International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5021

(07/2019)

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

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

Protocol for managing capability exposure APIs in IMT-2020 networks

Recommendation ITU-T Q.5021

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
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.5021

Protocol for managing capability exposure APIs in IMT-2020 networks

Summary

Recommendation ITU-T Q.5021 describes the protocol for managing capability exposure application programming interfaces (APIs) in International Mobile Telecommunications (IMT)-2020 networks. It includes signalling architecture, API management functions, signalling flows and their message format, and definition for management APIs. It also describes gap analysis and use cases for API management.

This protocol can be used by network operators and third parties to manage capability exposure APIs.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5021	2019-07-29	11	11.1002/1000/13980

Keywords

Capability exposure, capability exposure APIs, IMT-2020, managing API.

* 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 Q.5021

Protocol for managing capability exposure APIs in IMT-2020 networks

1 Scope

This Recommendation describes the protocol for managing capability exposure application programming interfaces (APIs) in International Mobile Telecommunications (IMT)-2020 networks. It includes signalling architecture, API management functions, signalling flows and their message format, and definition for management APIs. It also describes gap analysis and use cases for API management.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 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.

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

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF Application Function

API Application Programming Interface

CEF Capability Exposure Function

IMT International Mobile Telecommunications

OA&M Operations, Administration, and Management

UE User Equipment

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 "cardinality" indicate the number of parameter in message. "1" indicates olny one parameter while "N" indicates multiple parameter. "1..N" indicates one or more parameters.

6 Signalling architecture for API management

To avoid duplication and inconsistency of capability exposure APIs to various third-party application functions (AFs), development of a common capability exposure API framework was needed that includes common aspects (e.g., API registration, API discovery, API authorization) that were applicable to any functional APIs when used by a third-party.

Figure 6-1 shows the architecture model for the capability exposure API management system and the relationship with the capability exposure function (CEF), the third-party application and the IMT-2020 core network functions.

The capability exposure function provides functionalities to expose its capabilities as a service externally and capability exposure APIs to the third-party. For high-level descriptions of the functionalities and APIs refer to [b-ITU-T Y.IMT2020-CEF].

The API management function is mainly responsible for management of the capability exposure API, including API registration, API deregistration, API discovery, API authorization, API authentication, API suspension, API recovery, API charging and monitoring and API topology hiding.

The IF1 reference point is the southbound interface, which exists between the CEF and the IMT-2020 core network functions. It supports:

– subscription and unsubscription of network capabilities;

– query and reporting of network capabilities;

The IF2 reference point is the northbound interface, which exists between the CEF and the third-party application. It supports exposure of network capabilities to the third-party application through the invocation of capability exposure APIs.

The IF3 reference point is the northbound interface, which exists between the API management function and the third-party application. It supports discovery of capability exposure API.

The IF4 reference point exists between the CEF and the API management function. It supports:

– registration and deregistration of capability exposure API;

– invocation event report of capability exposure API;

– suspension and recovery of capability exposure API.

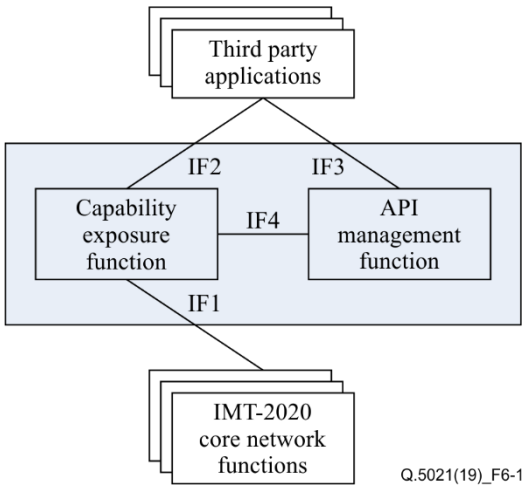

Figure 6-1 – Architecture of capability exposure API management system

7 Functions for API management

7.1 API registration

For the API management function to properly maintain the information of available CEF instances and their supported capability exposure APIs, each CEF instance informs the API management function of the list of capability exposure APIs that it supports.

The CEF instance may make this information available to API management function when the CEF instance becomes operative for the first time (registration operation) or upon individual CEF service instance activation/de-activation within the CEF instance (update operation), e.g., triggered after a scaling operation. The CEF instance may also update or delete the CEF service related parameters. Alternatively, another authorised entity (such as an operations, administration, and management (OA&M) function) may inform the API management function on behalf of an CEF instance triggered by an CEF service instance lifecycle event (register or de-registration operation depending on instance instantiation, termination, activation, or de-activation). Registration with the API management function includes capacity and configuration information at time of instantiation.

