International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3133

(12/2019)

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

Future networks

Capability exposure enhancement for supporting fixed mobile convergence in IMT-2020 networks

Recommendation ITU-T Y.3133

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.3133

Capability exposure enhancement for supporting fixed mobile convergence in IMT-2020 networks

Summary

Recommendation ITU-T Y.3133 describes the requirements of the capability exposure for supporting fixed mobile convergence (FMC) in IMT-2020 networks, then defines the functional architecture, the function entities, the procedures and the high level application programming interface (API) descriptions for network capabilities exposure for supporting FMC in IMT-2020 networks.

In particular, the enhancement capabilities requirements include, unified authentication, authorization and charging, user's access type and capability, multi-access edge computing, unified customization of quality of service (QoS) capabilities, FMC network slice control, session management and mobility management, unified user data.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3133	2019-12-14	13	11.1002/1000/14131

Keywords

API, capability exposure, FMC, IMT-2020.

[*] 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

Page

Recommendation ITU-T Y.3133

Capability exposure enhancement for supporting fixed mobile convergence in IMT-2020 networks

1 Scope

This Recommendation describes the requirements of the capability exposure for supporting FMC in IMT-2020 networks. It also defines the functional architecture, the functional entities, the procedures and the high-level API descriptions for network capabilities exposure for supporting FMC in IMT-2020 networks.

This Recommendation is also aligned with the requirements identified in [ITU-T Y.3101], [ITU-T Y.3130] and [ITU-T Y.3105]. Based on the capabilities exposure of the IMT-2020, the capability exposure requirements, architecture and processes are enhanced in order to support FMC.

In particular, the enhanced capabilities include, unified authentication, authorization and charging, user's access type and capability, multi-access edge computing, unified customization of QoS capabilities, FMC network slice control, session management and mobility management, unified user data.

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.1762] Recommendation ITU-T Q.1762/Y.2802 (2007), *Fixed-mobile convergence general requirements.*

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

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

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

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

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

[ITU-T Y.3130] Recommendation ITU-T Y.3130 (2018), *Requirements of IMT-2020 fixed mobile convergence*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 control plane [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 data plane [ITU-T Y.2011]: The set of functions used to transfer data in the stratum or layer under consideration.

3.1.3 fixed mobile convergence [ITU-T Y.3100]: In the context of IMT-2020, the capabilities that provide services and applications to end users regardless of the fixed or mobile access technologies being used and independently of the users' location.

3.1.4 fixed network [ITU-T Q.1762]: A network that provides wire-based (e.g., copper, fibre) or wireless access to its services. The fixed network may support nomadism, but does not support mobility.

3.1.5 mobile network [ITU-T Q.1762]: A network that provides wireless access to its services and supports mobility.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 IMT-2020 (Based on [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].

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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, Accounting
AN	Access Network
API	Application Programming Interface
ARP	Allocation and Retention Priority
BSS	Billing Supporting System
CE	Capability Exposure
FMC	Fixed Mobile Convergence
HSS	Home Subscriber Server
KPI	Key Performance Indicator
LTE	Long Term Evolution
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
MM	Mobility Management
OSS	Operation Supporting System
QCI	QoS Class Indicator

QoE	Quality of Experience
QoS	Quality of Service
SM	Session Management
WLAN	Wireless Local Area Network

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.

6 Overview of capability exposure in IMT-2020 FMC networks

The IMT-2020 network is envisioned to have an access network-agnostic unified core network supporting diverse fixed and mobile access networks. The IMT-2020 FMC network is required to support network capability exposure (CE) in order to allow third-party applications to access information regarding services provided by the IMT-2020 network, and to dynamically customize the network capabilities, especially the FMC network capability, for diverse use cases.

The network capability exposure for FMC is aligned with the requirements identified in [ITU-T Y.3101], [ITU-T Y.3130] and [ITU-T Y.3105]. The additional key FMC network exposure capability are expected to include, but are not limited to:

- Unified authentication, authorization, charging;
- User's access type and capability;
- Multi-access edge computing;
- Unified QoS customization capabilities;
- FMC network slice control;
- Session management (SM) and mobility management;
- Unified user data.

7 CE functional requirements of FMC

7.1 Unified authentication, authorization, and charging

7.1.1 Description

A unified authentication and authorization framework across heterogeneous access networks is desirable in the IMT-2020 FMC network. Efficient and effective user and device identification mechanisms are needed in order to cope with the diversity of service and device types to be supported by the IMT-2020 FMC network.

IMT-2020 FMC network can aggregate charging information, simultaneously and independently of the fixed access network or mobile access network, for a single user, to provide total charging information for the user.

7.1.2 Requirements

IMT-2020 FMC network is required to support a unified authentication and authorization framework for a unified identity of the end user for fixed and mobile access technologies.

IMT-2020 FMC network is required to provide the unified authentication and authorization capability application programme interfaces (APIs) to third-party applications.

IMT-2020 FMC network is required to support the provisioning of charging APIs to third-party applications.

7.2 User's access type and capability

7.2.1 Description

IMT-2020 FMC network provides different access technologies for users with different user experiences, such as broad bandwidth, low time delay, massive connections and high security. The main purpose of fixed and mobile convergence for multiple access technologies is to federate all means of access technologies including fixed and mobile accesses, providing users with the capability to access the network ubiquitously and to enjoy the best service experience under the circumstance. IMT-2020 FMC network needs to expose the user's access type and capability to provide versatile services.

