International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5024

(02/2022)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

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

Protocol for providing intelligent analysis services in IMT-2020 networks

Recommendation ITU-T Q.5024

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
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.5024

Protocol for providing intelligent analysis services in IMT-2020 networks

Summary

Recommendation ITU-T Q.5024 specifies architecture for supporting intelligent analysis services in IMT-2020 networks, and intelligent analysis services offered by the data analysis function (DAF) including load balancing, network functions fault location and advance warning, device on/off analysis, mobility analysis, etc. It includes signalling flows for network functions (NFs) event exposure to DAF and DAF analytics exposure to NFs, message formats, and security considerations.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Q.5024	2022-02-13	11	11.1002/1000/14926

Keywords

IMT-2020 network, intelligent analysis services.

[*] 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 Q.5024

Protocol for providing intelligent analysis services in IMT-2020 networks

1 Scope

This Recommendation specifies signalling architecture and protocol for providing intelligent analysis services in IMT-2020 networks. It specifies an architecture concept, signalling flows between the data analysis function (DAF) and other functions, message formats and 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 Q.5023] Recommendation ITU-T Q.5023 (2021), *Protocol for managing intelligent network slicing with AI-assisted analysis in IMT-2020 networks*.

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

[IETF RFC 6749] IETF RFC 6749 (2012), *OAuth2.0 authorization framework*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 data analysis function (DAF) [ITU-T Q.5023]: A network function that can collect, analyse, and provide data from/to International Mobile Telecommunications 2020 (IMT-2020) core network functions, network management and third-party applications.

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

3.1.3 management [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at fulfilment, assurance, and billing of services, network functions, and resources in both physical and virtual infrastructure including compute, storage, and network resources.

3.1.4 network function [b-ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

3.1.5 network slice [b-ITU-T Y.3100]: A logical network that provides specific network capabilities and network characteristics.

NOTE 1 – Network slices enable the creation of customized networks to provide flexible solutions for different market scenarios which have diverse requirements, with respect to functionalities, performance and resource allocation.

NOTE 2 – A network slice may have the ability to expose its capabilities.

NOTE 3 – The behaviour of a network slice is realized via network slice instance(s).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF	Application Function
CEF	Capability Exposure Function
DAF	Data Analysis Function
MS	Management System
NACF	Network Access Control Function
NF	Network Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDU	Protocol Data Unit
QoS	Quality of Service
RRC	Radio Resource Control
SMF	Session Management Function
UE	User Equipment
UP	User Plane
UPF	User Plane Function

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 Recommendation 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 this Recommendation.

The keywords "M" indicate the element is mandatory. The keywords "O" indicate the element is optional. The keywords "C" indicate the element is conditional.

6 Architecture for supporting intelligent analysis services in IMT-2020 network

Data analysis function (DAF) is defined in [ITU-T Q.5023], and DAF introduced in IMT-2020 networks [ITU-T Y.3104] can provide intelligent analysis services. Intelligent analysis services offered by DAF include load balancing, network function (NF) fault location and warning, device on/off analysis, mobility analysis, energy saving analysis, etc. It is necessary to enable network automation and intelligence. Figure 6-1 depicts an architecture reference model for supporting intelligent analysis services in IMT-2020 networks.

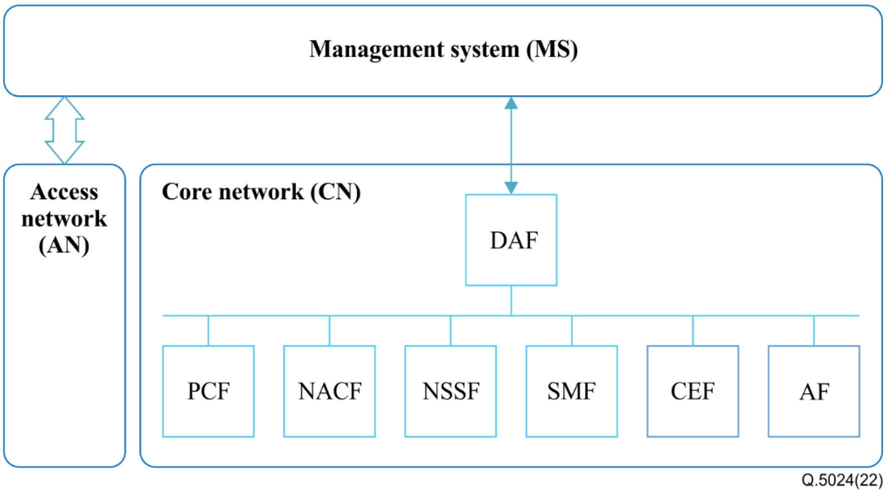

Figure 6-1 – Architecture reference model for supporting intelligent analysis services in IMT-2020 networks

DAF collects data from other functions such as policy control function (PCF), session management function (SMF), capability exposure function (CEF), application function (AF), etc. and provides intelligent analysis results to other functions (PCF, SMF, CEF, AF, etc.). Intelligent analysis information includes statistical information or forecast trend information based on a large amount of historical data.

