International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3074

(08/2019)

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

Future networks

Framework for directory service management of large numbers of heterogeneously-named objects in IMT-2020

Recommendation ITU-T Y.3074

ITU-T

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.3074

Framework for directory service management of large numbers of heterogeneously-named objects in IMT-2020

Summary

Recommendation ITU-T Y.3074 introduces a directory service function in the IMT-2020 architecture. It describes the components of the directory service function that can store a large volume of records associated with heterogeneous types of names of objects (i.e., devices and data), and that can provide a very low latency look-up service. It describes the general procedure of the directory service function to register, cache, look up, update and delete records.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3074	2019-08-13	13	11.1002/1000/13985

Keywords

Directory service, ICN, IMT-2020, information-centric networking.

* 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.3074

Framework for directory service management of large numbers of heterogeneously-named objects in IMT-2020

1 Scope

The scope of this Recommendation includes:

- the introduction of a directory service function in the IMT-2020 framework architecture to store a large volume of records associated with heterogeneous types of names of objects, and provide a very low latency look-up service;
- the description of the functional components and procedures to register, cache, look up, update and delete records.

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 X.500] Recommendation ITU-T X.500 (2016), *Information Technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

[ITU-T X.501] Recommendation ITU-T X.501 (2016), *Information technology – Open Systems Interconnection – The Directory: Models.*

[ITU-T Y.3001] Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals*.

[ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

[ITU-T Y.3031] Recommendation ITU-T Y.3031 (2012), *Identification framework in future networks*.

[ITU-T Y.3032] Recommendation ITU-T Y.3032 (2014), *Configurations of node identifiers and their mapping with locators in future networks*.

[ITU-T Y.3033] Recommendation ITU-T Y.3033 (2014), *Framework of data aware networking for future networks*.

[ITU-T Y.3071] Recommendation ITU-T Y.3071 (2017), *Data aware networking (information centric networking) – Requirements and capabilities*.

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

[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*.

3 Definitions

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

3.1.3 ICN [b-ITU-T Y Sup. 48]: A new approach to networking where named objects (not only devices) are the principal components for the network. Named data objects can be stored in network nodes (with caching capability) distributed throughout the network. Data objects are transmitted by using names to requesting consumers from any network node that can provide requested data. Locations of the nodes that store data objects in their caches are irrelevant to consumers because they send their requests for data objects by using names (not the data object locations).

NOTE – ICN is an alias to data-aware networking (DAN), and content-centric networking (CCN) and named data networking (NDN) are the example implementations of ICN.

3.1.4 identifier [b-ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.5 name [b-ITU-T Y.2091]: A name is the identifier of an entity (e.g., subscriber, network element) that may be resolved/translated into an address.

3.1.6 network function [ITU-T Y.3100]: This is a processing function in a network. It includes but is not limited to network node functionalities, e.g., session management, mobility management, switching, routing functions, whose functional behaviour and interfaces are defined. Network functions can be implemented as a network node on a dedicated hardware or as a virtualized software functions.

3.1.7 future network (FN) [ITU-T Y.3001]: A network able to provide services, capabilities, and facilities difficult to provide using existing network technologies. A future network is either: a) a new component network or an enhanced version of an existing one, or b) a heterogeneous collection of new component networks or of new and existing component networks that is operated as a single network.

3.1.8 IMT-2020 [ITU-R M.2083-0]: Systems, system components, and related aspects that support to provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

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.

3.1.9 named data object (NDO) [b-ITU-T Y Sup. 35]: This is a data object that is identifiable by a name.

3.1.10 physical resource [ITU-T Y.3100]: A physical asset for computation, storage and/or networking.

3.1.11 user plane [b-ITU-T Y.2011]: A synonym for data plane.

3.1.12 virtual resource [ITU-T Y.3011]: An abstraction of physical or logical resource, which may have different characteristics from the physical or logical resource and whose capability may be not bound to the capability of the physical or logical resource.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 data object: This is data, content or information.

3.2.2 device (ICN): This is an entity connected to the network that generates, holds, transmits or consumes data, content or information.

3.2.3 directory service: This is a network entity that stores information about objects as records and provides records to other entities that send look-up queries containing a search key of the requested records. A directory service stores and provides records that can be useful for the control and management functions of the network.

3.2.4 ICN data object: This is a data object transmitted in ICN.

3.2.5 ICN device: This is an entity connected to the network that generates, holds, transmits or consumes ICN data objects.

3.2.6 named device: This is a device that is assigned with or identified by a name.

3.2.7 named object: This is an object that is assigned with or identified by a name.

3.2.8 network slice (based on [ITU-T Y.3100]): This is a complete end-to-end logically partitioned network providing dedicated telecommunication services and network capabilities. The behaviour of the network slice is realized via network slice instance(s).

3.2.9 object: This refers to data, content, information or devices.

