International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3108

(12/2019)

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

Future networks

Capability exposure function in IMT-2020 networks

Recommendation ITU-T Y.3108

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3108

Capability exposure function in IMT-2020 networks

Summary

Recommendation ITU-T Y.3108 specifies the design principles, architecture and reference points of the capability exposure function (CEF) in International Mobile Telecommunication 2020 (IMT-2020) networks.

Recommendation ITU-T Y.3108 specifies exposed capabilities brought by network softwarization and the architecture of IMT-2020 and functionalities that support the capability exposure of IMT-2020.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3108	2019-12-14	13	11.1002/1000/14129

Keywords

5G, IMT-2020, capability exposure function, CEF.

* 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3108

Capability exposure function in IMT-2020 networks

1 Scope

This Recommendation specifies the design principles, functional architecture and reference points of the capability exposure function (CEF) in International Mobile Telecommunication 2020 (IMT-2020) networks.

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.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network.*

[ITU-T Y.3102] Recommendation ITU-T Y.3102 (2018), *Framework of the 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.3110] Recommendation ITU-T Y.3110 (2017), *IMT-2020 network management and orchestration requirements*.

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

[ITU-T Y.3131] Recommendation ITU-T Y.3131 (2019), *Functional architecture for supporting fixed mobile convergence in IMT-2020 networks*.

3 Definition

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 control plane [b-ITU-T Y.2011]: The set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control.

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

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

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

NOTE 1 – Network functions include but are not limited to network node functionalities, e.g., session management, mobility management and transport functions, whose functional behaviour and interfaces are defined.

NOTE 2 – Network functions can be implemented on a dedicated hardware or as virtualized software functions.

NOTE 3 – Network functions are not regarded as resources, but rather any network functions can be instantiated using the resources.

3.1.4 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).

3.1.5 PDU session [b-ITU-T Y.3100]: In the context of IMT-2020, an association between a user equipment (UE) and a data network that provides a protocol data unit (PDU) connectivity service.

NOTE – The type of the association includes IP type, non-IP type and Ethernet type.

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

NOTE 1 – An example of 3rd party, a virtual network operator (VNO) may use capabilities exposed by a network operator, e.g., to manage specific network slices. Another example of 3rd party, a service and/or application provider (e.g., an over the top (OTT) player) may provide applications and/or services to enhance the network capabilities.

NOTE 2 – Network end-users are not regarded as 3rd parties.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF	Application Function
AN	Access Network
API	Application Programming Interface
AS	Application Server
ASF	Authentication Server Function
CEF	Capability Exposure Function
CN	Core Network
CP	Control Plane
EC	Edge Computing
FMC	Fixed and Mobile Convergence
HTTP	Hypertext Transfer Protocol
ID	Identifier
IMT-2020	International Mobile Telecommunication 2020
NACF	Network Access Control Function
NF	Network Function

NFR	Network Function Repository
NSSF	Network Slice Selection Function
NWDA	Network Data Analytics
OTT	Over The Top
PCF	Policy Control Function
PDU	Protocol Data Unit
RP	Reference Point
QoS	Quality of Service
REST	Representational State Transfer
SLA	Service Level Agreement
SMF	Session Management Function
UE	User Equipment
UPF	User Plane Function
USM	Unified Subscription Management
UNIC	Unified Network Integrated Cloud
V2X	Vehicle to Everything
VNF	Virtual Network Function
VNO	Virtual Network Operator

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.

6 Design principles of the capability exposure function in IMT-2020 networks

Based on requirements identified in [ITU-T Y.3101], [ITU-T Y.3105] and other relevant studies, the following principles and characteristics are considered for the design of the CEF in IMT-2020 networks:

– the architectural design of the CEF should be flexible to adapt to the changes in third party applications and core network (CN) functions;

– the exposure of the IMT-2020 capabilities relies on the architecture of the CEF providing interaction between the IMT-2020 network and third parties;

– the architectural design of the CEF should support a unified northbound interface to facilitate easy invocation of the CEF by third party applications.

Key network capabilities that are expected to be exposed include, but are not limited to [ITU-T Y.3105]:

– network slicing management;

– edge computing (EC);

