International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4462

(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

Requirements and functional architecture of open IoT identity correlation service

Recommendation ITU-T Y.4462

ITU-T

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.4462

Requirements and functional architecture of open IoT identity correlation service

Summary

Open Internet of things (IoT) identity correlation service (ICS), or open IoT ICS, is a service to map identities among devices, third party services, and transactions. Recommendation ITU-T Y.4462 specifies the reference architecture of open IoT ICS which supports Internet of things (IoT) devices to access multiple third party service providers. This Recommendation clarifies the concept of the open IoT ICS, identifies its basic capabilities and common requirements and also provides the reference architecture and relevant high-level common procedures for open IoT ICS.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.4462	2020-01-13	20	11.1002/1000/14165

Keywords

ICS, ID, identity mapping, IoT, platform.

[*] 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.4462

Requirements and functional architecture of open IoT identity correlation service

1 Scope

This Recommendation provides information on the:

- Concept and requirements of the open Internet of things (IoT) identity correlation service.
- Functional architecture of the open IoT identity correlation service.
- Basic capabilities, relevant reference points and procedures of the open IoT identity correlation 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 G.9961] Recommendation ITU-T G.9961 (2018), *Unified high-speed wireline-based home networking transceivers – Data link layer specification*.

[ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network.*

[ITU-T X.1570] Recommendation ITU-T X.1570 (2011), *Discovery mechanisms in the exchange of cybersecurity information*.

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

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

[ITU-T Y.4203] Recommendation ITU-T Y.4203 (2019), *Requirements of things description in the Internet of things.*

[IETF RFC 4122] IETF RFC 4122 (2005), *A Universally Unique Identifier (UUID) URN Namespace.*

[IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 device [ITU-T Y.4000]: With regard to the Internet of things, this is 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 management [b-ITU-T X.1252]: A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for assurance of identity information (e.g., identifiers, credentials, attributes); assurance of the identity of an entity and supporting business and security applications.

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

3.1.5 device ID [ITU-T G.9961]: A unique identifier allocated to a node operating in the network by the domain master during registration.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 IoT identity correlation service: IoT identity correlation service or IoT ICS, is a service to map relationships among the identities of Internet of things (IoT) related entities (e.g., devices, services and transactions) and also open the capabilities to third party applications.

3.2.2 unique transaction identifier (UTI): An identifier that is generated by a third party service provider upon the initial authorization by the user and made available to the open Internet of things (IoT) identity correlation service (ICS). This identifier needs to be globally unique, anonymous and revocable.

3.2.3 IoT device serial number: A provenance information related to the Internet of things (IoT) device so that each of the IoT devices can be identified physically, as described in [ITU-T Y.4203].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS	Business Service System
ICS	Identity Correlation Service
ID	Identity
IdM	Identity Management
IoT	Internet of Things
PKI	Public Key Infrastructure
SP	Service Provider
TLS	Transport Layer Security
URI	Uniform Resource Identifier

UTI Unique Transaction Identifier

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 document 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.

6 Overview

The Internet of things (IoT) as described in [ITU-T Y.4000] has become an important area in the telecommunication and information technology industry. In recent years, many new and novel services based on IoT technologies have emerged in the market and many of them have been deployed widely.

Many of these IoT systems already have IoT identity management. The interoperability between those systems is required, for example, to leverage existing mechanism for the open IoT identity correlation service (open IoT ICS) which maps the third party services and IoT devices to provide identity mapping service, etc.

