ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Q.5026 (07/2023)

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

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

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

ITU-T Q-SERIES RECOMMENDATIONS

Switching and signalling, and associated measurements and tests

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1-Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4-Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60-Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100-Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS NO. 4, 5, 6, R1 AND R2	Q.120-Q.499
DIGITAL EXCHANGES	Q.500-Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600-Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM NO. 7	Q.700-Q.799
Q3 INTERFACE	Q.800-Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM NO. 1	Q.850-Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000-Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100-Q.1199
INTELLIGENT NETWORK	Q.1200-Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700-Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900-Q.1999
BROADBAND ISDN	Q.2000-Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000-Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710-Q.3899
TESTING SPECIFICATIONS	Q.3900-Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100-Q.4139
PROTOCOLS AND SIGNALLING FOR COMPUTING POWER NETWORKS	Q.4140-Q.4159
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000-Q.5049
Signalling requirements and architecture of IMT-2020	Q.5000-Q.5019
Protocols for IMT-2020	**Q.5020-Q.5049**
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050-Q.5069

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

Recommendation ITU-T Q.5026

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

Summary

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

History *

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

Keywords

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

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

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.5026

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

1 Scope

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

The scope is as follows:

– Overview of the network-oriented DIVS;

– Signalling architecture and signalling requirements of the network-oriented DIVS;

– Protocol procedures and message format of the network-oriented DIVS;

– Security considerations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2247] Recommendation ITU-T Y.2247 (2023), *Framework and requirements of network-oriented data integrity verification service based on blockchain in future networks*.

[ITU-T Y.2342] Recommendation ITU-T Y.2342 (2019), *Scenarios and capability requirements of blockchain in next generation network evolution*.

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

[ITU-T Y.3104] Recommendation ITU-T Y.3104 (2018), *Architecture of the IMT-2020 network*.

[ITU-T Y.3105] Recommendation ITU-T Y.3105 (2018), *Requirements of capability exposure in the IMT-2020 network*.

[ITU-T Y.3108] Recommendation ITU-T Y.3108 (2019), *Capability exposure function in IMT-2020 networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

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

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

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

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

5 Conventions

In this Recommendation:

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

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

6 Overview

In IMT-2020 network deployment, massive machine-type terminals, especially in the vertical industries, collect massive data which accelerates the digital transformation of industries such as agriculture, logistics, transportation, health care, environment and supply chain finance. This data is not only directly valuable for the service providers (SPs) who collect, aggregate and analyse it, but also for the data consumers, who exchange and reuse the data for derivative business. The importance of the data collected by IMT-2020 networks raises the concern of the raw data's integrity.

DIVS [ITU-T Y.2247] provides the information and mechanisms for service users to verify the integrity of the raw data collected by the UE of IMT-2020 networks. The network-oriented DIVS application server (AS) in the IMT-2020 network endorses the integrity verification parameters, maintains the mapping relationship between the integrity verification parameters and the network account statuses of the UE and provides the DIVS. The network-oriented DIVS provides a trusted verification anchor taking advantage of the IMT-2020 network for service users and reduces the cost of trust transfer in the industry digital transformation.