7.2 API discovery

The API discovery enables the third-party applications to discover a set of CEF instance(s) with specific capability exposure APIs.

Unless the expected CEF instance and capability exposure APIs information are locally configured on requester third-party applications, the API discovery is implemented via the API management function.

In order to access to the target CEF instance and get information of target capability exposure API, the requester third-party application initiates the API discovery procedures by providing the specific information of the third-party and APIs. The detailed service parameter(s) used for specific API discovery are defined in clause 9.

The API management function may provide the IP address or the node name of CEF instance(s) to the requester third-party application. Based on that information, the requester third-party application can select one specific CEF instance that is able to provide a particular capability exposure API.

7.3 API authorization

The API authorization is required to ensure the third-party application is authorized to access the capability exposure API provided by CEF, according to the API authorization information. The API authorization information is configured as one of the components in the CEF profile and provide to the API management function during the API registration procedures. It includes the type and other parameters of the third-party application such as the third-party application identity.

The API management function will check whether the third-party application is permitted to discover the requested capability exposure API during the API discovery procedure according to the API authorization information.

7.4 API authentication

The API authentication is required to ensure the mutual authentication between the third-party application and API management function, before the exposure of capability exposure APIs to the third-party application. The authentication method is used to provide integrity protection, replay protection and confidentiality protection via the IF3 reference point.

The API management function will authenticate the third-party application based on the identity and key of the third-party application.

7.5 API deregistration

APIs are required to be deregistered through API management, e.g., the operator may not provide the invocation of the API to third-party applications, the API is about to shutdown or disconnect from the network or API is expired. The API management indicates the deregistration of the API to the CEF. The CEF will delete the API context and inform the third-party application of the API deregistration.

7.6 API suspension

An API is required to be suspended according to the suspension indication from API management, e.g., API management preconfigures the time window of the permitted of the API usage, operator cannot provide the invocation of the API temporarily. The API management indicates the suspension of the API, and the CEF suspends the API from running state and stores the context of the API accordingly. Once the API runs into suspension state, the CEF will notify the suspension state of the API to the third-party applications.

7.7 API recovery

An API can be recovered from suspension state, e.g., operator resume the invocation of the API to the third-party applications, API management preconfigures the time of API resumption. The API management indicates the CEF that the API has been recovered to the running state. Accordingly, the CEF resumes the API based on the context of the API previously stored at the moment of the API suspended. And then the CEF notifies the third-party applications the permitted usage of the API.

7.8 API charging and monitoring

When the third-party application invokes CEF API, the CEF will send this API invocation event to the API management function.

The API management function will monitor the invoking event and charge based on it.

7.9 API topology hiding

The API topology hiding is required to ensure the API management function act as the entry point for service API invocation when the third-party application is not in the IMT-2020 network trust domain.

CEF invokes the topology hiding API before communication with the third party for first time. The API management function will hide the address of CEF and other related network functions, network inside topology and path information from the third-party application which is not in the trust domain of IMT-2020 network.

7.10 API location query

Specific kinds of third-party applications need to know the location of user equipment (UE), like map application, navigation application. CEF queries IMT-2020 core network for the location of UE and return it to the third-party.

8 Signalling flow

8.1 API registration procedure

Figure 8-1 illustrates the procedure for registration of the capability exposure API.

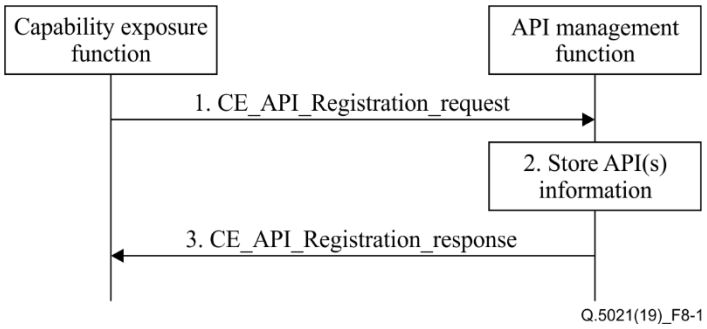

Figure 8-1 – API registration procedure

1. The capability exposure function sends a CE_API_Registration_request to the API management function. It includes the list of capability exposure function instance and API list.
2. The API management function stores the information of capability exposure function and marks the capability exposure function available.
3. The API management function sends a CE_API_Registration_response to the capability exposure function.