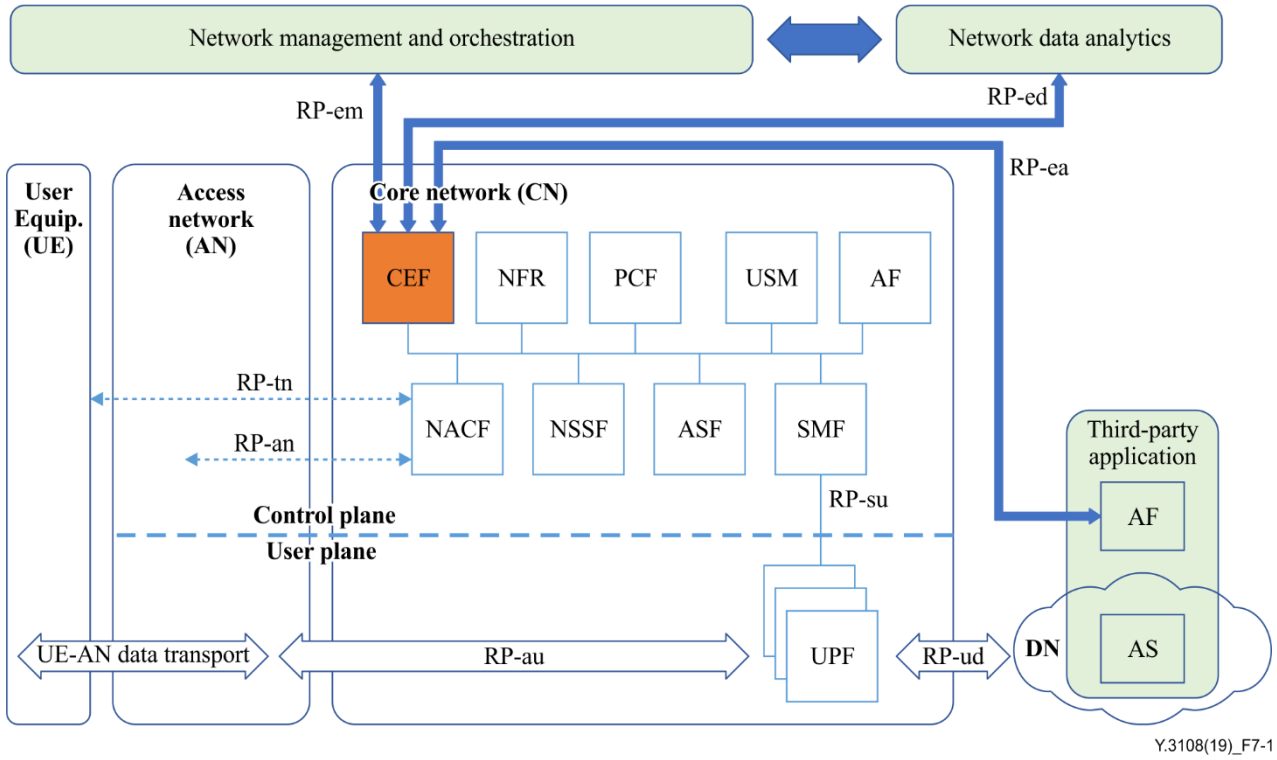
– network data analytics (NWDA);
– fixed and mobile convergence (FMC);
– quality of service (QoS).

7 Framework of the capability exposure function

7.1 General aspects

This clause describes the framework of the CEF and provides an overview of its role in IMT-2020 networks.

Based on the architecture of an IMT-2020 network [ITU-T Y.3104], Figure 7-1 shows the framework of the CEF, and its interaction with third party applications, NWDA, network management and orchestration, and other IMT-2020 network functions (NFs).



ASF: authentication server function; NFR: network function repository; NSSF: network slice selection function; UPF: user plane function

Figure 7-1 – Framework of capability exposure function in the IMT-2020 network

CEF is a control plane (CP) NF that provides functionalities for NFs to expose their capabilities as a service to third parties in the IMT-2020 network [ITU-T Y.3102].

A third party's application can be logically divided into two parts: application server (AS) and application function (AF). The AS interacts with the IMT-2020 network in the user plane, and executes the service logic of an application. The AF interacts with the IMT-2020 network in the CP to exchange configuration information. For example, the AF can provide session-related information to a policy control function (PCF) (directly or via CEF) so that a session management function (SMF) can finally use this information for session management.

NOTE – AFs considered to be trusted by the operator can be allowed to interact directly with relevant NFs. AFs not allowed to access directly the NFs are required to use CEF to interact with relevant NFs. This Recommendation focuses on the second scenario.

NWDA [ITU-T Y.3105] comprise an NF that provides operator-managed network analytics capabilities. NWDA support data collection from NFs, AFs and network management and orchestration, as well as supporting analytics information provisioning to NFs and the AF.

Network management and orchestration [ITU-T Y.3111] is a network subsystem for managing and orchestrating virtual network functions (VNFs) and other software components. More detail is specified in [ITU-T Y.3111].

Other CP NFs (e.g., SMF, network access control function (NACF), PCF) that support capability exposure are specified in [ITU-T Y.3104].

All the interactions between the CEF and other CP NFs (including the AF) are realized by service-based interfaces as specified in [ITU-T Y.3104].

The CEF has three distinct interfaces with: third party applications; network management and orchestration; and NWDA capabilities.

– Interface with a third-party application: the CEF can expose specific UE events and network status-related information to the AF of a third party to support the optimization of that party's application. The CEF can collect data from the AF of a third party for NWDA and network configuration.
– Interface with network management and orchestration: the CEF can deliver network management requirements of the third party to network management and orchestration, in supporting the customization of network slicing and mobile EC.
– Interface with NWDA capabilities: the CEF can forward collected data from the AF of a third party to NWDA, from which it obtains network status information that can be exposed to that party.