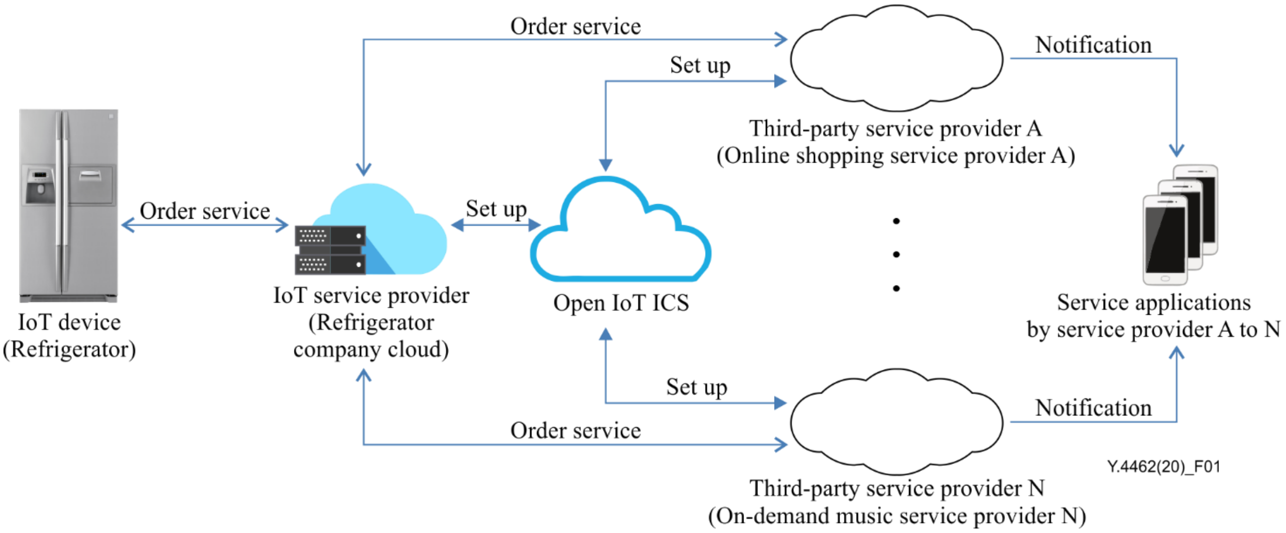


Figure 1 – Overview of open IoT ICS function

As shown in Figure 1, the user may hold several accounts in different third party service providers who can provide a variety of services, such as online shopping service, digital movie and music rental service and e-commerce. Also, the IoT device (for example, a smart refrigerator) has connected to its own IoT service provider which is allocated in the IoT device manufacturer's cloud. The IoT service provider offers cloud-based IoT device management functionalities, such as notification, instruction, firmware updating, etc. The IoT service provider which runs on the IoT device manufacturer's cloud needs to associate with third party service provider(s) to obtain a variety of services for the IoT device. For instance, the smart refrigerator could order eggs from an online market (third party service) automatically when it detects that the eggs stock is running low, or play on-demand songs using refrigerator's internal speaker from a music rental company (third party service).

Typically, an IoT device only has access to its own IoT service provider, but has limited access to other third party service providers. So, IoT devices can only acquire services from an IoT service provider, but may not be able to fully utilize a variety of third party services provided by other entities or enterprises. In order to let the IoT device access multiple third party services, the open IoT identity correlation service (open IoT ICS) provides an effective way to connect an IoT service provider and various third party service providers, then the IoT device can access the third party services via the relationship mapped by open IoT ICS. The open IoT ICS provides the identity mapping as a service for the IoT service provider(s) and third party service provider(s). Also, the open IoT ICS shall be a non-proprietary service and service provider independent and irrespective of the IoT device vendor or vertical industry.

The open IoT ICS shall map the third party services and the IoT device. In order to form relationship mapping, a unique transaction identifier (UTI) provided by third party service providers, an identifier of a certain service, and an identifier of an IoT device need to be filled in a mapping relationship. Once the mapping relationship is established, via the IoT service provider, the IoT device could be able to request multiple services from third party service providers, as shown in Figure 1. The open IoT ICS shall provide the identifier of a service and a UTI to the IoT device, and the IoT device could use this information to request third party services.

7 Requirements of open IoT identity correlation service

7.1 Requirements for establishing identity mapping

The open IoT ICS is required to collect the identifier of an IoT device, service and UTI. The open IoT ICS is required to provide the mapping function for the identifier that it has collected. Through the identity mapping function, the open IoT ICS establishes the mapping of the specific IoT device to single or multiple third party services that the user has selected.

7.2 Requirements for deleting identity mapping

The open IoT ICS is required to delete identity mapping in one or more of following situations:

- IoT device is unregistered from IoT service provider.
- The UTI is invalid.
- The third party service is invalid.
- The third party service no longer authorized by the user.

7.3 Requirements for querying identity mapping

The open IoT ICS is required to respond with the identity mapping information, including the identifier of the IoT device, the identifier of the service, and a UTI when an IoT device (via IoT service provider) or third party service provider query the identity mapping.

7.4 Security requirements

The open IoT ICS is required to provide authorization and access control functions for IoT service provider(s) and third party service provider(s) to prevent unauthorized access to the open IoT ICS.

To initialize a connection between an IoT service provider and any third party service provider(s) using the open IoT ICS, it is required that the entities are entered in a commercial contract or agreement governing this relationship prior to initialization. Moreover, user consent and agreement to using a third party service shall also be required before initializing this connection.

The open IoT ICS is required to provide an authorization mechanism for IoT service provider(s), and third party service provider(s) before establishing, deleting and querying identity mapping. The third party service provider is only authorized to access data that are strictly relevant to its own service provision and any IoT device is only authorized to access data relevant to services with which it has an initialized and unrevoked connection.

NOTE – This Recommendation will not define how to initialize connection among the open IoT ICS, IoT service provider(s), and third party service provider(s).

8 Functional architecture of open IoT ICS

The functional architecture of open IoT ICS is presented in Figure 2.

