International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4463

(01/2020)

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

Internet of things and smart cities and communities – Frameworks, architectures and protocols

Framework of delegation service for Internet of things devices

Recommendation ITU-T Y.4463

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.4463

Framework of delegation service for Internet of things devices

Summary

Recommendation ITU-T Y.4463 is a framework of the delegation service for transferring ownership (i.e., access rights to the Internet of things (IoT) devices) among authorized IoT devices. This Recommendation gives an overview and types of delegation service in IoT environment. It also describes the requirements and architectural models of delegation service.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4463	2020-01-13	20	11.1002/1000/14166

Keywords

Delegation service, IoT, ownership.

* 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

Recommandation ITU-T Y.4463

Framework of delegation service for Internet of things devices

1 Scope

This Recommendation describes a framework of delegation service for transferring ownership (i.e., access rights to the IoT devices) among authorized IoT devices.

In particular, the scope of this Recommendation includes:

– Overview of delegation service in an IoT environment;

– Types of delegation service among authorized IoT devices;

– Requirements of delegation service;

– Architectural model of delegation service.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

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

[ITU-T Y.4400] Recommendation ITU-T Y.4400/Y.2063 (2012), *Framework of the web of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 device [ITU-T Y.4000]: In the Internet of Things, a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.2 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).

3.1.3 identity [b-ITU-T Y.2720]: Information about an entity that is sufficient to identify that entity in a particular context.

3.1.4 Internet of things [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 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.5 object [b-ITU-T Y.2002]: An intrinsic representation of an entity that is described at an appropriate level of abstraction in terms of its attributes and functions.

NOTE 1 – An object is characterized by its behaviour. An object is distinct from any other object. An object interacts with its environment including other objects at its interaction points. An object is informally said to perform functions and offer services (an object which makes a function available is said to offer a service). For modelling purposes, these functions and services are specified in terms of the behaviour of the object and of its interfaces. An object can perform more than one function. A function can be performed by the cooperation of several objects.

NOTE 2 – Objects include terminal devices (e.g., used by a person to access the network such as mobile phones, Personal computers, etc.), remote monitoring devices (e.g., cameras, sensors, etc.), information devices (e.g., content delivery server), products, contents, and resources.

3.1.6 resource owner [b-ITU-T Y.2724]: An entity capable of granting access to a protected resource. When the resource owner is a person, they are referred to as an end-user.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 data model: A concrete and detailed representation as an abstraction of IoT devices in information world.

NOTE – The term "information world" is based on the illustration in Figure 2 of [ITU-T Y.4000]. [b-IETF RFC 3444] defines a data model from the viewpoint of a network operator and a developer.

3.2.2 delegation: Conveyance of privilege from one entity that holds such privilege, to another entity. It is also an action that assigns authority, responsibility, or a function to another entity.

NOTE – Definition adapted from [b-ITU-T X.509] and [b-ITU-T X.1252].

3.2.3 resource: An object of the information world, which inherits the same characteristics as a physical entity (e.g., IoT device) of the physical world and whose capability is bound to the capability of a physical entity.

NOTE 1 – The terms "information world" and "physical world" are based on the illustration in Figure 2 of [ITU-T Y.4000].

NOTE 2 – A resource in the information world is called a virtual object.

NOTE 3 – A set of resources is called "resource group" in the information world. The resource group is also called "virtual object." This is the abstracted, analysed or manipulated resources, which may have different characteristics from resources and whose capability may not be bound to the capability of the resources. The "different characteristics" means simplification or extension of the resource characteristics. "Different characteristics" allows the resource group to expose access or control methods from the original physical resource.

3.2.4 resource ownership: Capability of a resource owner to grant access to the resource.

NOTE – The ownership of resources can be transferred to other owner(s). Some resources can be possessed by many resource owners at the same time.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ABAC Attribute based Access Control

DLT	Distributed Ledger Technology
GDS	Group Delegation Service
I_{DR}	Interface between IoT Device(s) and Resources
I_{DS}	Interface between IoT Device(s) and Services
I_{DU}	Interface between IoT Device(s) and Users
I_{RR}	Interface between Roles and Resources
I_{RS}	Interface between Roles and Sessions
I_{UR}	Interface between Users and Roles
I_{US}	Interface between Users and Sessions
IoT	Internet of Things
Pa-PDS	Partial Pre-defined relational Delegation Service
Pa-SDS	Partial Single Delegation Service
Pe-PDS	Permanent Pre-defined relational Delegation Service
Pe-SDS	Permanent Single Delegation Service
PDS	Pre-defined relational Delegation Service
RBAC	Role based Access Control
REST	Representational State Transfer
SDS	Single Delegation Service
Te-PDS	Temporary Pre-defined relational Delegation Service
Te-SDS	Temporary Single Delegation Service
URI	Uniform Resource Locator
Wh-PDS	Whole Pre-defined relational Delegation Service
Wh-SDS	Whole Single Delegation Service
WoT	Web of Things

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**" and "**may**" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are 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 the specification.

6 Overview of delegation service

6.1 Delegation service

With the popularity of the Internet of things (IoT), various physical IoT devices are required to connect to the information world in order to process data speedily and efficiently in support of the cloud environment. It means that various physical devices can be easily converted to virtual devices by using web technologies [ITU-T Y.4000]. In this regard, web technologies, especially web of things (WoT) [ITU-T Y.4400], use a uniform resource identifier (URI) to identify and access things based on the representational state transfer (REST) architecture style.

Figure 1 gives an overview of many IoT devices, gateways and servers that are in the physical world. Some IoT devices are passive (e.g., sensors) that extract data from the physical environment (e.g., water, air and others), while others are active ones (e.g., actuators). IoT gateways have the same functions as IoT devices, and additionally networking features for connecting to the Internet. Users can also manage these IoT devices and gateways to communicate with IoT servers. There are four types of entities in the physical world: IoT device, gateway, server and user. In this Recommendation these four types of entities are referred to as physical objects. As such, these physical objects are represented as virtual objects in the information world. Virtual objects are expressed as the components of cloud service providers and third parties, and become the owner of physical objects in order to easily control the ownership of the objects (e.g., the access rights to the IoT devices and gateways).

This ownership could be transferred to other authorized virtual objects like security services for IoT devices, which are described in Appendix I.1. This Recommendation considers the "ownership transfer service for physical objects" as the delegation service. A physical object has many properties and functions. Ownership of the property and function can be transferred to others. There are two methods to support the delegation service: direct and indirect.

– A direct delegation service occurs between physical objects (e.g., IoT device and gateway). A physical object can transfer ownership to another physical object.

– An indirect delegation service is enabled between physical objects through virtual objects. For an indirect delegation service, the relationship between physical and virtual objects should be established in advance. After conforming the relationship between physical and virtual objects, physical objects can deliver their ownership indirectly through their own virtual objects. In other words, virtual objects can perform the delegation service on behalf of physical objects.

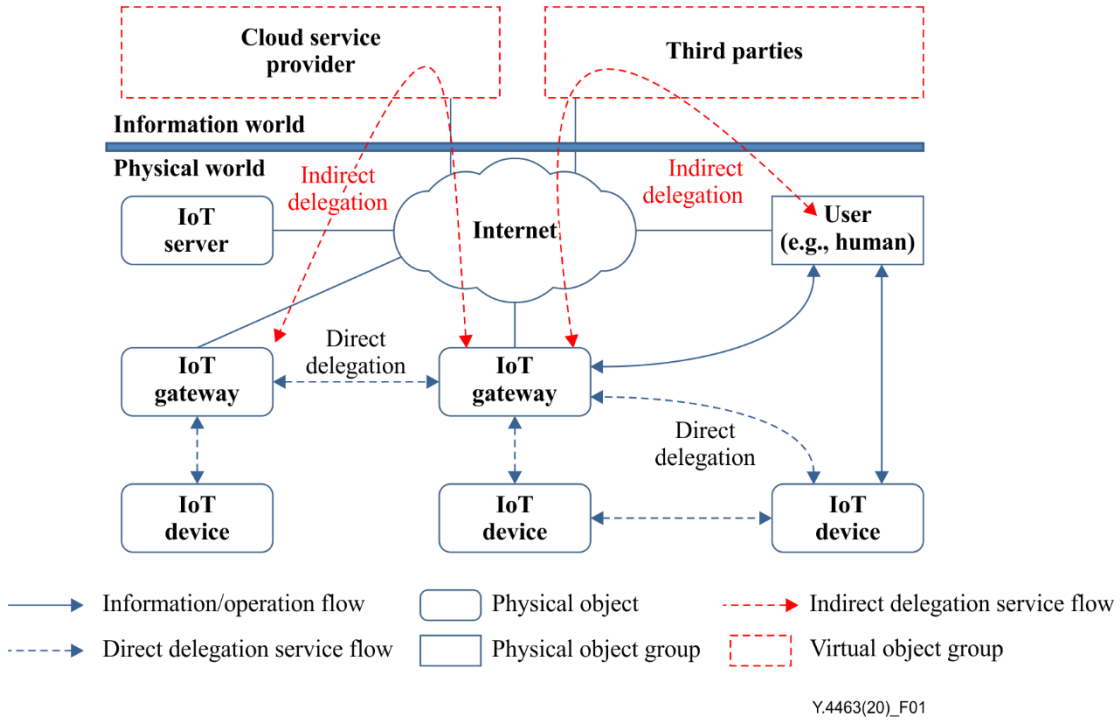

Figure 1 – Examples of delegation service

6.2 Key components of delegation service

The two types of object, i.e., physical and virtual objects, in Figure 2 are defined to support the delegation service.

The first is physical objects such as IoT servers and devices, authorities and human beings. These objects have properties and functions representing physical entities such as sensors and actuators. Through interface I_{DU}, physical objects can be created as virtual objects in the information world.

The second is virtual objects such as resources, resource groups and services. A resource represents the same functionality in the information world as physical object has in the physical world. In other words, a resource has the same capability as a physical object. A one-to-one mapping between a physical object and a resource occurs through interface I_{DU}. Resource groups are abstracted and manipulated from resources and the information of delegation and policy authorities through interfaces, I_{DR}. A resource service is a series of resources and resource groups with delegation operation (e.g., actuating of physical object). This resource service can be represented as delegation service when it performs a function to manipulate the physical objects. These resource services should also perform some operations through interface, I_{DS}.

In this Recommendation, resource(s), resource group(s) and resource service(s) have to use a globally unique identifier such as uniform resource identifier and object identifier [b-ITU-T Y.4500.1].