For a specific intelligent analysis service, DAF is required to collect multiple types of data from different data providers:

– collects user equipment (UE) location, amount of UEs, UE mobility related data, UE behavioural parameters, etc. from the network access control function (NACF), as a basis of analysis for user data congestion, network performance, UE mobility, abnormal behaviour, etc.;

– collects user plane (UP) path change, UE IP address change, protocol data unit (PDU) session establishment/release, UE behavioural parameters, anomaly events, etc. from the session management function (SMF), as a basis of analysis for UP load analysis, UE abnormal behaviour, signalling congestion status, etc.;

– collects policy control events, anomaly events, etc. from PCF, as a basis of analysis for load balancing, network performance, network resource allocation, etc.;

– collects service data related to UE mobility, exceptions information, service experience related data, etc. from AF directly or via CEF, as a basis of analysis for UE mobility, abnormal behaviour, service experience, etc.;

– collects UE mobility information, load data (e.g., current load data, historical load data), performance measurements (e.g., UE throughput, radio resource control (RRC) connection number, and radio resource utilization), cells and the neighbourhood areas which means the distance between stations are within a certain range, cell fault event(s) related to the management data, environmental information (e.g., weather and special events), etc. from the management system (MS), as a basis of analysis for UE mobility, NF load level, user data congestion, energy saving, device on/off analysis, etc.;

DAF can:

– subscribe EventSubscription services to collect data on a set of events;

– subscribe, modify and unsubscribe for event(s) related to UE access and mobility information and be notified of the related event(s) based on corresponding subscriptions by using NacfEventSubscription service;

- subscribe, modify and unsubscribe for event(s) related to PDU sessions and be notified of the related event(s) based on corresponding subscriptions by using SmfEventSubscription service;
- subscribe, modify and unsubscribe for event(s) related to policy control and be notified of the related event(s) based on corresponding subscription by using PcfEventSubscription service;
- subscribe, modify and unsubscribe for event(s) related to service data for an application (e.g., application communication information, exceptions information) and be notified of the related event(s) based on corresponding subscriptions by using AfEventSubscription service;
- subscribe, modify and unsubscribe for event(s) related to service data for an application when it is untrusted and be notified of the related event(s) based on corresponding subscriptions by using CefEventSubscription service;
- subscribe, modify and unsubscribe for performance measurement information, cells and the neighbourhood areas information, environmental information and fault event(s) related to the management data and be notified of the related event(s) based on corresponding subscription by using MsEventSubscription service.

7 Signalling flow

7.1 Signalling flow for event exposure to DAF

7.1.1 General description

The data collection process allows DAF to collect data from various sources (e.g., NF such as SMF, PCF, NACF and AF (possibly via CEF); MS), as a basis for network analysis by using EventSubscription services.

7.1.2 Signalling flow for NF event exposure to DAF

7.1.2.1 Signalling flow for SMF event exposure to DAF

The procedure in Figure 7-1 is used by DAF to collect data on event(s) related to SMF by invoking SmfEventSubscription service.

SmfEventSubscription service includes service operations as follows:

- SmfEventSubscription_Subscribe, which is used by a data requester such as DAF to subscribe to, or modify a subscription in the SMF for event notifications on sessions management.
- SmfEventSubscription_Unsubscribe, which is used by a data requester such as DAF to cancel a subscription in the SMF for event notifications on sessions management.
- SmfEventSubscription_Notify, which is used by SMF to report event(s) related to PDU Sessions to the requester which has subscribed to the event report service.

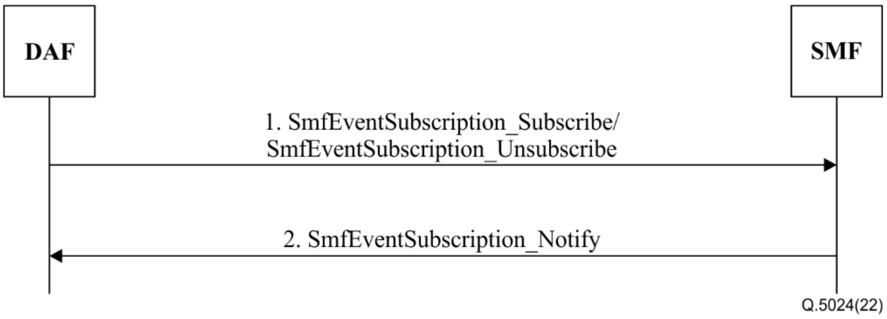
DAF
SMF
1. SmfEventSubscription_Subscribe/
SmfEventSubscription_Unsubscribe
2. SmfEventSubscription_Notify
Q.5024(22)

Figure 7-1 – Signalling flow for data collection based on events subscription from SMF

1) The DAF subscribes to or unsubscribes from a (set of) events (e.g., UE IP address change, UP path change, PDU session establishment/release, etc.) by invoking the SmfEventSubscription_Subscribe service operation.

2) The SMF notifies the DAF (e.g., with the event report) by invoking SmfEventSubscription_Notify service operation.

7.1.2.2 Signalling flow for PCF event exposure to DAF

The procedure in Figure 7-2 is used by DAF to collect data on event(s) related to the PCF by invoking PcfEventSubscription service.

PcfEventSubscription service includes service operations as follows:

– PcfEventSubscription_Subscribe, which is used by a data requester (such as DAF) to subscribe or modify a subscription in the PCF for event notification on policy control.

– PcfEventSubscription_Unsubscribe, which is used by a data requester (such as DAF) to cancel a subscription in the PCF for event notifications on policy control.

– PcfEventSubscription_Notify, which is used by PCF to report subscribed policy control event(s) to the requester of subscribed event reporting services.

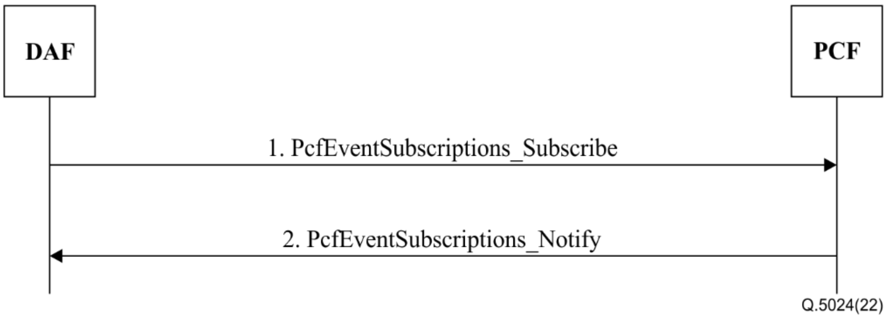
DAF
PCF
1. PcfEventSubscriptions_Subscribe
2. PcfEventSubscriptions_Notify
Q.5024(22)

Figure 7-2 – Signalling flow for data collection based on events subscription from PCF

1) The DAF subscribes to or unsubscribes from the policy control events by invoking PcfEventSubscriptions_Subscribe to create a new subscription and modify an existing subscription.