7 Signalling requirements

7.1 Signalling architecture of the network-oriented DIVS

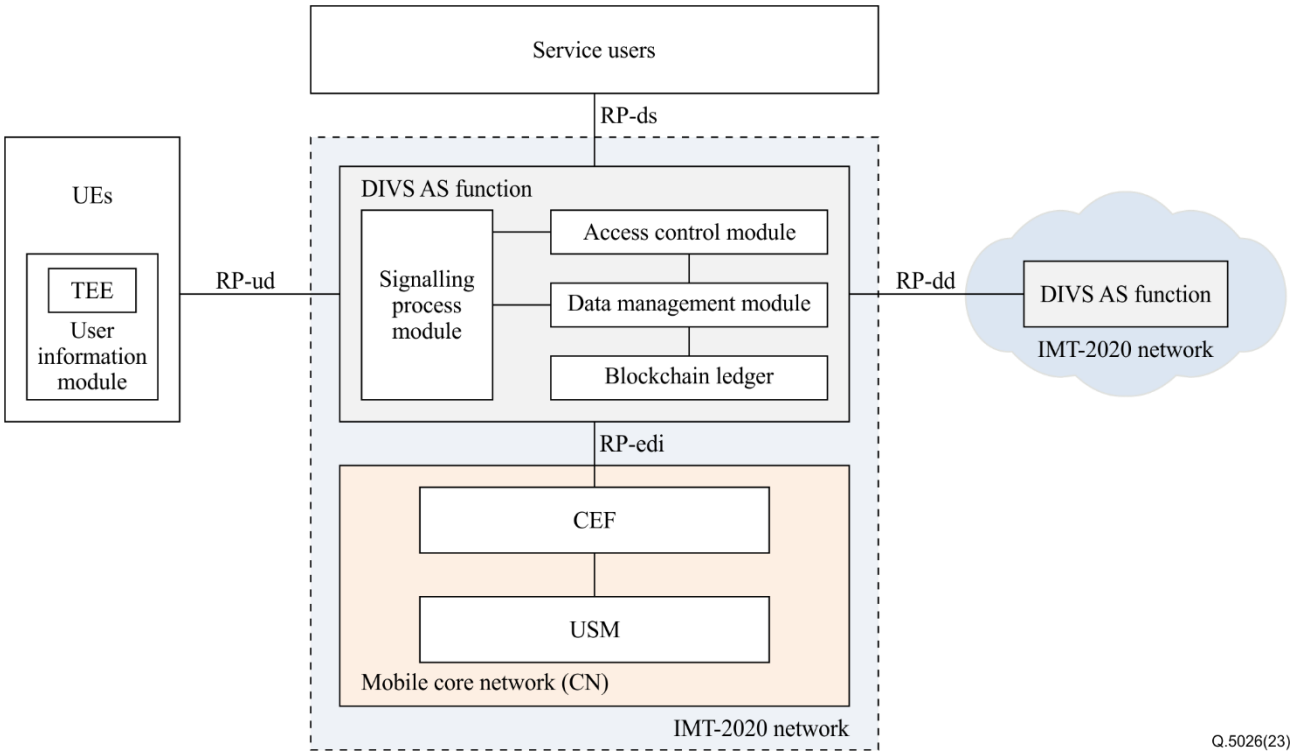

Figure 7-1 – Framework and reference architecture for network-oriented DIVS [ITU-T Y.2247]

Figure 7-1 shows the reference architecture 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 a framework of capability exposure function [ITU-T Y.3108]. The DIVS AS function provides the data integrity verification service to the service users (i.e., data consumers), the anti-tampered data storage of the endorsed integrity verification data, and the signalling process. The DIVS AS function has interfaces with the UEs, the service users, the CEF and other DIVS AS functions. Since the

reference architecture demonstrated in Figure 7-1 already contains the reference points, it could also be taken as the signalling architecture of the network-oriented DIVS.

For the DIVS, an AS function is required to support the service procedures and functions as follows as the basis of the signalling protocol procedures:

1) Integrity verification data endorsement:
   - DIVS AS function receives the registered integrity verification parameters, which include the public key, supported signature algorithms, the UE identity information and digital signature from the UE, and verifies the digital signature using the public key and supported signature algorithms;
   - DIVS AS function retrieves the network account contract status information based on the UE identity from the CEF and USM;
   - DIVS AS function combines the registered integrity verification parameters with the network account contract status information of the UE as the endorsing integrity verification data;
   - DIVS AS function records the endorsing integrity verification data, the corresponding digital signature based on the private key generated and signature algorithms supported in the DIVS AS, and certificate to the blockchain ledger;
   - DIVS AS function sends the transaction ID in the blockchain ledger and entry address of the record of the endorsed integrity verification data to the UE.
2) Integrity verification data endorsement update:
   - DIVS AS function receives the subscribed event notification regarding the network account contract status update of the UE from the CEF;
   - DIVS AS function queries the blockchain ledger to fetch the latest registered integrity verification parameters based on the UE identity in the event notification;
   - DIVS AS function combines the registered integrity verification parameters with the updated network account contract status information of the UE as the updated endorsing integrity verification data;
   - DIVS AS function records the updated endorsing integrity verification data, the corresponding digital signature based on the private key generated and signature algorithms supported in the DIVS AS, and the certificate to the blockchain ledger;
   - DIVS AS function sends the updated transaction ID in the blockchain ledger and entry address of the record of the endorsed integrity verification data to the UE.
3) Application data integrity verification service:
   - DIVS AS function receives data integrity verification request from the service user with the transaction ID and the entry address;
   - DIVS AS function queries the blockchain ledger based on the transaction ID;
   - DIVS AS function returns the endorsed integrity verification data to the service user.
4) UE network account contract status event subscribe service:
   - DIVS AS function could subscribe/unsubscribe the event(s) related to the network account contract status update of the UE to the CEF and USM.

The DIVS AS function includes four function modules, which are the signalling process module, the access control module, the data management module and the blockchain ledger module.

- The signalling process module supports receiving and processing the registered integrity verification parameters from the UEs, the endorsed integrity verification data queries from the service users, the network account contract status information of the UEs from the CEF, etc.