The CEF also needs to interact with other CN functions (e.g., SMF, NACF or PCF), to obtain information about the UE (e.g., reachability, location or roaming status) and network (e.g., status information or congestion level).

7.2 Exposure of network capabilities

7.2.1 Exposure of control plane capabilities

The CEF supports exposure of the control plane capabilities of the IMT-2020 network to third parties with the following functionalities.

– a) Monitoring of network events

  The CEF exposes interfaces for the authorized third party to monitor specific network events (e.g., roaming of UE, communication failure, UE location, UE connectivity status) mainly triggered by NACF and unified subscription management (USM) operations [ITU-T Y.3102]. The CEF maintains the subscription of a third party to notification of network events and notifies that party when one occurs.

– b) Provisioning of information by a third party

  The CEF exposes interfaces for the authorized third party to provision the parameters for network configuration, UE communication configuration, and service-specific configuration (e.g., UE mobility patterns, communication characteristics) maintained by USM [ITU-T Y.3102]. On request by the third party, the CEF requests USM to update the provisioned configuration parameters.

  NOTE – The update of network configuration parameters can cause operational changes in other NFs.

7.2.2 Exposure of network management and orchestration capabilities

In terms of interaction with the CEF, network management and orchestration capabilities [ITU-T Y.3110] expose a set of management data required by the customer and authorized by the

network operator. For example, network operation status and current network performance can be exposed to third parties through the CEF within operator's policy.

7.2.3 Exposure of network data analytics capabilities

The NWDA capabilities provide network analytics information (e.g., network load level information and network slice QoE data analytics) to application and services via CEF functionalities.

8 Capability exposure function functionalities and reference points

Clause 8.1 describes the CEF functionalities; while clause 8.2 describes CEF reference points (internal to CEF and external to the network capabilities to be exposed).

8.1 Capability exposure function functional architecture

Figure 8-1 depicts the architecture of the CEF.

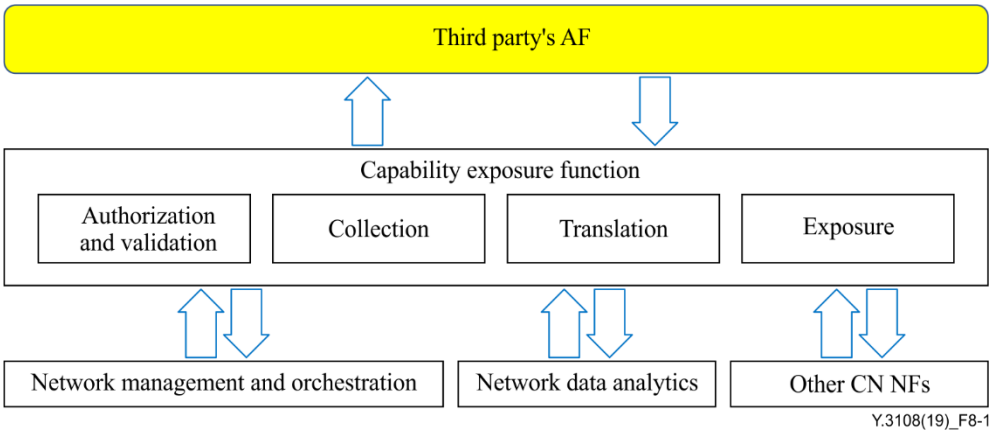


Figure 8-1 – Functional architecture of the capability exposure function

The CEF may include the following functionalities.

– Exposure: the CEF supports secured exposure to an authorized third party of network information, which is collected from IMT-2020 NFs and translated by the translation functionality.

– Collection: the CEF retrieves and stores network information as structured data using standardized interfaces with network management and orchestration [ITU-T Y.3110], network analytics capabilities and other core NFs.

– Authorization and validation: the CEF supports secure access of a third party to the exposed CEF interfaces, e.g., for monitoring and provisioning of network information.

– Translation: the CEF translates between information exchanged with third parties and that with NFs. As an example, the translation from service level agreement (SLA) requirements to specific network parameters.

The CEF handles masking of network and user sensitive information from external applications according to the network policy.

8.2 Capability exposure function reference points

The NFs within the CN CP interact using service-based interfaces. These service interfaces can be implemented by common protocols such as the hypertext transfer protocol (HTTP) 2.0 and RESTful application programming interfaces (APIs). The details of service-based interfaces lie outside the scope of this Recommendation.

The following reference points (RPs) are defined in the framework of capabilities exposure function:

– RP-ea: between the CEF and third party's AF;
– RP-em: between the CEF and the network management and orchestration;
– RP-ed: between the CEF and NWDA.

9 Procedures for the exposure of network capabilities

9.1 General aspects of the capability exposure procedure

This clause describes general procedures to provide each of the basic network services specified in clause 7.1 of [ITU-T Y.3105] for capability exposure services: authentication and authorization of third parties; facilitation of authorized third party subscription to and notification of a specific event concerning changes in exposed network information; and facilitation of authorized third parties to provision configuration parameters of the IMT-2020 network.