3.2.10 record: This is information about an object stored in and provided by a directory service function.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF	Application Function
AN	Access Network
ASF	Authentication Server Function
CEF	Capability Exposure Function
CM	Connection Management
CN	Core Network
DAN	Data-Aware Networking
DIB	Directory Information Base
DSF	Directory Service Function
GPS	Global Positioning System
ICN	Information-centric Networking
ID	Identifier
IoT	Internet of Things
IMT	International Mobile Telecommunications

IP	Internet Protocol
LDSCF	Local Directory Service and Cache Function
MAC	Media Access Control
NACF	Network Access Control Function
NDN	Named Data Networking
NDO	Named Data Object
NFR	Network Function Registry
NFV	Network Function Virtualization
NO	Named Object
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDU	Protocol Data Unit
RM	Registration Management
RP	Reference Point
SDN	Software Defined Networking
SMF	Session Management Function
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communications
USM	Unified Subscription Management function

5 Conventions

In this Recommendation:

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

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

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

6 Introduction

IMT-2020 networks are expected to incorporate information-centric networking (ICN) as one of the major component technologies for efficiently handling a large volume of data being transmitted through the network. Moreover, there would unprecedentedly be a considerable number of new devices (e.g., vehicles, sensors and actuators) getting connected to IMT-2020. Both data and devices (which are collectively called objects in this Recommendation) need to be named so that they can be accessed from anywhere in the network by their name and other attributes to obtain the services composed by data objects, or data generated by or stored in the devices. Note that IMT-2020 device registration has been covered by the registration management (RM) procedure of the IMT-2020 framework architecture. Therefore, this Recommendation does not describe the registration of devices for the subscription of network access services. Instead, this Recommendation describes the registration of other information (called records, each consisting of attributes such as host name, location, object type, group name, owner name, type of data it contains or generates, its public keys and certificates) related with named objects that would be made available publicly or with predefined access control for accessing the services or data provided by the named objects. Therefore, the registration of records in the directory service described in this Recommendation takes place after the registration of devices or UEs has been completed through the RM procedure and the device has already been successfully authorized for the network access or connectivity service.

The objects would have heterogeneous types of names assigned by different entities. Here, the heterogeneous types of names mean that the format or length of names may be different for different objects. Some objects may be identified by human-readable alphanumeric names, while the other objects by random numbers. Besides its name, each object possesses several attributes such as location, object type, owner name, group name, type of data it contains or generates, its public keys and certificates. Therefore, to manage a large number of heterogeneously named objects and access data and services offered by them in IMT-2020, this Recommendation introduces the directory service function in the IMT-2020 architecture and describes the functional components and procedures to register, cache, look up and update a large volume of records. Each record consists of several attributes associated with an object. The directory service is expected to provide a very low latency look-up service so that the records retrieved from the directory service would be utilized by new application services such as automated driving and interactive healthcare services that are required to obtain information from the network and surrounding devices instantly through a very low latency communication procedure. These records are used for various purposes, such as, identification, authentication, localization and knowing about their data and service types and various related parameters. Appendix 1 further illustrates a use case scenario of the directory service in the autonomous driving of connected vehicles.

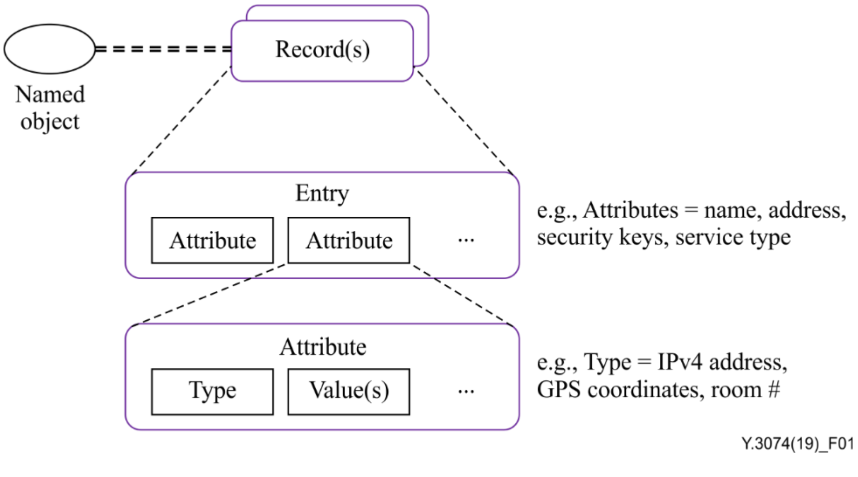

Named object
Record(s)
Entry
Attribute
Attribute
...
e.g., Attributes = name, address, security keys, service type
Attribute
Type
Value(s)
...
e.g., Type = IPv4 address, GPS coordinates, room #
Y.3074(19)_F01

Figure 1 – Structure of records stored in directory service

Records belonging to a named object are stored in the directory service as a single entry or multiple entries (implementation dependent) as shown in Figure 1. We follow the definition of directory entry of [ITU-T X.501] as a named collection of information stored in the directory information base (DIB). This means that each entry contains a unique name to get uniquely identified in the DIB. As shown in Figure 1, each entry consists of a set of attributes such as object name (e.g., host name), ID (e.g., serial number), location (e.g., GPS coordinates, room number in a building), network address (e.g., IP address), owner's name, generated data types (e.g., blood-pressure reading, body temperature by health monitoring devices), security keys and certificates for authentication. The attributes are classified by their types, namely, each attribute contains information about its type and one or more values. [ITU-T X.501] mentions that an attribute value may also contain additional information about the context of the value. However, this Recommendation assumes that the explicit description of the context and the content information, if any present, are also implicitly included in the attribute value.