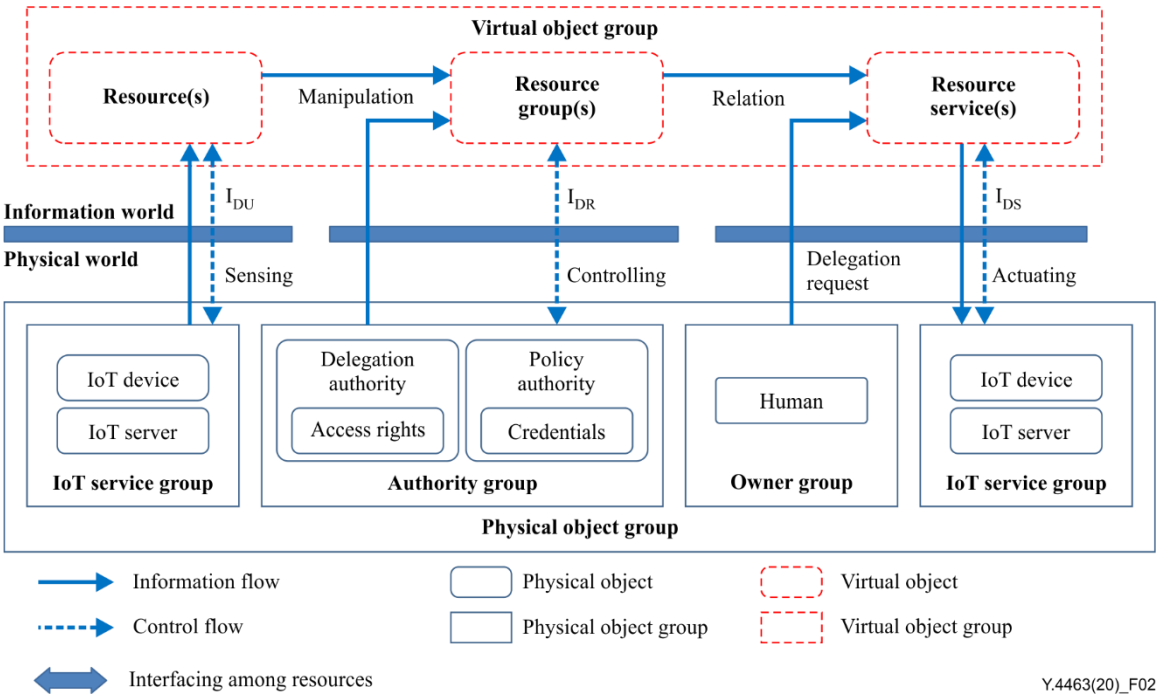

Figure 2 – Key components for delegation service

7 Types of delegation service

The delegation service applies to physical and virtual objects and are classified as three types: single, pre-defined relational and group delegation.

7.1 Single delegation service

A single delegation service (SDS) is initiated from a physical object to create a virtual object. There is a one-to-one mapping between a physical and a virtual object. The virtual object can then transfer ownership to another virtual object. After transferring the ownership, this information should not be allowed to others. More information of a single delegation is described in Appendix I.2.1.

In the scenario for camera devices in Figure 3, the IoT device has a camera entity with image generation capabilities. The images are stored in a secure way as resources in the information world. When partial-single delegation service (Pa-SDS) is applied to resources (virtual object A), the ownership of data in resources (virtual object A) is divided into resource groups (virtual object C and virtual object D). For resource (virtual object B) with the whole-single delegation service (Wh-SDS), resource group (virtual object D) can get the whole access rights of data from resource (virtual object B). Subsequently, a user can access the resource group (virtual object C) to view the images of the IoT device (physical object A). However, the user cannot show the full images without the help of others because resource group (virtual object C) has a Pa-SDS about the resources (virtual object A). Meanwhile, a user can access resource group (virtual object D) to show the whole image of the IoT device (physical object B).

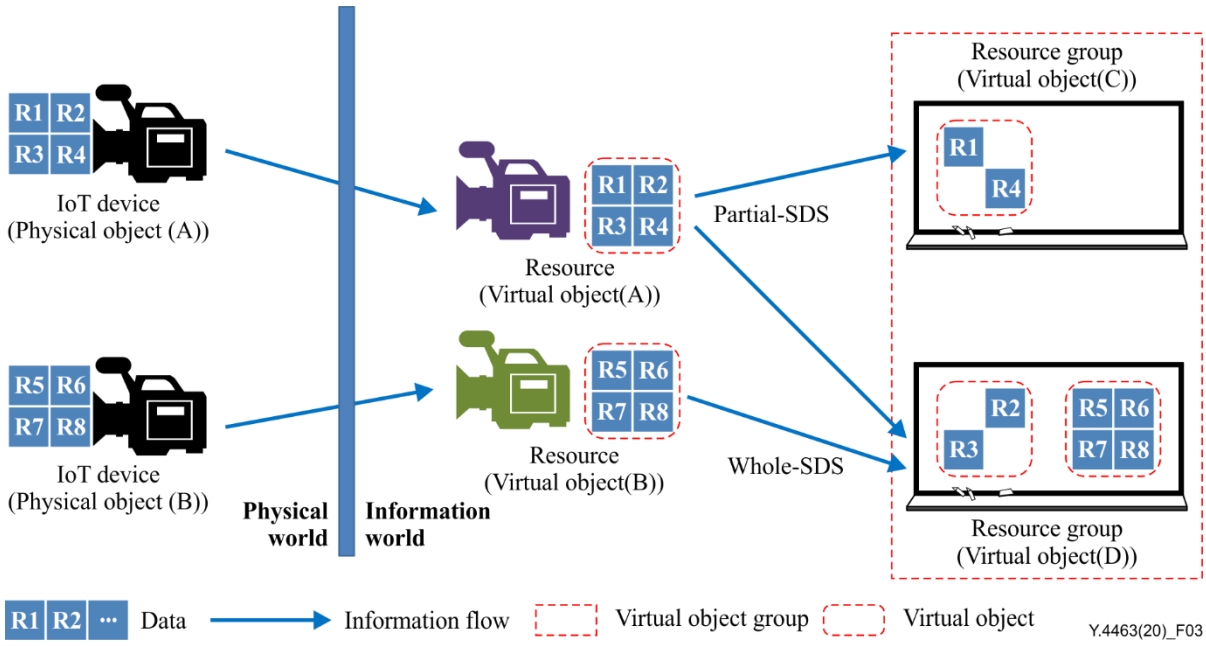

Figure 3 –Single delegation service in camera devices

7.2 Pre-defined relational delegation service

A pre-defined relational delegation service (PDS) is similar to a single delegation service. However, PDS has a different transfer rule of delegated information. This PDS must allow the transfer of delegated information to others in accordance with policy rules. More information is given in Appendix I.2.2.

Figure 4 shows a scenario for an online map application. According to the data collection policy of the online map application, the pre-defined relationship will be established before the data collection. Policy information should be obtained from delegation and policy authorities. Data from IoT devices is then collected in the online map application (resource group (virtual object E)). According to the collection policy of the resource (virtual object A), some of the collected data must be transferred from the resource (virtual object A) into the resource group (virtual object E). This is an instance of partial-pre-defined relational delegation service (Pa-PDS). At the same time, the whole data of the IoT device (physical object B) are collected in the resource group (virtual object E) through the resource (virtual object B). This is an instance of the whole pre-defined relational delegation service (Wh-PDS). In other words, full ownership of collected data must be transferred to the resource group (virtual object E). Finally, the resource group (virtual object E) actuates the IoT device (physical object C) with collected data from the IoT devices (physical object A and physical object B).

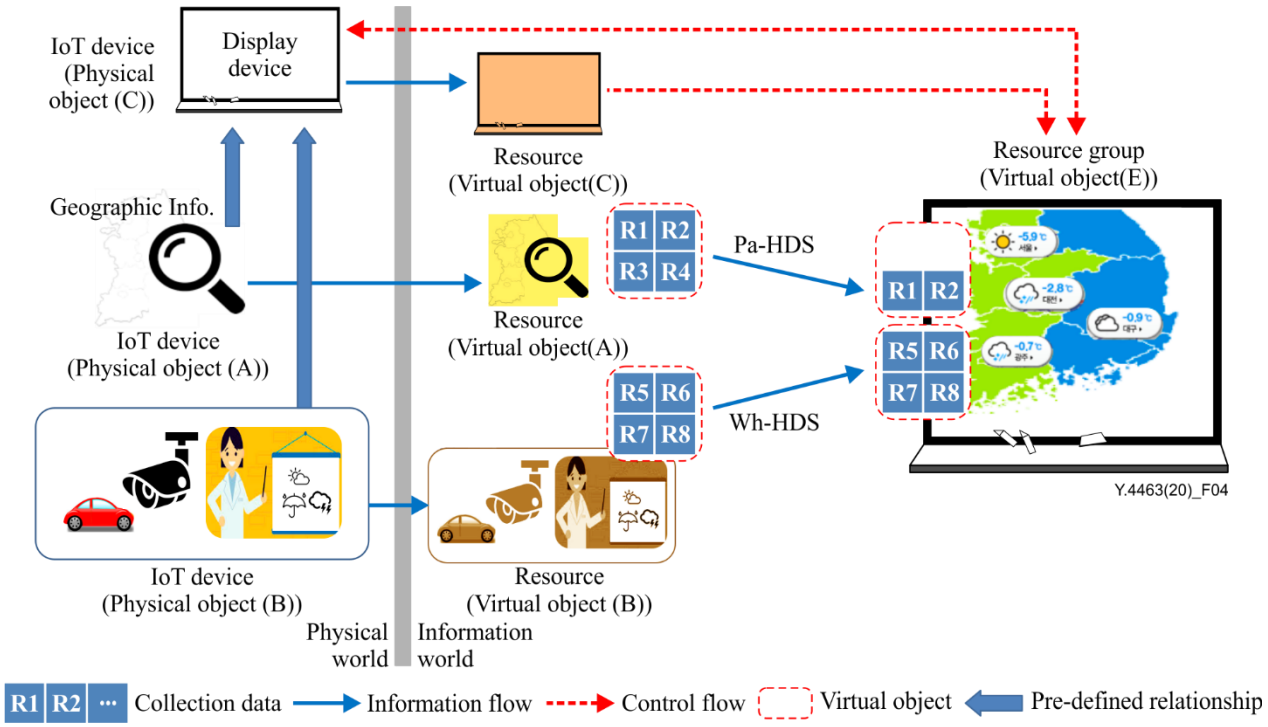

Figure 4 – A pre-defined relational delegation service in an online map application

7.3 Group delegation service

A group delegation service (GDS) is applied to a virtual object group, unlike the previous two services that are applied to a virtual object. This group can be comprised of resources and resource groups. More information of the group delegation is described in Appendix I.2.3.

