International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.676

(11/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Naming, Addressing and Registration

Object identifier-based resolution framework for IoT grouped services

Recommendation ITU-T X.676

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	**X.650–X.679**
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems management framework and architecture	X.700–X.709
Management communication service and protocol	X.710–X.719
Structure of management information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, concurrency and recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300–X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1599
CLOUD COMPUTING SECURITY	X.1600–X.1699

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

Recommendation ITU-T X.676

Object identifier-based resolution framework for IoT grouped services

Summary

Recommendation ITU-T X.676 specifies an object identifier (OID)-based resolution framework for identifying various services in IoT environments. OID is an identifier to name an object with a hierarchically assigned namespace. In Internet of things (IoT), thousands of IoT services based on heterogeneous resources will be provided as combinations of various services. For efficiency, various technologies, such as service binding, dynamic services or frequently switching services will be required, along with resolution and identification of grouped services. This Recommendation describes the concepts of IoT grouped services, considerations, architectures, and procedures for an OID-based resolution framework for IoT grouped services.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.676	2018-11-29	17	11.1002/1000/13712

Keywords

Grouped services, Internet of things (IoT), object identifiers, OID, OID resolution.

---

* 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 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 X.676

Object identifier-based resolution framework for IoT grouped services

1 Scope

This Recommendation includes the following items:

– overview of object identifier (OID)-based resolution framework for Internet of things (IoT) grouped services;

– requirements for resolution framework for IoT grouped services; and

– OID-based resolution framework and scenarios for IoT grouped services.

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.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*.

[ITU-T X.672] Recommendation ITU-T X.672 (2010) | ISO/IEC 29168-1:2011, *Information technology – Open systems interconnection – Object identifier resolution system (ORS)*.

[ITU-T X.675] Recommendation ITU-T X.675 (2015), *OID-based resolution framework for heterogeneous identifiers and locators*.

[ITU-T Y.4000] ITU-T Recommendation Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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).

3.1.2 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.3 OID resolution system [ITU-T X.672]: Implementation of the OID resolution process.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 grouped services: Two or more services that are assigned to the same group.

NOTE – The services are provided sequentially or non-sequentially when the group is triggered.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

GRS Group Service Resolution Server

ID Identifier

IoT Internet of Things

LDAP Lightweight Directory Access Protocol

MIB Management Information Base

OID Object Identifier

ORS Object Identifier Resolution Server

SNMP Simple Network Management Protocol

SP Service Provider

SR Service Registry

URI Uniform Resource Identifier

5 Conventions

None.

6 Considerations on a resolution framework for IoT grouped services

OID consists of a node in a hierarchically-assigned namespace, formally defined using [ITU-T X.660]. OIDs have been used for various implementations. For example, OIDs serve to name almost every object type in ITU-T X.509 certificates in computer security. They are used within ITU-T X.500 directory schemas and protocols, to uniquely name each attribute type and object class, and other elements of schema. Within lightweight directory access protocol (LDAP) schemas, each object class and each attribute type has a unique OID. In computer networking, an OID, in the context of simple network management protocol (SNMP), consists of the object identifier for an object in a management information base (MIB). Health level seven international (HL7), digital imaging and communications in medicine (DICOM) and other healthcare related information interchange standards use OIDs for globally unique identifiers for both individual information objects as well as references to code systems and data element dictionaries.

In IoT [ITU-T Y.4000], thousands of IoT services based on heterogeneous resources will be provided. In addition, in the future, IoT services are expected as complicated service provision systems by using grouped services. Therefore, service binding, dynamic services or frequently switching services can be required. If so, each IoT service could need identification.

One of the solutions that OIDs can support is to identify IoT services. OIDs can identify not only tangible things (e.g., home appliances) but also intangible data (e.g., attribute types in ITU-T X.500 directory schemes and LDAP schemes). There are no technical problems in using OIDs for identifying intangible services. If OIDs are used for thousands of IoT services, performance could be raised as an issue for dynamically switching services and service bindings.

Consequently, an OID-based resolution framework for identifying various services is required in IoT.