8.2 API discovery procedure

Figure 8-2 illustrates the procedure for discovery of the capability exposure API.

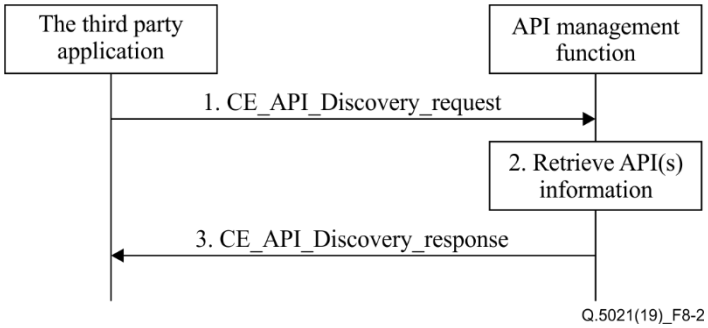

Figure 8-2 – API discovery procedure

1. The third-party application sends a CE_API_Discovery_request to the API management function. It includes the third-party application identity, type of the third-party application identity, name of the third-party application vendor and query information.

2. Upon receiving the CE_API_Discovery_request, the API management function verifies the identity of the third-party application (via authentication procedure). The API management function retrieves the stored API(s) information. Further, the API management function applies the discovery policy and performs filtering of service APIs information retrieved from the API management function.
3. The API management function sends a CE_API_Discovery_response to the third-party application with the list of CEF instance for which the third-party application has the required authorization.

8.3 API authorization procedure

Figure 8-3 illustrates the procedure for authorization of the capability exposure API.

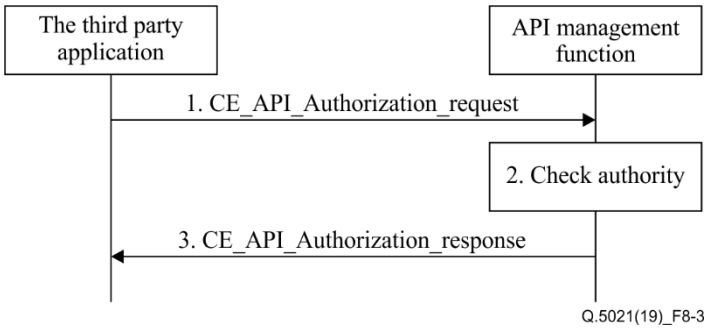

Figure 8-3 – API authorization procedure

1. The third-party application sends a CE_API_Authorization_request to the API management function. It includes the type of the third-party application, the third-party application identity, name of the third-party application vendor and query information.
2. The API management function checks the authorization information to make sure whether the third-party application is authorized to access the capability exposure API provided by CEF.
3. The API management function sends a CE_API_Authorization_response to the third-party application.

8.4 API authentication procedure

Figure 8-4 illustrates the procedure for authentication of the capability exposure API.

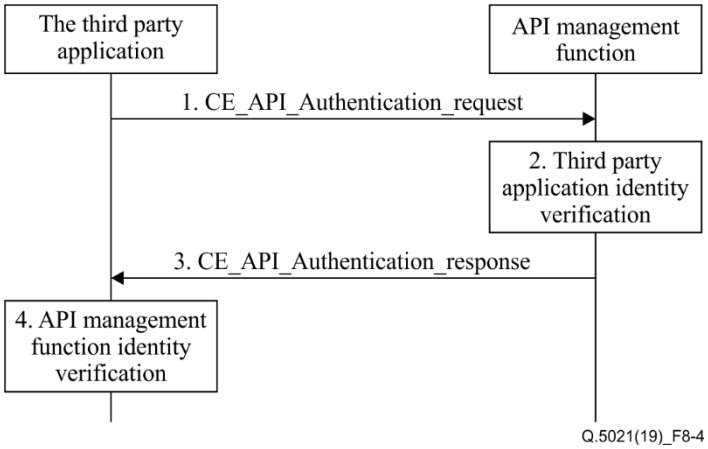

Figure 8-4 – API authentication procedure

1. The third-party application sends a CE_API_Authentication_request to the API management function. It includes the third-party application identity and key.

2. Then the API management function receives the authentication request, it verifies the identity information and validity of the key.
3. The API management function returns a CE_API_Authentication_response to the third-party application. The response message also contains the key of the API management function.
4. The third-party application checks the validity of the key of the API management function.