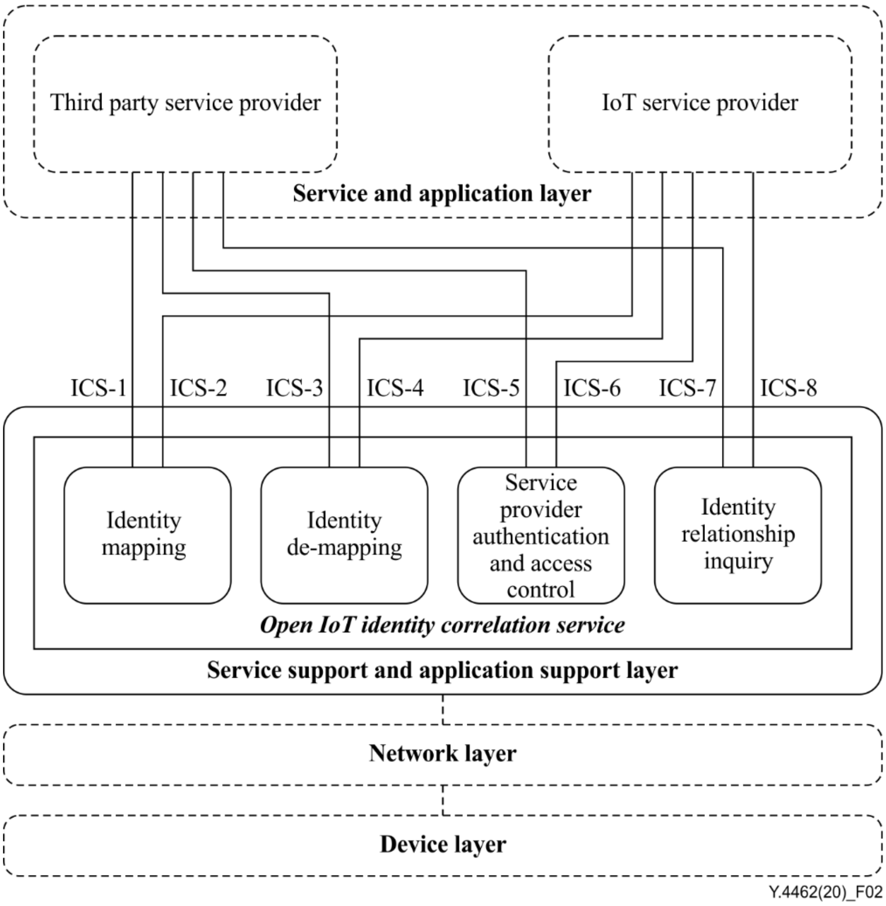

Third party service provider
IoT service provider
Service and application layer
ICS-1
ICS-2
ICS-3
ICS-4
ICS-5
ICS-6
ICS-7
ICS-8
Identity mapping
Identity de-mapping
Service provider authentication and access control
Identity relationship inquiry
Open IoT identity correlation service
Service support and application support layer
Network layer
Device layer
Y.4462(20)_F02

Figure 2 – Functional architecture of open IoT ICS

The open IoT ICS has four functional entities: identity mapping, identity de-mapping, identity relationship inquiry and finally service provider authentication and access control functions.

A brief description of these four functional entities of open IoT ICS is provided below:

– **Identity mapping**: This function is used to create a mapping table between multiple identities of IoT related entities (UTI, IoT device and third party service). The identity mapping table contains three elements: device ID, service URI and unique transaction identifier (UTI). The identity mapping table will be stored in the open IoT ICS.

– **Identity de-mapping**: This function is used to delete the mapping between multiple identities of IoT related entities (UTI, IoT device and third party service). Both IoT service provider and third party service providers can request to delete the identity mapping table through this function.

– **Identity relationship inquiry**: This function is used to query the identity mapping of IoT related entities (UTI, IoT device and third party services) and check on the existence of the identity mapping before the interaction between the IoT device and third party service(s).

– **Service provider authentication and access control**: This function is used to manage the access control and provide an authentication service to IoT service provider and third party services.

NOTE – The IoT service provider will provide identity management (IdM) for the IoT device. The IdM is outside of the scope in this Recommendation.

9 Reference points of open IoT ICS

A description of reference points of open IoT ICS, as shown in Figure 2, is provided below:

- ICS-1: Reference point ICS-1 supports communication between a third party service provider and open IoT ICS. It enables the open IoT ICS to interact with the third party service provider in order to provide the identity mapping function.
- ICS-2: Reference point ICS-2 supports communication between the IoT service provider and open IoT ICS. It enables the open IoT ICS to interact with the IoT service provider in order to provide the identity mapping function.
- ICS-3: Reference point ICS-3 supports communication between a third party service provider and open IoT ICS. It enables the open IoT ICS to interact with the third party service provider in order to provide the identity de-mapping function.
- ICS-4: Reference point ICS-4 supports communication between the IoT service provider and open IoT ICS. It enables the open IoT ICS to interact with the IoT service provider in order to provide the identity de-mapping function.
- ICS-5: Reference point ICS-5 supports communication between a third party service provider and open IoT ICS. It enables the open IoT ICS to interact with the third party service provider in order to provide security functions as needed, such as authentication and access control.
- ICS-6: Reference point ICS-6 supports communication between an IoT service provider and open IoT ICS. It enables the open IoT ICS to interact with the IoT service provider in order to provide security functions as needed, such as authentication and access control.
- ICS-7: Reference point ICS-7 supports communication between a third party service provider and open IoT ICS. It enables the open IoT ICS to interact with the third party service provider in order to provide the identity relationship inquiry function.
- ICS-8: Reference point ICS-8 supports communication between an IoT service provider and open IoT ICS. It enables the open IoT ICS to interact with the IoT service provider in order to provide the identity relationship inquiry function.

10 Basic capabilities and common procedures of open IoT ICS

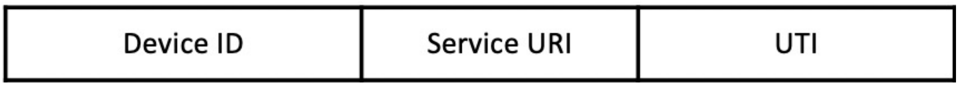
10.1 Identity mapping

The identity mapping function is used to map the relationship between multiple identities of IoT related entities.

The open IoT ICS establishes a service relationship among the identities of IoT related entities - between devices, services and transactions. In this case, a mapping table with a flat data model [b-FG-DPM TS D2.3] should be established, which consists of a two-dimensional array of data elements where all elements of a given row are related to one another and all elements of a given column are similar objects. For example, a single row of the mapping table consists of the device ID, service URI and UTI which are related to each other, as shown in Table 1.

Table 1 shows the elements involved in the identity mapping function.