Figure 1 – Use case for emergency services

Figure 1 shows a use case for emergency services. When a traffic accident occurs and people are seriously injured, many emergency services are rapidly required. For instance, first aid, ambulance, police (or 911), hospital notification, and so on. These services are heterogeneous; therefore, it is difficult for them to operate in an integrated approach. However, these services need a concept of service chaining for effective cooperation.

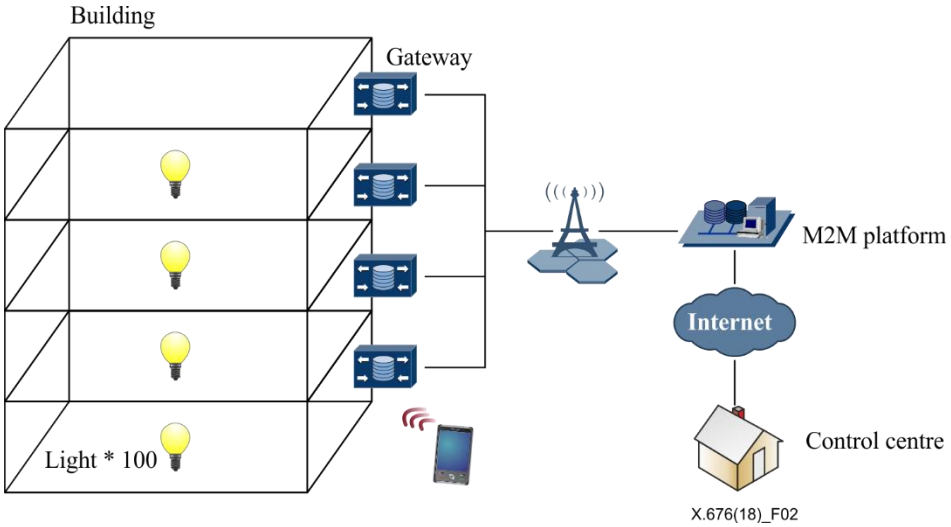

Figure 2 – Use case of smart building

Figure 2 (see [b-ITU-T TR UseCase]) depicts a smart building as one use case for IoT services. Smart building is a machine-to-machine (M2M) service that utilizes a collection of sensors, controllers, alerts, and gateways deployed in the correct places in a building combined with applications and servers that reside on the Internet to enable the automatic management of the building with limited human labour [b-ITU-T Y.4500.1]. In the smart building use case, there could be many heterogeneous IoT devices. One service provider (SP) platform can provide all the IoT devices, but multiple service providers will possibly provide them if their base resources are heterogeneous. If the devices are not

controlled by one provider, it is required to control them by one system. When a customer enters the building, the customer needs integrated guidance toward a targeted location. For doing this, all devices (e.g., signs, notices, lamps, doors, windows, appliances, cameras) simultaneously cooperate. If the customer is revealed as a criminal, all devices should protect the building from the criminal in an integrated approach.

If the concept of service grouping (or service chaining) is combined with such services, performance and efficiency can be improved. Appendix I shows other use cases for grouped services in IoT.

7 Requirements for resolution framework of grouped services

The uniform resolution framework for IoT grouped services shall address the following requirements.

7.1 Support for service grouping

In IoT, thousands of various services and applications will be provided, and some can be categorized into the same group because of similar characteristics. Even though they have different characteristics, they can have the same objectives. Services and applications that have the same objectives can belong to the same group. IoT services can be grouped and conducted together for specific events. For instance, when a traffic accident occurs, there are many emergency services required within a rapid period of time, such as first aid, ambulance, police (or 911), hospital notification and so on. These services are simultaneously conducted for the same objectives. Therefore, the resolution framework is required to support service grouping.

7.2 Support for identification of service groups

The resolution framework is required to support a uniform identification scheme for service groups. A service group would be evoked by resolving an identifier representing the group when an event occurs. Therefore, the identifier for the group is resolved into identifiers of specific services.