– The access control module supports the authentication and authorization capability to verify the access of the service users and UEs.
– The data management module supports writing the endorsing integrity verification data, the digital signature and certificate to the blockchain ledger, querying the endorsed integrity verification data, maintaining configuration data and the private keys of DIVS AS function.
– The blockchain ledger module supports recording the endorsed integrity verification data and synchronizing the records among blockchain ledger modules in DIVS AS functions.
– According to the signalling architecture of the network-oriented DIVS [ITU-T Y.2247], the reference points exist as follows:
  – RP-edi: between the DIVS AS function and the CEF;
  – RP-ud: between the DIVS AS function and the UEs;
  – RP-ds: between the DIVS AS function and the service users;
  – RP-dd: between the DIVS AS functions.

7.2 Signalling requirements

7.2.1 Signalling requirements for reference point RP-ud

The interface and messages between the UEs and DIVS AS function are required to support delivering 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.

7.2.2 Signalling requirements for reference point RP-ds

The interface and messages between the service users and DIVS AS function are required to support delivering the endorsed integrity verification data request and response.

7.2.3 Signalling requirements for reference point RP-edi

The interface and messages between the CEF and DIVS AS function are required to support retrieving the network account contract status information of the UEs, subscribe/unsubscribe for event(s) related to the network account contract status update of the UE to the CEF, and delivering the event notification.

7.2.4 Signalling requirements for reference point RP-dd

The interface and messages between the DIVS AS functions are required to support synchronizing the endorsed integrity verification data. The reference point RP-dd is considered an overlay logical interface built on the P2P protocol or other broadcast protocols between the blockchain ledger nodes.

8 Signalling protocol procedures

8.1 Integrity verification parameter registration

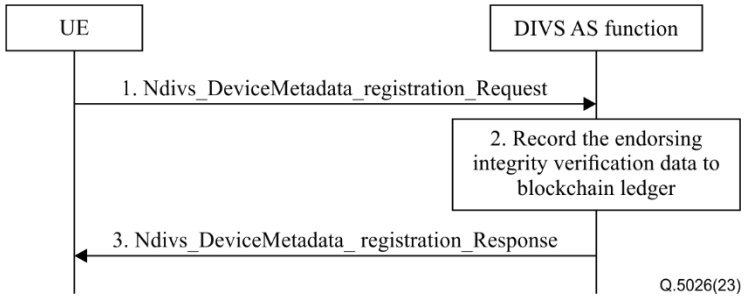

Figure 8-1 – Signalling flow for integrity verification parameter registration

The integrity verification parameter registration procedure in Figure 8-1 is used to register the integrity verification parameters of the UE to the DIVS AS function.

1) The UE generates a public–private key pair, binds the public key with the UE identity information including the IMEI, ICCID/eUICCID and MSISDN, and generates the digital signature of the integrity verification parameters using the private key. The UE sends the integrity verification parameters in the Ndivs_DeviceMetadata_registration_request message to the DIVS AS function.

2) Once the Ndivs_DeviceMetadata_registration_request message is received, the DIVS AS function verifies the signature based on the public key and supported signature algorithm and retrieves the UE network account contract status based on the UE identity information. The DIVS AS function combines the registered integrity verification parameters and UE network account contract status as the endorsing integrity verification data. The DIVS AS function generates the digital signature of the endorsing integrity verification data based on its private key locally, and records the endorsing integrity verification data, the digital signature and certificate corresponding to the private key in the blockchain ledger.

3) The DIVS AS function sends the transaction ID in the blockchain ledger and entry address of the record regarding the endorsed integrity verification data to the UE in the Ndivs_DeviceMetadata_ registration_Response message.

8.2 Retrieve network account contract status of the UE

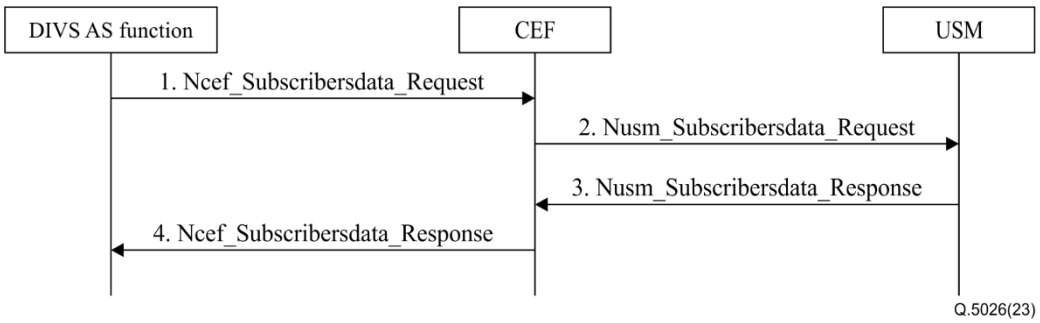

Figure 8-2 – Signalling flow for retrieving network account contract status of the UE

The UE network account contract status retrieve procedure in Figure 8-2 is used to retrieve the network account contract status information based on the UE identity information for the DIVS AS function.