Table 1 – Identity mapping table



Device ID	Service URI	UTI

The description of each element in Table 1 is as follows:

- Device ID: For each IoT device which registered in the IoT service provider. The IoT service provider shall define and assign a unique, anonymous, and revocable identifier (Device ID [ITU-T G.9961]) for the individual IoT device. The revocation function that solely performed by IoT service provider.

NOTE 1 – This Recommendation will not define the format of device ID.

- Service URI: A URI provided by a third party service provider to indicate a specific service that the user selects in their third party service application [ITU-T Q.1743].

NOTE 2 – This Recommendation will not define the format of service URI.

- UTI: A unique transaction identifier (UTI) is an identifier to identify a user transaction that is generated by the third party service provider upon the authorization by the user. UTI is defined in the clause 3.2.2. The relationship between the specific IoT device and a third party service provider is identified with this unique transaction identifier. Upon establishing a mapping, both the IoT device and user (via the service provider) should be able to revoke an Identifier to signal that the relationship is terminated and transactions are no longer authorized. This UTI shall be administered by the third party service provider who generated it until this UTI has been revoked. A framework describing how to create an identifier that meets these requirements is described in [IETF RFC 4122].

To initiate the process of establishing an identity mapping, the user of a third party service shall execute the following operations:

- Step 1.1: The user shall login in the service application which is a service enabler deployed by third party service provider [ITU-T Q.1743].
- Step 1.2: The user collects the IoT device serial number using the service application from the IoT device casing that manufacturer physically printed.
- Step 1.3: The user selects the service offered by the third party service provider that plans to have the interact with the IoT device.
- Step 1.4: The service application informs the third party service provider that it is ready to initiate the identity mapping process with open IoT ICS, and send the IoT device serial number and user selected service to the third party service provider.
- Step 1.5: The third party service provider can start the identity mapping process with open IoT ICS.

By accomplishing these steps, the third party service provider gains the following identities:

- Service URI which is generated by the third party service provider based on the service that the user selects in step 1.3.
- UTI which is generated by the third party service provider based on the login account in step 1.1.
- IoT device serial number that the user scanned or typed in step 1.2.

The process of establishing a mapping between the device ID, the service URI and the UTI is shown in Figure 3 and described below:

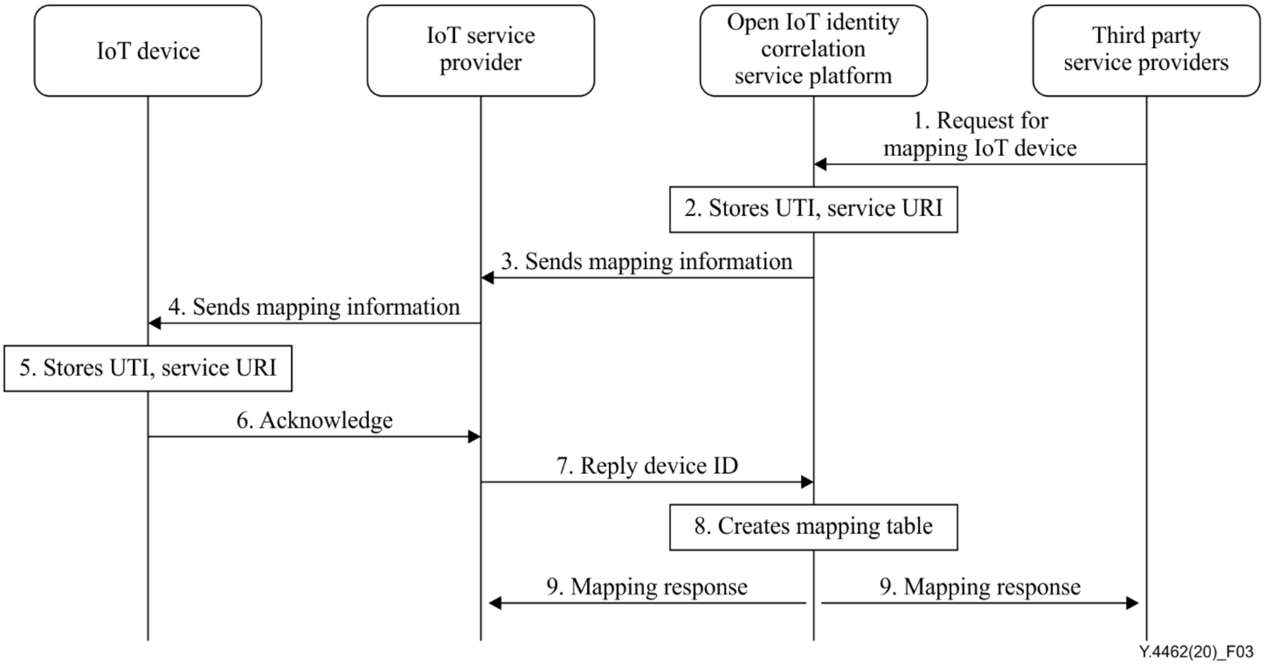

IoT device
IoT service provider
Open IoT identity correlation service platform
Third party service providers
1. Request for mapping IoT device
2. Stores UTI, service URI
3. Sends mapping information
4. Sends mapping information
5. Stores UTI, service URI
6. Acknowledge
7. Reply device ID
8. Creates mapping table
9. Mapping response
9. Mapping response
Y.4462(20)_F03

Figure 3 – Procedures of establishing an identity mapping

Step 1: Third party service provider sends a mapping IoT device request to the open IoT ICS through the reference point ICS-1. The request includes information such as the service URI, UTI, and IoT device serial number.