8.5 API deregistration procedure

Figure 8-5 illustrates the procedure for deregistration of the capability exposure API.

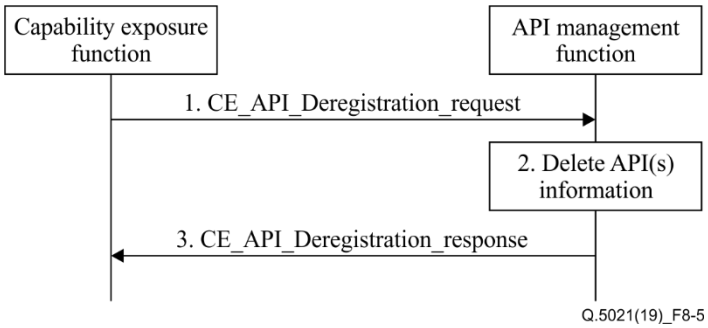

Figure 8-5 – API deregistration procedure

1. The capability exposure function sends a CE_API_Deregistration_request to the API management function. It includes the API name, API function description, capability exposure function instance, serving the third-party application list.
2. The API management function deletes the API-related information.
3. The API management function sends a CE_API_Deregistration_response to the capability exposure function.

8.6 API suspension procedure

Figure 8-6 illustrates the procedure for suspension of the capability exposure API.

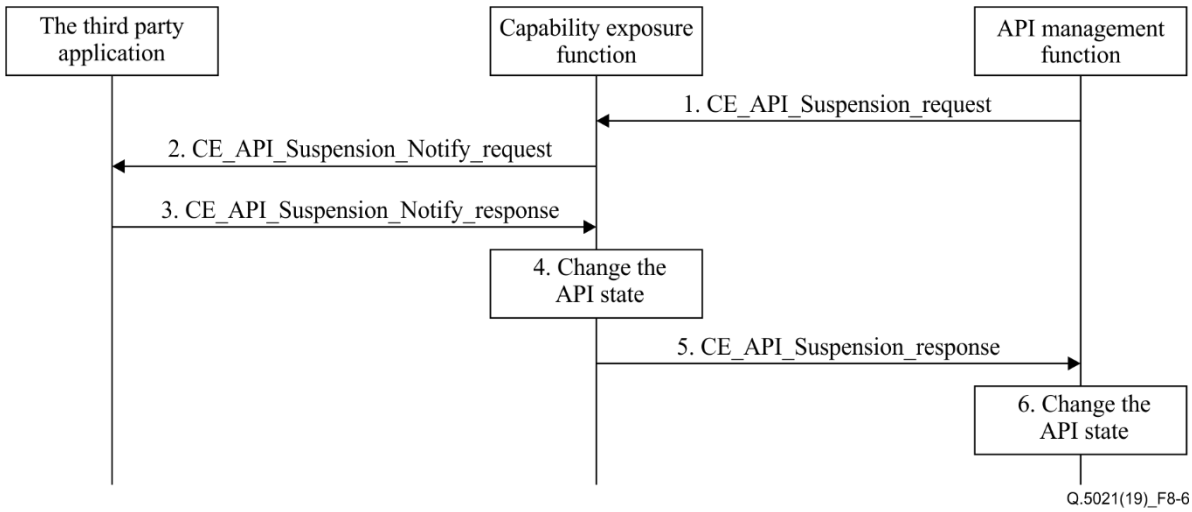

Figure 8-6 – API suspension procedure

1. The API management function sends a CE_API_Suspension_request to the capability exposure function. It includes the API name, API function description, capability exposure function instance, serving the third-party application list, duration of suspension.

2. The capability exposure function sends a CE_API_Suspension_Notify_request to the third-party applications according to the list. It includes the API name, API function description, capability exposure function instance, duration of suspension.
3. The third-party application sends a CE_API_Suspension_Notify_response to the capability exposure function.
4. The capability exposure function changes the API into suspension state and stop to support capability exposure to the third-party applications temporarily.
5. The capability exposure function sends a CE_API_Suspension_response to the API management function.
6. The API management function changes the API into suspension state and stop to support capability exposure temporarily.

8.7 API recovery procedure

Figure 8-7 illustrates the procedure for recovery of the capability exposure API.