9.1.1 Authentication and authorization of third parties

See Figure 9-1.

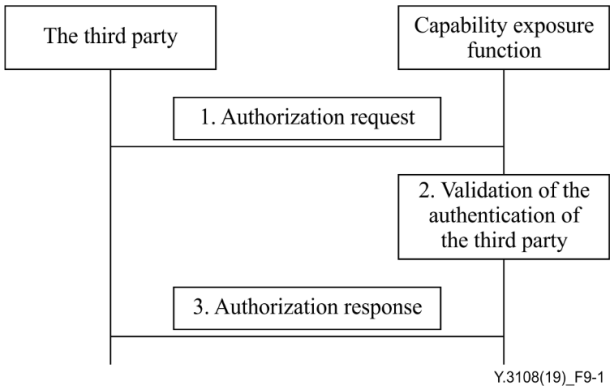


Figure 9-1 – Procedure for third party authorization and authentication

1) The third party sends an authorization request to the CEF to obtain permission to access a specific network capability by including the third-party identity information and any other information required for authentication of that party.
2) The CEF validates the authentication of the third party (using authentication information) and checks whether the third party is permitted to access the requested network capability.
3) Based on the third-party subscription information, authorization information for access by the third party is sent to that party as an authorization response.

9.1.2 Subscription and notification of network event monitoring

Specific network events, such as loss of UE network connectivity, UE roaming and communication failure, can be monitored by the CEF and notified to the third party on occurrence. The CEF provides exposed interfaces to support the subscription to and notification of network events by monitoring them in the NACF and USM.

Figure 9-2 depicts the detailed procedure.

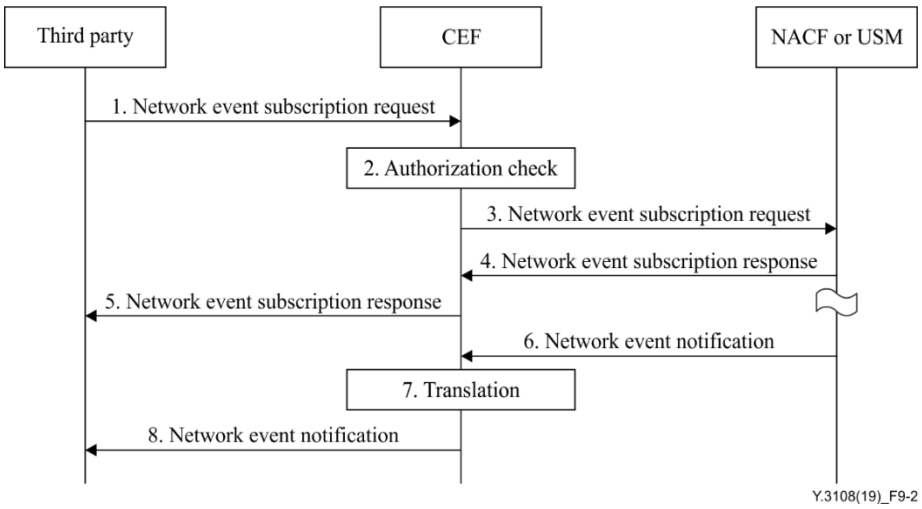


Figure 9-2 – Procedure for subscription and notification of network event monitoring

1) The third party (application) subscribes to the network event by sending a network event subscription request to the CEF, specifying the target event(s), which may include loss of UE network connectivity, UE roaming status or communication failure.
2) The CEF checks whether the third party is authorized for the request. If not, the procedure proceeds to step 5).
3) The CEF subscribes the target event(s) to the corresponding NF (NACF or USM) by sending a network event subscription request.
4) The corresponding NF (NACF or USM) registers and maintains the association of the target monitoring event and the CEF to be notified; and the NF acknowledges the subscription by sending a network event subscription response to the CEF.
5) The CEF registers and maintains the association of the target monitoring event and the target third party to be notified; and the CEF acknowledges the subscription by sending a network event subscription response to the third party. If authorization fails, the CEF responds indicating the authorization failure and the procedure ends at this step.
6) When the corresponding NF detects that a target monitoring event occurred, the NF notifies it to the target CEF by sending a network event notification.
7) The CEF translates the internal network information by masking it from the external use.
8) The CEF notifies the monitoring event to the target third party by sending a network event notification.

NOTE – The subscription and notification procedure can be used for one-time retrieval of network information from the third party.

9.1.3 Provisioning of configuration parameters

The operations of the CP NFs of an IMT-2020 network can be customized by third parties by provisioning the configuration parameters for network configuration, UE communication configuration and service-specific configuration, such as UE mobility patterns, communication characteristics and QoS parameters.

The CEF provides exposed interfaces to support the provisioning of configuration parameters by updating the target configuration parameters in USM.

Figure 9-3 depicts the detailed procedure.