Visitors without any access rights want to enter the smart home, as shown in Figure 5. Visitors request appropriate access rights from the owner of the smart home. The owner then transfers or copies the access rights for the physical objects (such as lights, doors, appliances, etc.) to the visitors in the physical world. According to the properties of the visitor, the owner must decide between SDS and PDS. If the visitor is a guest of a hotel, he will get the Wh-SDS and the temporary-single delegation service (Te-SDS) for the group of physical objects. In contrast, if a visitor buys a house, it is appropriate to choose Wh-SDS and permanent-single delegation service (Pe-SDS) for full access rights of the whole IoT devices in the smart home. More details of the Te-SDS and Pe-SDS are described in Appendix I.2.1.

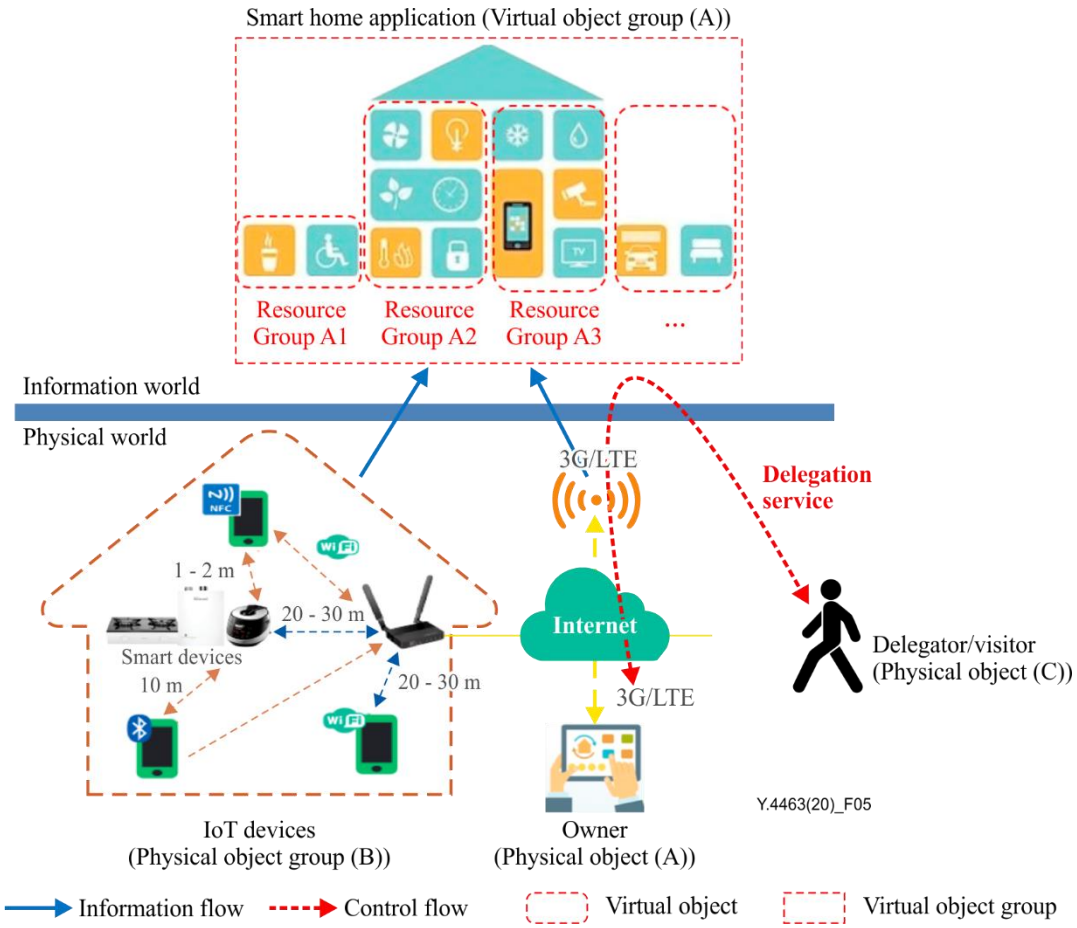

Figure 5 –Group delegation scenario in a smart home

8 Requirements of the delegation service

According to the physical and virtual objects in Figure 2, the following requirements are described.

8.1 Physical/Virtual object requirements

8.1.1 Requirements for physical objects

– Physical objects (e.g., human, IoT devices, gateways and servers and authorities) are required to manage their access rights;

– Physical objects are required to be sensed and actuated according to ownership of physical objects (i.e., access rights);

– Physical objects are required to have policies of transferring ownership;

– Physical objects are recommended to get information from policy and delegation authorities;

– Ownership of a physical object is recommended to be divided into resource groups.

8.1.2 Requirements for virtual objects

– Virtual objects (e.g., cloud service provider and third parties) are required to manage their access rights;

– Virtual objects are recommended to manage the revocation information;

– Virtual objects are required to manage their ownership in attributes of resources and resource groups;

– Virtual objects are recommended to maintain the history of their ownerships to mitigate the threat caused by abnormal operations;

– Virtual objects are recommended to use attributes in separate resources to manage information from policy and delegation authorities;
– Resources are required to manage the history of the delegation service about the one-to-one mapped physical objects;
– Resources are required to prevent the conflict of policy rules;
– Resources are required to support the pre-defined relational delegation service;
– Resource groups are required to manage the access rights of physical objects;
– Resource groups are required to prevent the conflict of policy rules;
– Resource groups are required to support the pre-defined relational delegation service.

8.1.3 Requirements for interactions between physical and virtual objects

– Physical objects in physical world are required to have the mapping with resources in information world;
– Physical objects are recommended to have one-to-one mapping with resources;
– Physical objects are recommended to have a mapping with resource groups;
– Physical objects are recommended to have means that transfer the access rights between physical and virtual objects;
– Physical objects are required to represent their ownership (i.e., access rights) as attributes in resources;
– Physical objects are recommended to represent their ownership as attributes in resource groups;
– Delegation authorities are recommended to support the creation and deletion of resource groups;
– Policy authorities are recommended to manage the policy rules for resources and resource groups.

8.2 Services requirements

8.2.1 Requirements for the single delegation service

– SDSs are recommended to apply the same resources and resource groups;
– SDSs are required to validate resources and resource groups.

8.2.2 Requirements for the pre-defined relational delegation service

– PDSs are required to have trust relationships among physical objects before the execution of the delegation service;
– PDSs are recommended to support the pre-defined relation features;
– PDSs are required to support the continuous the delegation service among resources and resource groups;
– PDSs are required to prevent the conflict of policy rules to support the pre-defined relational features.

8.2.3 Requirements for the group delegation service

– A group in GDS is recommended to be established according to physical and virtual object types;
– All physical and virtual objects in a group are required to have the same ownership policy;
– GDSs are required to have selection rules for a group manager;

– Group manager (e.g., user and IoT device) is recommended to select the members for the group;
– GDSs are required to manage the transfer of ownership between resources and resource groups through the group manager.

9 Architectural model of the delegation service

The architectural model of the delegation service is shown in Figure 6. The model extends the concept of physical and information world depicted in [ITU-T Y.4000]. The role-based access control (RBAC) and the attribute-based access control (ABAC) reference models [b-INCITS 359] and [b-NIST.SP.800-162] are used to describe the details of physical and virtual objects.

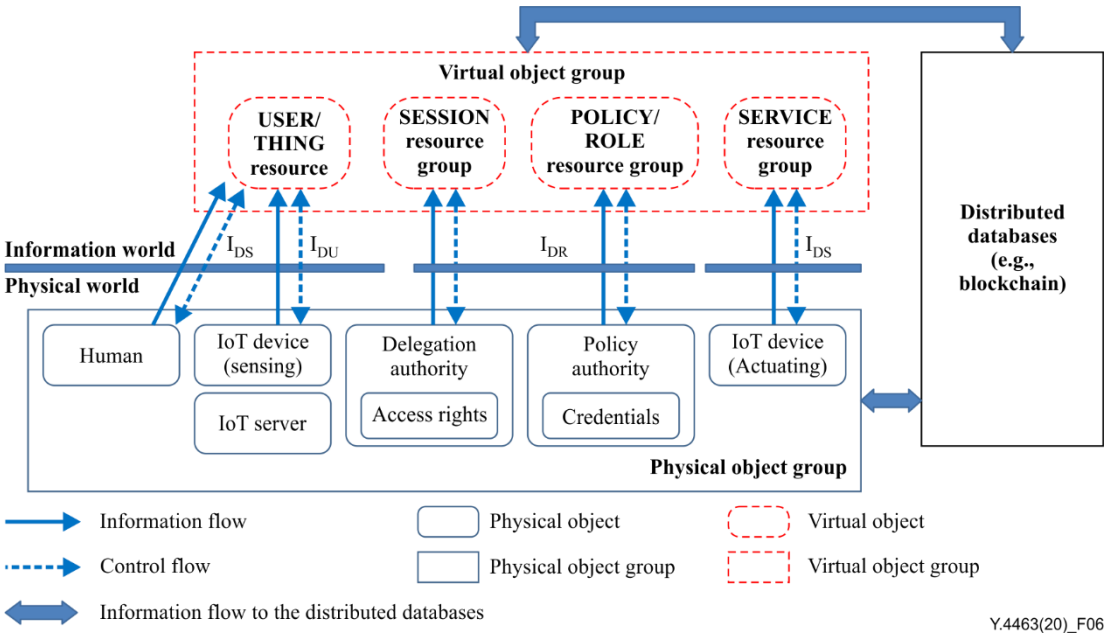

Figure 6 –Architectural model of delegation service

Figure 6 shows the RBAC model that includes eleven objects and three mapping relationships between the information world and the physical world. Six virtual objects are mapped into either resource or resource group roles based on the RBAC model. Five physical objects for sensing and data processing are located in the physical world to control resource ownership (i.e., access rights) based on the RBAC and ABAC models. These physical objects are mapped into the following six resource/resource group roles of information world:

– THING resource: An IoT server and an IoT device will be used to collect and store data from the physical environment. They will be mapped into THING resources through interface I_{DU};
– USER resource: Humans will be asked to create USER resource through interface I_{DS}. This resource will be used to identify a human-being;
– SESSION resource group: Delegation authority manages the access rights of resources. These access rights are mapped into SESSION resource group through interface I_{DR}. The SESSION resources are changed with time-dependency according to delegation service;
– POLICY resource group: Policy authority manages the credentials of USER and THING resources. Policy authority with these credentials has human-oriented policies and is mapped into POLICY resource group through interface I_{DR}. According to POLICY resources, the relation between USER/THING and SESSION resources will be decided. That is, POLICY resources are used when human-oriented conditions are met in order to support delegation service;

– ROLE resource group: Policy authority manages the credentials of USER and THING resources. These credentials are machine-oriented policies and mapped into ROLE resource group through interface I_{DR}. According to ROLE resources, the relation between USER/THING and SESSION resources will be decided. That is, ROLE resources are used as the machine-oriented conditions in order to manipulate IoT devices for delegation service;

– SERVICE resource group: An IoT device is mapped into a SERVICE resource group through interface I_{DS}, according to the request of delegation service from a human or an IoT server.