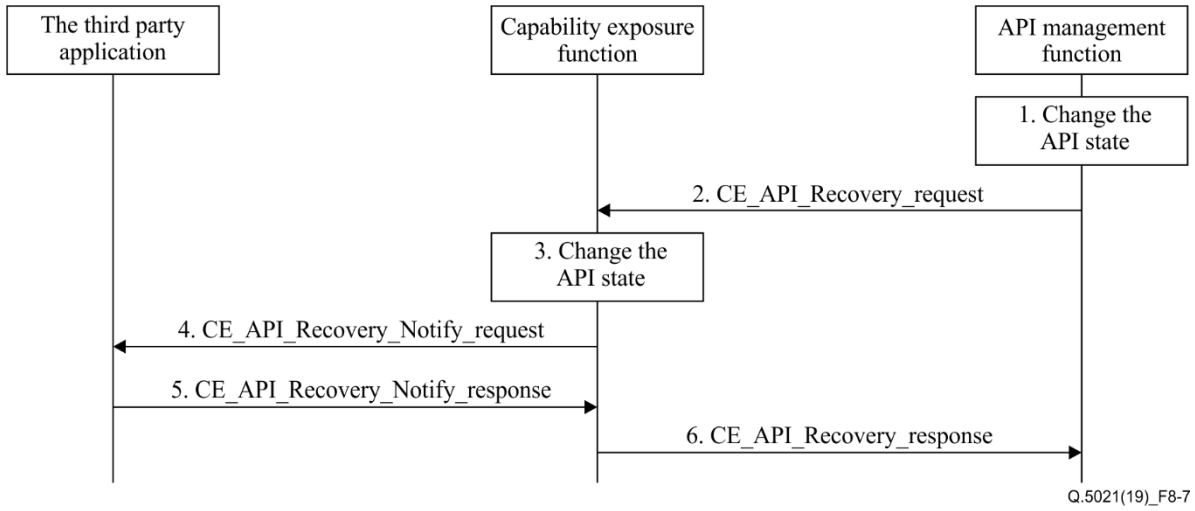

Figure 8-7 – API recovery procedure

1. The API management function changes the API into active state.
2. The API management function sends a CE_API_Recovery_request to the capability exposure function. It includes the API name, API function description, capability exposure function instance, serving the third-party application list, duration of suspension.
3. The capability exposure function change the API into active state and recovery the third-party application to invoke it.
4. The capability exposure function sends a CE_API_Recovery_Notify_request to the third-party application. It includes the API name, API function description, capability exposure function instance, duration of suspension.
5. The third-party application sends a CE_API_Recovery_Notify_response to the capability exposure function.
6. The capability exposure function sends a CE_API_Recovery_response to the API management function.

8.8 API charging and monitoring procedure

Figure 8-8 illustrates the procedure for monitoring of the capability exposure API.

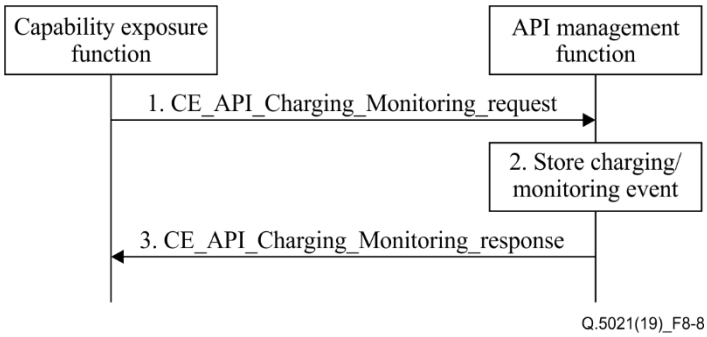

Figure 8-8 – API charging and monitoring procedure

1. The capability exposure function sends a CE_API_Charging_Monitoring_request to the API management function. It includes the third-party application identity, request capability exposure API.
2. The API management function stores the monitoring event information and charge based on it.
3. The API management function sends a CE_API_Charging_Monitoring_response to the capability exposure function.

8.9 API topology hiding procedure

Figure 8-9 illustrates the procedure for topology hiding of the capability exposure API.

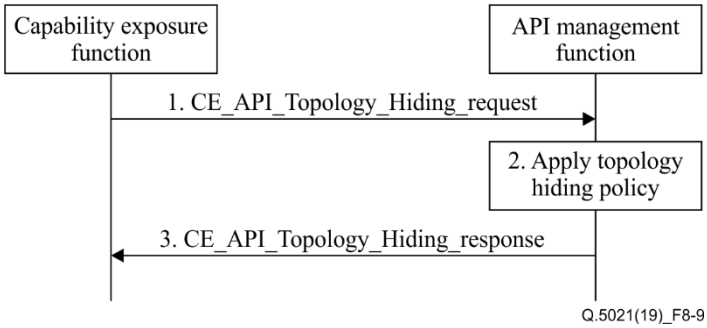

Figure 8-9 – Topology hiding procedure

1. The capability exposure function sends a CE_API_Topology_Hiding_request. It includes the list of capability exposure function instance, and the API list.
2. The API management function applies the policy of topology hiding and determines itself as the entry point for service API invocation.
3. The API management function sends a CE_API_Topology_Hiding_response to the capability exposure function.