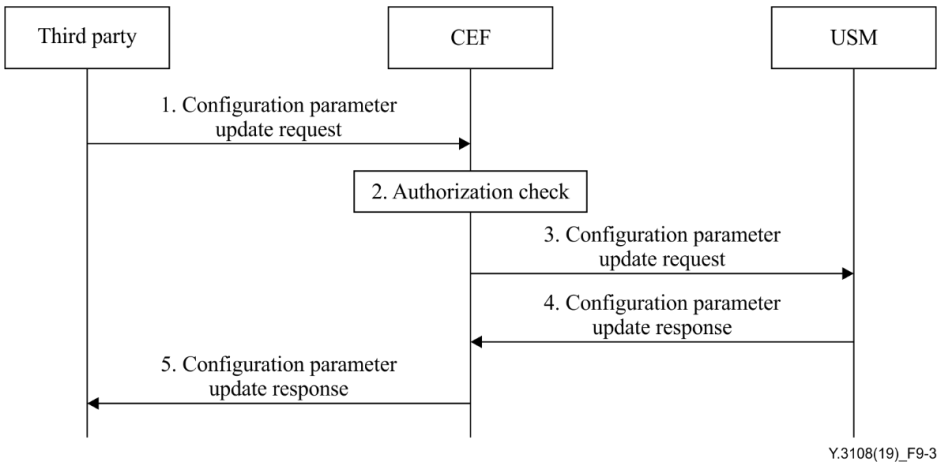


Figure 9-3 – Procedure for provisioning of configuration parameters

1) The third party (application) sends a configuration parameter update request to the CEF, specifying the target parameter(s), which may include network configuration, UE communication configuration and service-specific configuration.
2) The CEF checks whether the third party is authorized for the request. If not, the procedure proceeds to step 5).
3) The CEF sends a target configuration parameter(s) update request to the USM.
4) The USM updates the given configuration parameter(s) in its repository and responds by sending a configuration parameter update response to the CEF.
5) The CEF sends a configuration parameter update response to the third party. If authorization fails, the CEF responds, indicating the authorization failure.

9.2 Network slice management capability exposure procedure

9.2.1 Creation of a network slice

This clause describes general procedures to provide each of the basic network services specified in clause 7.2 of [ITU-T Y.3105] for network slice management.

See Figure 9-4.

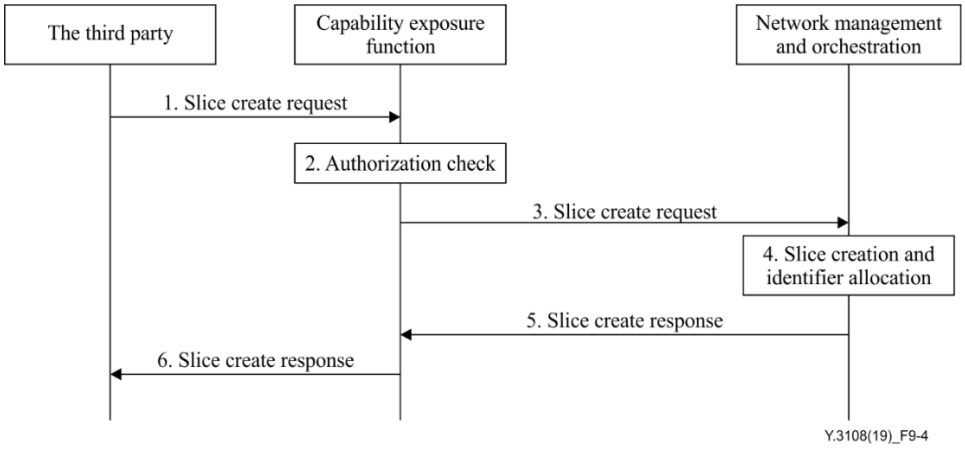


Figure 9-4 – Procedure for network slice management capability exposure – creation of a network slice

1) The third party AF applies for the creation of a new network slice. The functional and performance requirements of the network slice are carried in the slice create request message.

2) The CEF performs a validation and authorization check: the CEF authorizes the third party request.

3) After step 2), the CEF transfers the network slice creation request to network management and orchestration [ITU-T Y.3110].

4) Based on resource availability and operator policy, network management and orchestration decides whether the network slice creation request is accepted. If the request is accepted, network management and orchestration creates the customized network slice for the third party (application) and allocates the identifier (ID) for this slice.

5) Network management and orchestration sends a response to the CEF. The network slice ID and information is delivered if the network slice is created.

6) The CEF forwards the network management and orchestration response to the third party.

9.2.2 Modification of a network slice

See Figure 9-5.