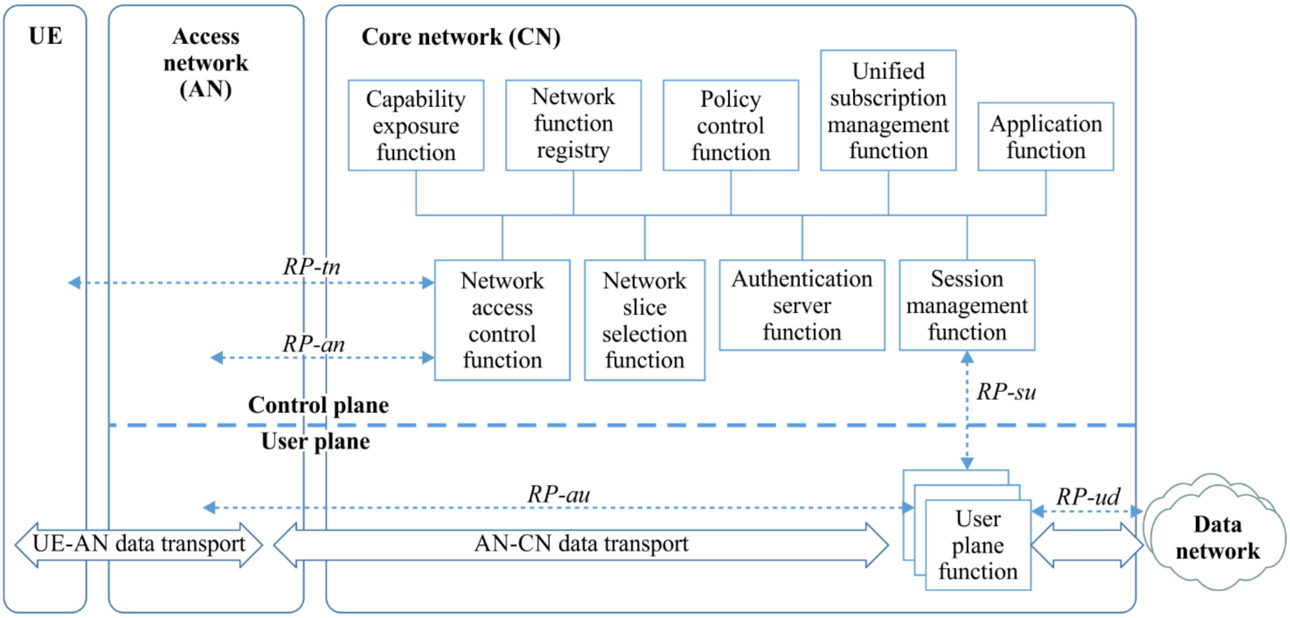
7 Positioning of directory service function in IMT-2020 architecture

This clause first provides an overview of the IMT-2020 framework and reference architecture specified in [ITU-T Y.3102] and [ITU-T Y.3104], and then describes the position of the directory service function in the IMT-2020 architecture. It describes the procedure of interaction of the directory service function with the various functional components of IMT-2020.

7.1 IMT-2020 framework and reference architecture overview

[ITU-T Y.3102] specifies the IMT-2020 network framework, including the high-level description of network functions and basic network services. Similarly, [ITU-T Y.3104] specifies the reference architecture and the procedures of interactions between various network functions.

Figure 2 shows the IMT-2020 reference architecture from a functional point of view.


UE
Access network (AN)
Core network (CN)
Capability exposure function
Network function registry
Policy control function
Unified subscription management function
Application function
RP-tn
RP-an
Network access control function
Network slice selection function
Authentication server function
Session management function
RP-su
Control plane
User plane
RP-au
RP-ud
UE-AN data transport
AN-CN data transport
User plane function
Data network

Y.3074(19)_F02

Figure 2 – Reference architecture of the IMT-2020 network [ITU-T Y.3102] [ITU-T Y.3104]

The reference architecture contains the user equipment (UE), access network (AN), core network (CN) and data networks. It lists the core network common functions required to develop a basic IMT-2020 network service framework that would be applicable to most of the application services envisioned to be supported by the IMT-2020 network. This is the reference framework for designing a general purpose IMT-2020 network architecture that is not required to be dependent on a particular service or access technology. It categorises the core network functions into control plane and user plane functions. The following functions exist in the control plane (details provided in [ITU-T Y.3102]):