1) DIVS AS function sends the Ncef_Subscribersdata_Request message with the UE identity obtained from the registered integrity verification parameters to CEF to retrieve the network account contract status.

2) The CEF obtains the UE identity from Ncef_Subscribersdata_Request message and sends the Nusm_Subscribersdata_Request to the USM. If necessary, the CEF is required to support the UE identity translation.

3) When receiving the Ncef_Subscribersdata_Request message, the USM queries its local database based on the UE identity, and sends the Nusm_Subscribersdata_Response message to the CEF with the network account contract status information.

4) The CEF forwards the query results carried by the Nusm_Subscribersdata_Response message to the DIVS AS function with the Ncef_Subscribersdata_Response message.

8.3 Application data integrity verification

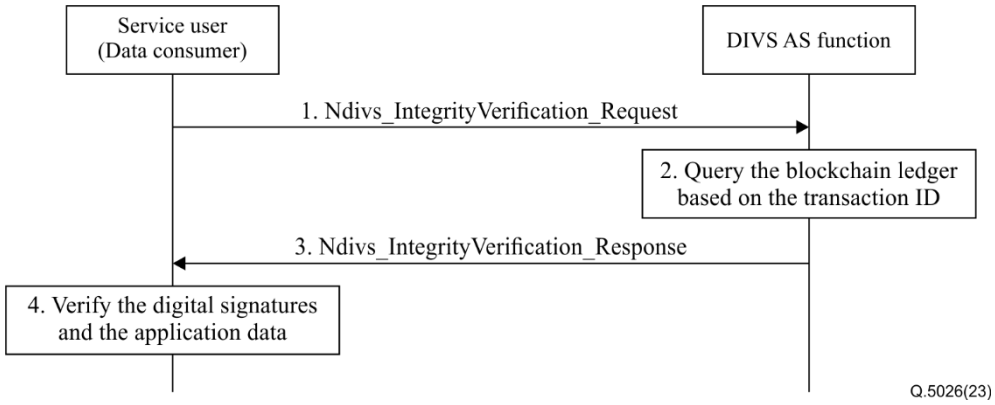

Figure 8-3 – Signalling flow for application data integrity verification

The application data integrity verification procedure in Figure 8-3 is used to obtain the data integrity verification parameters for the service user (i.e., data consumer) to verify if the received data is the raw data collected and if the data has been tampered with.

1) The service user sends the Ndivs_IntegrityVerification_Request message with the transaction ID to the DIVS AS function.
2) When receiving the Ndivs_IntegrityVerification_Request message, the DIVS AS function queries the blockchain ledger based on the transaction ID.
3) The DIVS AS function sends the Ndivs_IntegrityVerification_Response message with the endorsed integrity verification data.
4) When receiving the Ndivs_IntegrityVerification_Response message, the service user verifies the digital signature of the endorsed integrity verification data. Utilizing the public key and signature algorithm of the endorsed integrity verification data, the service user verifies the signature of the application data and validates the timestamp of the signature which is generated in the valid network account contract time of the terminal that collects the application data.

8.4 Signalling flow of event subscription from the DIVS AS function

The procedure in Figure 8-4 is used by the DIVS AS function to obtain the status update of the subscriber network account contract from the CEF by invoking the event subscription service. The service operations are as follows:

– Ncef_EventExposure_SubscribeRequest, which is used by a DIVS AS function to subscribe or modify a subscription in the CEF for event notification on status update of the subscriber network account contract. The Ncef_EventExposure_UnsubscribeRequest message is used to cancel the corresponding event subscription to the CEF.
– Nusm_EventExposure_SubscribeRequest, which is used by a CEF to subscribe or modify a subscription in the USM for event notification on status update of the subscriber network account contract. The Nusm_EventExposure_UnsubscribeRequest message is used to cancel the corresponding event subscription to the USM.
– Nusm_EventExposure_SubscribeResponse, which is used by the USM to return the event subscription result. The Nusm_EventExposure_UnsubscribeResponse message is used to return the result of cancelling the corresponding event subscription to the CEF.
– Ncef_EventExposure_SubscribeResponse, which is used by the CEF to return the event subscription result. The Ncef_EventExposure_UnsubscribeResponse message is used to

return the result of cancelling the corresponding event subscription to the DIVS AS function.

The events on status update of the subscriber network account contract include:

– Event of eSIM/SIM cancellation or inactivation;

– Event of subscriber network account cancellation;

– Event of unbinding of the USIM/eSIM with the IMEI;

– Event of unbinding of the eUICC with the eSIM;

– Event of unbinding of UICCID/eUICCID with the MSISDN;

– Event of applet cancellation or inactivation;

– Event of reservation.