8.10 API location query procedure

Figure 8-10 illustrates the procedure for location query of the capability exposure API.

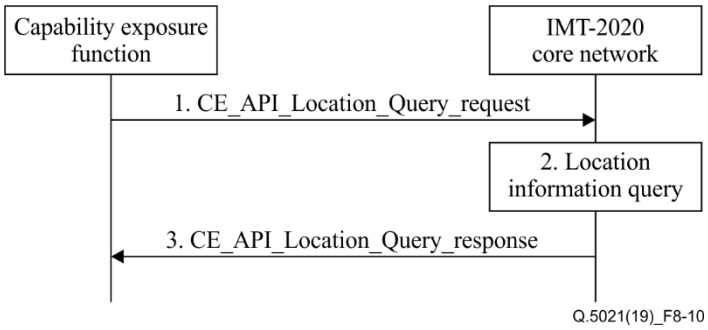

Figure 8-10 – API location query procedure

1. The capability exposure function sends a CE_API_Location_Query request to IMT-2020 core network. It includes the third-party application identity, type of the third-party application identity, name of the third-party application vendor and UE information.
2. The IMT-2020 core network queries the location information based on the UE information.
3. The IMT-2020 core network sends a CE_API_Location_Query response to the capability exposure function.

9 Message format and API definition

This clause specifies the details of each message for API management. 'M' in status field of each table in this clause means mandatory.

9.1 CE_API_Registration

This API enables the capability exposure function to communicate with the API management function to register CEF instance(s) with specific capability exposure APIs over IF4.

Table 9-1 describes the detailed information of CE_API_Registration_request.

Table 9-1 – CE_API_Registration_request

Information element	Status	Data type	Cardinality	Description
capability exposure function instance	M	string	1..N	List of capability exposure function instance corresponding to the request, including the IP address, port number of the capability exposure function instance
API list	M	string	1..N	List of APIs that the capability exposure function support, including the API name, API function description, serving user list

Table 9-2 describes the detailed information of CE_API_Registration_response.

Table 9-2 – CE_API_Registration_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	201 400 500	Indicates the success or failure of the registration of the service API information 201 Created 400 Input Parameter Error 500 Server Internal Error

9.2 CE_API_Discovery

This API enables the third-party application to communicate with the API management function to discover CEF instance(s) with specific capability exposure APIs over IF3.

Table 9-3 describes the detailed information of CE_API_Discovery_request.

Table 9-3 – CE_API_Discovery_request

Information element	Status	Data type	Cardinality	Description
third-party application identity information	M	string	1	Identity information of the third-party application
type of the third-party application identity information	M	string	1	The type of the third-party application identity information
name of the third-party application vendor	M	string	1..N	The name of the third-party application vendor
query information	M	string	1..N	Criteria for discovering matching service APIs (e.g., API type, API name)

Table 9-4 describes the detailed information of CE_API_Discovery_response.

Table 9-4 – CE_API_Discovery_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the discovery of the service API information 200 OK 400 Input Parameter Error 500 Server Internal Error
capability exposure function instance	M	string	1..N	N/A	List of capability exposure function instance corresponding to the request, including the IP address, port number of the capability exposure function instance
API list	M	string	1..N	N/A	List of APIs that the capability exposure function support, including the API name, API description, serving user list

9.3 CE_API_Authorization

This API enables the third-party application to communicate with the API management function to check whether the third-party application is authorized to access the capability exposure APIs over IF3.

Table 9-5 describes the detailed information of CE_API_Authorization_request.

Table 9-5 – CE_API_Authorization_request

Information element	Status	Data type	Cardinality	Description
third-party application identity information	M	string	1	Identity information of the third-party application
type of the third-party application identity information	M	string	1	The type of the third-party application identity information
name of the third-party application vendor	M	string	1..N	The name of the third-party application vendor
query information	M	string	1..N	Criteria for authorized matching service APIs (e.g., API type, API name)

Table 9-6 describes the detailed information of CE_API_Authorization_response.