7.2.2 Requirements

IMT-2020 FMC network is required to support the exposure of the end user's access type APIs, including single (fixed or mobile) access type and multiple (fixed and mobile) access type, accessible by third-party applications.

7.3 Multi-access edge computing

7.3.1 Description

Multi-access edge computing, as its name implies, enables the hosting of applications close to the end users in a telecommunications network that consists of different multiple access technologies. Multi-access edge computing is acknowledged as one of the key pillars for meeting the demanding key performance indicators (KPIs) of 5G, especially as far as low latency and bandwidth efficiency are concerned. However, not only is multi-access edge in telecommunications networks a technical enabler for the demanding KPIs, it also plays an essential role in the transformation of the telecommunications business, where telecommunications networks are turning into versatile service platforms for industry and other specific customer segments. This transformation is supported by multi-access edge computing, as it opens the network edge for applications and services, including those from third-party applications.

– **Optimizing QoE and resource utilization in multi-access network**

From the end user device's point of view, this results in multi-connectivity scenarios where the devices can be simultaneously connected to applications and services of a distributed cloud over different access technologies such as wireless local area network (WLAN), long term evolution (LTE), 5G and fixed broadband access technologies. In such an environment, the overall quality of experience (QoE) perceived by the end users as well as utilization of the resources can be optimized with smart selection and a combination of the paths used for the user plane. In an advanced solution, the network paths can be dynamically selected based on knowledge of the current conditions in the relevant access networks.

– **Traffic routing**

When third-party applications are deployed on the FMC network edge, some data traffic can be routed to the FMC network edge or to a remote application server.

7.3.2 Requirements

The IMT-2020 FMC network is required to provide access network information APIs to multi-access edge computing (MEC) systems. There should be a MEC service that exposes up-to-date information regarding specific access network technology and the access network information should include:

- Access technology type, for example WLAN, 4G, 5G, and fixed broadband access technologies, etc.;
- Bi-directional bandwidth information that is delivered to/from the specific user;
- Granular bi-directional bandwidth information that is delivered to/from the specific user on the level of specific application, class of service, etc.
- Latency information;
- Access technology specific information such as network identifiers, physical link conditions, radio link conditions, etc., and network conditions such as congestion, overload, etc.

The IMT-2020 FMC network is required to provide APIs that allow authorized third-party applications to send/receive user plane traffic to user equipment, and route selected uplink and/or downlink user plane traffic from the FMC network to authorized MEC applications.

7.4 Unified QoS customization capabilities

7.4.1 Description

In the IMT-2020 FMC network, the QoS of the mobile network is based on the bearers and QoS class indicator/allocation and retention priority (QCI/ARP), while the QoS of wireline networks is based on hierarchical scheduling at the service edge and Diffserv/DSCP or 802.1p/P-bits in the rest of the access network. End-to-end unified QoS control is needed to support proper QoS integration between the different network segments of the IMT-2020 FMC network.

The IMT-2020 FMC network is expected to provide the required QoS for a variety of different services with different characteristics, enable unified QoS customization by network functionalities in order to support diverse third-party application requirements. Information related to the unified QoS parameterization of FMC network capabilities, provided by the network, is needed for a third-party application to analyse and make a decision on the services in order to get the required user experience.

7.4.2 Requirements

The IMT-2020 FMC network is required to support unified FMC QoS control mechanisms independently of network access technologies.

The IMT-2020 FMC network is required to expose unified QoS information and APIs related to network capabilities to third-party applications.

The IMT-2020 FMC network is required to support configuring the FMC QoS parameters on network element according to the API invocation.

7.5 FMC network slice control

7.5.1 Description

A FMC network slice is formed by combining resources from both fixed and mobile networks. A FMC slice takes advantage of the development of common network functions and interfaces in IMT-2020 networks. A FMC slice allows the support of data plane across different accesses with various degrees of deterministic performance in terms of throughput, latency, resiliency, etc. It also allows to provide a common control plane that can optimize the service provision and availability to offer a continuous service experience across fixed and mobile networks.

7.5.2 Requirements

The IMT-2020 FMC network is required to provide APIs which allow authorized third-party applications to create, modify and delete the FMC network slices used for the third-party applications.

The IMT-2020 FMC network is required to provide APIs which allow authorized third-party applications to monitor the state of the FMC network slices used for the third-party applications.

The IMT-2020 FMC network is required to provide APIs which allow authorized third-party applications to specify and update the capabilities supported by the FMC network slices used for the third-party applications.

The IMT-2020 FMC network is required to provide APIs which allow authorized third-party applications to adapt the capacity (elastic scaling of the capacity) of the FMC network slices used for the third-party applications.

The IMT-2020 FMC network is required to provide APIs which allow authorized third-party applications to be notified of the status, usage and expenses of the FMC network slices used for the third-party applications.

The IMT-2020 network should also be able to provide a charging APIs that enables independent charging for each network slice.

NOTE – Different charging models may be applied to each network slice at the cost of complexity.

7.6 Session management and mobility management

7.6.1 Description

IMT-2020 FMC network session management supports user selecting the access network(s) to transport traffic, and dividing traffic into multiple pieces which are transported through different access networks and moving traffic from one access network to another one.

IMT-2020 FMC network mobility management (MM) supports user equipment moving within an access network (such as mobile network) or switches between different access networks (such as mobile network and fixed network) and changes its access point.

7.6.2 Requirements

IMT-2020 FMC network is required to provide APIs supporting traffic switching, splitting, and steering between fixed access network and mobile access network on the network side.

