Draft Recommendation ITU-T Y.frd

Framework and Requirements of Network- oriented Data Integrity Verification Service based on Blockchain in Future Network

1. Scope

This recommendation aims to study the framework and requirements of network-oriented data integrity verification service based on blockchain in future networks.

The scope of the new work item is as follow, but not limited to:

- Service framework of network-oriented data integrity verification service based on blockchain
- Requirements of network-oriented data integrity verification service based on blockchain
- Service scenarios and use cases of network-oriented data integrity verification service based on blockchain

Editor's Note: the scenarios and use cases mainly focus on the data integrity verification service. The security related scenarios and use cases are out of scope.

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

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

TBD

3. Definitions

3.1 Terms defined elsewhere

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

3.1.2 blockchain [b-ITU-T X.1400]: A type of distributed ledger (see clause 6.21) 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.

TBD

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

TBD

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BC Blockchain

DIVS Data Integrity Verification Service

TBD

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 prohibited from**" 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.

6. Overview and Concept of network-oriented data integrity verification service

As the 5G network deployment, massive machine-type terminals especially in the verticals collect massive data which enables the digital transformation of vertical industries, such as the agriculture, logistics, transportation, healthcare, environment, supply chain finance, .etc. It is not only valuable directly for the SPs who collect, aggregate and analyse the data, but also for the upstream data consumers which reuse the data for derivative business, e.g. the environment data (e.g. temperature and windspeed) for agricultural insurance, the driving behavior data of vehicles for second-hand transaction, the transportation traffic data for AI algorithm training, .etc. The importance of the data collected by 5G networks raises the concern to the data integrity and the trust anchor.

Usually the data integrity is validated by the data consumer leveraging the signature of the data provider[b-ITU-T X.509][b-IETF RFC 4880]. However, it is difficult for the data consumer to examine if the data is the same as it was collected originally. Furthermore, when the data is reused by upstream data consumers as mentioned above, there is no way for the upstream SPs to validate the data integrity originally either. The upstream data consumers have to trust the data provider unconditionally. While the new services derivatived from the (vertical industry devices) data, such as the agricultural insurance and distributed AI applications, are sensitive to the data integrity. The modified data may lead to unnecessary economic losses and even security attacks. Thus, the data integrity verification service oriented network is necessary for the services of the upstream data consumers.

The network-oriented data integrity verification service (DIVS) provides the information and mechanisms for the data consumers to validate the integrity of the original data collected by the 5G networks based on some specified network parameters. Leveraging the network-oriented DIVS, the data consumers could retrieve the public key, Hash algorithm, timestamp and other metadata to

validate the integrity in the whole life cycle of the data. The network-oriented DIVS provides a trust anchor take advantage of the network for the data consumers and reduces the cost of trust transfer in the digital transformation. The conceptual diagram of network-oriented DIVS is shown as Figure 6-1.

Editor's Note: The concept of network-oriented DIVS should be explained. Usecases are required standing on the service user's view.

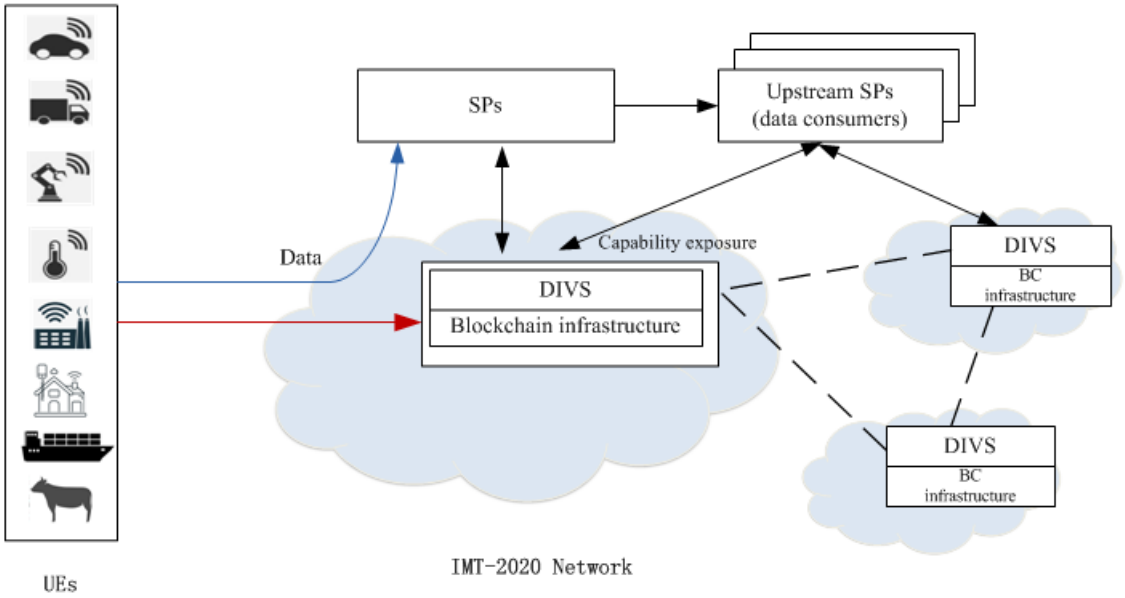


Figure 6-1. Conceptual diagram of network-oriented DIVS

7. Service requirements of network-oriented data integrity verification service

Editor's Note: This section provides the service requirements of the network-oriented DIVS based on blockchain.

