumulated data of electricity consumption. 4) The authority for issuing the green electricity certificate accesses to the DIVS AS function to get the data integrity verification parameters and verifies the data integrity. Based on the verification result, the authority for issuing the green electricity certificate decides whether to issue the green electricity certificate.
Derived requirements	Based on the operational flows, The DIVS AS function provides the data integrity verification service throughout the lifecycle of the data, even if the UE switches mobile network operators. The DIVS AS function is able to handle massive machine-type terminals, in the terms of configuration distribution and integrity verification parameter registration. The UE can sign the collected data in a trusted environment to guarantee the signature is from the true source.

I.3 Trustworthy source verification of industry digital twin

Title	Trustworthy source verification of industry digital twin
Description	Digital twin of vertical industry maps the physical space to the digital space by collecting the manufacturing and process data of the physical counterpart. The digital twin could provide the monitoring, simulation, prediction, and optimization and make decisions regarding the physical space. Thus, it is important to manifest not only the trustworthiness of the data-generating sources but also the original of the data collected, to avoid injecting false data to the digital space. The network-oriented DIVS could provide the trustworthy source verification based on the binding of the terminal ID, public key and USIM/eSIM UICCID for the industry digital twin system. Furthermore, the network-oriented DIVS could also provide the service to verify whether the data collected is tampered.
Pre-conditions (optional)	1) The UE has completed the network service provisioning and is able to access the IMT-2020 dedicated network. The UE has registered the data integrity verification parameters to the DIVS AS function. 2) The DIVS AS function has endorsed the data integrity verification parameters. 3) The UE has sent the collected manufacturing data with the signature and necessary identity information to the data aggregation platform.
Post-conditions (optional)	None.
Roles	UE (Industrial terminal): The UE collects the specific manufacturing data, generates the digital signature of the data and sends it to the data aggregator. The UEs are network connected industrial terminals, such as the industrial cameras and industrial inspection robots. The data aggregator: The data aggregator could be a data aggregation platform which receives and stores the data from the UEs. The data aggregator provides the APIs for the industry digital twin system to request data. The DIVS AS function: The DIVS AS function is an application function in IMT-2020 network, which is providing the data integrity verification service. The industry digital twin system: The industry digital twin system requests data from the data aggregators to establish the digital space. The industry digital twin system needs to verify the trustworthiness of the data source and data integrity from the network-oriented DIVS.
Figure and operational flows (optional)	 Operational flows: 1) The DIVS functions obtain and store the data integrity verification parameters from the UEs and MCNs if necessary.

	2) The UEs collect the specific manufacturing data, generates the digital signature of the data and sends it to the data aggregators through the data plane of the IMT-2020 network. 3) The industry digital twin system retrieves the collected manufacturing data maintained at the data aggregators. 4) The industry digital twin system accesses the DIVS AS functions to get the data integrity verification parameters, verifies the data integrity if the collected data is from the trustworthy sources. 5) The industry digital twin system establishes digital space and performs the simulation and data analysis.
Derived requirements	Based on the operational flows, The DIVS AS function provides a measure to enable the service user to verify if the collected data is from the trustworthy source, e.g., by binding the terminal ID, public key and USIM/eSIM UICCID.

Bibliography

[b-ITU-T Q.1290] Recommendation ITU-T Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*.

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

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T X.1402] ITU-T Recommendation X.1402 (2020), *Security framework for distributed ledger technology*.

[b-ITU-T Y.2701] ITU-T Recommendation Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y.3001] Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-T Y.3102] Recommendation ITU-T Y.3102 (2018), *Framework of the IMT-2020 network.*

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

[b-IETF RFC 4880] IETF RFC 4880 (2007), *OpenPGP Message Format.*

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, 2023