7.3 Support for management of grouped services

The service group can be dynamically managed according to changes in objectives. If a specific service is not required in a group, the group can delete the specific service or exchange it for another appropriate service. For example, if a 911 call covers both ambulance and hospital notification, then a separate ambulance call and hospital reservation notification can be withdrawn from the emergency service group.

7.4 Support for heterogeneity of specific services

The identification scheme should be uniform, but identifiers for specific services in a group can be heterogeneous. The specific services would be based on different IoT resources. In addition, an identifier will only be exploited for its own specific service. The resolution framework is required to support heterogeneity of specific services.

8 OID-based resolution framework of grouped services

8.1 General architecture

Figure 3 presents a general architecture of an OID-based resolution framework for IoT grouped services. In Figure 3, there are three types of components: object identifier resolution server (ORS), group service resolution server (GRS), and service registries operated by service providers. The key components of the framework are ORS and GRS. The ORS is interconnected with the GRS, and the GRS is interconnected with service registries of service providers to manage the information about groups of services. Each service registry manages the information of specific services provided by service providers.

Service providers have their own identification schemes for providing specific services on their own, and they have a service registry to manage service-related information. The GRS manages information about groups of services and connects the user to the specific services that are required.

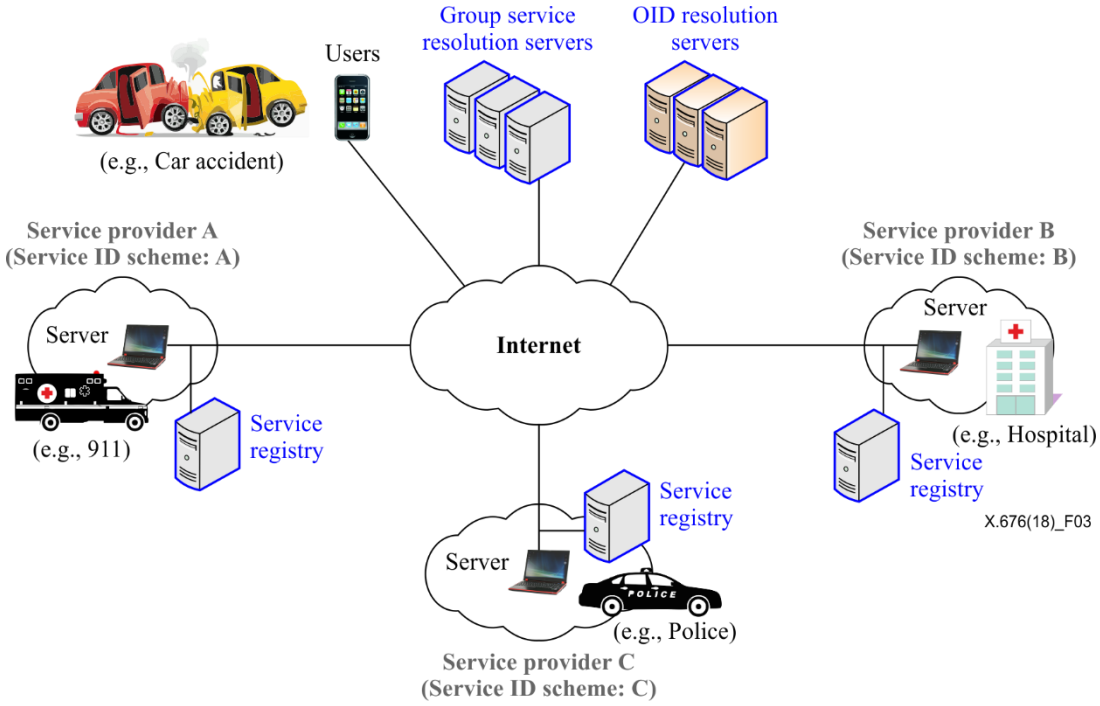

Figure 3 – General architecture of OID-based resolution framework for IoT grouped services

8.2 Components

8.2.1 Group service resolution server

Group service resolution server plays the role of group management for IoT services and identification for groups. The GRS has a database including OIDs and corresponding group IDs. The OIDs in the GRS are also exploited as the key values to identify group IDs; thus, the GRS returns corresponding group IDs and an address of service registry. In addition, the GRS manages another mapping database for mapping group IDs and corresponding service IDs. Finally, the GRS requests to conduct a required IoT service to its SP by using the mapping database.