IMT-2020 FMC network is required to provide APIs supporting traffic switching, splitting, and steering on the user equipment side.

IMT-2020 FMC network is required to provide APIs supporting session continuity capability for the end user applications when the end user moves between fixed and mobile access networks.

IMT-2020 FMC network is also required to provide unified mobility state management capability APIs for third-party applications.

7.7 Unified user data

7.7.1 Description

The location and structure of user data storage vary in different access networks. For example, user data is stored by authentication, authorization, accounting (AAA) server in fixed networks, while it is stored and managed by home subscriber server (HSS) in 4G networks. This kind of data separation results in several drawbacks such as data redundancy and service development difficulties.

7.7.2 Requirements

IMT-2020 FMC network is required to provide APIs of unified user data capability to reduce maintenance cost and provide conditions for service development and big data analysis.

8 Architecture and function entities of enhanced CE for supporting FMC

8.1 General architecture

This clause provides an overview of the architecture for enhanced capability exposure and describes the architecture of enhanced network capability exposure for supporting FMC.

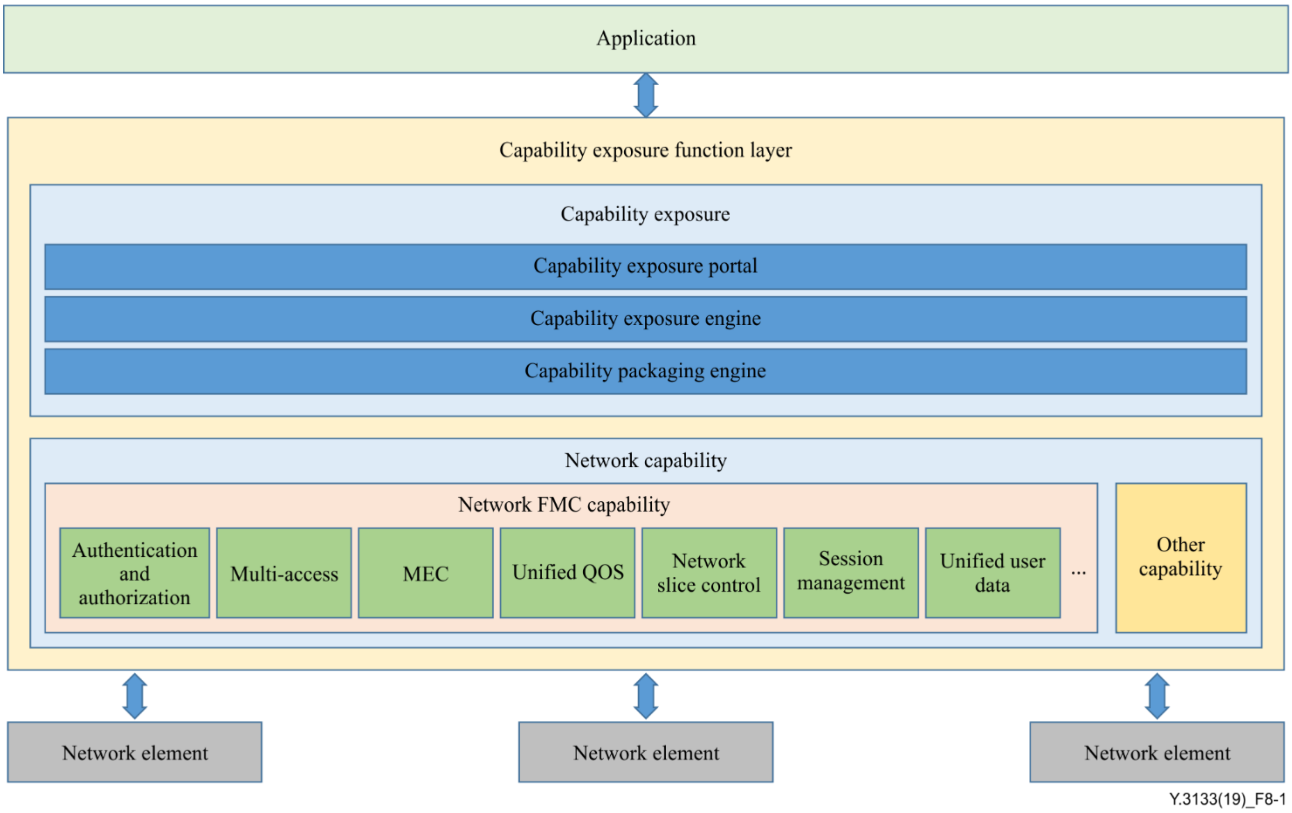

Figure 8-1 – Architecture for enhanced capability exposure for supporting FMC

Architecture for enhanced capability exposure for supporting FMC includes three parts, that is, application, capability exposure function layer and network element.

The application is to implement the invocation of the network capability APIs and then use the network capabilities via the APIs.

The capability exposure function layer includes two parts, that is, the network capability and capability exposure. Network capability refers to the ability of IMT-2020 FMC network to exposure, including FMC capabilities and other capabilities. The capability exposure mainly implements APIs encapsulation, capability orchestration and operation management of network capability engines, as well as unified operation and maintenance management and access control.

The network element refers to the network elements of the operator such as the operators' wireless access networks, fixed access networks, billing supporting system/operation supporting system (BSS/OSS), management and orchestration (MANO), network slicing, MEC, and big data analytics platforms, etc.