Step 2: Upon receiving the request, the open IoT ICS stores the service URI and UTI as an initial identity mapping table, the full table will be created in step 8.

Step 3: Open IoT ICS sends the mapping information to the IoT service provider through the reference point ICS-2, including service URI, UTI and IoT device serial number.

Step 4: The IoT service provider finds the IoT device that corresponds to IoT device serial number and then sends the mapping information to the IoT device, including service URI and UTI.

Step 5: The IoT device stores the service URI and UTI in the internal storage.

Step 6: The IoT device acknowledges the receipt of service URI and UTI to IoT service provider.

Step 7: The IoT service provider sends the IoT device ID to the open IoT ICS.

Step 8: Open IoT ICS creates an identity mapping table with device ID, service URI and UTI.

Step 9: Open IoT ICS sends a response to both third party service provider and IoT service provider to indicate the result of identity mapping.

10.2 Identity de-mapping

Identity de-mapping function is to remove the relationship between multiple identities of IoT related entities.

Identity de-mapping can be requested by the third party service provider or IoT service provider through reference point ICS-3 or ICS-4 if one of the following conditions is met:

- IoT device is unregistered from IoT service provider;
- the UTI is invalid;
- third party service is invalid;
- third party service no longer authorized by the user.

If the IoT service provider or third party service provider needs to terminate the mapping between IoT device and third party service, the IoT service provider or third party service provider shall send a request to open IoT ICS to delete the identity mapping, then the open IoT ICS responds to the related entities that the identity mapping table has been successfully deleted.

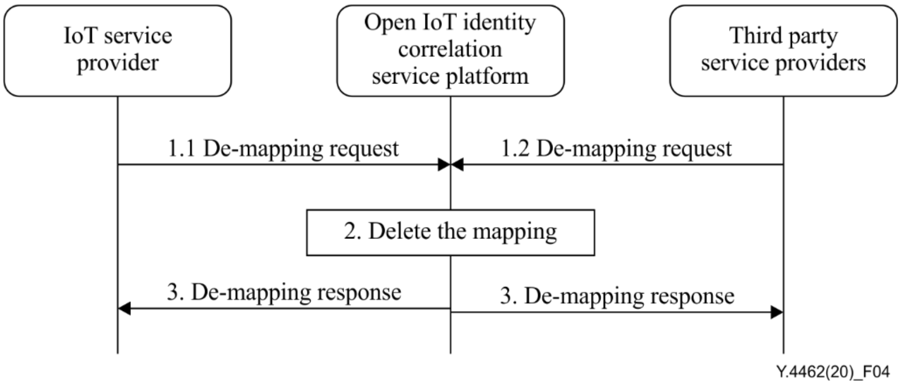


Figure 4 – Procedures of identity de-mapping

Step 1 (1.1 and 1.2) represents the de-mapping workflow. There are 2 options:

- Case 1 (shown as 1.1 in Figure 4) represents the de-mapping request initiated from the IoT service provider through the reference point ICS-4.
- Case 2 (shown as 1.2 in Figure 4) represents the de-mapping request initiated from the third party service provider through the reference point ICS-3.

Step 2 upon receiving the request, the open IoT ICS is responsible for processing the request locally, such as delete the mapping.

Step 3 open IoT ICS returns a response to indicate the result of deletion of mapping to both IoT service provider and third party service provider.

10.3 Identity relationship inquiry

The identity relationship inquiry function, as shown in Figure 5, is used to query the relationship of identities of IoT related entities and check the existence of the identity mapping before the interaction between the IoT device and a third party service.

There are two cases of inquiry, Case 1 is shown as Figure 5 and Case 2 is shown as Figure 6.

Case 1: The IoT device requests for query mapping information by sending its own device ID. In this case, the IoT device has access to query the service URI and UTI corresponding to that device ID which is located in a specific row of the mapping table.

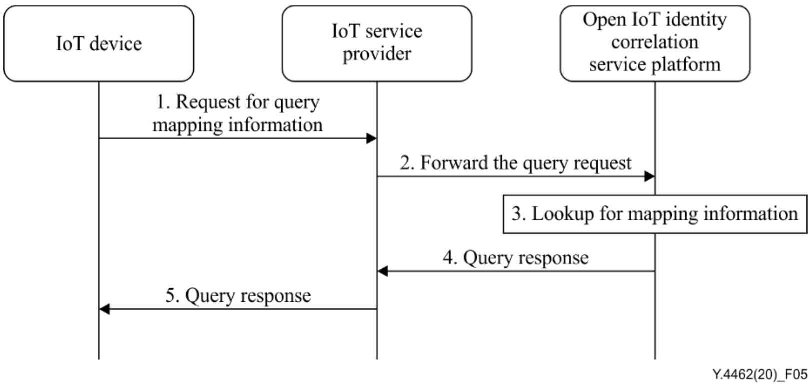

IoT device
IoT service provider
Open IoT identity correlation service platform
1. Request for query mapping information
2. Forward the query request
3. Lookup for mapping information
4. Query response
5. Query response
Y.4462(20)_F05

Figure 5 – Procedures of identity relationship inquiry (Case 1)

Step 1 represents the IoT device's request to query identity mapping information with its own device ID.

Step 2 the IoT service provider forwards the request to open IoT ICS through reference point ICS-6.

Step 3 upon receiving the request, the open IoT ICS is responsible for looking-up the mapping table to retrieve the service URI and UTI correspond to that device ID.