8.2.2 Object identifier resolution server

An ORS [ITU-T X.672] plays the role of a centralized management and identification server for the GRS. The ORS includes databases of OIDs and uniform resource identifiers (URIs) (based on UINF [ITU-T X.672], see https://www.itu.int/itu-t/recommendations/rec.aspx?rec=10831) of the GRSs. OIDs are utilized as key values to identify GRSs. When a user sends an OID value to the ORS, the ORS returns the URI value of a corresponding GRS.

8.2.3 Service registry

Service registry (SR) is a local resolution system to support specific services. A local SP has and manages one SR, and the SR manages a database(s) of service IDs and corresponding services. This database is used for the SR to lookup a service ID for a corresponding service, which its SP conducts. The service ID schemes can be heterogeneous according to SPs, so none of the service IDs need to be created with the same rule.

8.3 OID assignment

OIDs are predefined and have globally unique values, which are respectively assigned to all GRSs. This means that each group of IoT services can be identified by assigned OIDs because a group ID is assigned to only one GRS. OIDs are used as well-known values in public-like port numbers of transmission control protocol/Internet protocol (TCP/IP). Therefore, this enables all nodes to be aware of OID values related to a group of IoT services.

9 Procedures of OID-based resolution framework of grouped services

9.1 Registration procedure

First, IoT services are required to be registered for grouping and management; furthermore, groups of IoT services are also required to be identified by OIDs. Therefore, the OID-based resolution framework provides a two-level registration approach, such as specific IoT services from service providers to GRSs and GRSs to ORS as shown in Figure 4. The OIDs (2.999.1.1, 2.999.1.2, 2.999.2.1) are used as exmaples.