1 network access control function (NACF) for registration management, connection management and session management function (SMF) selection;

2 session management function (SMF) for the setup of IP or non-IP protocol data unit (PDU) connectivity (i.e., PDU session) for a UE and the control of the user plane for that connectivity;

3 policy control function (PCF) for the control and management of policy rules, including rules for QoS enforcement, charging and traffic routing;

4 capability exposure function (CEF) of network functions and network slices to expose their capabilities as a service to third parties;

5 network function registry (NFR) for the discovery and selection of required network functions;

6 unified subscription management function (USM) for storing and managing UE context and subscription information;

7 network slice selection function (NSSF) for the selection of appropriate network slice instances for a UE;

8 authentication server function (ASF) for the authentication between the UE and the network;

9 application function (AF) for providing session-related information to the policy control function so that the session management function can finally use this information for session management.

The following function exists in the user plane:

1 user plane function (UPF) for traffic routing and forwarding, PDU session tunnel management and QoS enforcement.

The following reference points are also defined in the IMT-2020 network architecture reference model [ITU-T Y.3104]:

1 RP-tn: reference point between the UE and NACF.

2 RP-an: reference point between the AN and NACF.

3 RP-au: reference point between the AN and UPF.

4 RP-su: reference point between the SMF and UPF.

5 RP-ud: reference point between the UPF and data network.

These reference points are described in clause 7 of [ITU-T Y.3104].

7.2 Directory service function in IMT-2020 architecture

This Recommendation adds the directory service function to the IMT-2020 architecture as shown in Figure 3.

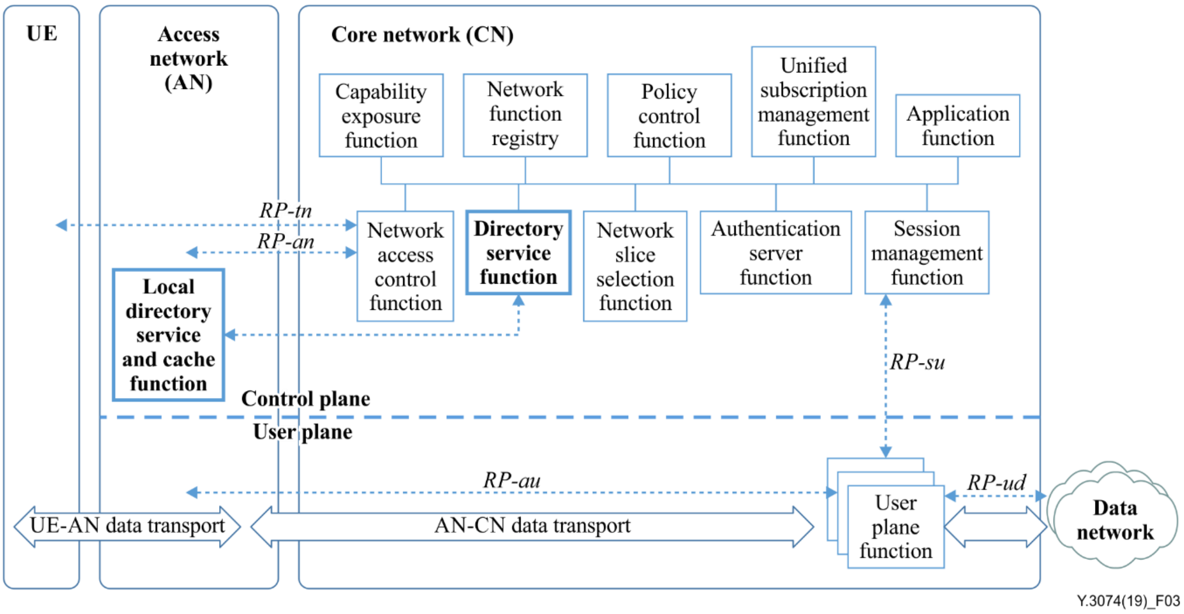

UE
Access network (AN)
Core network (CN)
Capability exposure function
Network function registry
Policy control function
Unified subscription management function
Application function
RP-tn
RP-an
Network access control function
Directory service function
Network slice selection function
Authentication server function
Session management function
Local directory service and cache function
RP-su
Control plane
User plane
RP-au
RP-ud
User plane function
Data network
UE-AN data transport
AN-CN data transport
Y.3074(19)_F03

Figure 3 – Position of directory service function in the IMT-2020 architecture

The directory service function (DSF) exists in the control plane as one of the core network functions. Similarly, in the access network there exists the local directory service and cache function (LDSCF). The directory service function interacts with several other functions such as the capability exposure function, network function registry, policy control function, unified subscription management functions, network access control function and the authentication server function. The local directory service and cache function stores the records in the access network to guarantee a very low latency look-up service for URLLC service scenarios such as automated driving.