Step 4 if the mapping table exists, the open IoT ICS returns a response with the service URI and UTI which correspond to that device ID to the IoT service provider. Otherwise, returns an error message.

Step 5 the IoT service provider forwards the response to the IoT device.

Case 2: The third party service provider requests query mapping information by sending both service URI and UTI. In this case, only when the combination of service URI and UTI exist in the same row of the mapping table, will the open IoT ICS respond to the query with the device ID. Otherwise, the open IoT ICS will respond with an error message.

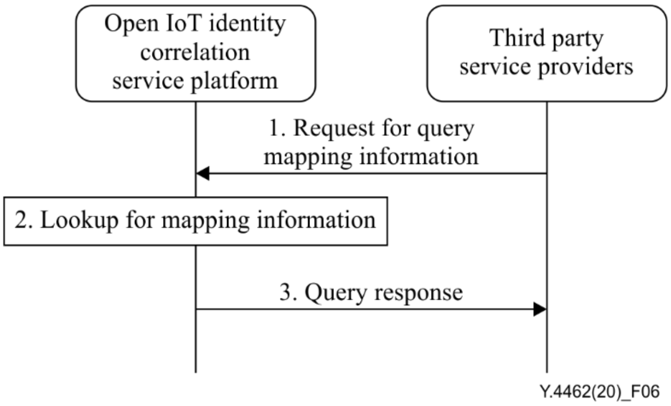

Open IoT identity correlation service platform
Third party service providers
1. Request for query mapping information
2. Lookup for mapping information
3. Query response
Y.4462(20)_F06

Figure 6 – Procedures of identity relationship inquiry (Case 2)

Step 1 represents one third party service provider request to query identity mapping information with both service URI and UTI.

Step 2 upon receiving the request, the open IoT ICS is responsible for looking-up the mapping table using service URI and UTI. Only if both of the service URI and UTI are located in one single row in the mapping table, the open IoT ICS shall then retrieve the device ID corresponding to the combination of service URI and UTI.

Step 3 if the given row from the mapping table exists, the open IoT ICS returns a response with the device ID to the third party service provider. Otherwise, the open IoT ICS will respond with an error message.

10.4 Service provider authentication and access control

To set up a secure connection with IoT service provider(s) and third party service provider(s), the open IoT ICS should provide authorization and access control functions. The certificates of [b-ITU-T X.509] and public key infrastructure (PKI) is recommended for the open IoT ICS to provide these authorization and access control functions. The authorization and access control flow are shown in Figure 7 and described below:

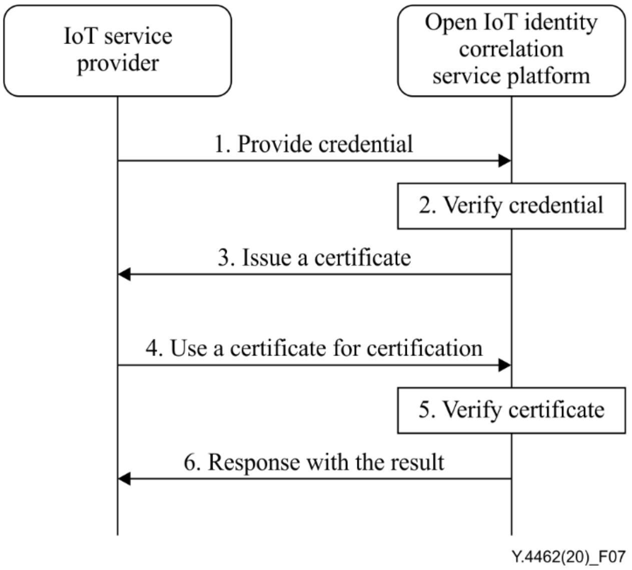


Figure 7 – Procedure of authorization and access control flow

Step 1 represents the IoT service provider's provision of credentials to open IoT ICS through reference point ICS-5.

Step 2 represents open IoT ICS verifying the validity of the credentials.

Step 3 represents the open IoT ICS issuing of certificates to the IoT service providers.

Steps 4 to 6 represents the process of certification of IoT service providers.

11 Security considerations

11.1 Discovery mechanisms in identity information exchange

As mentioned in clause 10.3 which describes the identity relationship inquiry, for security considerations, only the IoT device already existing in the mapping list has permission to initiate a query operation. Based on that requirement, the whole system needs a mechanism to publish identity information, obtain the mapping list and acquire the needed information. The framework for discovering cybersecurity information and the mechanism presented in [ITU-T X.1570] is recommended.

The stages of discovery in the framework of identifying and locating the source of cybersecurity information is shown in Figure 8.

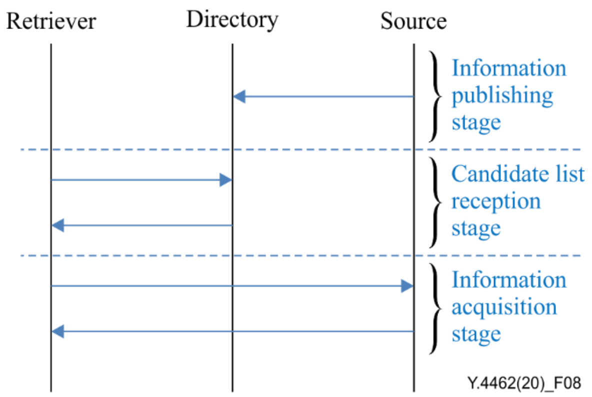

Retriever
Directory
Source
Information publishing stage
Candidate list reception stage
Information acquisition stage
Y.4462(20)_F08

Figure 8 – Stages of discovery in the framework of identifying and locating the source of cybersecurity information

A unique identifier is needed to identify identity information. Any globally unique identifier used for global cybersecurity information exchange shall have the following characteristics:

- Simplicity, usability, flexibility, extensibility, scalability, and deployability.
- Distributed management of diverse identifier schemes.
- Long-term reliability of identifier registrars, and the availability of high-performance tools for discovering information associated with any given identifier.