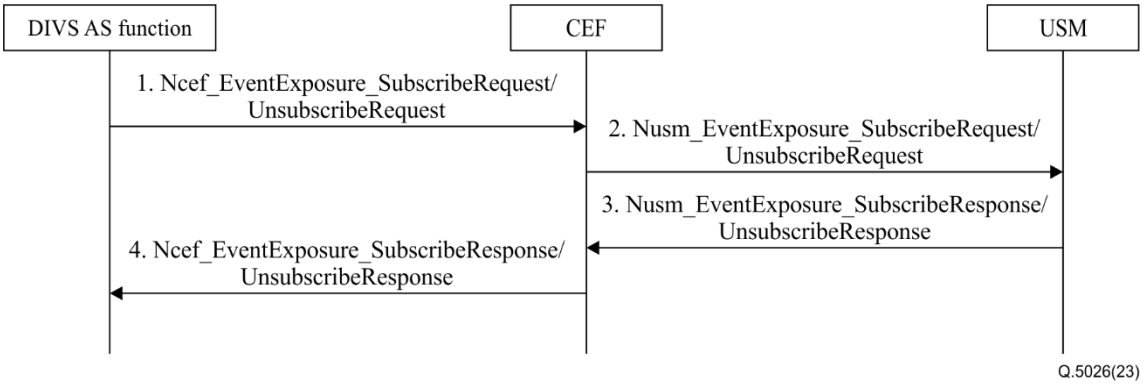

Figure 8-4 – Signalling flow of event subscription from DIVS AS function

1) The DIVS AS function subscribes/unsubscribes to the CEF for event notification on the status update of the subscriber network account contract.

2) The CEF subscribes/unsubscribes to the USM for event notification on status update of the subscriber network account contract.

3) The USM returns the event subscription result to the CEF.

4) The CEF returns the event subscription result to the USM.

8.5 Signalling flow for event notification to DIVS AS function

The procedure in Figure 8-5 is used by DIVS AS function to obtain the status update of the subscriber network account contract from the CEF through the event notification subscribed. The service operations are as follows:

– Nusm_EventExposure_Notify is used by the USM to notify the event with regard to the status update of the subscriber network account contract to the CEF which has subscribed to the corresponding event notification service. The Nusm_EventExposure_NotifyResponse message is used to indicate the success or failure of receiving the event notification.

– Ncef_EventExposure_Notify is used by the CEF to notify the event with regard to the status update of the subscriber network account contract to the DIVS AS function which has subscribed to the corresponding event notification service. The Ncef_EventExposure_NotifyResponse message is used to indicate the success or failure of receiving the event notification.

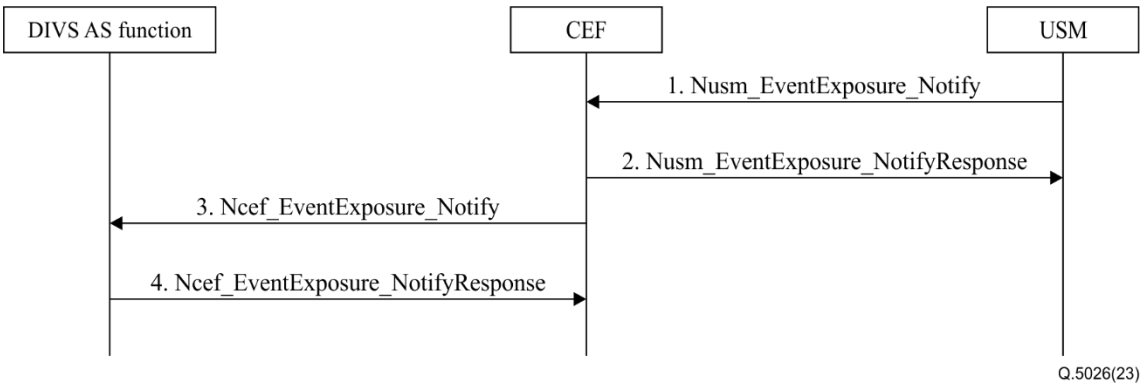

Figure 8-5 – Signalling flow of event notification to DIVS AS function

1) The USM notifies the event with regard to the status update of the subscriber network account contract to the CEF.
2) The CEF responses to the USM for indicating the success or failure of receiving the event notification.
3) The CEF notifies the event with regard to the status update of the subscriber network account contract to the DIVS AS function.
4) The DIVS AS function responses to the CEF for indicating the success or failure of receiving the event notification.