7.3 Relationship of directory service function with other functions

The relationship of the DSF with other network functions in the IMT-2020 architecture is described in the following subclauses.

7.3.1 Network function registry function

When a directory service function instance is activated, it is registered in the network function registry so that it would be discovered to be included in slices for new network services. The NFR registration and discovery request procedures are common as used to discover any other network functions, such as the SMF, ASF and PCF.

7.3.2 Unified subscription management function

Since the USM function stores and manages UE context and subscription information, the DSF interacts with the USM function to obtain the UE attributes (e.g., public identification, name, owner's name, location, device type, types of data generated, security parameters) and store them in directory service records. The USM function and DSF maintain the interaction to update DSF records wherever there are updates of USM information.

7.3.3 Network access control function

The DSF is activated after completion of the NACF's network access registration, connection management and SMF selection. The NACF initiates the UE authentication by invoking the authentication service function. SMF selection takes place only after the completion of authentication.

7.3.4 Session management function

While providing the functionalities to set up the IP and non-IP protocol data unit connectivity for a UE the SMF also provides access parameters of the DSF (e.g., IP addresses) and security context (e.g., shared access keys, public keys) so that the UE can access the DSF securely without requiring the exchange of additional signalling messages for discovering the DSF and establishing new security context. It would help in keeping the look-up latency for retrieving records from the directory service function very low. The SMF obtains policy information related with the DSF from the PCF.

7.3.5 Policy control function

The DSF is registered in the PCF as a high priority service that should be able to provide a very low latency look-up service to retrieve the records stored in it.

7.3.6 Network slice selection function

The network slice selection function is executed in the background as triggered by the slice selection request issued from the NACF when a UE requests the NACF for its registration and authorization for network access. The NSSF provides a list of network slice instances available or suitable for the UE to the NACF, which selects the appropriate slice instances that include the directory service function as a network function instance.

7.3.7 Capability exposure function

The CEF stores DSF capability information and provides to the network on capability discovery requests to expose the availability of DSF capabilities to 3rd parties, so that they can utilize the directory service function for their application services.

7.3.8 Application function

The application function provides DSF-related capability requirements and policy information to the PCF so that the SMF can obtain this information and use it for guaranteeing the low latency requirements of record lookup from the DSF.

8 General working procedure of directory service function

This clause describes the procedures for record registration in the directory service function, record caching in the local directory service and cache function, record lookup from the local directory service and cache function, record update and record deletion. While describing the procedure this clause has considered only devices (or UEs) as the objects whose records are registered in and provided by the directory service function. The procedure for the registration of records for data objects would be described by a future Recommendation. It is assumed that the DSF exists in the common network slice instance, which is shared by various network slices configured for various UEs.

8.1 Record registration in directory service function

When a UE has been registered with the network and authorized to access the network service by the completion of the registration management (RM) procedure as described in [ITU-T Y.3104], its records are registered in the directory service function. As shown in Figure 4, the DSF performs signalling exchange with the USM, SMF, PCF, ASF, CEF and NACF to collect the UE profile information. For example, a subscription profile such as device ID, name, owner name, device type can be obtained from the USM; a connectivity profile such as IP address and MAC address can be obtained from the SMF; security context such as group shared key, access control rules, public key and certificate can be obtained from the ASF; a policy profile such as computation and network resource requirements for the DSF function can be obtained from the PCF; a capacity profile of the UE such as protocols and platform available for interaction with other client UE can be obtained from the CEF. Some of these parameters or new parameters can also be obtained from the NACF.

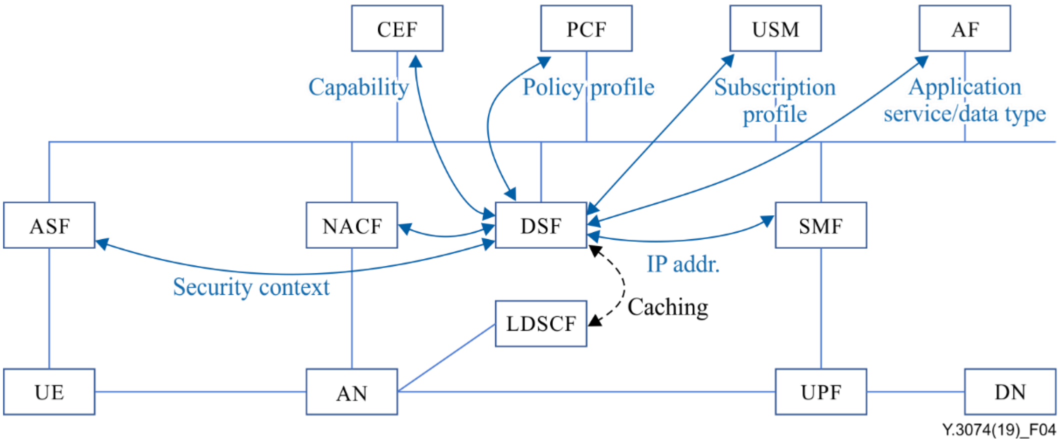


Figure 4 – Interaction of directory service function with other functions in IMT-2020 architecture