Table 9-6 – CE_API_Authorization_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the authorization of the service API information 200 OK 400 Input Parameter Error 500 Server Internal Error

9.4 CE_API_Authentication

This API enables the third-party application to communicate with the API management function to obtain mutual authentication over IF3.

Table 9-7 describes the detailed information of CE_API_Authentication_request.

Table 9-7 – CE_API_Authentication_request

Information element	Status	Data type	Cardinality	Description
third-party application identity information	M	string	1	Identity information of the third-party application
type of the third-party application identity information	M	string	1	The type of the third-party application identity information
third-party application key information	M	string	1..N	Key information of third-party application

Table 9-8 describes the detailed information of CE_API_Authentication_response.

Table 9-8 – CE_API_Authentication_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the authorization of the service API information 200 OK 400 Input Parameter Error 500 Server Internal Error
API management function key information	M	string	1..N	N/A	Key information of API management function, e.g., server-side certificate or key

9.5 CE_API_Deregistration

This API enables the capability exposure function to communicate with the API management function to deregister CEF instance(s) with specific capability exposure APIs over IF4.

Table 9-9 describes the detailed information of CE_API_Deregistration_request.

Table 9-9 – CE_API_Deregistration_request

Information element	Status	Data type	Cardinality	Description
API name	M	string	1	The name of deregistration API
API function description	M	string	1	The function description of deregistration API
capability exposure function instance	M	string	1..N	List of capability exposure function instance support the deregistration API, including the IP address, port number of the capability exposure function instance
serving the third-party application list	M	string	1..N	List of serving the third-party applications that the deregistration API support, including the application name, vendor name

Table 9-10 describes the detailed information of CE_API_Deregistration_response.

Table 9-10 – CE_API_Deregistration_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the deregister of the API 200 OK 400 Input Parameter Error 500 Server Internal Error

9.6 CE_API_Suspension

This API enables the capability exposure function to communicate with the API management function to suspended API invocation over IF4.

Table 9-11 describes the detailed information of CE_API_Suspension_request.

Table 9-11 – CE_API_Suspension_request

Information element	Status	Data type	Cardinality	Description
API name	M	string	1	The name of suspension API
API function description	M	string	1	The function description of suspension API
capability exposure function instance	M	string	1..N	List of capability exposure function instance support the suspension API, including the IP address, port number of the capability exposure function instance
serving the third-party application list	M	string	1..N	List of serving the third-party applications that the suspension API supports, including the application name, vendor name
duration of suspension	M	num	1	Duration of API suspension, from 0 to maximum number. 0 represents indefinite duration

Table 9-12 describes the detailed information of CE_API_Suspension_response.

Table 9-12 – CE_API_Suspension_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the suspension of the API 200 OK 400 Input Parameter Error 500 Server Internal Error

9.7 CE_API_Suspension_Notify

This API enables the capability exposure function to communicate with the third-party application to notify the suspension state of CEF instance(s) with specific capability exposure APIs over IF2.

Table 9-13 describes the detailed information of CE_API_Suspension_Notify_request.

Table 9-13 – CE_API_Suspension_Notify_request

Information element	Status	Data type	Cardinality	Description
API name	M	string	1	The name of suspension API
API function description	M	string	1	The function description of suspension API
capability exposure function instance	M	string	1..N	List of capability exposure function instance support the suspension API, including the IP address, port number of the capability exposure function instance
duration of suspension	M	num	1	Duration of API suspension, from 0 to maximum number. 0 represents indefinite duration

Table 9-14 describes the detailed information of CE_API_Suspension_Notify_response.

Table 9-14 – CE_API_Suspension_Notify_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the suspension notification of the API 200 OK 400 Input Parameter Error 500 Server Internal Error

9.8 CE_API_Recovery

This API enables the capability exposure function to communicate with the API management function to recover the invocation of API over IF4.

Table 9-15 describes the detailed information of CE_API_Recovery_request.

Table 9-15 – CE_API_Recovery_request

Information element	Status	Data type	Cardinality	Description
API name	M	string	1	The name of recovery API
API function description	M	string	1	The function description of recovery API
capability exposure function instance	M	string	1..N	List of capability exposure function instance support the recovery API, including the IP address, port number of the capability exposure function instance

Table 9-15 – CE_API_Recovery_request

Information element	Status	Data type	Cardinality	Description
serving the third-party application list	M	string	1..N	List of serving the third-party applications that the recovery API supports, including the application name, vendor name
duration of suspension	M	num	1	Duration of API suspension, from 0 to maximum number. 0 represents indefinite duration

Table 9-16 describes the detailed information of CE_API_Recovery_response.