2) The PCF notifies the DAF by invoking a PcfEventSubscriptions_Notify operation.

7.1.2.3 Signalling flow for AF event exposure to DAF

The procedure in Figure 7-3 is used by DAF to collect data on event(s) related to AF by invoking AfEventSubscription service.

AfEventSubscription service includes service operations as follows:

- AfEventSubscription_Subscribe, which is used by a data requester (such as DAF) or via the CEF to subscribe or modify a subscription in the AF for event notifications on service data for an application, application communication information, exceptions information, UE mobility, abnormal behaviour, service experience, and so on.
- AfEventSubscription_Unsubscribe, which is used by a data requester (such as DAF) or via the CEF to cancel a subscription in the AF for event notifications on application communication information, exceptions information, UE mobility, abnormal behaviour, service experience, etc.
- AfEventSubscription_Notify, which is used by the AF to report application communication information, exceptions information, UE mobility, abnormal behaviour, service experience, etc. to the requester which has subscribed to the event report service.

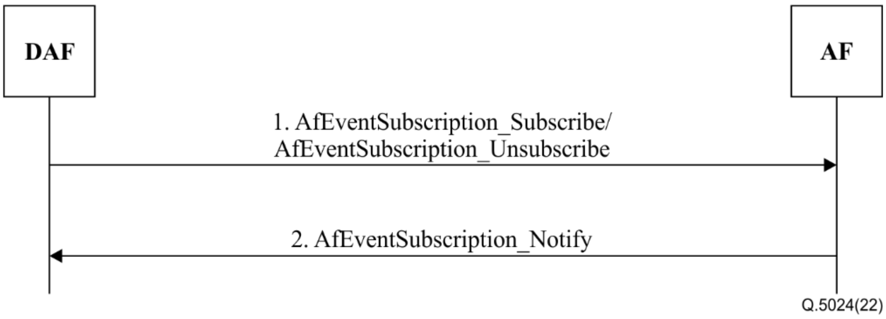
DAF
AF
1. AfEventSubscription_Subscribe/
AfEventSubscription_Unsubscribe
2. AfEventSubscription_Notify
Q.5024(22)

Figure 7-3 – Signalling flow for data collection based on events subscription from AF

1) The DAF subscribes to or unsubscribes from a (set of) events (e.g., UE mobility information, UE communication information, expected UE behavioural information, service experience, etc.) by invoking the AfEventSubscription_(un)Subscribe service operation.

2) The AF notifies the DAF (e.g., with the event report) by invoking AfEventSubscription_Notify service operation.

7.1.2.4 Signalling flow for CEF event exposure to DAF

The procedure in Figure 7-4 is used by DAF to interact with CEF by invoking CefEventSubscription service.

CefEventSubscription service includes service operations as follows:

- CefEventSubscription_Subscribe, which is used by a data requester (such as DAF) to subscribe or modify the subscription in CEF to obtain event notification of specified application or user related events on application communication information, exceptions information, UE mobility, abnormal behaviour and service experience.
- CefEventSubscription_Unsubscribe, which is used by a data requesters (such as DAF) to cancel a subscription of event notification on application communication information, exceptions information, UE mobility, abnormal behaviour and service experience.
- CefEventSubscription_Notify, which is used by CEF to report application or user related events on application communication information, exceptions information, UE mobility, abnormal behaviour and service experience to requesters which have subscribed to the event report service.

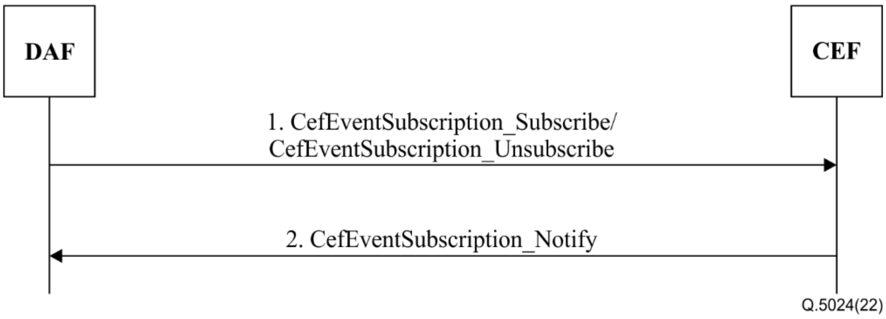
DAF
CEF
1. CefEventSubscription_Subscribe/
CefEventSubscription_Unsubscribe
2. CefEventSubscription_Notify
Q.5024(22)

Figure 7-4 – Signalling flow for interacting with CEF to collect data from AF based on events subscription

1) The DAF (un)subscribes to a (set of) events related to AF (e.g., service experience, UE mobility, UE communication, exceptions and so on.) by invoking the CefEventSubscription_(un)Subscribe service operation.

2) The CEF notifies the DAF (e.g., with the event report) by invoking CefEventSubscription_Notify service operation.

7.1.2.5 Signalling flow for NACF event exposure to DAF

The procedure in Figure 7-5 is used by DAF to collect data on event(s) related to NACF by invoking NacfEventSubscription service.

NacfEventSubscription service includes service operations as follows:

– NacfEventSubscription_Subscribe, which is used by a data requester such as DAF to subscribe to, or modify a subscription in the NACF for event notifications on UE access and mobility related event(s).