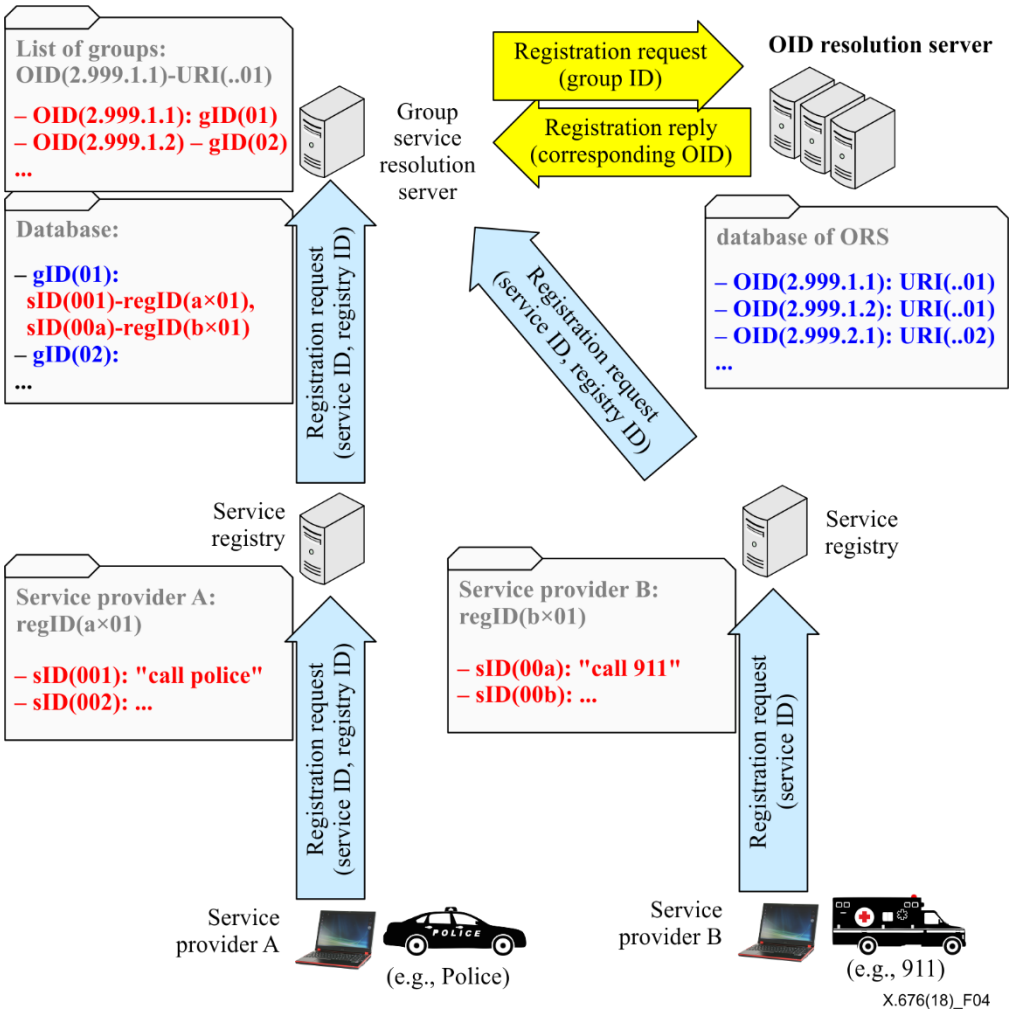

Figure 4 – Service and OID registration procedure

9.1.1 Registration to group service resolution server

To start, SPs have an SR, and the corresponding IoT service gets registered by the SPs. Next, a new service ID corresponding to the IoT service is created, and the two-tier information (service ID-IoT service) is stored in and managed by the SR. The service IDs can be created by different generation mechanisms with different ID formats; that is, different SPs can make service IDs with different ID

formats. There is no problem in managing and identifying them by the GRS because the GRS utilizes additional pairing information, such as an SR ID with its service ID.

All of the SRs are connected to the GRS. The SRs send their own IDs and service IDs to the GRS whenever any IoT service is registered or every regular time. Then the GRS manages a database including all the information of IoT services, such as service ID, its SR ID, its SP information and service-related details. In addition, the GRS manages another list including group IDs and corresponding OIDs. The group IDs is generated by the GRS on demand from GRS operators. If a group of IoT services is required, a group is made in the database, and an ID for the group is generated. However, the GRS cannot generate OIDs by itself, so when a group of IoT services is created, the GRS requests an OID to the ORS by sending its URI.

9.1.2 Registration to OID resolution server

At this next stage, when the ORS is requested by the GRS, the ORS assigns an OID for the group ID reply to the assigned OID to the GRS. Finally, the GRS manages the pairing information of a group ID and its corresponding OID in the list of groups.

9.2 Resolution procedures

This clause presents OID-based resolution procedure for a group of IoT services as shown in Figure 5. This procedure assumes that all the components are interconnected for networking through the Internet and information for networking to the GRS and ORS is well known. In addition, these procedures are presented under the situation where an emergency (i.e., accident) occurs.