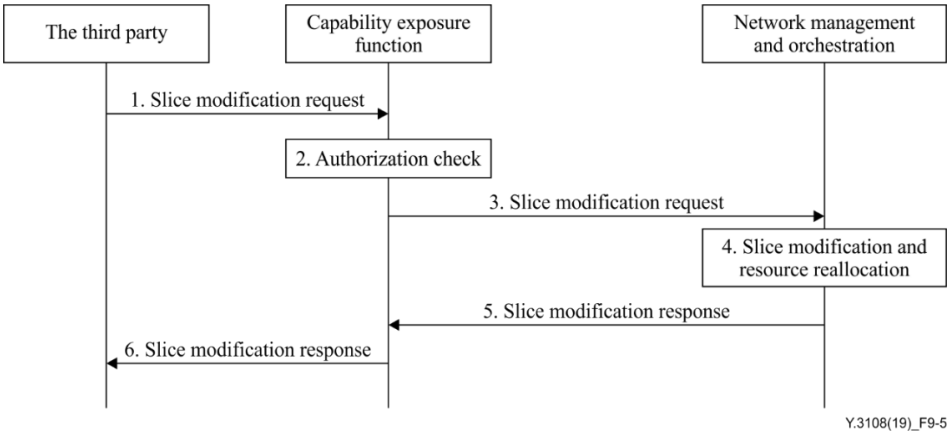


Figure 9-5 – Procedure for network slice management capability exposure – modification of a network slice

1) The third party (application) indicates the functional and performance requirements of the network slice in the request message.

2) The CEF performs a validation and authorization check: CEF authorizes the third-party request.

3) After step 2), the CEF transfers the network slice modification request to network management and orchestration [ITU-T Y.3110]. It also considers the network slice sharing scenario and determine the network parameters and resources related to modification of the non-sharing part.

4) Network management and orchestration determine whether the network slice modification-related resources are allowed (according to the configuration for this third party) and, if allowed, update all network resources which have been determined in step 3).

5) The network management and orchestration notifies the CEF whether the resource request is granted.

6) If it is granted, the CEF notifies the third party of the result.

9.2.3 Deletion of a network slice

See Figure 9-6.

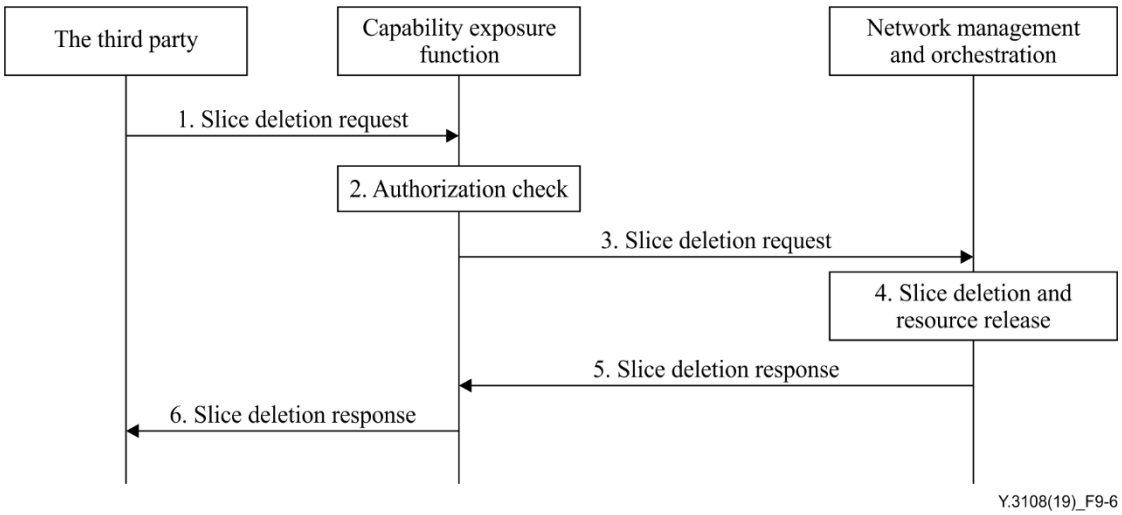


Figure 9-6 –Deletion of a network slice

1) The third party (application) identifies the network slice to be deleted in a request message to the CEF.
2) The CEF performs a third-party request validation related to the deletion: the CEF authorizes the third party request.
3) After step 2, the CEF transfers the network slice deletion request to network management and orchestration [ITU-T Y.3110]. It also considers sharing network slices and determines the network parameters and resources related to deletion of non-sharing resources.
4) Network management and orchestration determines whether the network slice deletion of the related resources is allowed (according to the configuration for this third party) and, if allowed, releases all network resources that have been determined in step 3).
5) Network management and orchestration notifies the CEF whether the network slice deletion request has been granted.
6) The CEF notifies the third party of the response.

9.3 Edge-computing exposure procedure

This clause describes general procedures to provide each of the basic network services specified in clause 7.3 of [ITU-T Y.3105] for EC.

See Figure 9-7.