The virtual objects for storing information of delegation service are located in the information world. That is, distributed databases (e.g., based distributed ledger technologies such as blockchain) are included to collect all information for delegation service.

Figure 7, which is an extension of Figure 6, shows the relations of resources and resource groups in the information world. Here, five mapping relationships via interfaces between resources and resource groups are shown in the information world:

– I_{UT} interface: A USER resource has one-to-one mapping with a physical object (e.g., Human). A THING resource also has one-to-one mapping with a physical object (e.g., IoT device, gateway and server). Therefore, the USER resource has the ownership of physical objects from the THING resource through the interface I_{UT};

– I_{US} interface: A USER resource will manage a SESSION resource group to show the current ownership information through the interface I_{US}. The SESSION resource group is time-dependent;

– I_{RS} interface: A relationship between a USER resource and a SESSION resource group will be decided according to policy information from POLICY and ROLE resource groups. These resource groups will communicate with SESSION resource through interface I_{RS};

– I_{RR} interface: USER and THING resources requests to make the SERVICE resource group with SESSION and ROLE resources. In other words, the SERVICE resource group will be established according to the composition of the SESSION, POLICY and ROLE resource groups through interface I_{RR}. And then the SERVICE resource group will be able to manage the functions of an IoT device;

– I_{UR} interface: USER and THING resources manage POLICY and ROLE resource groups through interface I_{UR}.

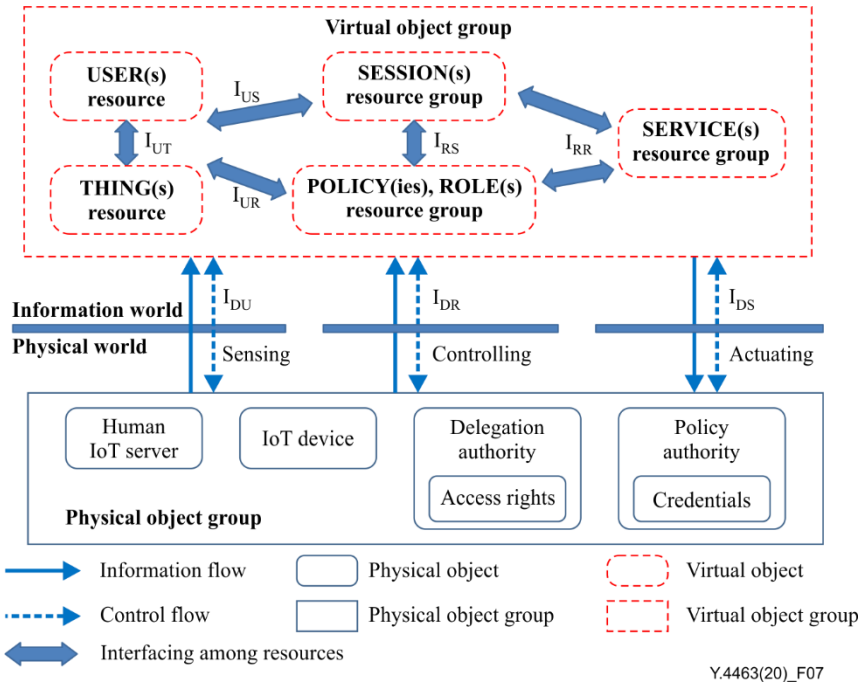

Figure 7 –Mapping relation between virtual objects

Figure 8 shows the mapping relation of SESSION, POLICY and ROLE resource groups for policy management in detail. More detail descriptions are given in Figure III.5 of Appendix III.2.

– SESSION resource group: The SESSION resource group has the inner resource – EVENT, which invokes and triggers some virtual objects;

– ROLE resource group: The ROLE resource group is mapped into USER and THING resources with information of the delegation service from a policy authority. The ROLE resource group also has inner resources – CONDITION and ACTION. The CONDITION resource could be used to trigger the ACTION resources. The types of ACTION resources may be CRUDN (Create, retrieve, update, delete and notification).

– POLICY resource group: The POLICY resource group will be transferred from a policy authority in the physical world. The POLICY resource group has inner resource – COMMAND. The COMMAND resource can be used to manage the delegation request from the physical world.

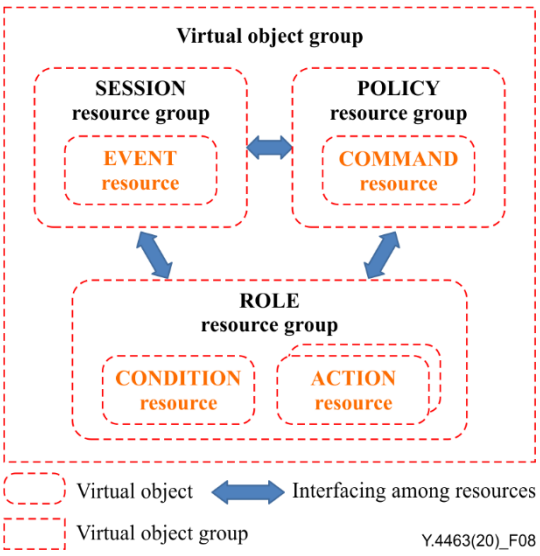

Figure 8 –Mapping relation for policy management

Figure 9 shows the SERVICE resource group in detail. The SERVICE resource group has three inner resources: SERVICE, OPERATION and CONTROL. There are three inner mapping relationships between three resources in the SERVICE resource group. More detailed descriptions are presented in Figure III.6 of Appendix III.2.

– SERVICE resource: The SERVICE resource is mapped into many resource groups such as SESSION, POLICY and ROLE as shown in Figure 8;

– CONTROL resource: The CONTROL resource has a mapping relation with an IoT device with actuating capability;

– OPERATION resource: The OPERATION resource has the execution information (e.g., smart contracts). That is, The OPERATION resource has execution codes and the triggering conditions from SERVICE resources.

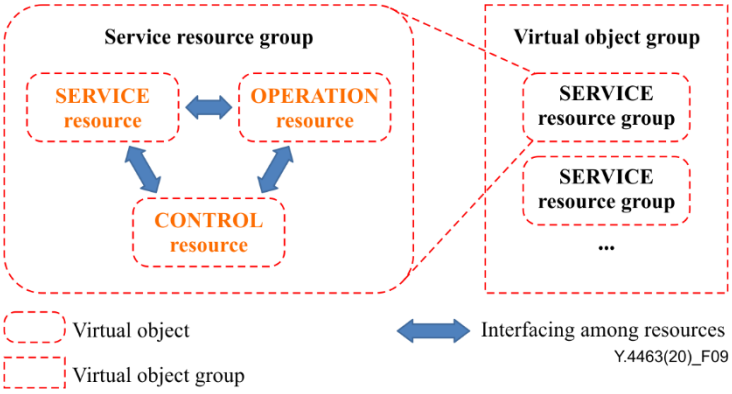

Figure 9 – Mapping relation in the SERVICE resource group

Appendix I

Types of delegation device

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

This appendix presents security phases for IoT devices cited from security services of [b-oneM2M] and defines delegation service.

I.1 Security phases for IoT devices

Security services for IoT devices are generally composed of four phases as shown in Figure I.1 [b-oneM2M]. The first phase is network connectivity establishment to register network service. This phase is independent of the other phases. The second phase is security provisioning. During this phase, security credentials and identifiers are exchanged between the IoT device and the IoT server through established network connection in order to provide security keys and related algorithms for each other, referred to as the "enrolment phase." The third phase is security association establishment. In this phase, access right of resource(s) for IoT devices is negotiated and determined. The last phase is access control. This phase is the execution step in accordance with the results of negotiations in previous steps.

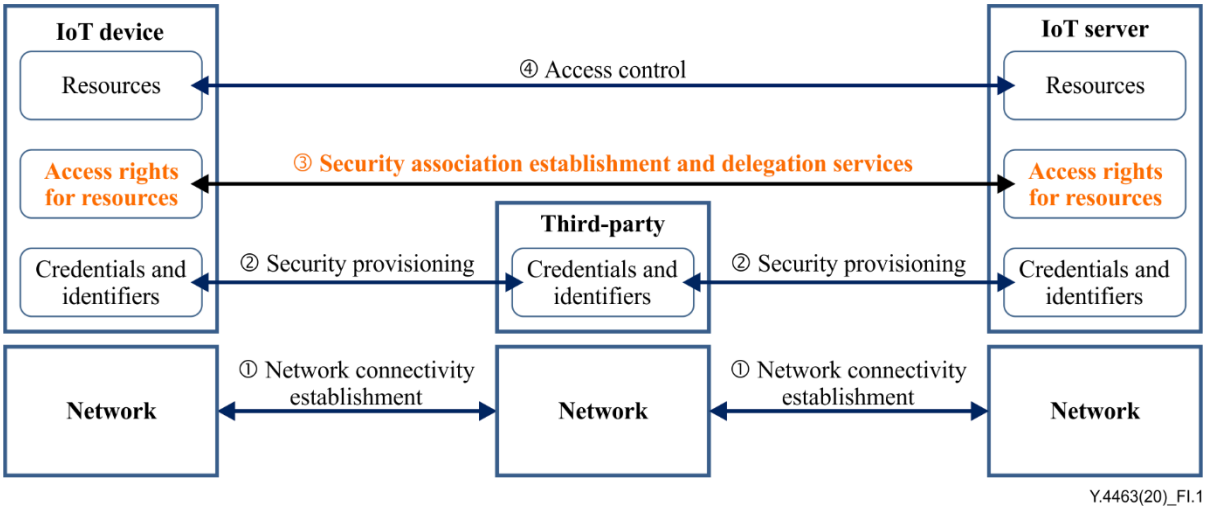

Figure I.1 – Four security phases of IoT devices

Delegation service refers to the third phase in Figure I.1. During this phase, ownership of the IoT device will be negotiated and transferred to an IoT server. These ownerships are access rights of IoT devices. For example, access right means the functional operation of IoT devices such as create, read, update, delete and notify (CRUDN).