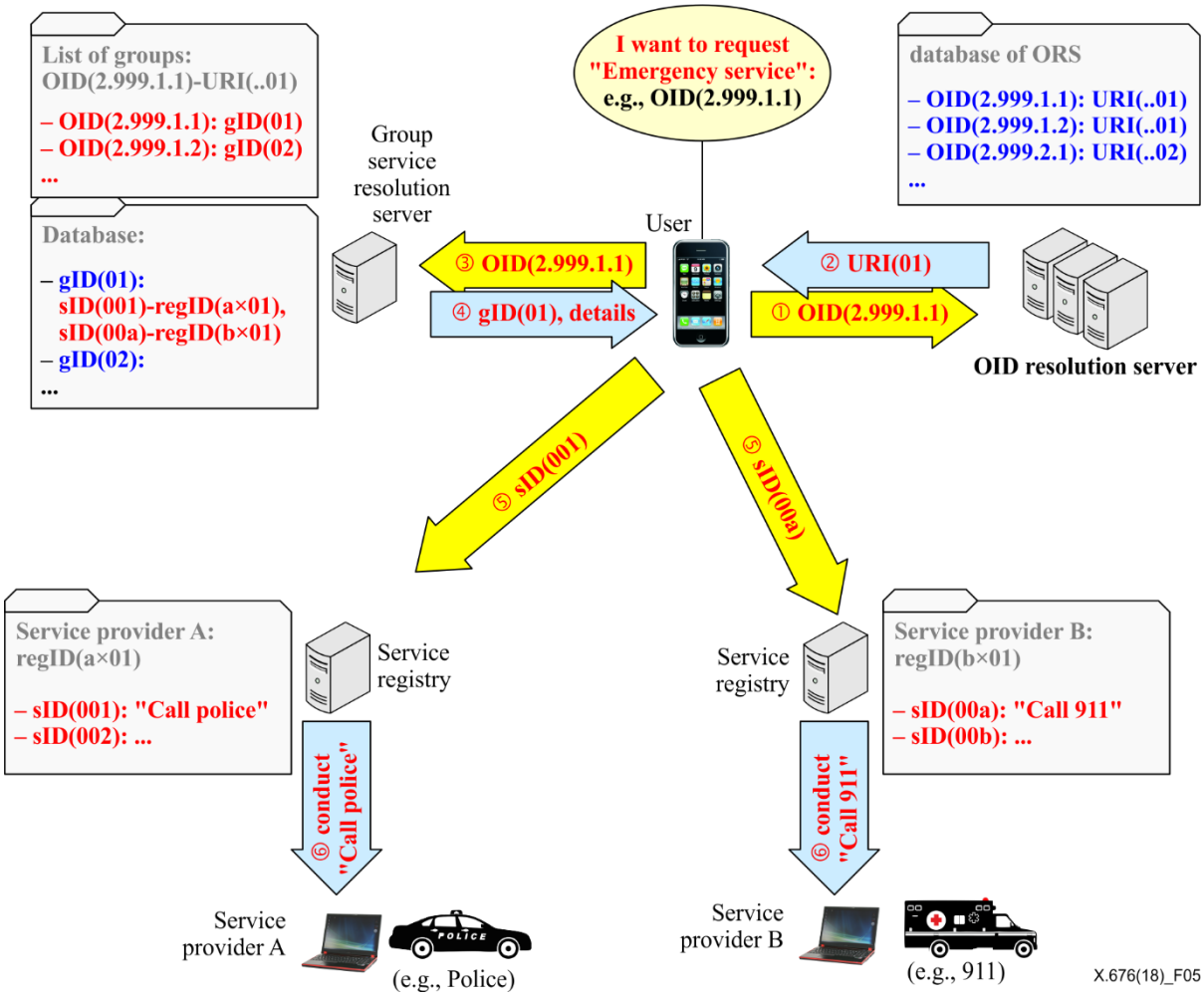

Figure 5 – OID-based resolution procedure for a group of IoT services

1) User sends OID (e.g., 2.999.1.1) to ORS.

: An emergency (i.e., accident) occurs. One of the people nearby (i.e., the user) opens an application in their mobile phone to request a group of IoT services, "Emergency Service". When the user clicks a button for "Emergency Service", a corresponding OID (2.999.1.1) is sent to a designated ORS inside the application.

2) The ORS retrieves a corresponding value (URI) of the OID (2.999.1.1) from its database, and the correct URI (e.g., 01) of a GRS is replied from the ORS to the user's application.

3) The user sends the OID (2.999.1.1) to the GRS.

: The user's application gets information for connection to the GRS from the replied URI (01) information. The user's application sends the OID (2.999.1.1) to the GRS for obtaining information about a group of IoT services of "Emergency Service".

4) The GRS returns a group ID (e.g., 01) and information for "Emergency Service" to the user.

: The GRS receives the OID (2.999.1.1) and retrieves a group ID with the OID (2.999.1.1) from its list of groups. Then the retrieved group ID (01) is exploited to look up information of IoT services which belong to the group. Finally, the group ID (01) and related information about SR and SP (e.g., a network address, specific service ID) is sent to the user's application.

5) Each service ID (e.g., 001 and 00a) is separately sent to the SR.