According to the description from clause 8.8 (Security and privacy protection requirements) in [ITU-T Y.4100], in order to meet these requirements, the following characteristics of device identity are recommended:

- Tamper-resistant, anti-counterfeiting, unpredictable, unique.
- Including vendor and product model information.

Other identity schemes which comply with these requirements could be implemented with arbitrary mechanisms.

11.2 Communication security

For security consideration, the services provided by open IoT ICS such as identity mapping, de-mapping, and access control need communication security capabilities. The implementation of transport layer security (TLS) Version 1.3, as specified in [IETF RFC 8446], for securing communication between open IoT ICS and an IoT service provider/third party service provider is recommended.

TLS provides a secure communication path between two entities. It allows open IoT ICS to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery and mutual authentication on both parties.

These capabilities fulfil the IoT common requirements on security and privacy protection specified in [ITU-T Y.4100].

Appendix I

Use cases

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

This appendix provides some use cases to illustrate the concept of the open IoT identity correlation service.

I.1 Use case 1: Smart refrigerator

A smart refrigerator can monitor the food left in it. When it finds that there is not enough food, for example, not enough milk in the refrigerator, it can notify the user's e-commerce mobile application, to remind the user to buy milk from the user's e-commerce mobile application.

When the refrigerator vendor's device management platform detects that the light bulb of the refrigerator is broken, the refrigerator vendor's device management platform can send a notification message to the e-commerce server to remind the user to buy a new light bulb.

Figure I.1 shows a refrigerator sending notification to a third party e-commerce service provider.

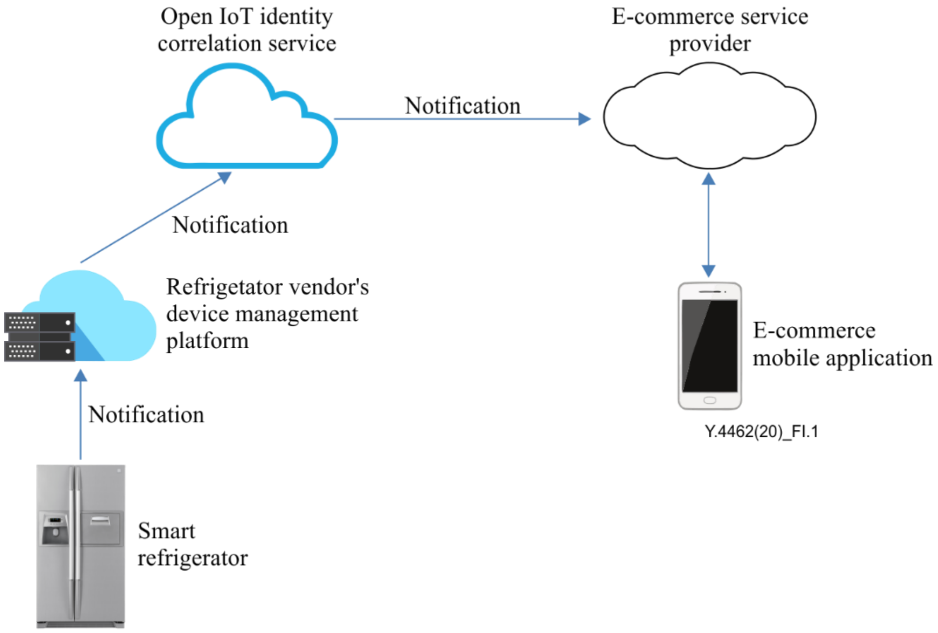

Open IoT identity correlation service
E-commerce service provider
Notification
Notification
Refrigetator vendor's device management platform
E-commerce mobile application
Notification
Smart refrigerator
Y.4462(20)_FI.1

Figure I.1 – Smart refrigerator sending notification to a third party e-commerce service provider

In this use case, there is a need to provide the mapping between the refrigerator's identifier and user's e-commerce UTI and to open this capability to other entity.

I.2 Use case 2: Smart lock

In the case of a smart house, one smart lock can interact with other smart things such as lights and an air-conditioning system. Once the smart lock is unlocked, it can trigger the switch of the smart light and can set the temperature on the air-conditioning system.

In the scenario where there is a third party smart home service provider which had connected to multiple smart things such as light bulbs or an air-conditioning system. Once a new smart lock is installed, the user of a third party service provider can bind this lock to the smart home service provider via open IoT ICS and establish the connection with other smart things in the house.

Figure I.2 shows the mapping of a new lock to a third party smart home service.