I.2 Delegation service among IoT devices

I.2.1 Single delegation service

The single delegation service (SDS) is classified from two viewpoints: whole or partial ownership transfer and time dependency. According to whole or partial ownership transfer viewpoint, there exists the whole and partial SDS (Wh-SDS and Pa-SDS). The time dependency viewpoint, encompasses permanent and temporary SDS (Pe-SDS and Te-SDS).

A Wh-SDS transfers whole ownership to peer IoT device(s). That is, after whole ownership transfer, IoT devices may share whole ownership with peer IoT devices according to the policies. On the other hand, a Pa-SDS transfers ownership of IoT device to a peer partially.

Figure I.2 shows whole and partial-based single delegation services. At first, IoT device (A) has connectivity to physical entities such as sensors. It means that IoT device (A) has full access rights for its physical entities. IoT device (A) may be assumed to have six data. IoT device (A) then transfers the whole access rights into resource (B). That is, resource (B) will have full ownership for IoT device (A) after a Wh-SDS service. On the other hand, resource (B) transfers a part of the access rights into IoT device (C). That is, IoT device (C) has only partial ownership for resource (B). Therefore, if IoT device (C) uses full functions of IoT device (A), IoT device (C) will have to obtain ownership of the remaining resources from IoT device (A) or resource (B) temporarily.

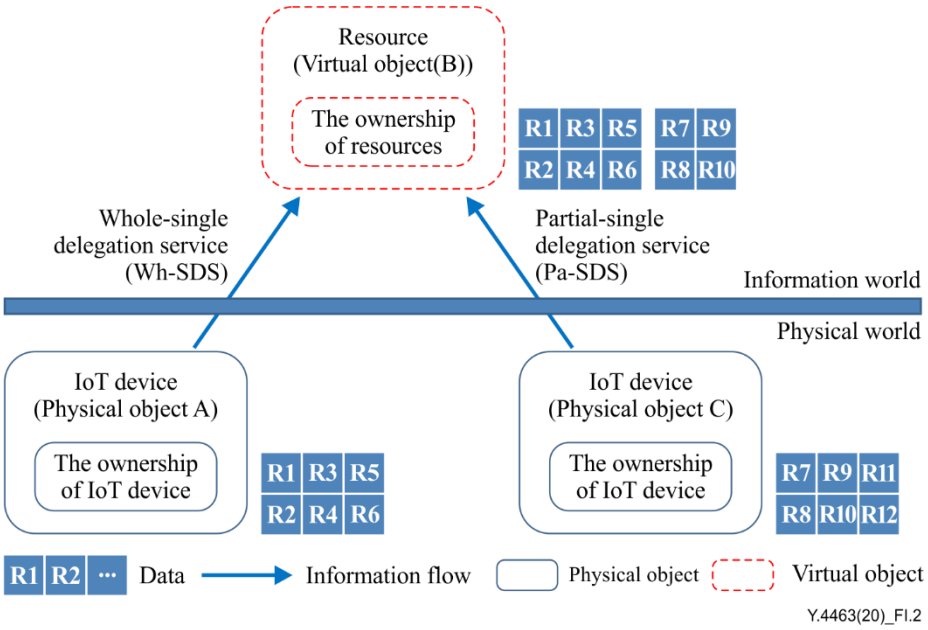

Figure I.2 – Whole and partial-based single delegation services

Figure I.3 shows time-based delegation services such as Pe-SDS and Te-SDS. A Pe-SDS transfers ownership of resources permanently while a Te-SDS transfers it temporally. The Pe-SDS is not able to withdraw transferred ownership. On the other hand, Te-SDS will be able to withdraw ownership in future. That is, the delegated information of Te-SDS will be cancelled automatically after a defined time period.

Resource (virtual object B) transfers partial ownership temporally to IoT device (physical object A). That is, IoT device (physical object A) has only partial ownership for resource (virtual object B) like Pa-SDS. After the elapse of a given time period, ownership of IoT device (physical object A) about resource (virtual object B) will be withdrawn. In case of Pe-SDS, ownership of IoT device (physical object C) should not be withdrawn.

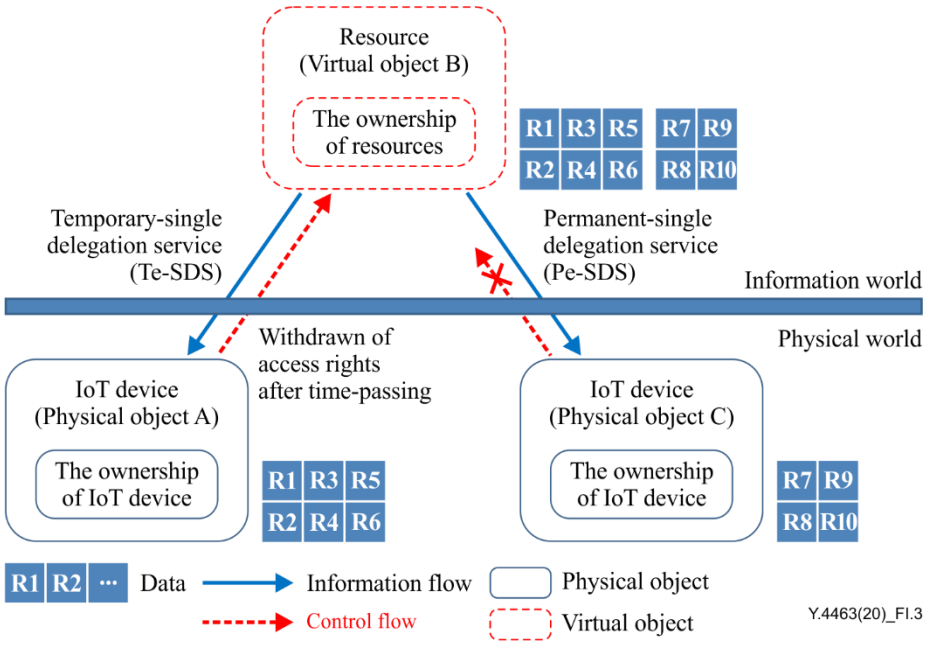

Figure I.3 – Time-based single delegation services

I.2.2 Pre-defined relational delegation service

A pre-defined relational delegation service is classified into two categories: whole or partial ownership transfer and time-based types. In the whole or partial ownership transfer, there are both whole pre-defined relational delegation service (Wh-PDS) and partial pre-defined relational delegation service (Pa-PDS). Wh-PDS transfers full ownership information from the parent IoT device into the child IoT devices and then the reverse process can also be possible. These operations take place through the resource in information world or directly, otherwise, the Pa-PDS transfers the ownership information partially. In time-based, there are both permanent PDS (Pe-PDS) and temporary PDS (Te-PDS). In case of Pe-PDS, the first-level child IoT device can transfer ownerships to secondlevel IoT devices.

The PDS is different from the SDS from the viewpoint of prerequisite requirements. A group delegation described in clause I.2.3 is a super set of PDS because PDS should agree with the policy rule among IoT devices in advance. PDS should have relations of ownership policies between parent and child IoT devices in advance. In Figure I.4, IoT device (A) manages resource (D) for the PDS. That is, IoT device (A) already obtained ownership of IoT device (B)'s data from IoT device (C). In this case, the parent device, IoT device (A) has the role of the manager for PDS. IoT device (B) and (C) also have the policy rule of resource ownership in advance. Thus, PDS may only occur automatically according to the policy rule. That is, delegated ownership information may or may not be transferred to third parties.

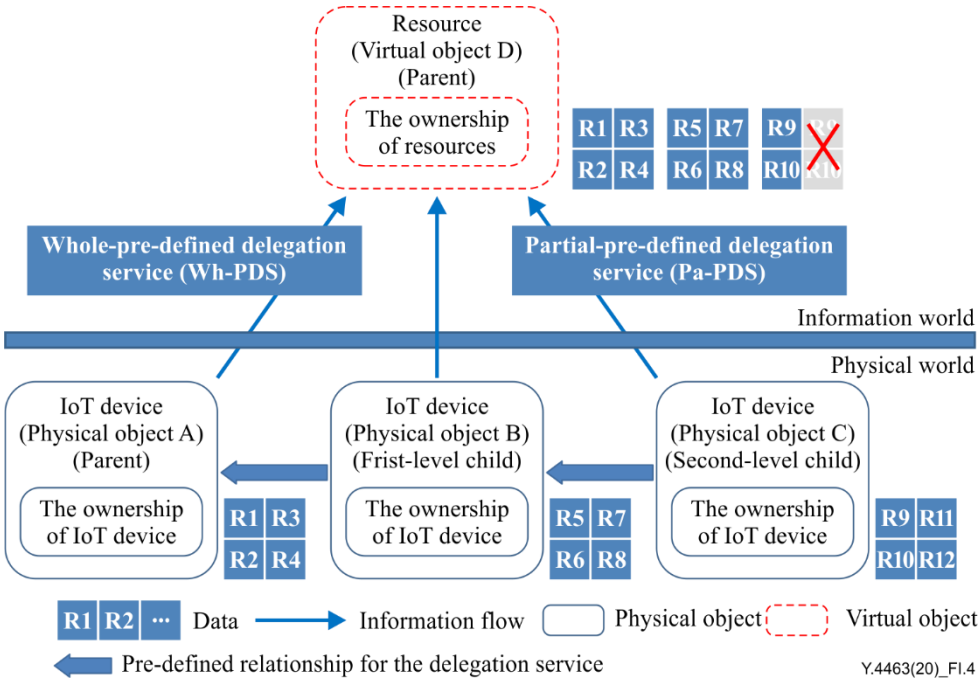

Figure I.4 – Pre-defined relational delegation services

I.2.3 Group delegation service

The group delegation service will be transferred and copied among sets of IoT devices. A resource should be selected for a group. When transferring its ownership information about a resource to group, each IoT device should do so either permanently or temporally. The manager of a group should also be selected among IoT devices in order to manage the resource. Subsequently, the ownership of a group will be transferred to the other IoT device by the manager of the group. The change of ownership should also be disseminated to all IoT devices in the group by the manager.