: The user receives all the information required for requesting the grouped services. The user separately requests the related IoT services of the group with service IDs (001 and 00a) to the corresponding SRs. When an SR receives the request from the GRS, the SP is notified for conducting a service.

6) The SP initiates and conducts the services (i.e., "call police" and "call 911").

: All the IoT services which belong to the group are conducted via a one-stop request.

10 Security considerations

The OID-based resolution framework is processed with the assumption that the GRS and ORS information is well known. If the information of the GRS and ORS is attacked by a third party, the IoT services and group management cannot be provided, and it also can also have negative results for users. All of the input and output values of the GRS and ORS must be secured.

Appendix I

Use cases for grouped services in IoT

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

For understanding the key concepts of OID-based resolution framework for grouped services, this appendix introduces possible use cases for grouped services.

Hundreds and thousands of IoT services will be provided based on heterogeneous resources in converged manners, and also some tightly coupled IoT services can have a common service plan and the same objective for higher efficiency than separate services as shown in Figure I.1. For these reasons, the tightly coupled services can be grouped and provided simultaneously as one service (e.g., one-stop-service).

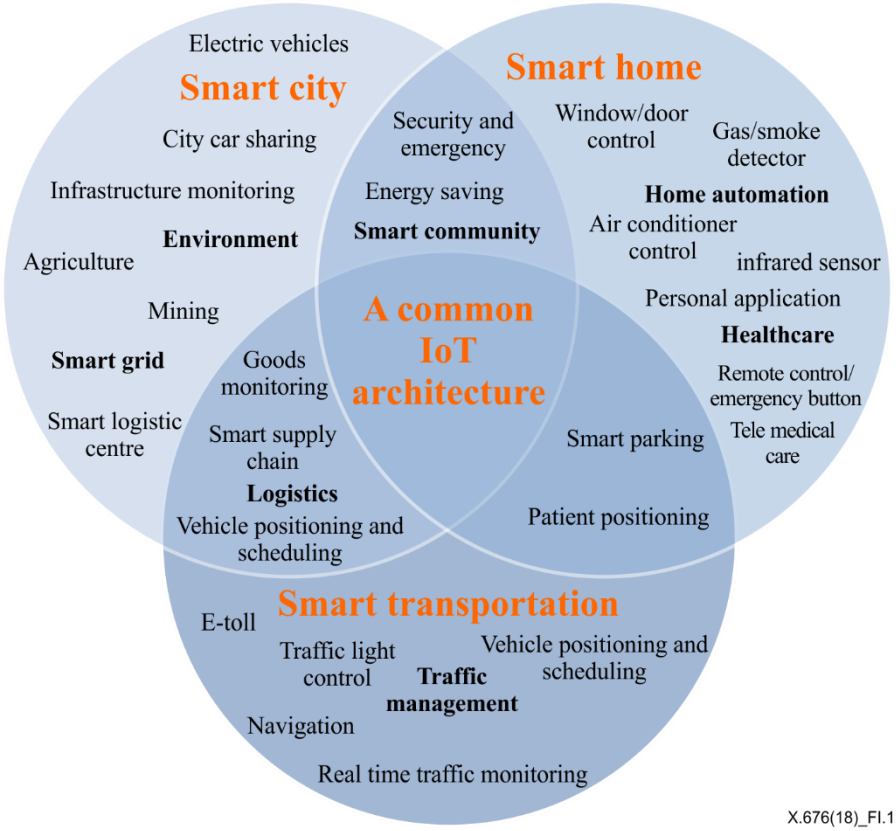

Figure I.1 – Examples of common services among different domains

I.1 Grouped services for a building on fire

There are many services which should be provided in a critical time period. For example, when a building is suddenly on fire, cooperative work and processes are required to rescue people and to rapidly fight the fire.

Figure I.2 – Building on fire

First, the building operators should activate fire alarms in the building, and 911 and police should be called. All built-in devices (e.g., doors, locks, lights, elevators) are operated together as an emergency evacuation system. If one button for emergency is clicked, all devices should cooperatively work to help people escape from inside the building. This can be done with an one-stop-service based on IoT technologies.