8.6 Signalling flow for synchronizing the endorsed integrity verification data

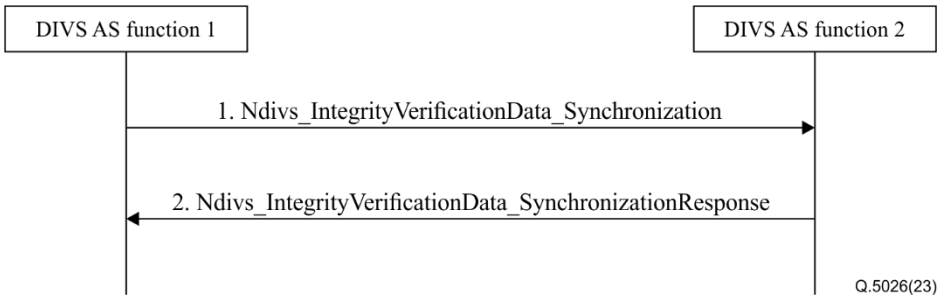

Figure 8-6 – Signalling flow for synchronizing the endorsed integrity verification data

The procedure in Figure 8-6 is used to synchronize the endorsed integrity verification data between the DIVS AS functions. The DIVS AS functions may not be connected directly but are connected over the blockchain ledger nodes.

1) The DIVS AS function 1 sends the Ndivs_IntegrityVerificationData_Synchronization message with the endorsed integrity verification data to the DIVS AS function 2 and synchronizes the records in the blockchain ledger.
2) The DIVS AS function 2 responses to the DIVS AS function 1 for indicating the success or failure of receiving the endorsed integrity verification data.

9 Message format

9.1 Integrity verification parameters registration

This message is sent to DIVS AS function to register the integrity verification parameters from the UE. The discovery of the DIVS AS function address could be set in the default configuration when provisioning the network service for the UE.

Table 9-1 describes the detailed information of Ndivs_DeviceMetadata_registration_request.

Table 9-1 – Ndivs_DeviceMetadata_registration_request

Information element	Status	Data type	Cardinality	Description
IMEI	M	String	1	Indicate the IMEI of the UE
UICCID	M	String	1	Indicate the UICCID of the UE, mutual exclusion with eUICCID
MSISDN	M	String	1	Indicate the MSISDN of the UE
eUICCID	M	String	1	Indicate the eUICCID of the UE, mutual exclusion with UICCID
Public key	M	String	1	Indicate the public key of the UE in this registration
Signature algorithms	M	String	1	Indicate the signature algorithms supported by the UE in this registration, e.g., ECDSA
Device serial number	M	String	1	Indicate the device serial number of the UE
Signature	M	String	1	Indicate the signature of the integrity verification parameters

Table 9-2 describes the detailed information of Ndivs_DeviceMetadata_registration_Response.

Table 9-2 – Ndivs_DeviceMetadata_registration_Response

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	201 400 500	Indicate the success or failure of the registration 201 Created 400 Input parameter error 500 Server internal error
TransactionID	M	String	1	N/A	Indicate the Transaction ID on the blockchain ledger that recorded the endorsed integrity verification data
URL	M	String	1	N/A	Indicate the entry URL to query the integrity verification data
Blockchain instance ID	O	String	1	N/A	Indicate the blockchain instance ID if multiple blockchain instances exist

9.2 Retrieve network account contract status of the UE

These messages are used to retrieve the network account contract status information of the UE from the USM via CEF. The network account contract status information would subsequently be used to generate the endorsing integrity verification data.

Table 9-3 describes the detailed information of Ncef_Subscribersdata_Request.

Table 9-3 – Ncef_Subscribersdata_Request

Information element	Status	Data type	Cardinality	Description
IMEI	O	String	1	Indicate the IMEI of the UE
UICCID	M	String	1	Indicate the UICCID of the UE, mutual exclusion with eUICCID
eUICCID	M	String	1	Indicate the eUICCID of the UE, mutual exclusion with UICCID
MSISDN	M	String	1	Indicate the MSISDN of the subscriber

Table 9-4 describes the detailed information of Nusm_Subscribersdata_Request.

Table 9-4 – Nusm_Subscribersdata_Request

Information element	Status	Data type	Cardinality	Description
IMEI	O	String	1	Indicate the IMEI of the UE
UICCID	M	String	1	Indicate the UICCID of the UE, mutual exclusion with eUICCID
eUICCID	M	String	1	Indicate the eUICCID of the UE, mutual exclusion with UICCID
MSISDN	M	String	1	Indicate the MSISDN of the subscriber

Table 9-5 describes the detailed information of Nusm_Subscribersdata_Response.