Figure I.5 demonstrates that the data of all IoT devices will be transferred to resource (D). The manager for resource (D) should be selected among IoT devices and the selected manager maintains the collected resources. The selection methods of the group manager are outside the scope of this Recommendation.

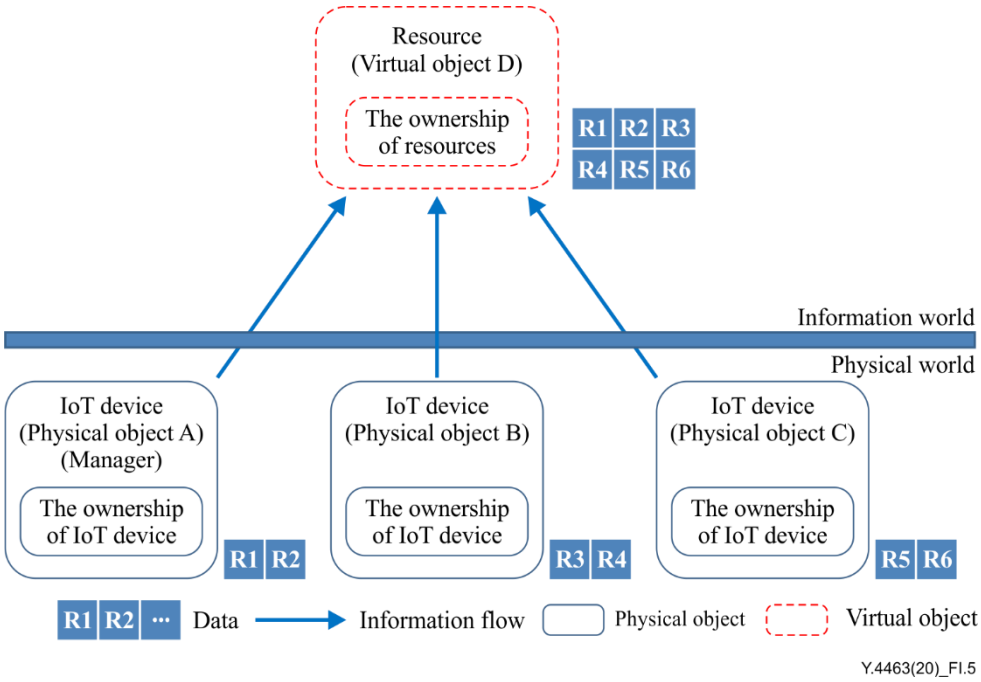

Figure I.5 – Group delegation service

Appendix II

Procedures of delegation service

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

This appendix provides the procedures of delegation service to illustrate delegation scenarios.

II.1 Single delegation service

As shown in Figure 3, IoT devices (physical object A and physical object B) are the camera entities. They have the function of image generation. These images will be then stored in a secured method as resources (virtual object A and virtual object B) for each physical object. IoT device (physical object A) generates images (R1 to R4) and registers them as image data into resource (virtual object A). IoT device (physical object B) also registers images (R5 to R8) into resource (virtual object B). The control and policy information for a single delegation service should then be obtained with the help of delegation and policy authorities. Thereafter, resource groups (virtual object C and virtual object D) will be composed as a result of a single delegation service.

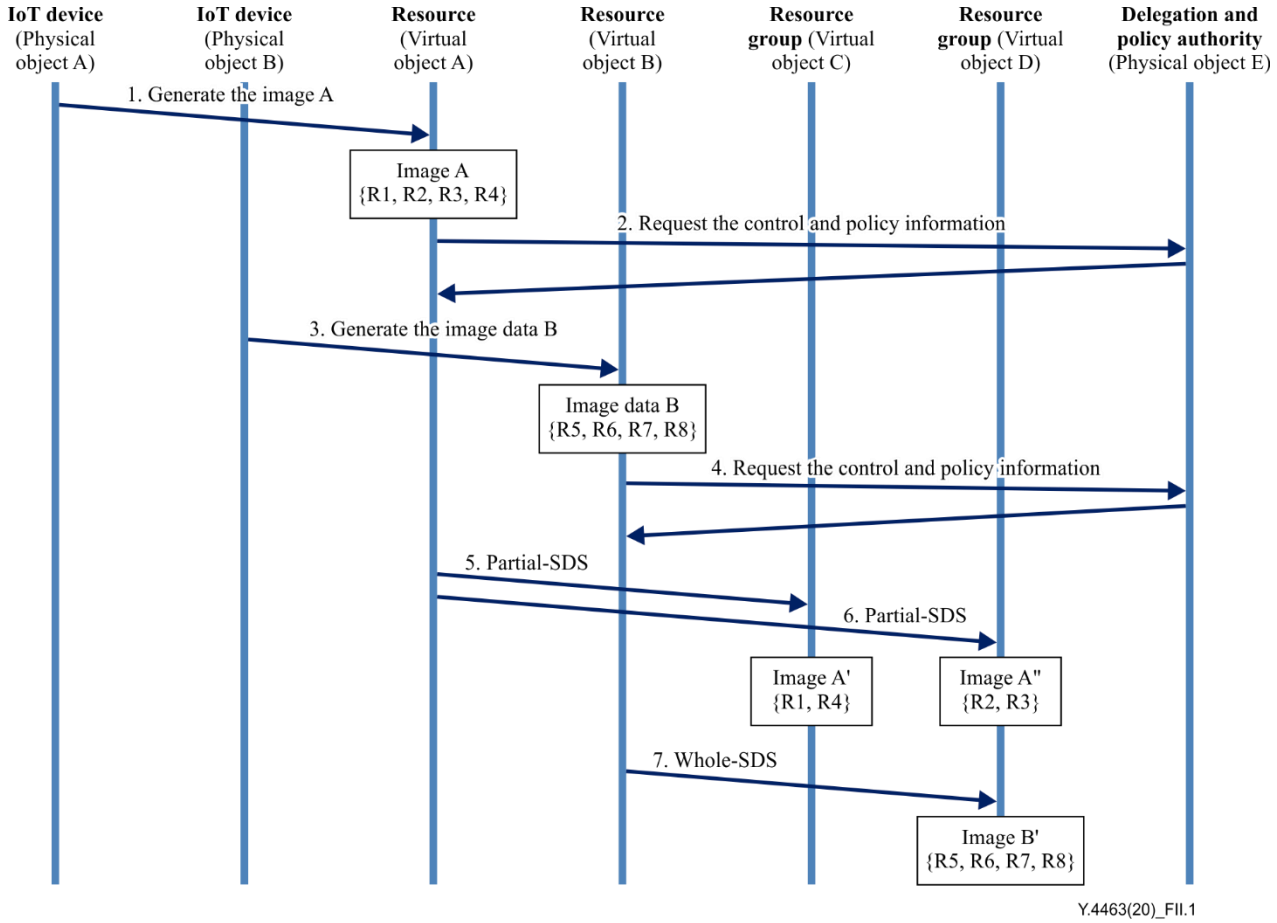

Figure II.1 – Detailed procedures of single delegation scenario

II.2 Pre-defined relational delegation service

According to a PDS policy, the pre-defined relation for online map application will be established for collecting data in the virtual object A, B and C before the data collection service. In Figure 4, the IoT devices (physical object A, physical object B and physical object C) should have the pre-defined relation for the delegation service. IoT device (physical object C) then generates resource group (virtual object E) through resource (virtual object C) for online map service. Thereafter, IoT device

(physical object A) generates geographic information and registers the information into resource (virtual object A) and afterwards resource (virtual object A) transfers part of its data into resource group (virtual object E).

The remaining data in resource (virtual object A) will be maintained in its own storage, and this is a partial-PDS. At the same time, IoT device (physical object B) gets traffic and weather information. It then registers this information into resource group (virtual object E) through resource (virtual object B), and this is a whole-PDS. Finally, combined data will be transferred to IoT device (physical object C) such as a display device.

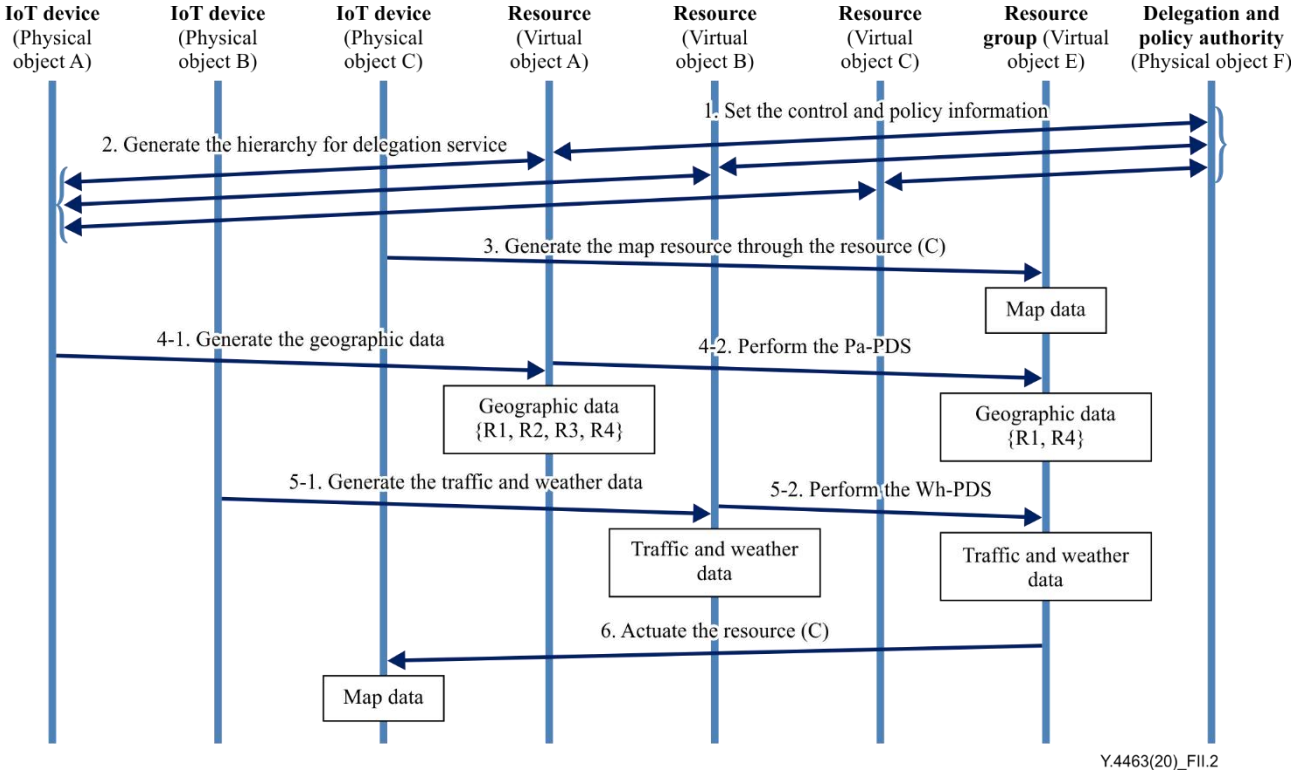

Figure II.2 – Detailed procedures of pre-defined relational delegation scenario

II.3 Group delegation service

Figure II.3 shows detail procedures to instantiate a smart home service to illustrate the concept of group delegation service illustrated in Figure 5. At first, the owner of the smart home should make resource groups for IoT devices in order to make group delegation easy. Thereafter, the owner will transfer ownership of the group to a visitor.