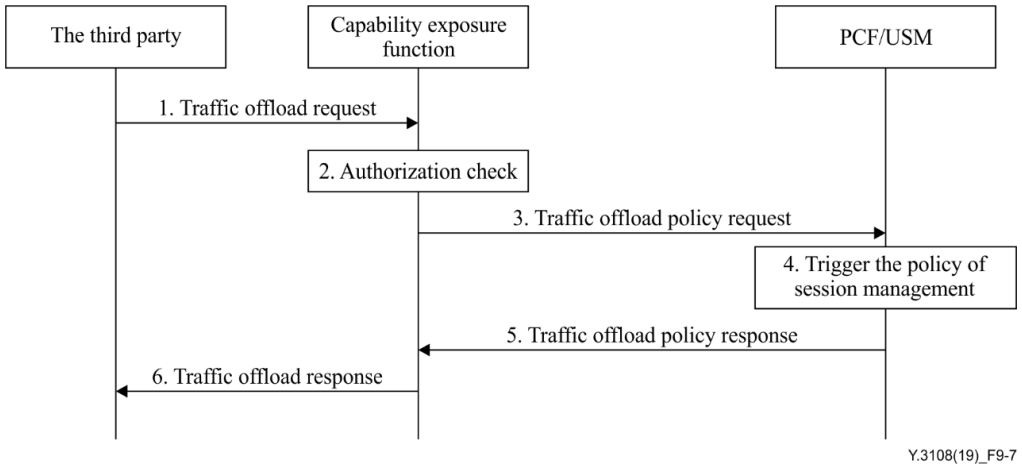


Figure 9-7 – Procedure for the edge-computing capability exposure

1) According to the location of the UEs, service area of EC, and operator policy, the third party application sends a traffic offload request to CEF in order to re-route the UE traffic to EC. The request can target a specific UE or a group of UEs.

2) The CEF checks whether the third party is authorized for the request. If not, the procedure proceeds to step 6).

3) The CEF translates the information provided by the third party's AF into the information needed by the IMT-2020 NF (e.g., PCF or USM) and forwards the policy request to the targeting NFs.

4) The NF (PCF or USM) can determine whether the existing PDU sessions are affected by the traffic-offloading policy in the AF request. For an affected PDU session, the PCF triggers the SMF for the PDU session modification procedure.

5) The NF (PCF or USM) send a response to the CEF to update the result of policy enforcement.

6) Based on the determination of the NF, the CEF sends a response to the third party for an UE application context update.

9.4 Network data analytics exposure procedure

This clause describes the procedures to provide each of the basic network services specified in clause 7.4 of [ITU-T Y.3105].

See Figure 9-8.

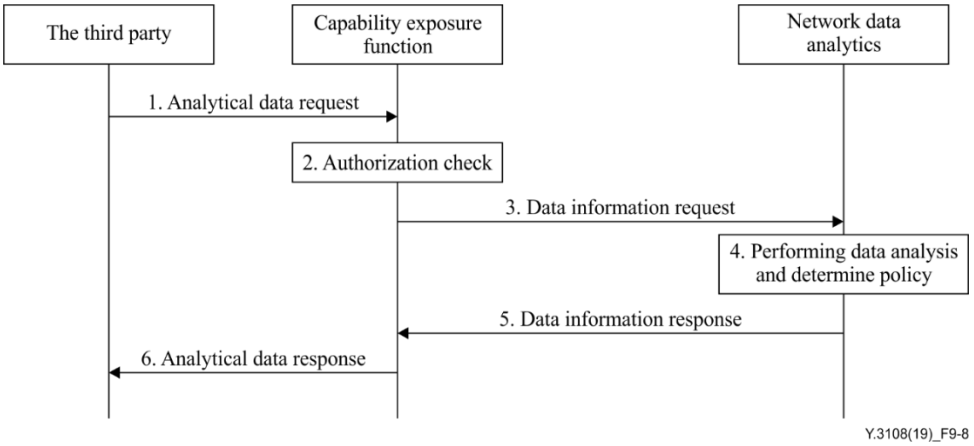


Figure 9-8 – Procedure for network data analytics exposure

1) The third party (e.g., automotive vehicle to everything (V2X) application) sends a network status information request to the CEF.

2) The CEF authorizes the third party.

3) After successful authorization, the CEF sends the data information request to NWDA.

4) NWDA perform network data analysis based on the collected data from other NFs, e.g., third party information, network performance related information, network slice load level or QoS experience.

5) The output of NWDA is delivered to the CEF via data information response.

6) The CEF notifies the third party about the analytical data result.

9.5 Fixed and mobile convergence exposure procedure

This clause describes general procedures to provide each of the basic network services specified in clause 7.5 of [ITU-T Y.3105] for FMC.

See Figure 9-9.