The service requirements of network-oriented DIVS mainly involves the service capabilities, service interaction and service management.

7.1 Requirements of network-oriented DIVS

It is required that the network-oriented DIVS provides data integrity verification service to the service users. The service includes verifying the data signature or returning the data signature verification metadata.

It is required that the network-oriented DIVS provides anti-tamper storage of the data integrity verification parameters.

8. Framework of network-oriented data integrity verification service

Editor's Note: This section would provide a service framework and architecture of the network-oriented DIVS. Based on the framework, the high-level requirements are raised.

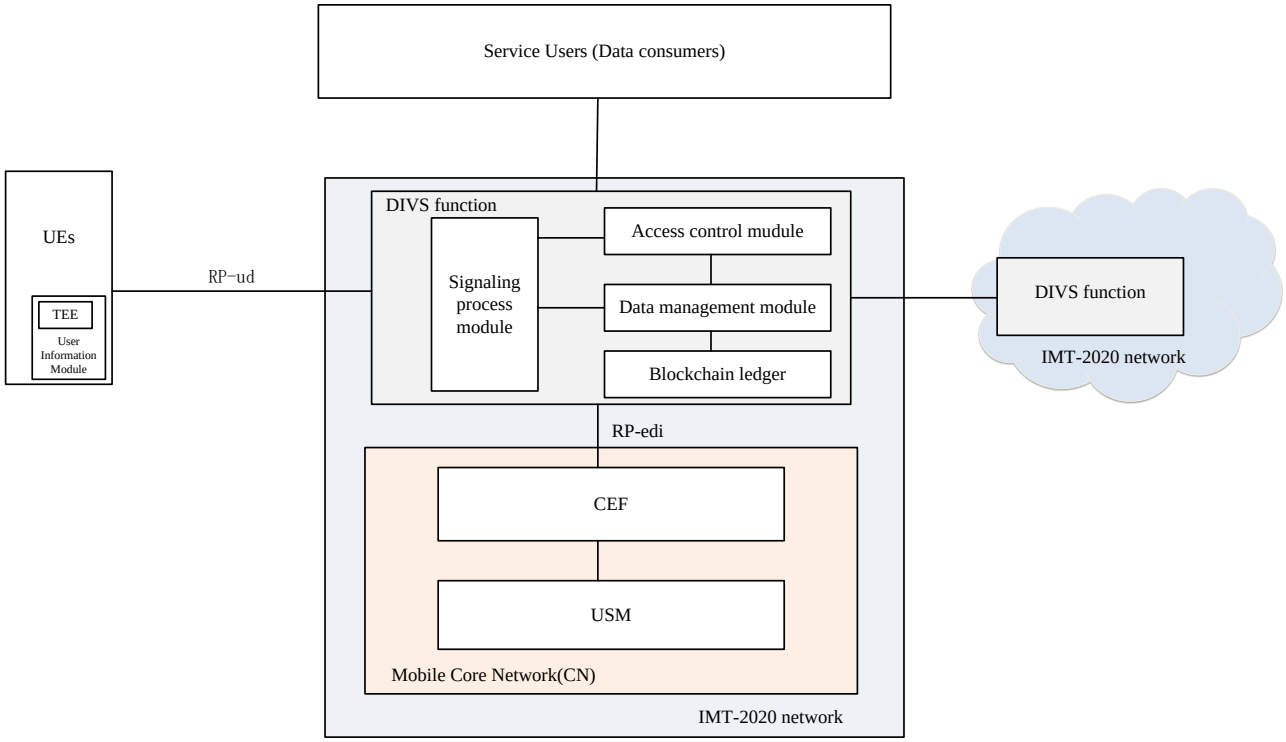


Figure 2 – Framework and reference architecture for network-oriented DIVS

Figure 2 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 and DIVS function. The UE function is intended to provide the necessary data for the signature generation and verification to the DIVS function. The DIVS function provides the data integrity verification service to the service user (i.e. data consumer), the anti-tampering data storage of the integrity verification parameters, the signaling process and translation between UE function and CEF.

8.1 DIVS Function

As illustrated in the reference architecture of the DIVS, the DIVS function includes 4 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 signaling process functional module provides the signaling process and signaling translation between UE function and CEF:

- Receiving the data integrity verification parameters request from the service users and response;
- Receiving the necessary data for the signature generation and verification from UE and UE configuration parameters, and transferring the signaling to the CEF and USM;
- Subscribing the event to the CEF and receiving the response, providing the event data subscribed to the data management functional module;

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;

8.1.3 Data management functional module

The data management functional module carries out functionalities as follows：

- Receiving the data integrity verification parameters query from the signaling process functional module and response;
- Providing the data management of the access control for the service users and UEs;
- Reading and writing data integrity verification parameters from or to the blockchain ledger;

8.1.4 Blockchain ledger functional module

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

- Recording the integrity verification parameters (e.g. public key, signature algorithm, MNO endorsement signature) in the blockchain ledger;
- Synchronizing the records among blockchain ledger modules in DIVS functions;

8.2 UE Function

The UE Function carries out the following functionalities:

- Sending the integrity verification parameters to the DIVS function. The integrity verification parameters could be self-generated in a trusted execution environment in the UE or pre-written by the network operator;
- Generating the signature for the application data leveraging a private key and signature algorithm.