– NacfEventSubscription_Unsubscribe, which is used by a data requester such as DAF to cancel a subscription in the NACF for event notifications on UE access and mobility related event(s).

– NacfEventSubscription_Notify, which is used by NACF to report UE access and mobility related event(s) to the requester which has subscribed to the event report service.

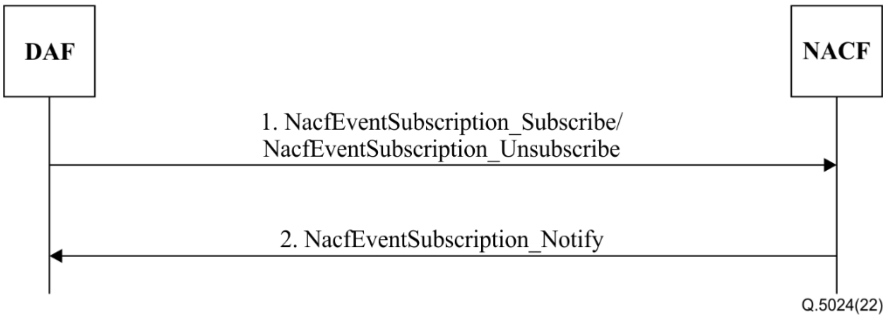
DAF
NACF
1. NacfEventSubscription_Subscribe/
NacfEventSubscription_Unsubscribe
2. NacfEventSubscription_Notify
Q.5024(22)

Figure 7-5 – Signalling flow for data collection based on events subscription from NACF

1) The DAF subscribes to or unsubscribes from a (set of) events (e.g., UE location, amount of UEs, UE mobility related data, etc.) by invoking the NacfEventSubscription_Subscribe service operation.

2) The NACF notifies the DAF (e.g., with the event report) by invoking NacfEventSubscription_Notify service operation.

7.1.3 Signalling flow for MS event exposure to DAF

The procedure in Figure 7-6 is an abstraction of the MS performance data report management service, which is used by DAF to collect data on event(s) related to MS service by invoking MsEventSubscription service.

MsEventSubscription service includes service operations as follows:

- MsEventSubscription_Subscribe, which is used by a data requester such as DAF to subscribe to, or modify a subscription in the MS for event notifications on load data, performance measurements, cells and the neighbourhood areas information, environmental information and cell fault event(s) related to the management data.
- MsEventSubscription_Unsubscribe, which is used by a data requester such as DAF to cancel a subscription in the MS for event notifications on load data, performance measurements, cells and the neighbourhood areas information, environmental information and cell fault event(s) related to the management data.
- MsEventSubscription_Notify, which is used by MS to report load data, performance measurements, cells and the neighbourhood areas information, environmental information and cell fault event(s) related to the management data to the requester which has subscribed to the event report service.

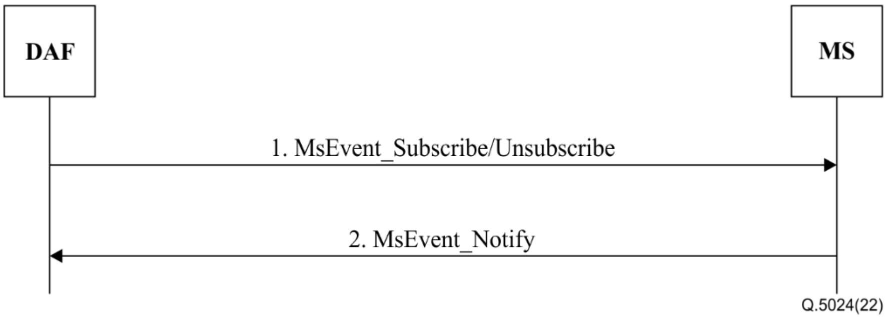

Figure 7-6 – Signalling flow for data collection based on events subscription from MS

1) The DAF subscribes to or unsubscribes from load data, the performance measurement information, cells and the neighbourhood areas information, environmental information and fault events by invoking MsEvent_Subscribe service operation.

2) The MS notifies the DAF with the requested load data, measurement information, cells and the neighbourhood areas information, environmental information and fault events, and performs the tasks that may include data processing by invoking MsEvent_Notify service operation.

7.2 Signalling flow for DAF analytics exposure to NFs

7.2.1 Signalling flow for Analytics Subscribe/Unsubscribe

The procedure in Figure 7-7 is used by NF service consumers (e.g., SMF, PCF, AF, CEF, NACF, MS, etc.) to subscribe to or unsubscribe from the notification for analytics information from DAF by invoking DafAnalysisSubscriptions service.

DafAnalysisSubscriptions service includes service operations as follows:

- DafAnalysisSubscriptions_Subscribe, which is used by a NF consumer to subscribe to, or modify a subscription for analysis notifications on a specified application related event.
  - For SMF, these analysis notifications may include load information of the user plane function (UPF).
  - For PCF, these analysis notifications may include the network resource allocation policy, traffic control policy, transmission strategy and QoS policy.

  - For AF, these analysis notifications may include UE mobility information, abnormal behaviour and service experience.
  - For CEF, these analysis notifications may include UE mobility information, abnormal behaviour and service experience.
  - For NACF, these analysis notifications may include UE access and mobility information and load information of SMF.
  - For MS, these analysis notifications may include performance measurement information, NF load information and fault events.
- DafAnalysisSubscriptions_Unsubscribe, which is used by a NF consumer to cancel a subscription from analytic events.
- DafAnalysisSubscriptions_Notify, which is used by DAF to report analytics related to observed events which have subscribed to the event analysis service.