8.2 Record caching in directory service cache function

The caching of records in the local directory service and cache function (LDSCF) located in the access network takes place as soon as the UE connection management (CM) procedure completes and the UE goes into CM CONNECTED mode. Since the NACF knows about the time of completion of the CM, it provides a trigger through a signalling message to the LDSCF to start downloading the UE's record from the DSF and storing it in its cache. It is assumed that the LDSCF exists in the common network slice instance, which is shared by various network slices configured in the access network. The existence of the LDSCF in a common and sharable network slice instance would enable it to be accessible by all UEs that may belong to various network slices. Figure 4 shows the positions of the DSF and LDSCF, and the caching of records through signalling exchange between the DSF and LDSCF. The existence of records in the LDSCF is tracked by the DSF so that whenever there is an update in any attribute of a record stored in the DSF, the update can be propagated to the LDSCF as well by sending a signalling message from the DSF. If the UE is associated with more than one AN, its record is cached in all LDSCFs located in each of these ANs.

8.3 Record lookup from directory service cache function

When a client UE wants to communicate with other target UEs to obtain data or services offered by the latter, the client UE performs DSF record lookup by sending a look-up request to the LDSCF located in the AN. The client UE includes the target UE's name or ID as the look-up key in the look-up request signalling message. Alternatively, it may include more abstract values such as location or group name, which may match with many records (e.g., UEs located in a certain location or UEs offering a certain type of service/data). In this case, all the matched records containing the requested attributes are provided in the response message. The LDSCF is provided with enough computing and networking resources so that the look-up latency would not exceed a specified limit.

8.4 Record update in directory service function

The record update procedure is initiated either by the UE itself or the network function, such as the NACF that detects changes in the UE's records stored in the DSF and LDSCF. For example, when a UE moves from one AN to another, its new location is detected by the NACF. The NACF initiates a signalling message containing the updated attribute (in this case IP address and other location-related parameters) and sends it to the DSF. The DSF updates the record and responds back with an acknowledgement message. The DSF also sends a signalling message containing the update to all LDSCFs that have stored the record in their cache. The LDSCF updates the cache records and responds back to the DSF with an acknowledgement.

8.5 Record deletion from directory service function

A record is deleted from both the DSF and LDSCF when the UE is de-registered from the network. The NACF initiates the signalling procedure for deletion of the record from the DSF and LDSCF as soon as it completes the signalling procedure of the de-registration as specified in [ITU-T Y.3104]. The record from the LDSCF is deleted when the UE turns into CM IDLE mode. In general, a record is deleted from the LDSCF whenever the record is considered not useful in the AN, that is, there are no client UEs that look up the record.

9 Design approach of directory service function

To meet the requirements of very low look-up latency and scalability to store dynamic records of a large number of heterogeneously named objects, the directory service function is recommended to be designed with the following approaches.

1) **Application-wise directory service instances**: To meet the distinct performance requirements in diverse operating environments of various applications, it is assumed that each application service will have its own directory service instance. For example, automated

driving and grid-control application services will have two different directory service instances because they differ in the types of end devices or UEs, communication patterns and latency requirements. This design approach is related to the optimization of deployment and operation costs because the application services that can tolerate higher latency can utilize a directory service deployed with less networking and computing resources.

2) **Dynamic updating of records**: Records stored in the directory service can change at any time. Therefore, the directory service is designed to be able to update records within a tolerable latency.

3) **On-demand caching of records**: The directory service records stored in the DSF are distributed to different LDSCFs located closer to the application clients in access networks. These LDSCFs are able to serve records to the clients in very low look-up latency because of the short communication distance between the clients and the LDSCF.

4) **Trackable cache function servers**: The locations of a record stored in various LDSCFs are always remembered by the DSF so that all cache records are updated as soon as the record is updated in the DSF. In this way, the system maintains the consistency of all copies of a record stored in the DSF and LDSCF.

5) **Flexible database with various search keys**: Since objects can be identified by heterogeneous types of names (e.g., text, number and binary data), the DSF is designed to be able to efficiently store records containing various types and numbers of attributes in the database without requiring to define complex structures and database schemas in advance. It should be flexible enough to permit the use of any attribute as a search key to find target records in the LDSCF. For instance, records can be found using the target object's name, identifier, location or even the type of data it generates.

6) **Dynamic resource provisioning**: The directory service is designed with the assumption of two layers of service providers: application service providers and infrastructure providers. The application service providers lease resources (e.g., server and network bandwidth) on-demand from infrastructure providers to dynamically add/remove the cache servers in different locations of access networks. This assumption has been aligned with the recent trend in software defined networking (SDN), network function virtualization (NFV) and edge computing in which a network component equipped with the necessary resources can be instantiated instantly in the network edge by leasing required amounts of resources from infrastructure providers. To ensure that the performance requirements of the directory service function are met despite the fluctuation in workload, the required amount of computing, storage and network resources allocated to the cache replica servers are adjusted dynamically.