8.2 Application

The application provider has service agreements with IMT-2020 FMC network operators. The application invokes the network capability APIs. The application supports the following capabilities:

– Supporting the authentication by providing the identity and other information required for authentication of the IMT-2020 FMC network operator;

- Supporting mutual authentication with IMT-2020 FMC network operator;
- Obtaining the authorization prior to accessing the service APIs;
- Discovering capabilities APIs information.

8.3 Capability exposure function

The capability exposure function consists of the following capabilities:

- Authenticating the third-party application based on the identity and other information required for authentication of the capabilities invocation;
- Supporting mutual authentication with the third-party applications;
- Providing authorization for the 3rd applications prior to accessing the network capability APIs;
- Publishing, storing and supporting the discovery of network capability APIs information;
- Controlling the network capability APIs access based on IMT-2020 FMC network operator configured policies;
- Storing the logs for the network capability APIs invocations and providing the network capability APIs invocation logs to authorized applications;
- Charging based on the logs of the network capability APIs invocations;
- Monitoring the status of the network capability APIs;
- On boarding a new APIs invocation and off boarding an APIs invocation;
- Support accessing the logs for auditing (e.g., detecting abuse).
- Logging the network capability API invocations.

8.4 Network element

Network elements provide atomic network capabilities and capabilities information to application via the network capability exposure function.

9 Procedures and high-level API descriptions for network capabilities exposure

9.1 Unified authentication, authorization, and charging

A unified authentication and authorization mechanism and unified aggregated charging across heterogeneous access networks are desirable in the IMT-2020 FMC network. The capability exposure function provides exposed unified authentication, authorization, and charging APIs to the third-party application. The detailed procedure is depicted in Figure 9-1.

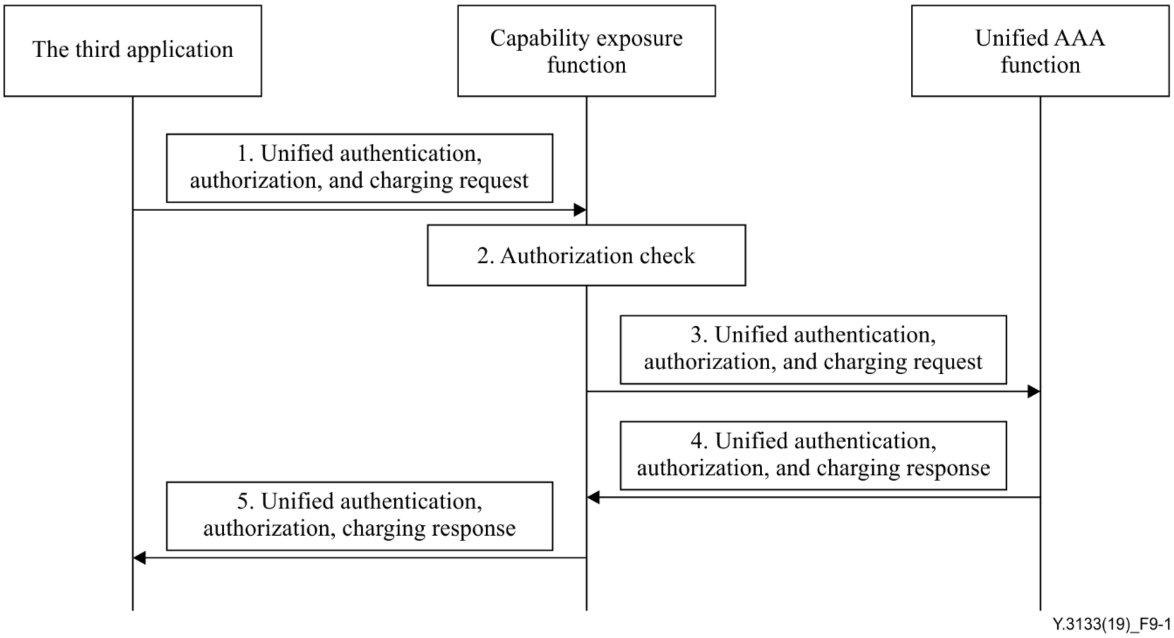
The third application
Capability exposure function
Unified AAA function
1. Unified authentication, authorization, and charging request
2. Authorization check
3. Unified authentication, authorization, and charging request
4. Unified authentication, authorization, and charging response
5. Unified authentication, authorization, charging response
Y.3133(19)_F9-1

Figure 9-1 – Unified authentication, authorization, and charging procedure

1) The third-party application sends a unified authentication, authorization and charging request to the capability exposure function in order to obtain permission to access a specific network capability by including the third-party application identity information and any other information required for authentication, authorization and charging of the third-party application.

2) The capability exposure function validates the authentication of the third-party application and checks whether the third-party application is permitted to access the requested network capability.

3) Then the capability exposure function sends the request to the unified AAA function.

4-5) Based on the third-party application subscription information, the authorization information for the access by the third-party application is sent to the third-party application as authorization response. Unified billing information is provided after the end of the capabilities invocation.

9.2 User's access type and capability

The capability exposure function can exposure the IMT-2020 FMC network end user's access type APIs and capability to third-party application to provide the user with the capability to access the network ubiquitously and to enjoy the best service experience. The detailed procedure is depicted in Figure 9-2.