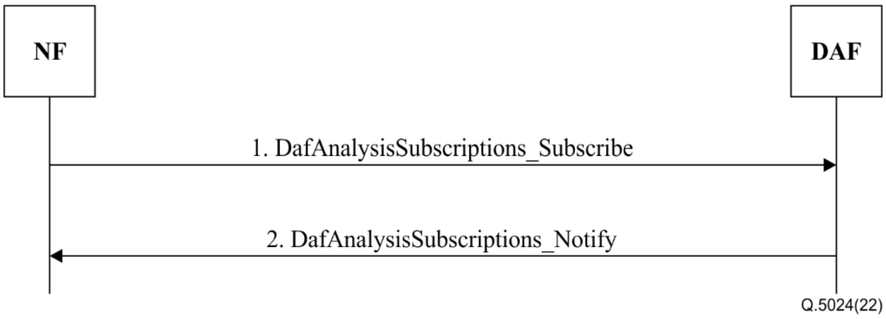
NF
DAF
1. DafAnalysisSubscriptions_Subscribe
2. DafAnalysisSubscriptions_Notify
Q.5024(22)

Figure 7-7 – Signalling flow for analytics subscribe/unsubscribe from DAF

1) The NF subscribes to or unsubscribes from a (set of) data analytic events by invoking the DafAnalysisSubscriptions_Subscribe service operation.

- Subscription requirements of data analytic events may include:
  - Load information of UPF for SMF.
  - Analysis of network resource allocation policy, traffic control policy, transmission strategy and QoS policy for PCF.
  - UE mobility information, abnormal behaviour and service experience for AF and CEF.
  - UE access and mobility information and load information of SMF for NACF.
  - Performance measurement information, cells and the neighbourhood areas information, environmental information, NF load information, energy saving policy, device on/off analysis and fault events for MS.

2) The DAF notifies the NF and MS about analysis events by invoking DafAnalysisSubscriptions_Notify service operation.

7.2.2 Signalling flow for analytics request

This procedure describes signalling flow in NF for analytics request.

The procedure in Figure 7-8 is used by NF service consumers (e.g., SMF, PCF, AF, CEF, NACF, MS, etc.) to request analytics information from DAF by invoking DafAnalysis_Request service.

DafAnalysisRequest service includes service operations as follows:

- DafAnalysis_Request, which is used by a NF consumer to request the analytics report from DAF, such as mobility analysis and prediction, load analysis and prediction, NF fault location and warning, device on/off analysis, network performance analysis and prediction, abnormal behaviour, etc.
  - For SMF, the analytics report from DAF may include load information of UPF.

  - For PCF, the analytics report from DAF may include the network resource allocation policy, traffic control policy, transmission strategy and QoS policy.
  - For AF, the analytics report from DAF may include UE mobility information, abnormal behaviour and service experience.
  - For CEF, the analytics report from DAF may include UE mobility information, abnormal behaviour and service experience.
  - For NACF, the analytics report from DAF may include UE access and mobility information and load information of SMF.
  - For MS, the analytics report from DAF may include performance measurement information, cells and the neighbourhood areas information, environmental information, NF load information, energy saving policy, device on/off analysis and fault events.
- DafAnalysis_Response, which is used by DAF to report analytics which have been requested by NF consumers.

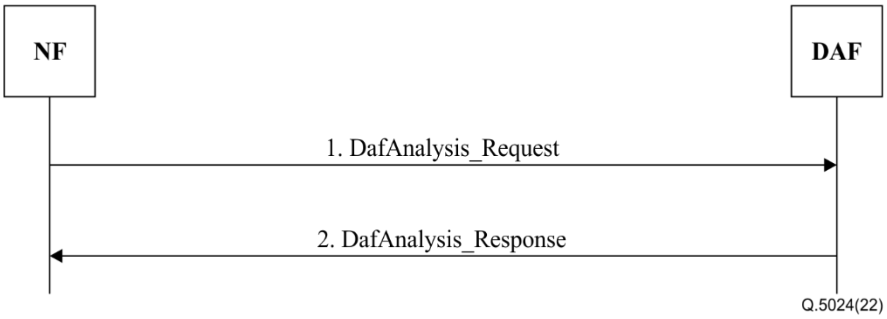

Figure 7-8 – Signalling flow for analytics request from DAF

1) NF service consumer requests the analytics report from DAF by invoking DafAnalysis_Request service on related event.

- Requirements of the analytics report from DAF may include:
  - Load information of UPF for SMF.
  - Analysis of network resource allocation policy, traffic control policy, transmission strategy and QoS policy for PCF.
  - UE mobility information, abnormal behaviour and service experience for AF and CEF.
  - UE access and mobility information and load information of SMF for NACF.
- Performance measurement information, cells and the neighbourhood areas information, environmental information, NF load information, energy saving policy, device on/off analysis and fault events for MS.

2) The DAF notifies the NF and MS of the specific analytics by invoking DafAnalysis_Response service.

8 Message format

8.1 SMF event exposure

This message is sent to SMF to subscribe for events on PDU sessions. Table 8-1 describes the information details of SmfEventSubscription_Subscribe:

Table 8-1 – SmfEventSubscription_Subscribe

Information element	Status	Data type	Cardinality	Description
event list	M	string	1…N	Identity list of event of the SMF which data requester (e.g., DAF) subscribes.
UE ID	O	array	1…N	Identity the UE(s) that data requester (e.g., DAF) subscribes to related information.
eventNotify ID	M	string	1	Notification correlation ID assigned by the requester (e.g., DAF).
time window	M	string	1	Time window of event notification.
NotifReq	M	string	1	Indicates the event notification requirements for session management related events of the subscription.
NotifMeth	O	string	0..1	Indicates the notification method (periodic, one time, on event detection).
MaxRepNum	O	Uinteger	0..1	Indicates the maximum number of reports, after which the subscription ceases to exist (that is, the end of the report). If omitted, there is no limit.
MonTime	C	string	0..1	Indicates the monitoring time when the subscription ceases to exist, after which SMF shall not send any event notifications and the subscription becomes invalid. If omitted, the subscription has no time limit.
RepPeriod	O	string	0..1	Indicates repetition period for periodic reporting.
ImmRep	O	boolean	0..1	Indicates immediate reporting of the subscribed events when it is set to true. Otherwise, reporting will occur when the event is detected.