I.2 Grouped daily services at a smart home

IoT technology is applied to many home services in smart homes. For instance, air-conditioning, security (locks), lighting, electronics, charging devices (e.g., car), wake-up calls, coffee-making, bath preparation, robot-cleaning, tracking (e.g., CCTV), laundry, delivery, and so on.

All of these services are not always required 24 hours per day, but each service or some of them are temporarily required during certain situations. When people are sleeping at night, some appliances are activated to ensure the best conditions for sleeping (e.g., air-conditioning, door/window locking, lighting for proper sleep, electronics turned off). Home services are reorganized to make the optimized home conditions for different objectives.

According to the objectives of a smart home, work can be grouped. Figure I.3 (a) shows an example grouping of smart home services, such as sleeping mode, going to work, being-out, returning home, and break time. Figure I.3 (b) also shows a real example of a smart phone app used to control home appliances according to the grouped services.

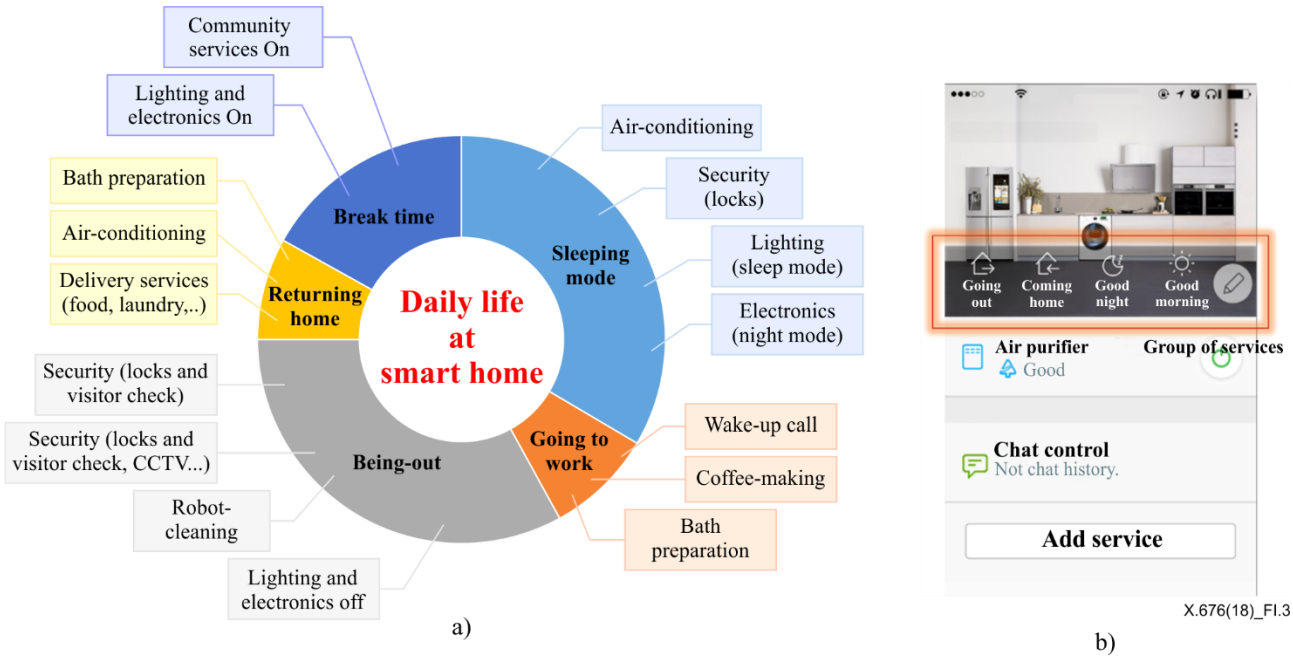

Figure I.3 – Grouped services in a smart home

Bibliography

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-ITU-T Y.4500.1] Recommendation ITU-T Y.4500.1 (2018), *oneM2M – Functional architecture*.

[b-ITU-T TR UseCase] Technical Report ITU-T YSTR-M2M-UseCase (2017), *oneM2M – Use case collection*.

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