Table 9-5 – Nusm_Subscribersdata_Response

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	200 400 500	Indicate the success or failure of the subscriber data retrieval. 200 OK 400 Input parameter error 500 Server internal error
eUICCID	M	String	1	N/A	Indicate the eUICCID of the UE, mutual exclusion with UICCID
IMEI	M	String	1	N/A	Indicate the IMEI of the UE
MSISDN	M	String	1	N/A	Indicate the MSISDN of the subscriber
UICCID	M	String	1	N/A	Indicate the UICCID of the UE, mutual exclusion with eUICCID
Device owner entity name	M	String	1	N/A	Indicate the device owner entity name
Designated district	M	String	1	N/A	Indicate the designated network district for the UE access
Owner email	M	String	1	N/A	Indicate the owner email of the UE device

Table 9-5 – Nusm_Subscribersdata_Response

Information element	Status	Data type	Cardinality	Code value	Description
Device owner email	M	String	1	N/A	Indicate the device owner email
Network service provisioning time	M	String	1	N/A	Indicate network service provisioning time of the subscriber
Network contract termination time	M	String	1	N/A	Indicate network contract termination time of the subscriber
Latest update time of the network contract	M	String	1	N/A	Indicate latest update time of the network contract of the subscriber
Reservation	O	String[]	1	N/A	Indicate the information elements reserved

Table 9-6 describes the detailed information of Ncef_Subscribersdata_Response.

Table 9-6 – Ncef_Subscribersdata_Response

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	200 400 400	Indicates the success or failure of the subscriber data retrieval. 200 OK 400 Input Parameter Error 500 Server Internal Error
Device owner entity name	M	String	1	N/A	Indicate the device owner entity name
Designated district	M	String	1	N/A	Indicate the designated network district for the UE access
Owner email	M	String	1	N/A	Indicate the owner email of the UE device
eUICCID	M	String	1	N/A	Indicate the eUICCID of the UE, mutual exclusion with UICCID
IMEI	M	String	1	N/A	Indicate the IMEI of the UE device
MSISDN	M	String	1	N/A	Indicate the MSISDN of the subscriber
UICCID	M	String	1	N/A	Indicate the UICCID of the UE, mutual exclusion with eUICCID

Table 9-6 – Ncef_Subscribersdata_Response

Information element	Status	Data type	Cardinality	Code value	Description
Network service provisioning time	M	String	1	N/A	Indicate network service provisioning time of the subscriber
Network contract termination time	M	String	1	N/A	Indicate network contract termination time of the subscriber
Latest update time of the network contract	M	String	1	N/A	Indicate latest update time of the network contract of the subscriber
Reservation	O	String[]	1…N	N/A	Indicate the information elements reserved

9.3 Application data integrity verification

This message is sent to DIVA AS function to obtain the endorsed data integrity verification data.

Table 9-7 describes the detailed information of Ndivs_IntegrityVerification_Request.

Table 9-7 – Ndivs_IntegrityVerification_Request

Information element	Status	Data type	Cardinality	Description
TransactionID	M	String	1	Indicate the Transaction ID in the blockchain ledger record the endorsed integrity verification data requested

Table 9-8 describes the detailed information of Ndivs_IntegrityVerification_Response.

Table 9-8 – Ndivs_IntegrityVerification_Response

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	200 400 400	Indicates the success or failure of the data retrieval. 200 OK 400 Input parameter error 500 Server internal error
eUICCID	M	String	1	N/A	Indicate the eUICCID of the UE, mutual exclusion with UICCID
IMEI	M	String	1	N/A	Indicate the IMEI of the UE
MSISDN	M	String	1	N/A	Indicate the MSISDN of the subscriber
UICCID	M	String	1	N/A	Indicate the UICCID of the UE, mutual exclusion with eUICCID
Endorsed data integrity verification data	M	String[]	1…N	N/A	Indicate the endorsed integrity verification data

Table 9-8 – Ndivs_IntegrityVerification_Response

Information element	Status	Data type	Cardinality	Code value	Description
Signature of the endorsed data integrity verification data	M	String	1	N/A	Indicate the signature of the endorsed integrity verification data
DIVS AS certificate	M	String	1	N/A	Indicate the certificate of DIVS AS function
Network contract termination time	M	String	1	N/A	Indicate the network contract termination time of the subscriber

9.4 Event subscription from DIVS AS function

These messages are used to subscribe to the event notification of the status update of the subscriber network account contract for the DIVS AS function.

Table 9-9 describes the detailed information of Ncef_EventExposure_SubscribeRequest.

Table 9-9 – Ncef_EventExposure_SubscribeRequest

Information element	Status	Data type	Cardinality	Description
Event list	M	String	1	Indicate the event list the DIVS AS function subscribed
UE ID	M	String[]	1…N	Indicate the UE(s) that the DIVS AS function subscribes to event notification for
eventNotify ID	M	String	1	Indicate the notification correlation ID assigned by the DIVS AS function

Table 9-10 describes the detailed information of Nusm_EventExposure_SubscribeRequest.