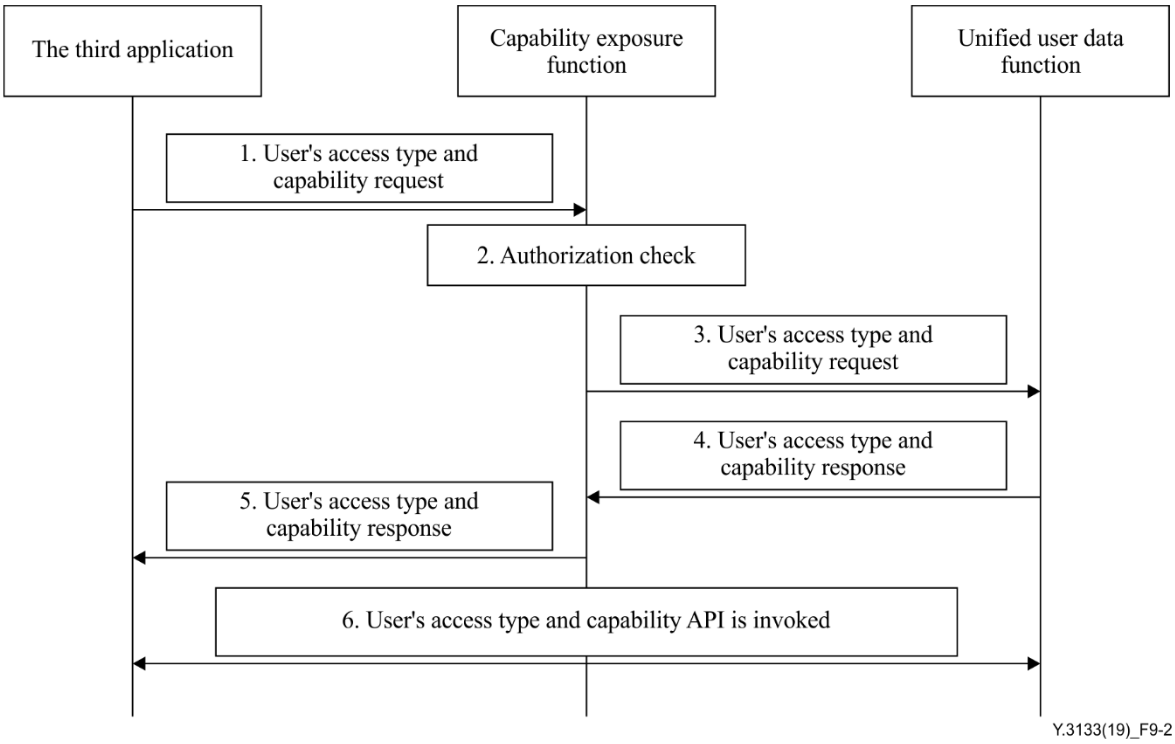
The third application
Capability exposure function
Unified user data function
1. User's access type and capability request
2. Authorization check
3. User's access type and capability request
4. User's access type and capability response
5. User's access type and capability response
6. User's access type and capability API is invoked
Y.3133(19)_F9-2

Figure 9-2 – User's access type and capability procedure

1) The third-party application sends a user's access type and capability request to the capability exposure function in order to obtain permission to access user's access type and capability.

2) The capability exposure function validates the authentication of the third-party application and checks whether the third-party application is permitted to access the requested network capability.

3) The capability exposure function sends the request to the unified user data function.

4) Based on the third-party application subscription information, the unified user data function acknowledges the subscription by sending the user's access type and capability response to the capability exposure function.

5) The capability exposure function registers and maintains the association of the user's access type and capability to invoke and inform the third-party application.

6) The third-party application initiates the invocation of user's access type and capability.

9.3 Multi-access edge computing

Multi-access edge computing capabilities is aligned with the procedure for edge computing identified in [ITU-T Y.3108], in particular with the additional requirements stating that when third-party applications are deployed on the FMC network edge, the network paths can be dynamically selected based on the conditions of multiple access networks and MEC service requirement. The detailed procedure is depicted in Figure 9-3.

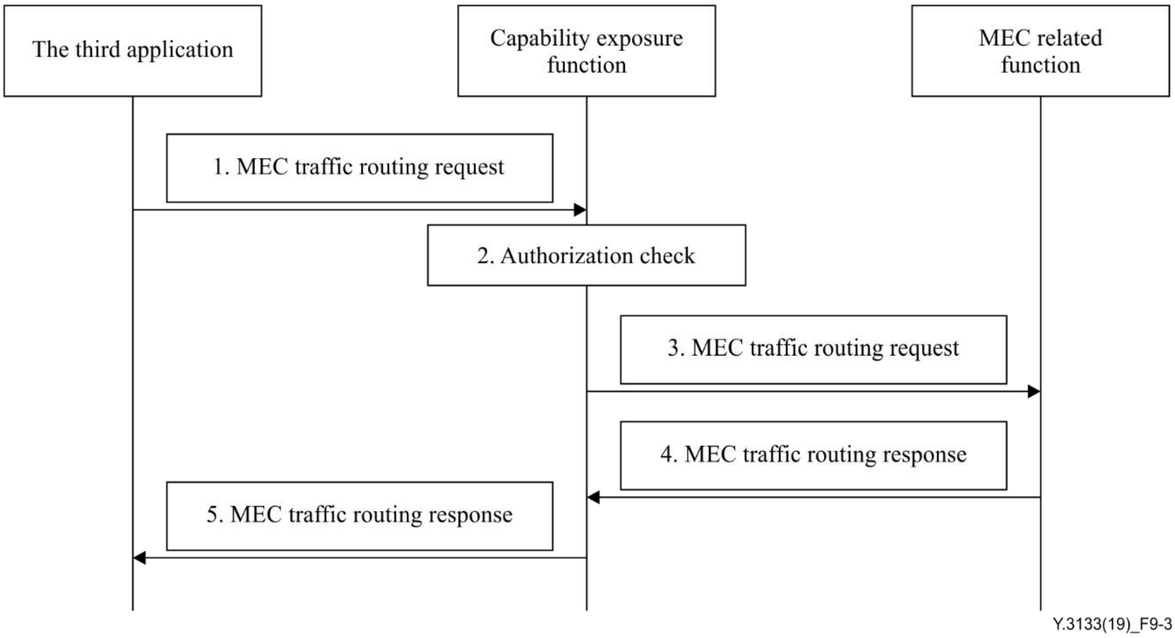
The third application
Capability exposure function
MEC related function
1. MEC traffic routing request
2. Authorization check
3. MEC traffic routing request
4. MEC traffic routing response
5. MEC traffic routing response
Y.3133(19)_F9-3