Table 8-2 describes the information details of SmfEventSubscription_Notify:

Table 8-2 – SmfEventSubscription_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the event exposure subscription. 200 OK 400 input parameter error 500 server internal error
eventNotify ID	M	string	1	N/A	Indicates the notification correlation ID, which identifies the subscription corresponding to the event notification from SMF.
eventNotify	M	array	1..N	N/A	Indicates the notification events, such as expected UE behavioural information, UE IP address change, UP path change and other session management related events.
Time information	M	string	1	N/A	Indicates the time information of observed related events.

8.2 PCF event exposure

This message is sent to PCF to subscribe for events on policy control. Table 8-3 describes the information details of PcfEventSubscriptions_Subscribe:

Table 8-3 – PcfEventSubscriptions_Subscribe

Information element	Status	Data type	Cardinality	Description
event list	M	string	1	Identity list of exposure events of PCF which DAF requires to subscribe.
eventNotify ID	M	string	1	Notification correlation ID assigned by the requester (e.g., DAF).
NotifReq	M	string	1	Indicates the event notification requirements for policy control related events of the subscription.
NotifMeth	O	string	0..1	Indicates the notification method (periodic, one time, on event detection).
MaxRepNum	O	Uinteger	0..1	Indicates the maximum number of reports, after which the subscription ceases to exist (that is, the end of the report). If omitted, there is no limit.
MonTime	C	string	0..1	Indicates the monitoring time when the subscription ceases to exist, after which PCF shall not send any event notifications and the subscription becomes invalid. If omitted, the subscription has no time limit.
RepPeriod	O	string	0..1	Indicates repetition period for periodic reporting.
DataCollectionFreq	O	string	1..N	This IE indicates frequency for data collection.
time window	M	string	1	Time window of event exposure report.

Table 8-4 describes the information details of PcfEventSubscriptions_Notify:

Table 8-4 – PcfEventSubscriptions_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the event exposure subscription. 200 OK 400 input parameter error 500 server internal error
eventNotify ID	M	string	1	N/A	Indicates the notification correlation ID, which identifies the subscription corresponding to the event notification from PCF.
eventNotify	M	array	1..N	N/A	Indicates the notification events, such as policy control events, anomaly events.
Time information	M	string	1	N/A	Indicates the time information of observed related events.

8.3 AF event exposure

This message is sent to AF to subscribe for application events. Table 8-5 describes the information details of AfEventSubscription_Subscribe:

Table 8-5 – AfEventSubscription_Subscribe

Information element	Status	Data type	Cardinality	Description
event list	M	string	1…N	Identity list of events of AF to which data requester (e.g., DAF) subscribes.
UE ID	O	array	1…N	Identity of the UE(s) that data requester (e.g., DAF) subscribes to relate information.
eventNotify ID	M	string	1	Notification correlation ID assigned by the data requester (e.g., DAF).
time window	M	string	1	Time window of event notification.
NotifReq	M	string	1	Indicates the event notification requirements for service and application related events of the subscription.
App ID	O	string	1..N	Identity information of the application data subscribed to by the data requester (e.g., DAF).
NotifMeth	O	string	0..1	Indicates the notification method (periodic, one time, on event detection).
MaxRepNum	O	Uinteger	0..1	Indicates the maximum number of reports, after which the subscription ceases to exist (that is, the end of the report). If omitted, there is no limit.
MonTime	C	string	0..1	Indicates the monitoring time when the subscription ceases to exist, after which AF shall not send any event notifications and the subscription becomes invalid. If omitted, the subscription has no time limit.
RepPeriod	O	string	0..1	Indicates repetition period for periodic reporting.
ImmRep	O	boolean	0..1	Indicates immediate reporting of the subscribed events when it is set to true. Otherwise, reporting will occur when the event is detected.

Table 8-6 describes the information details of AfEventSubscription_Notify:

Table 8-6 – AfEventSubscription_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the event exposure subscription. 200 OK 400 Input Parameter Error 500 Server Internal Error
eventNotify ID	M	string	1	N/A	Indicates the notification correlation ID, which identifies the subscription corresponding to the notification.
eventNotify	M	array	1..N	N/A	Indicates the notification events, such as service experience information about the application, UE flow information about the application, application communication information and abnormal behaviour information of service flow.
Time information	M	string	1	N/A	Indicates the time information of observed related events.

8.4 CEF event exposure

This message is sent to CEF to subscribe for application events. Table 8-7 describes the information details of CefEventSubscription_Subscribe:

Table 8-7 – CefEventSubscription_Subscribe

Information element	Status	Data type	Cardinality	Description
event list	M	string	1…N	Identity list of events of CEF to which data requester (e.g., DAF) subscribes.
UE ID	O	array	1…N	Identity the UE that data requester (e.g., DAF) subscribes to relate information.
eventNotify ID	M	string	1	Notification correlation ID assigned by the data requester (e.g., DAF).
time window	M	string	1	Time window of event notification.
NotifReq	M	string	1	Indicates the event notification requirements for service and application related events of the subscription.
NotifMeth	O	string	0..1	Indicates the notification method (periodic, one time, on event detection).
MaxRepNum	O	Uinteger	0..1	Indicates the maximum number of reports, after which the subscription ceases to exist (that is, the end of the report). If omitted, there is no limit.
MonTime	C	string	0..1	Indicates the monitoring time when the subscription ceases to exist, after which CEF shall not send any event notifications and the

Table 8-7 – CefEventSubscription_Subscribe

Information element	Status	Data type	Cardinality	Description
				subscription becomes invalid. If omitted, the subscription has no time limit.
RepPeriod	O	string	0..1	Indicates repetition period for periodic reporting.
ImmRep	O	string	0..1	Indicates immediate reporting of the subscribed events when it is set to true. Otherwise, reporting will occur when the event is detected.