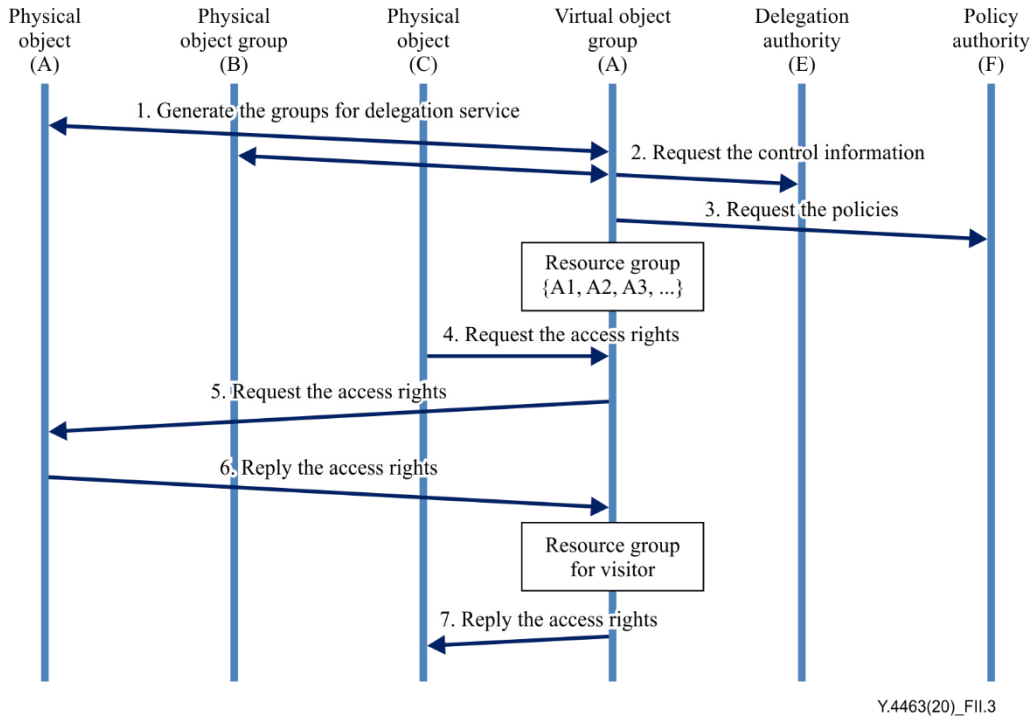

Figure II.3 – Detailed procedures of group delegation scenario in smart homes

Appendix III

Data model of delegation service

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

This appendix provides the data model of delegation service in an IoT environment.

III.1 Physical objects for delegation service

Figure III.1 shows the core function in the IoT gateway and the IoT device as the physical objects for the delegation service. First of all, the IoT device has four modules: session, thing, user and service modules. The IoT device may also have physical things at the same place. The IoT gateway has three more additional modules compared to the IoT device. In particular, distributed ledger technology (DLT) module has the key function for security services such as integrity, access control and extra.

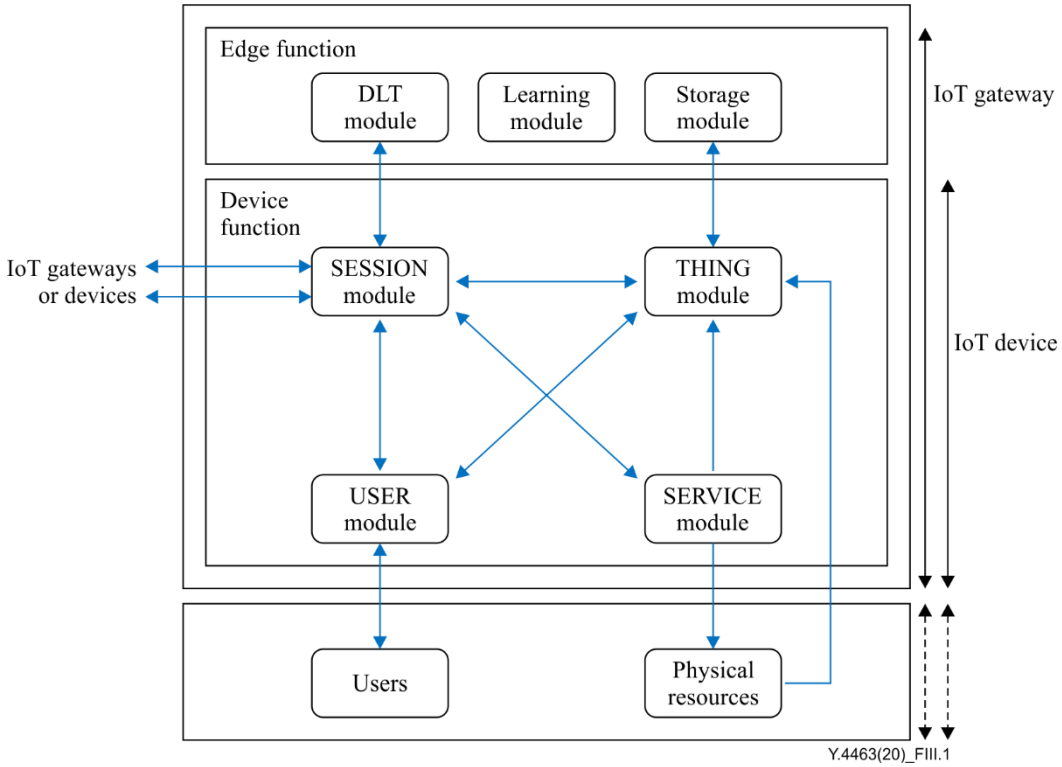

Figure III.1 – Core functions in IoT gateways and devices

Figure III.2 and Figure III.3 describe various interfaces in the IoT gateway and the IoT device. Figure III.2 shows the twelve interfaces in the IoT gateway and the IoT device. Figure III.3 also describes four types of messages (Command, Event, Control and Context) for IoT services, which are used through the twelve interfaces.

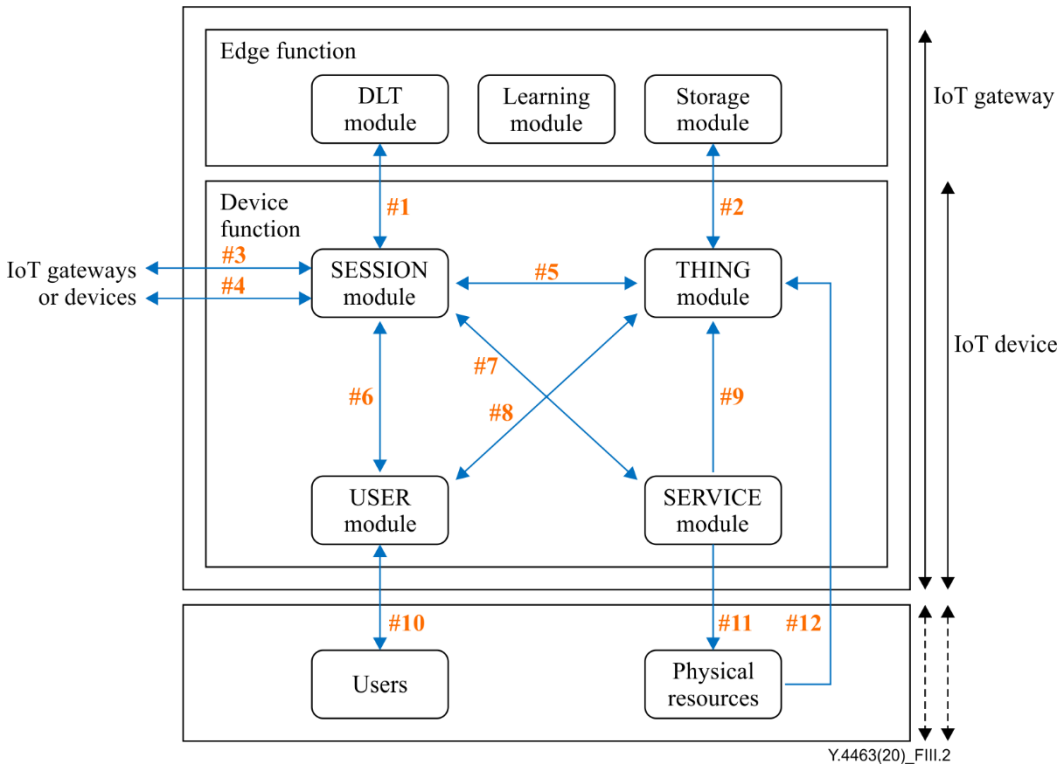

Figure III.2 – Interfaces of IoT gateways and devices

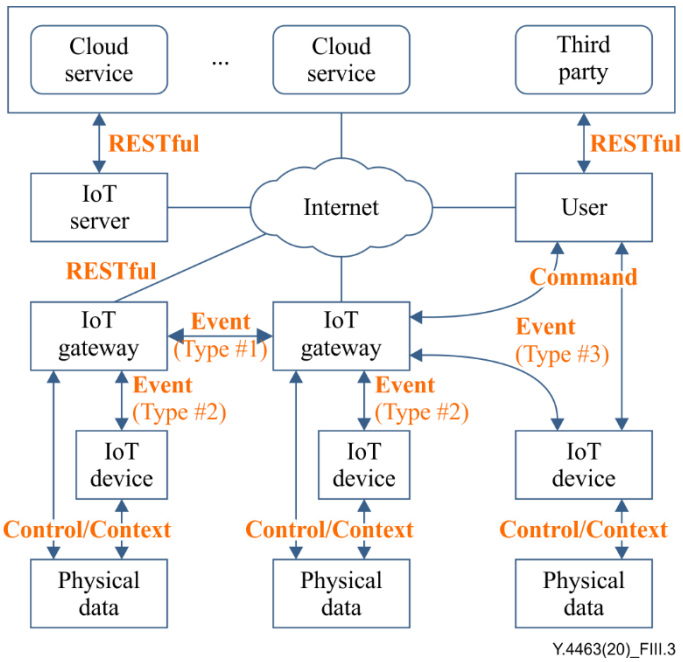

Figure III.3 – Four types of messages for delegation service

Figure III.4 shows Event messages. There are three different types of Event messages according to the subject of communication such as the IoT gateways and the devices.