Figure 9-3 – MEC traffic routing procedure

1) The third-party application sends a MEC traffic routing request to the capability exposure function in order to obtain permission to invoke the APIs of MEC traffic routing.

2) The capability exposure function validates the authentication of the third-party application and checks whether the third-party application is permitted to access the requested network capability.

3) The capability exposure function sends the MEC traffic routing request to MEC related functions.

4) Based on the third-party application subscription information, the MEC related functions acknowledges the subscription by sending the third-party applications response to the capability exposure function.

5) The capability exposure function registers and maintains the association of the multi-access edge computing capability to invoke and inform the third-party application. Subsequently, the third-party application initiates the invocation of multi-access edge computing capability to route traffic.

9.4 Unified QoS customization capabilities

Unified QoS customization capabilities is aligned with the procedure for customization of QoS capabilities identified in [ITU-T Y.3108], in particular with the additional requirements that is needed to support unified QoS integration between the different network segments of the IMT-2020 FMC network. The detailed procedure is depicted in Figure 9-4.

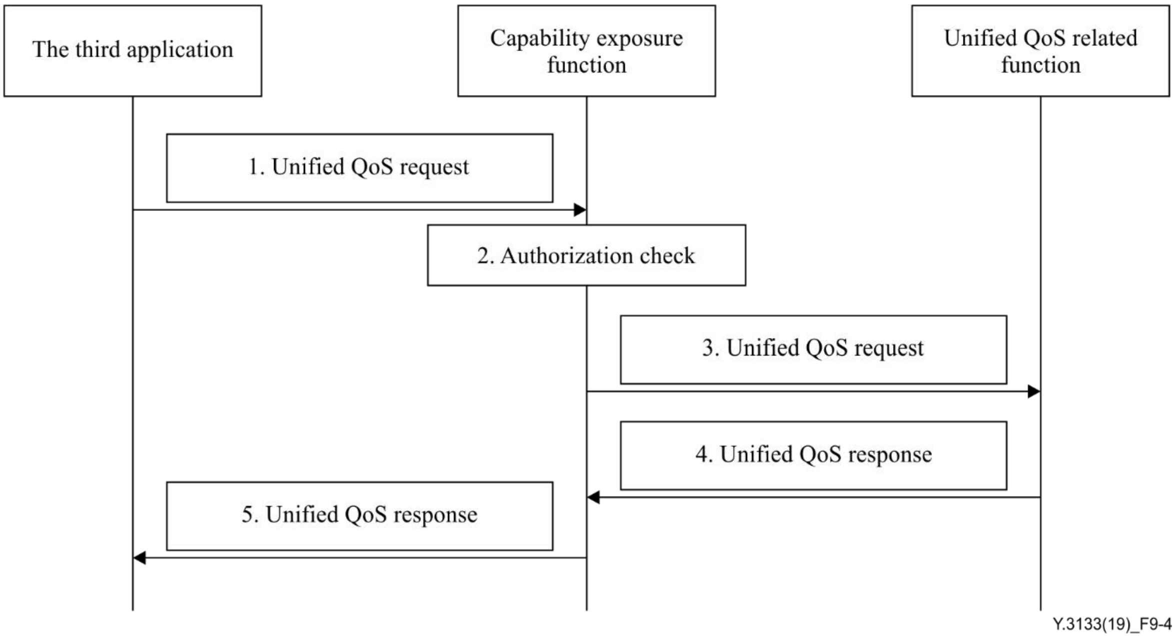

Figure 9-4 – Unified QoS customization procedure

1) The third-party application sends a unified QoS request to the capability exposure function in order to obtain permission to invoke the APIs of unified QoS customization capabilities.

2) The capability exposure function validates the authentication of the third-party application and checks whether the third-party application is permitted to access the requested network capability.

3) The capability exposure function sends the request to the unified QoS related function.

4) Based on the third-party application subscription information, the unified QoS related function acknowledges the subscription by sending the third-party applications response to capability exposure function.

5) The capability exposure function registers and maintains the association of the unified QoS customization capabilities to invoke and inform the third-party application. Thereafter, the third-party application initiates the invocation of unified QoS customization capabilities.

9.5 FMC network slice control

FMC network slice control is aligned with the procedure for the network slice management capability exposure identified in [ITU-T Y.3108], in particular with the additional requirements that is needed to support unified network slice control between the different network segments of the IMT-2020 FMC network. FMC network slice allows to provide a common control plane that can optimize the service provision and the availability to offer a continuous service experience across fixed and mobile networks. The detailed procedure is depicted in Figure 9-5.