Table 8-8 describes the information details of CefEventSubscription_Notify:

Table 8-8 – CefEventSubscription_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the event exposure subscription. 200 OK 400 input parameter error 500 server internal error
eventNotify ID	M	string	1	N/A	Indicates the notification correlation ID, which identifies the subscription corresponding to the notification.
eventNotify	M	array	1..N	N/A	Indicates the notification events, such as service experience information about the application, UE flow information about the application, application communication information, etc. (from AF to the data requester when AF is untrusted.)
Time information	M	string	1	N/A	Indicates the time information of observed related events.

8.5 NACF event exposure

This message is sent to NACF to subscribe for events related to UE access and mobility. Table 8-9 describes the information details of NacfEventSubscription_Subscribe:

Table 8-9 – NacfEventSubscription_Subscribe

Information element	Status	Data type	Cardinality	Description
event list	M	string	1…N	Identity list of event of NACF to which data requester (e.g., DAF) subscribes e.g., UE location, number of UEs and UE mobility related data.
UE ID	O	array	1…N	Identity the UE that data requester (e.g., DAF) subscribes to relate information
eventNotify ID	M	string	1	Notification correlation ID assigned by the data requester (e.g., DAF).
time window	M	string	1	Time window of event notification.
NotifReq	M	string	1	Indicates the event notification requirements for mobility management related events of the subscription.
NotifMeth	O	string	0..1	Indicates the notification method (periodic, one time, on event detection).
MaxRepNum	O	Uinteger	0..1	Indicates the maximum number of reports, after which the subscription ceases to exist (that is, the end of the report). If omitted, there is no limit.
MonTime	C	string	0..1	Indicates the monitoring time when the subscription ceases to exist, after which NACF shall not send any event notifications and the subscription becomes invalid. If omitted, the subscription has no time limit.
RepPeriod	O	string	0..1	Indicates repetition period for periodic reporting.
ImmRep	O	string	0..1	Indicates immediate reporting of the subscribed events when it is set to true. Otherwise, reporting will occur when the event is detected.

Table 8-10 describes the information details of NacfEventSubscription_Notify:

Table 8-10 – NacfEventSubscription_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the event exposure subscription. 200 OK 400 input parameter error 500 internal server error
eventNotify ID	M	string	1	N/A	Indicates the notification correlation ID, which identifies the subscription corresponding to the notification.
eventNotify	M	array	1..N	N/A	Indicates the notification events, such as location report information, expected UE behavioural information (UE mobility and/or UE communication), etc.
Time information	M	string	1	N/A	Indicates the time information of observed related events.

8.6 MS event exposure

This message is sent to MS to subscribe for events related to performance data report. Table 8 -11 describes the information details of MsEvent_Subscribe:

Table 8-11 – MsEvent_Subscribe

Information element	Status	Data type	Cardinality	Description
event list	M	string	1…N	Identity list of event of performance measurement information to which data requester (e.g., DAF) subscribes. e.g., rate, bandwidth, throughput, latency, round trip time, number of UEs, PRB utilization, radio resource control (RRC) connection number, cells priority, cells and nationhood area information, traffic service type, and environmental information.
UE ID	O	array	1…N	Identity the UE that data requester (e.g., DAF) subscribes to relate information
time window	M	string	1	Time window of event notification.
NotifReq	M	string	1	Indicates the event notification requirements for specific management events of the subscription.
NotifMeth	O	string	0..1	Indicates the notification method (periodic, one time, on event detection).
ImmRep	O	string	0..1	Indicates immediate reporting of the subscribed events when it is set to true. Otherwise, reporting will occur when the event is detected.

Table 8-12 describes the information details of MsEvent_Notify:

Table 8-12 – MsEvent_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the event exposure subscription. 200 OK 400 input parameter error 500 internal server error
eventNotify ID	M	string	1	N/A	Indicates the notification correlation ID, which identifies the subscription corresponding to the notification.
eventNotify	M	array	1..N	N/A	Indicates the notification events, such as rate, bandwidth, throughput, latency, round trip time, number of UEs, etc.
Time information	M	string	1	N/A	Indicates the time information of observed related management events.

8.7 DAF event exposure

This message is sent to NF consumer to subscribe for events related to specific analytics and prediction. Table 8-13 describes the information details of DafEventSubscription_Subscribe:

Table 8-13 – DafEventSubscription_Subscribe

Information element	Status	Data type	Cardinality	Description
AnalysisEvent ID	M	string	1	Identify events related to specific analytics service for a subscription.
time window	M	string	1	Time window of event notification.
AnalysisAccuracy	M	string	1	Indicates the required accuracy of the analytics and prediction.
AnalysisReq	M	string	1	Indicates the event analysis requirements of the subscription.
NotifMeth	O	string	0..1	Indicates the notification method (periodic, one time, on event detection).
MaxRepNum	O	Uinteger	0..1	Indicates the maximum number of reports, after which the subscription ceases to exist (that is, the end of the report). If omitted, there is no limit.
MonTime	C	string	0..1	Indicates the monitoring time when the subscription ceases to exist, after which DAF shall not send any event notifications and the subscription becomes invalid. If omitted, the subscription has no time limit.
RepPeriod	O	string	0..1	Indicates repetition period for periodic reporting.
ImmRep	O	string	0..1	Indicates immediate reporting of the subscribed events analysis is ready.
LoadThreshold	C	string	0..1	Indicates that DAF should report the network slice load situation to the NF consumer when it is reached.
CongestionLevel	C	string	0..1	Indicates the congestion threshold levels if the subscribed event is user data congestion. Otherwise, it is optional.