Table 9-16 – CE_API_Recovery_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the recovery of the API 200 OK 400 Input Parameter Error 500 Server Internal Error

9.9 CE_API_Recovery_Notify

This API enables the capability exposure function to communicate with the third-party application to notify recovery of CEF instance(s) with specific capability exposure APIs over IF2.

Table 9-17 describes the detailed information of CE_API_Recovery_Notify_request.

Table 9-17 – CE_API_Recovery_Notify_request

Information element	Status	Data type	Cardinality	Description
API name	M	string	1	The name of recovery API
API function description	M	string	1	The function description of recovery API
capability exposure function instance	M	string	1..N	List of capability exposure function instance support the recovery API, including the IP address, port number of the capability exposure function instance
duration of suspension	M	num	1	Duration of API suspension, from 0 to maximum number. 0 represents indefinite duration

Table 9-18 describes the detailed information of CE_API_Recovery_Notify_response.

Table 9-18 – CE_API_Recovery_Notify_response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the recovery notification of the API 200 OK 400 Input Parameter Error 500 Server Internal Error

9.10 CE_API_Charging_Monitoring

This API enables the capability exposure function to communicate with the API management function to notify the invocation of APIs and charge based on it over IF4.

Table 9-19 describes the detailed information of CE_API_Charging_Monitoring_request.

Table 9-19 – CE_API_Charging_Monitoring_request

Information element	Status	Data type	Cardinality	Description
third-party application identity information	M	string	1	Identity information of the third-party application
type of the third-party application identity information	M	string	1	The type of the third-party application identity information
API list	M	string	1..N	List of APIs that the third-party application invoke

Table 9-20 describes the detailed information of CE_API_Charging_Monitoring_response.

Table 9-20 – CE_API_Charging_Monitoring_response

Information element	Status	Data type	Cardinality	Code Value	Description
result	M	num	1	201 400 500	Indicates the success or failure of the invocation event notification response of the service API information 201 Created 400 Input Parameter Error 500 Server Internal Error

9.11 CE_API_Topology_Hiding

This API enables the capability exposure function to communicate with the API management function to determine API management function as the entry point for service API invocation for third-party application outside the IMT-2020 network trust domain.

Table 9-21 describes the detailed information of CE_API_Topology_Hiding_request.

Table 9-21 – CE_API_Topology_Hiding_request

Information element	Status	Data type	Cardinality	Description
third-party application identity information	M	string	1	Identity information of the third-party application
type of the third-party application identity information	M	string	1	The type of the third-party application identity information
capability exposure function instance	M	string	1..N	List of capability exposure function instance corresponding to the request, including the IP address, port number of the capability exposure function instance
API list	M	string	1..N	List of APIs that the capability exposure function support

Table 9-22 describes the detailed information of CE_API_Topology_Hiding_response.

Table 9-22 – CE_API_Topology_Hiding_response

Information element	Status	Data type	Cardinality	Code Value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the topology hiding of capability exposure function from the third-party application 200 OK 400 Input Parameter Error 500 Server Internal Error

9.12 CE_API_Location_Query

This API enables the capability exposure function communicate with the IMT-2020 core network to query UE location over IF1.

Table 9-23 describes the details information of CE_API_Location_Query request.

Table 9-23 – CE_API_Location_Query request

Information element	Status	Data type	Cardinality	Description
third-party application identity information	M	string	1	Identity information of the third-party application
type of the third-party application identity information	M	string	1	The type of the third-party application identity information
name of the third-party application vendor	M	string	1..N	The name of the third-party application vendor
UE information	M	string	1..N	UE ID which CEF query location information for

Table 9-24 describes the details information of CE_API_Location_Query response.

Table 9-24 – CE_API_Location_Query response

Information element	Status	Data type	Cardinality	Code value	Description
result	M	num	1	200 400 500	Indicates the success or failure of the discovery of the service API information 200 OK 400 Input Parameter Error 500 Server Internal Error
location information	M	string	1..N	N/A	Location information of UE which CEF query for.
time information	M	string	1..N	N/A	Time information of the location information.

Bibliography

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

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

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

[b-ITU-T Y.IMT2020-CEF] Draft Recommendation ITU-T Y.IMT2020-CEF, *Network capability exposure function in the IMT-2020 networks*.

[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.2083-0] 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, 2019