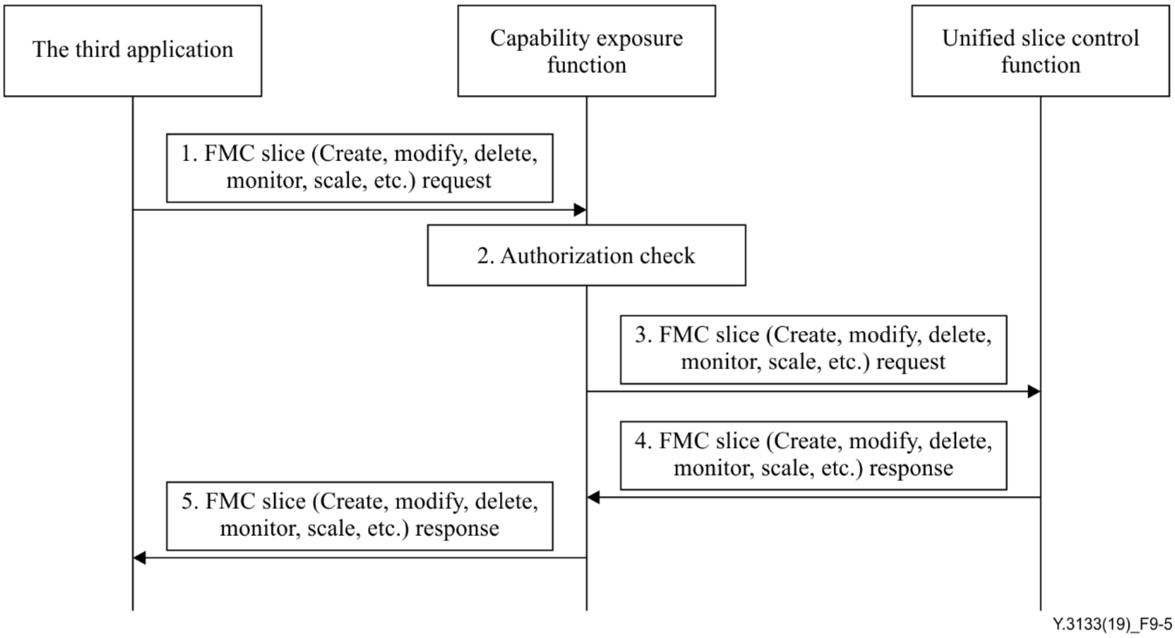
The third application
Capability exposure function
Unified slice control function
1. FMC slice (Create, modify, delete, monitor, scale, etc.) request
2. Authorization check
3. FMC slice (Create, modify, delete, monitor, scale, etc.) request
4. FMC slice (Create, modify, delete, monitor, scale, etc.) response
5. FMC slice (Create, modify, delete, monitor, scale, etc.) response
Y.3133(19)_F9-5

Figure 9-5 – FMC network slice control procedure

1) The third-party application sends a FMC slice (create, modify, delete, monitor, scale, etc.) request to the capability exposure function in order to obtain permission to invoke the APIs of FMC network slice control.

2) The capability exposure function validates the authentication of the third-party application and checks whether the third-party application is permitted to access the requested network capability.

3) The capability exposure function sends the request to the unified slice control function (e.g., unified MANO).

4) Based on the third-party application subscription information, the unified slice control function acknowledges the subscription by sending the FMC slice (create, modify, delete, monitor, scale, etc.) response to the capability exposure function.

5) The capability exposure function registers and maintains the association of the FMC network slice control capabilities to invoke and inform the third-party application. Then the third-party application initiates the invocation of FMC network slice control capabilities.

9.6 Session management and mobility management

The capability exposure function can exposure the APIs of session management and mobility management to provide a third-party application with user mobility and service continuity capability. The detailed procedure is as depicted in Figure 9-6.

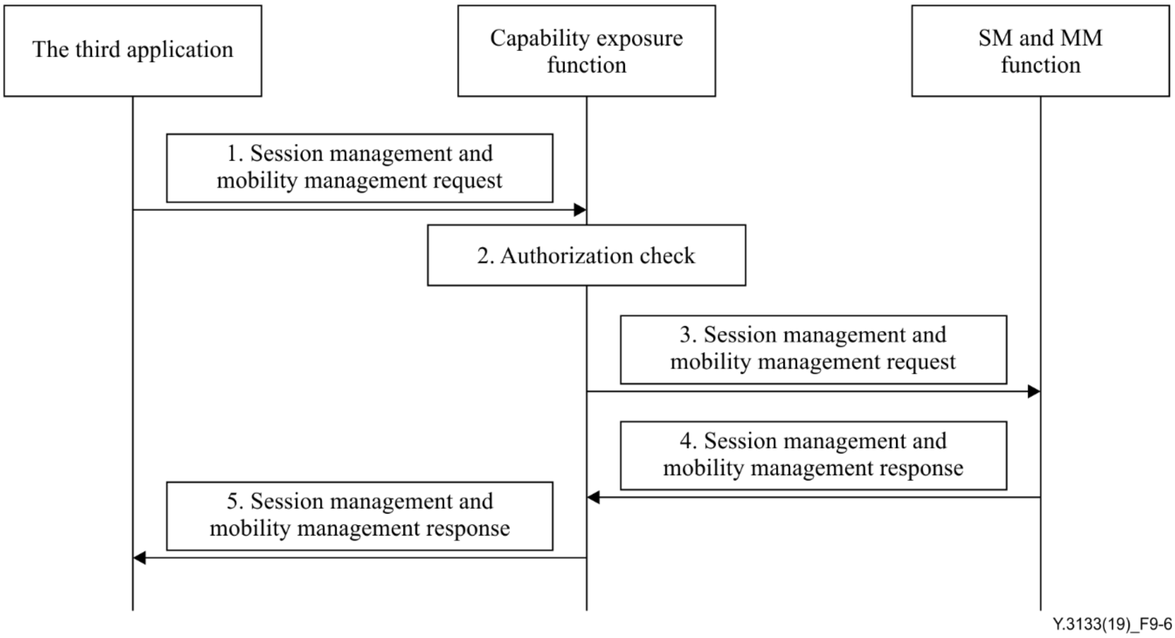
The third application
Capability exposure function
SM and MM function
1. Session management and mobility management request
2. Authorization check
3. Session management and mobility management request
4. Session management and mobility management response
5. Session management and mobility management response
Y.3133(19)_F9-6