Table 8-14 describes the information details of DafEventSubscription_Notify:

Table 8-14 – DafEventSubscription_Notify

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure of the subscription for specific analytics service. 200 OK 400 input parameter error 500 server internal error
AnalysisEvent ID	M	string	1	N/A	Indicates the analysis correlation ID, which identifies the analytics subscription.

Table 8-14 – DafEventSubscription_Notify

Information element	Status	Data type	Cardinality	Code value	Description
AnalysisEventNotify	M	array	1..N	N/A	Indicates the relevant analysis results and the corresponding accuracy, such as network slice load information and prediction, NF fault location and warning, UE mobility analysis and prediction, network performance analysis and prediction, abnormal behaviour, user data congestion, etc.
Time information	M	string	1	N/A	Indicates the time information of the analysis events report.
LoadThresholdNotify	C	integer	0..1	N/A	Indicates the network slice load situation to the NF consumer when it is reached the load threshold.
NFFaultInfo	C	array	1..N	N/A	Indicates that DAF should report the NF fault location and warning when the event analysis is subscribed.
CongestionLevelNotify	C	string	0..1	N/A	Indicates the congestion levels notification if the subscribed event is user data congestion.
UE mobility	C	array	1..N	N/A	Indicates UE mobility analysis and prediction result when the event analysis is subscribed.
Abnormal behaviour	C	array	1..N	N/A	Indicates abnormal behaviour analysis result when the event analysis is subscribed.
Service experience	C	array	1..N	N/A	Indicates service experience analysis result when the event analysis is subscribed.

8.8 DAF analytics request

This message is sent by NF consumers to request specific analytics and prediction. Table 8-15 descr ibes the information details of DafAnalysis_Request:

Table 8-15 – DafAnalysis_Request

Information element	Status	Data type	Cardinality	Description
AnalysisReqID	M	string	1	Identifies the specific requested analytics service
time window	M	string	1	Time window of requested analytics.
AnalysisAccuracy	M	string	1	Indicates the required accuracy of the analytics and prediction.
AnalysisReq	M	string	1	Indicates the analysis requirements.
RespfMeth	O	string	0..1	Indicates the response method (periodic, one time, on event detection).
MaxRepNum	O	Uinteger	0..1	Indicates the maximum number of reports, after which the request ceases to exist (that is, the end of the report). If omitted, there is no limit.
MonTime	C	string	0..1	Indicates the monitoring time when the request ceases to exist, after which DAF shall not send any responses and the request becomes invalid. If omitted, the request has no time limit.
ImmRep	O	string	0..1	Indicates immediate reporting of the requested analysis is ready.
LoadThreshold	C	string	0..1	Indicates that DAF should report the network slice load situation to the NF consumer when it is reached.
CongestionLevel	C	string	0..1	Indicates the congestion threshold levels if the subscribed event is user data congestion. Otherwise, it is optional.

Table 8-16 describes the information details of DafAnalysis_Response:

Table 8-16 – DafAnalysis_Response

Information element	Status	Data type	Cardinality	Code value	Description
Result	M	num	1	200 400 500	Indicates the success or failure for specific analytics service. 200 OK 400 input parameter error 500 server internal error
AnalysisReq ID	M	string	1	N/A	Indicates the analysis correlation ID, which identifies the analytics request.
AnalysisResp	M	array	1..N	N/A	Indicates the relevant analysis results and the corresponding accuracy, such as network slice load information and prediction, NF fault location and warning, UE mobility analysis and prediction, network performance analysis and prediction, abnormal behaviour, user data congestion, etc.

Table 8-16 – DafAnalysis_Response

Time information	M	string	1	N/A	Indicates the time information of the analysis response.
LoadThreshold Notify	C	integer	0..1	N/A	Indicates the network slice load situation to the NF consumer when it is reached the load threshold.
NFFaultInfo	C	array	1..N	N/A	Indicates that DAF should report the NF fault location and warning when it is requested.
CongestionLevelNotify	C	string	0..1	N/A	Indicates the congestion levels if the request is about user data congestion.
UE mobility	C	array	1..N	N/A	Indicates UE mobility analysis and prediction result when the analysis is requested.
Abnormal behaviour	C	array	1..N	N/A	Indicates abnormal behaviour analysis result when the analysis is requested.
Service experience	C	array	1..N	N/A	Indicates service experience analysis result when the analysis is requested.

9 Security considerations

This clause defines security requirements for intelligent analysis services in IMT-2020 network. The security requirements are based on [b-ITU-T Y.3111].

The intelligent analysis services have the following security requirements:

R-01 It is required to perform user authentication and authorization before the consumer accesses the intelligent analysis services.

R-02 It is recommended to have the capabilities for analysing the monitored data and providing reports on the abnormal behaviour of the consumers.

R-03 It is required to support management of security data (e.g., fault, configuration, performance, security related to management functions such as logs) of intelligent analysis services.

The subscribers or requesters may need to be authorized by means of the OAuth2 protocol [IETF RFC 6749] before access to intelligent analysis services [b-ITU-T X.1047].

Bibliography

[b-ITU-T X.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration*.

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

[b-ITU-T Y.3111] Recommendation ITU-T Y.3111 (2017), *IMT-2020 network management and orchestration framework*.

[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-ITU-R M.2083] Recommendation ITU-R M.2083-0 (2015), *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

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

Printed in Switzerland
Geneva, 2022