10 Requirements of directory service function

The framework of the directory service function is required to be designed to satisfy the following requirements:

1 It is required to store a large volume of records.

2 It is required to provide a very low latency look-up service (latency of only few milliseconds).

3 It is recommended to perform the look-up service either by using a single attribute or a combination of many attributes.

4 It is recommended to properly handle the record owner-centric privacy policy.

5 It is recommended to be scalable so that the performance can be kept at the desired level by adjusting the amount of network and computing resources assigned to it despite fluctuation in the workload.

6 It is recommended to store records in a distributed manner so that records are available in locations closer to the clients and the communication latency to obtain the record is very low.

7 It is recommended to track the existence of all copies of records in the distributed directory service system so that it can update the record immediately whenever an attribute of the record changes.

11 Security considerations

Proper security mechanisms need to be considered for both maintaining the records in the directory service function and transferring records from the directory service function to the local directory service and cache function. Only the records coming through secured communications method from authenticated sources have to be registered in the directory service function. Similarly, the procedures of record caching, retrieval, update and deletion should take place only through proper security considerations.

Appendix I

Use case scenarios of directory service in autonomous driving of connected vehicles

(This appendix does not form an integral part of the Recommendation.)

Connected vehicles are considered to constitute a large portion of new UEs that would be getting connected to the IMT-2020/5G networks. According to a recent estimation, there would be 220 million connected vehicles by 2020 [b-BII-report 2016]. These vehicles would constitute 15% of 1.5 billion new devices expected to get connected to cellular networks [b-Ericsson-report 2016]. This appendix illustrates two use case scenarios of the directory service for realizing secure and real-time communication in connected vehicles. These use case scenarios are referenced from [b-IEEE-VTC 2018]. In both use case scenarios, the response time of the directory service must be very short because autonomous driving has communication requirements that vehicles exchange messages within a few milliseconds (usually 20-100 millisecond) [b-VSCP-report 2006]. To make the directory service applicable for connected vehicles to quickly obtain the necessary records of target vehicles, its response time should be kept less than 10 millisecond so that vehicles can send their messages to the target vehicles within the given time budget of 20 millisecond, as communication latency in 5G networks is expected to be 1-10 millisecond [ITU-R M.2083-0].

I.1 Obtaining necessary records for message authentication

A vehicle has to be provided with the capability to obtain the necessary information required to verify that a message received from another vehicle is authentic. For example, in Figure I.1, when Car A is approaching the intersection, it formulates a message containing its current position, speed, direction and so on and transmits the message to Car B so that Car B can visualize the expected arrival time of Car A in the intersection and carry out necessary safety measures to avoid collisions. The message from Car A to Car B can be transmitted through any of the three different paths shown by broken arrows: (1) direct communication, also known as device to device (D2D) communication; (2) through a road side unit (RSU); and (3) through an IMT-2020/5G cellular base station. Since connected vehicles require highly dependable communication infrastructure, it is highly possible that the connected vehicles will be equipped with the aforementioned all three means of communication so that they would remain connected despite a momentary failure in one type of communication method.

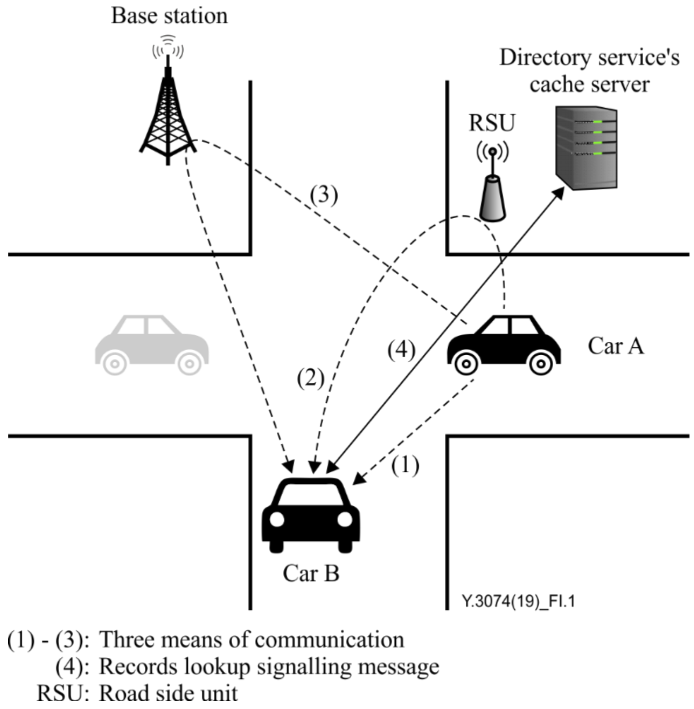

Base station
Directory service's cache server
RSU
(3)
(4)
(2)
Car A
(1)
Car B
Y.3074(19)_FI.1
(1) - (3): Three means of communication
(4): Records lookup signalling message
RSU: Road side unit