Figure 9-6 – Session management and mobility management procedure

1) The third-party application sends a session management and mobility management request to the capability exposure function in order to obtain permission to invoke the APIs of session management and mobility management.

2) The capability exposure function validates the authentication of the third-party application and checks whether the third-party application is permitted to access the requested network capability.

3) The capability exposure function sends the request to the SM function and the MM function.

4) Based on the third-party application subscription information, the SM function and MM function acknowledges the subscription by sending the third-party applications response to the capability exposure function.

5) The capability exposure function registers and maintains the association of the session management and mobility management capability to invoke and inform the third-party application. Thereafter the third-party application initiates the invocation of the session management and mobility management capability.

9.7 Unified user data

The capability exposure function can exposure the APIs of the unified user data capabilities to third-party applications to reduce the maintenance cost and provide conditions for service development and big data analysis. The detailed procedure is depicted in Figure 9-7.

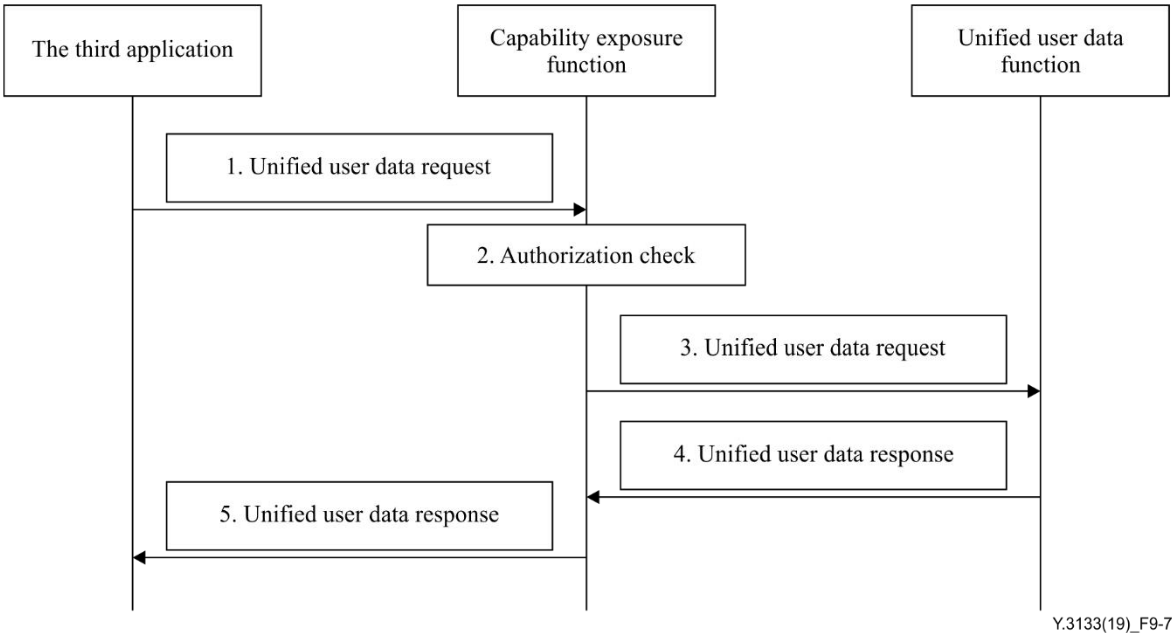
The third application
Capability exposure function
Unified user data function
1. Unified user data request
2. Authorization check
3. Unified user data request
4. Unified user data response
5. Unified user data response
Y.3133(19)_F9-7

Figure 9-7 – Unified user data procedure

1) The third-party application sends a unified user data request to the capability exposure function in order to obtain permission to invoke the APIs of the unified user data capability.

2) The capability exposure function validates the authentication of the third-party application and checks whether the third-party application is permitted to access the requested network capability.

3) The capability exposure function sends the request to the unified user data function.

4) Based on the third-party application subscription information, the unified user data function acknowledges the subscription by sending the third-party applications response to the capability exposure function.

5) The capability exposure function registers and maintains the association of the unified user data capability to invoke and inform the third-party application. Then the third-party application initiates the invocation of unified user data capability.

10 Security consideration

The capability exposure enhancement in IMT-2020 FMC network should take into account the issues of security and privacy. Each capability exposure component of FMC network should adopt the measures of network information protection and user information protection, to avoid unauthorized access and information leaking.

Security and privacy concerns should be aligned with the requirements specified in [ITU-T Y.3101] and [ITU-T Y.2701].

Bibliography

[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