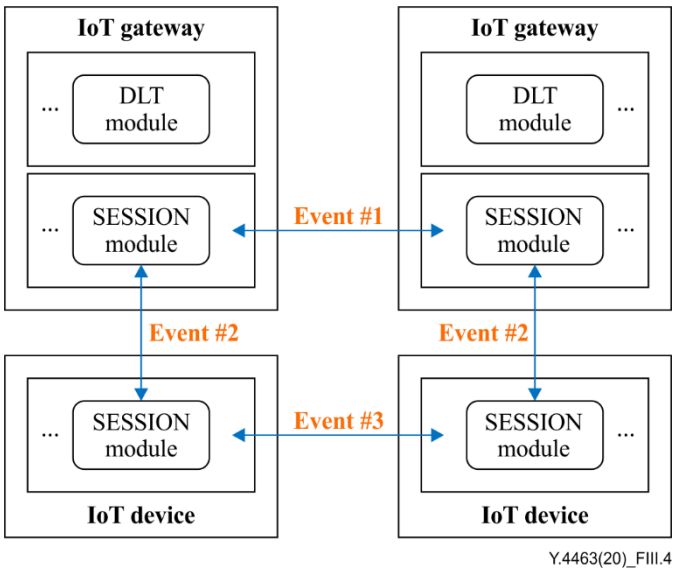

Figure III.4 – Different types of Event messages for delegation service

III.2 Data models for delegation service

Figure III.5 shows the data model for SESSION resource to support the session module of Figure III.1. The ROLE resource has "condition" field. The "condition" field is composed of context name, event name and token. Here, "token" has timing information to support various types of delegation services. And "action" field is composed of two components: action type and action name. There are six types of actions: create, retrieve, update, delete, notification and no-operation. There are also four names of action: event, control, context and command.

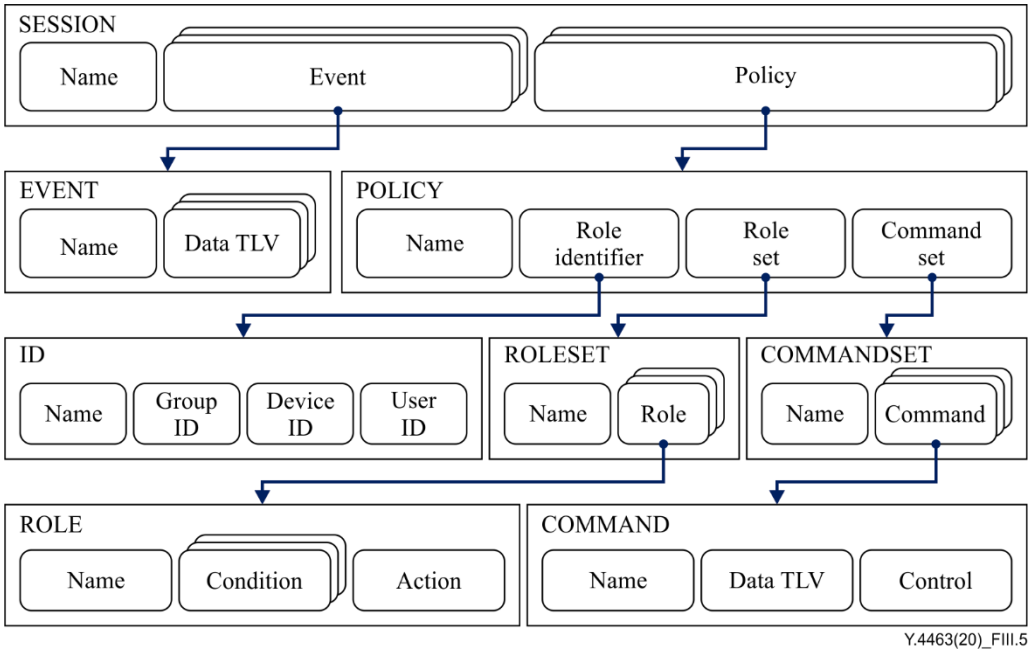

Figure III.5 – Data model for SESSION resource

Figure III.6 shows the data model for SERVICE resource to support the service module of Figure III.1. SERVICE resources are used to manage the physical objects through interface #11 in Figure III.2

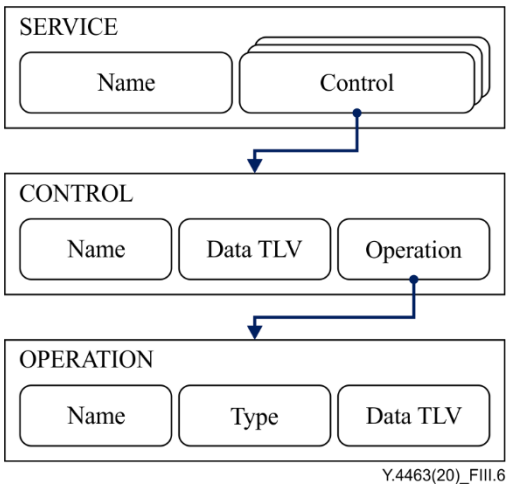

Figure III.6 – Data model for SERVICE resource

Figure III.7 shows the data model for USER resource to support the user module of Figure III.1. Here, this data model defines USER resource and these resources are managed by a human through interface #10 of Figure III.2.

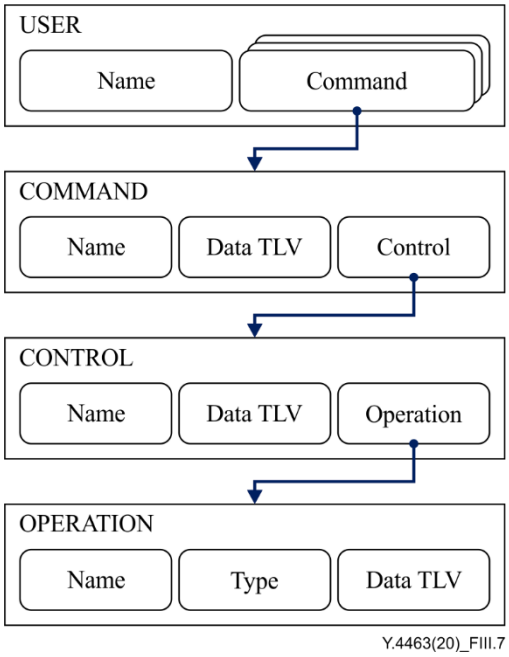

Figure III.7 – Data model for USER resource

Figure III.8 shows the data model for THING resource to support the thing module of Figure III.1. The thing module based on this data model gathers some raw data through interface #12 in Figure III.2. THING resource will then be made from the raw data with their syntax.

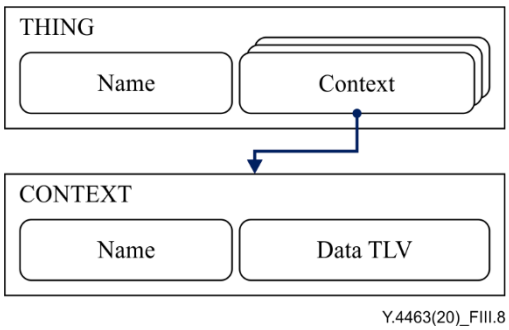

Figure III.8 – Data model for THING resource

Figure III.9 shows the data model for the distributed database of Figure 6. This data model defines new DLT resource group and supports the session module of Figure III.1. The DLT resource is transferred for discovery and security matters. This DLT resource is outside the scope of this Recommendation.

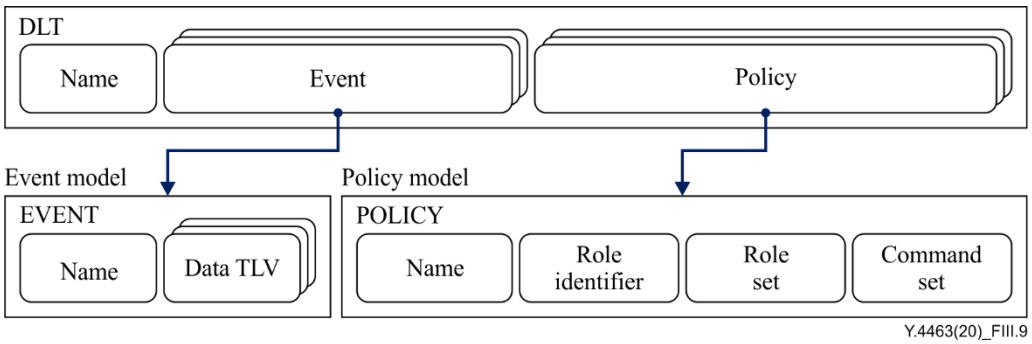

Figure III.9 – Data model for distributed database

Bibliography

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T Y.2002] Recommendation ITU-T Y.2002 (2009), *Overview of ubiquitous networking and of its support in NGN*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for next generation networks.*

[b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

[b-ITU-T Y.2724] Recommendation ITU-T Y.2724 (2013), *Framework for supporting OAuth and OpenID in next generation networks*.

[b-ITU-T Y.4500.1] Recommendation ITU-T Y.4500.1 (2017), *oneM2M-Functional Architecture*.

[b-IETF RFC 3444] IETF RFC 3444, *On the Difference between Information Models and Data Models*.

[b-INCITS 359] ANSI INCITS 359-2012, Information technology – *Role Based Access Control*

[b-NIST.SP.800-162] NIST Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*.

[b-oneM2M] oneM2M-TS-0003-Security_Solutions-V-2014-8, *oneM2M Security Solutions.*

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