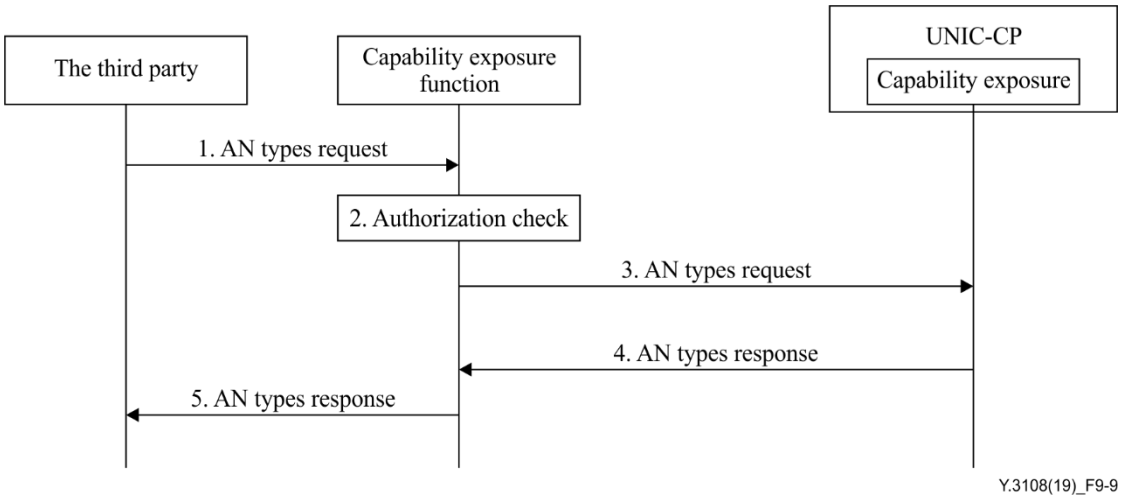


Figure 9-9 – Procedure for fixed and mobile convergence capability exposure

1) The third party (application) requests exposed network information by sending an access network (AN) type request to the CEF, specifying the target information that may also include UE location, UE connectivity status, UE reachability and network status.
2) The CEF checks whether the third party is authorized for the request. If not, the procedure proceeds to step 5).
3) The CEF sends an AN types request for the target information to the corresponding CEF in the unified network integrated cloud-control plane (UNIC-CP) [ITU-T Y.3131].
4) The CEF in UNIC-CP [ITU-T Y.3131] responds with the exposed network information by sending an AN types response to the CEF.
5) The CEF responds with the exposed network information by sending an AN type response to the third party. The third-party application can provide different services or contents based on the UE AN type.

NOTE – The CEF in UNIC-CP [ITU-T Y.3131] enables the UNIC-CP to provide network capabilities and desensitized user data to applications through capability exposure interfaces.

9.6 Customization of QoS capability exposure procedure

This clause describes general procedures to provide each of the basic network services specified in clause 7.6 of [ITU-T Y.3105] for customization of QoS capabilities.

See Figure 9-10.

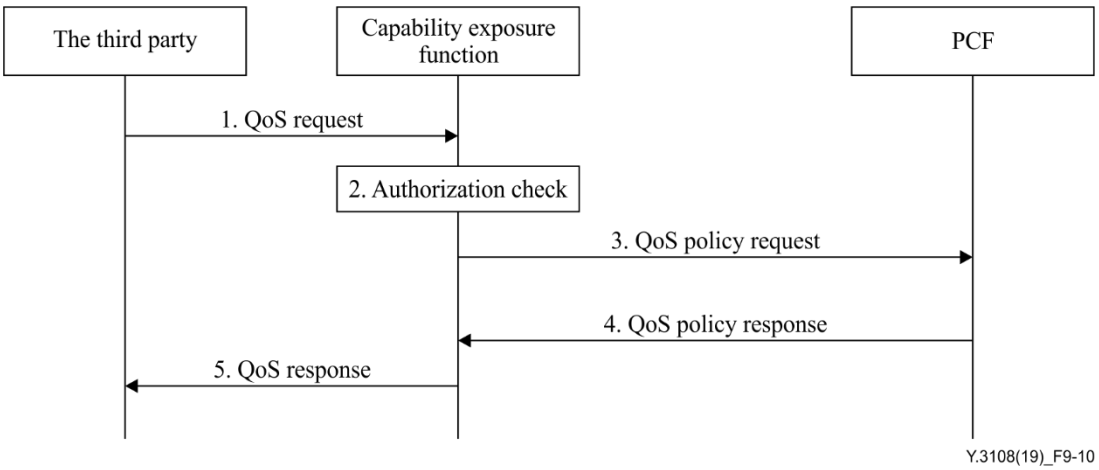


Figure 9-10 – Procedure for a third party QoS request authorization and authentication

1) The third party AF sends a QoS request message (e.g., UE ID, third party ID, SLA) to the CEF.
2) The CEF authorizes the third party's QoS request and may apply policies to create or modify QoS flows for the third party.
3) The CEF interacts with the PCF to notify it of the QoS request from a third party.
4) The PCF analyses the requested QoS information provided by the CEF and determines whether a new QoS flow or modification to the existing QoS flow is required. The PCF may further interact with other NFs (e.g., SMF, USM) to implement the QoS configuration. The PCF notifies the CEF via a QoS policy response. If the requested QoS flow is accepted, the QoS parameters are delivered with the response.
5) The CEF sends a QoS response message to the third party. If the requested QoS flow is accepted, the QoS parameters are delivered with the response.

10 Security considerations

The IMT-2020 network is subject to security and privacy measures. Sensitive information should be protected as a high priority in order to avoid leaking and unauthorized access. The security and privacy-related requirements specified in [ITU-T Y.3101] [ITU-T Y.3105] apply to this Recommendation.

Specific security concerns related to the CEF are addressed in clause 9.

Bibliography

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

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

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

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, 2020