**Figure I.1 – Use case scenarios of directory service in connected vehicles
Car B obtaining records of Car A from the directory service for the authentication of messages received from Car A**

The communication infrastructure must support Car B to obtain the necessary records to verify that the received message has been sent by authentic Car A. For this purpose, the directory service function is used, which stores the vehicle's records in the directory service cache function placed closer to the vehicle's current and potential future locations proactively. The cache functions are deployed closer to the intersections and connected to the RSU and the base station access networks so that the propagation delay between the querying vehicle and directory service's cache function servers is very low (usually ~1 millisecond). The cache server stores all records related to Car A. Car B extracts Car A's name or ID included in the received message, and configures a look-up query message containing the ID and types of attributes of Car A it wishes to obtain. The look-up query message, shown by arrow (4) in Figure I.1, is transmitted to the cache server through either the RSU or the base station network, or both. The directory service cache server searches its database for the record associated with Car A's ID and retrieves the requested attributes. The cache server then configures a look-up response message containing the attributes and transmits them to Car B. Car B uses the attributes contained in the response to verify if the message previously sent by Car A is authentic. If the message is authentic, it executes the necessary action, for instance, momentarily stopping before entering the interaction and verifying safety on the basis of subsequently received messages.

I.2 Identifying or notifying all vehicles possessing common features

In connected vehicle applications, a vehicle or any authorized entity (e.g., transportation management and control agency) should be able to communicate with all vehicles possessing a common feature, such as location, vehicle type, owner group and manufacturer. For example, in Figure I.2, when Car A is approaching the intersection, it may need to send a message containing information about its current position, speed and direction to all vehicles approaching the intersection (i.e., located within the circle shown in the figure) so that it can safely pass through the intersection.

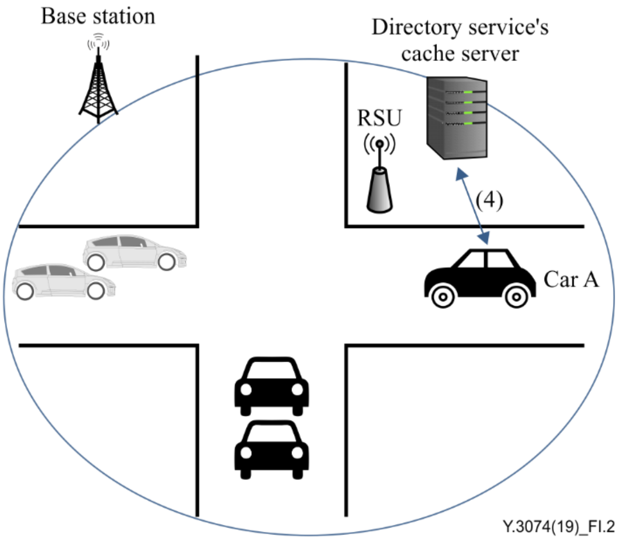


Figure I.2 – Use case scenarios of directory service in connected vehicles: Car A finding the identity of all cars approaching an intersection

The directory service function integrated in the communication infrastructure must support Car A to obtain the identity or network address of all relevant vehicles so that it can send the message to them. Car A configures a look-up query message containing the required record types that it wants to obtain from the directory service function satisfying the common feature. It sends the look-up query message to the cache server through the access network connected to the RSU and/or IMT-2020/5G cellular base station. Upon receiving the query message, the cache server searches its database and retrieves the relevant records satisfying the query condition. The cache server then configures a look-up response message containing the records and transmits it to Car A. Using the received records about the other vehicles, Car A can send them relevant notification or alert messages.

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 Sup. 35] Supplement 35 to ITU-T Y-series Recommendations (2016), *ITU-T Y.3033 – Data aware networking – scenarios and use cases*.

[b-ITU-T Y Sup. 48] Supplement 48 to ITU-T Y-series Recommendations (2018), *Proof of concept for data service using information centric networking in IMT-2020*.

[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-BII-report 2016] Business Insider Intelligence: *Here's how the Internet of Things will explode by 2020*, <http://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2> *(Accessed on 22 March 2018).*

[b-Ericsson-report 2016] Ericsson Mobility Report (2016), *On the Pulse of the Networked Society*.

[b-IEEE-VTC 2018] V. P. Kafle, Y. Fukushima, P. Martinez-Julia, and H. Harai (2018*), Directory Service for Connected Vehicles, IEEE Vehicular Technology Conference (VTC2018-Spring).*

[b-VSCP-report 2006] Vehicle Safety Communications Project – Final Report (2006), *U.S. Department of Transport, National Highway Traffic Safety Administration*.

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