8.3 DIVS Function reference points

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

- RP-edi: between the DIVS function and the CEF;
- RP-ud: between the DIVS function and the UE;

9. Network capability requirements of network-oriented data integrity verification service

Editor's Note: This section provides the network capability requirmetns of the network-oriented DIVS

10. Service model and scenarios

Editor's Note: This section provides the service requiments and network requirmetns of the network-oriented DIVS based on blokchain.

11. Security considerations

Editor's Note: This section provides the security considerations of the service framework of the network-oriented DIVS based on blokchain.

Appendix I Use cases and workflow of data integrity verification service

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

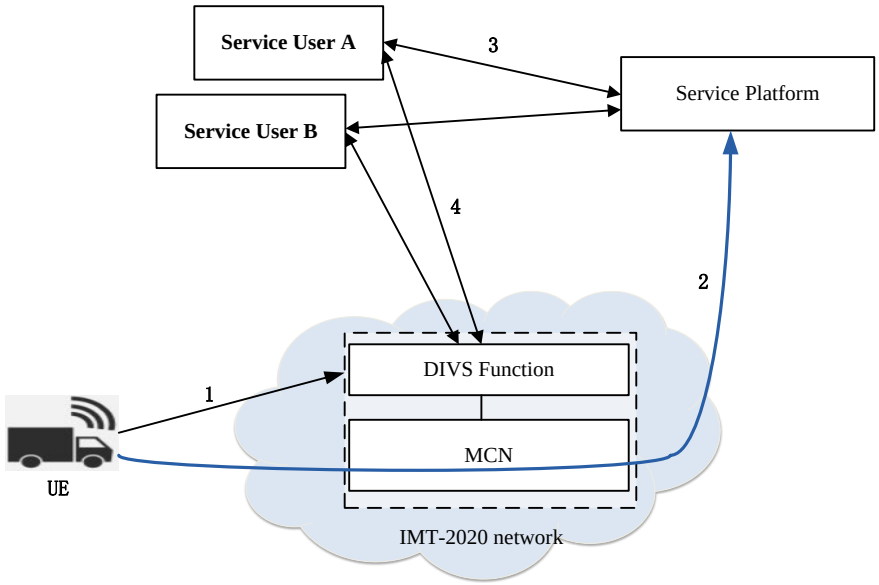
I.1 Use case template

The use cases developed in Appendix I should adopt the following unified format for better readability and convenient material organization.

Title	Note: The title of the use case
Description	Note: Scenario description of the use case
Pre-conditions (optional)	Note: The necessary pre-conditions should be achieved before starting the use case.
Post-conditions (optional)	Note: The post-condition that will be carried out after the termination of current use case.
Figure and operational flows (optional)	Note: Figures and operational flows to explain the use case if necessary
Derived requirements	Note: Requirements derived from the use cases, whose detailed description are presented in the dedicated chapter.

I.2 Data integrity verification of transport vehicles in logistics industry

Title	Data integrity verification of transport vehicles in logistics industry
Description	The transport vehicles in logistics industry generate massive valuable data in different dimensions, such as the driving behaviour data, the location and route, the running speed and distance, .etc. On one hand, the service platform/operation platform could optimize the service operations making use of the data collected, such as dispatching vehicles, safety reminding, route optimization and so on. On the other hand, the collected data may drive to generate derivative business, e.g. the second-hand transaction and finance lease. However, the collected data has a chance to be tampered when data 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 it collected originally based on DIVS, in the entire lifecycle of the data.
Pre-conditions (optional)	1. The DIVS function has obtain 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 data with signature and necessary identity information to the service platform/operation platform.
Post-conditions	None

(optional)	
Roles	UE(Transport vehicle): The UE generates and collects the specific source data, signs 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 data from UEs. The DIVS function: The DIVS function is an application function in network, which providing the data integrity verification service. The service user: The service user needs to verify the data integrity from the service platform and makes use the data.
Figure and operational flows (optional)	 Operational flows: 1. The DIVS function obtains and stores the data integrity verification parameter from UE(Transport vehicle) and MCN if necessary. 2. The UE(Transport vehicle) generates and collects the data specified by the service platform, signs 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 to the DIVS 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 function provides data integrity verification service to the service users. The service includes verifying the data signature or returning the data signature verification metadata. The DIVS function obtains and stores the data integrity verification parameter once the service of UE provision. The DIVS function provides anti-tamper storage of the data integrity verification parameters.

Bibliography

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

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