Table 9-10 – Nusm_EventExposure_SubscribeRequest

Information element	Status	Data type	Cardinality	Description
Event list	M	String	1	Indicate the event list the CEF subscribed to
UE ID	M	String[]	1…N	Indicate the UE(s) that the CEF function subscribes to event notification for
eventNotify ID	M	String	1	Indicate the notification correlation ID assigned by the CEF

Table 9-11 describes the detailed information of Nusm_EventExposure_SubscribeResponse.

Table 9-11 – Nusm_EventExposure_SubscribeResponse

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	201 400 400	Indicate the success or failure of the event subscription. 201 Created 400 Input parameter error 500 Server internal error

Table 9-12 describes the detailed information of Ncef_EventExposure_SubscribeResponse.

Table 9-12 – Ncef_EventExposure_SubscribeResponse

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	201 400 400	Indicate the success or failure of the event subscription. 201 Created 400 Input parameter error 500 Server internal error

9.5 Event notification to DIVS AS function

These messages are used to obtain the status update of the subscriber network account contract through the event notification subscribed by the DIVS AS function.

Table 9-13 describes the detailed information of Nusm_EventExposure_Notify.

Table 9-13 – Nusm_EventExposure_Notify

Information element	Status	Data type	Cardinality	Description
eventNotify ID	M	Num	1	Indicate the notification correlation ID
eventNotify	M	Array[]	1...N	Indicate the notification events of the status update of the subscriber network account contract
Time information	M	String	1	Indicate the time information of observed events

Table 9-14 describes the detailed information of Nusm_EventExposure_NotifyResponse.

Table 9-14 – Nusm_EventExposure_NotifyResponse

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	200 400 400	Indicate the success or failure of receiving the event notification. 200 OK 400 Input parameter error 500 Server internal error

Table 9-15 describes the detailed information of Ncef_EventExposure_Notify.

Table 9-15 – Ncef_EventExposure_Notify

Information element	Status	Data type	Cardinality	Description
eventNotify ID	M	Num	1	Indicate the notification correlation ID
eventNotify	M	Array[]	1...N	Indicate the notification events of the status update of the subscriber network account contract
Time information	M	String	1	Indicate the time information of observed events

Table 9-16 describes the detailed information of Ncef_EventExposure_NotifyResponse.

Table 9-16 – Ncef_EventExposure_NotifyResponse

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	200 400 400	Indicate the success or failure of receiving the event notification. 200 OK 400 Input parameter error 500 Server internal error

9.6 Event notification to DIVS AS function

These messages are used to synchronize the endorsed integrity verification data between the DIVS AS functions.

Table 9-17 describes the detailed information of Ndivs_IntegrityVerificationData_Synchronization.

Table 9-17 – Ndivs_IntegrityVerificationData_Synchronization

Information element	Status	Data type	Cardinality	Description
DIVS AS function ID	M	String	1	Indicate the ID of the DIVS AS function
DIVS AS certificate	M	String	1	Indicate the certificate of the DIVS AS function
Endorsed integrity verification data	M	string[]	1	Indicate the endorsed integrity verification data
Signature of the endorsed integrity verification data	M	string	1	Indicate the signature of the endorsed integrity verification data

Table 9-18 describes the detailed information of Ndivs_IntegrityVerificationData_Synchronization Response.

Table 9-18 – Ndivs_IntegrityVerificationData_SynchronizationResponse

Information element	Status	Data type	Cardinality	Code value	Description
Results	M	Num	1	200 400 400	Indicate the success or failure of receiving the endorsed integrity verification data. 200 OK 400 Input parameter error 500 Server internal error

10 Security considerations

The security and privacy considerations in term of signalling and protocol of network-oriented data integrity verification service based on blockchain in IMT-2020 network include the following aspects.

End-to-end communication security, which includes the security considerations on the end-to-end secure connection established in different layers, message confidentiality and integrity, private key management, etc.

Authentication and authorization, which includes the security considerations on the authentication of accessing the functions descripted in clause 7, data access authorization, subscriber data privacy protection, etc.

Blockchain security, which includes security considerations on the communication between blockchain ledger nodes, multivendor blockchain interoperability, certificate management and so on. The additional blockchain security consideration can be optionally aligned with the capability requirements specified in [b-ITU-T X.1402] [ITU-T Y.2342].

In addition, the security and privacy considerations in term of signalling and protocol of network-oriented DIVS based on blockchain can be optionally aligned with the security requirements specified in [ITU-T Y.3105] [ITU-T Y.3108].

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

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