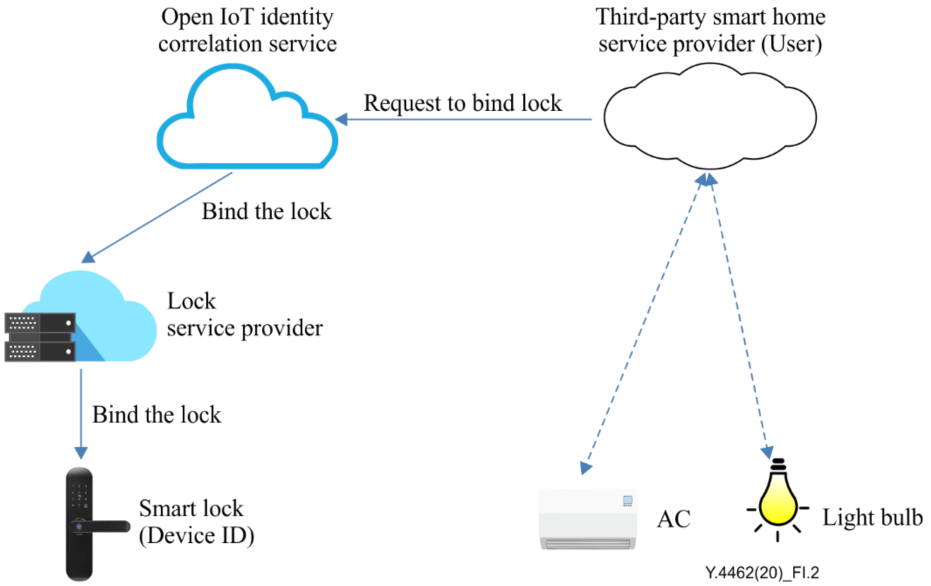


Figure I.2 – Mapping a new lock to a third party smart home service

I.3 Use case 3: Device based service charge sharing

In this use case, one smart loudspeaker can use third party music services. Based on the business agreement, the smart loudspeaker box's software vendor may charge the music provider according to how much music is consumed by the smart loudspeaker. The rational for this business model is that the software vendor provides the integration capability with the third party music service and hence will increase the consumption of the third party's music service. The revenue is shared with the hardware vendor of the smart loudspeaker.

In this use case, the identity service platform is used to map/bind the smart loudspeaker's device identifier and the URI from the music service provider.

Figure I.3 shows mapping of a smart speaker device ID with a third party music service URI.

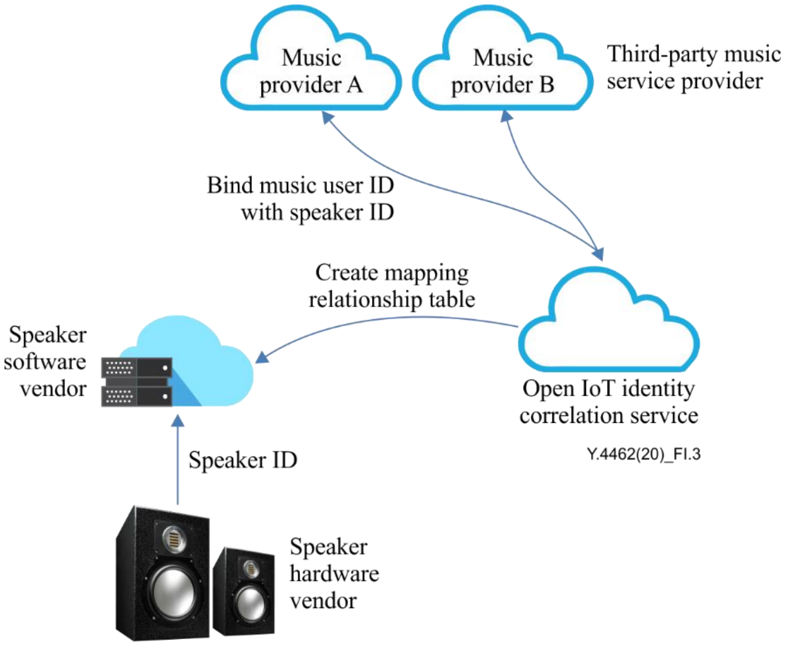

Music provider A
Music provider B
Third-party music service provider
Bind music user ID with speaker ID
Create mapping relationship table
Speaker software vendor
Open IoT identity correlation service
Y.4462(20)_FI.3
Speaker ID
Speaker hardware vendor

Figure I.3 – Mapping a smart speaker device ID with a third party music service URI

I.4 Use case 4: Promoting data package sharing between different services

This use case uses a simple example to illustrate how the open IoT ICS promotes the users sharing data communication packages among a family's IoT devices. As shown in Figure I.4, a family (user) has three IoT devices (a watch, a bulb and a car), and the family subscribes to a data communication package which binds those three IoT devices. In this data communication package, data communication traffic is free if those three IoT devices access indicated services respectively (such as the watch for the message service, the bulb for the monitoring service and the car for the navigation service).

Each month, the network operator should combine the bills for data communication traffic for the family's IoT devices with that from the three services. Each of the family's IoT devices has a special identity in the service (named service-id), and in the communication network it also has another identity (named network-id, for example an E.164/E.212 number or a special IP address). The family (user) has a user identity (named user-id) in the network's business service system (BSS). Typically, the BSS should coordinate with each of the services one by one to exchange identity-related information, which leads to high costs and has a lack of scalability and operational capabilities.

The open IoT ICS provides a uniform open identity mapping service (see Figure I.4) for the BSS and those services. Those services and the BSS can forward dynamically (or periodically) their identity-related information to the identity correlation service, and they can also get dynamically (or periodically) relevant information from the identity correlation service. Through the open IoT ICS, the BSS does not coordinate with each of those services one by one to exchange identity-related information, which can cut the costs and improve the scalability and operational capabilities.

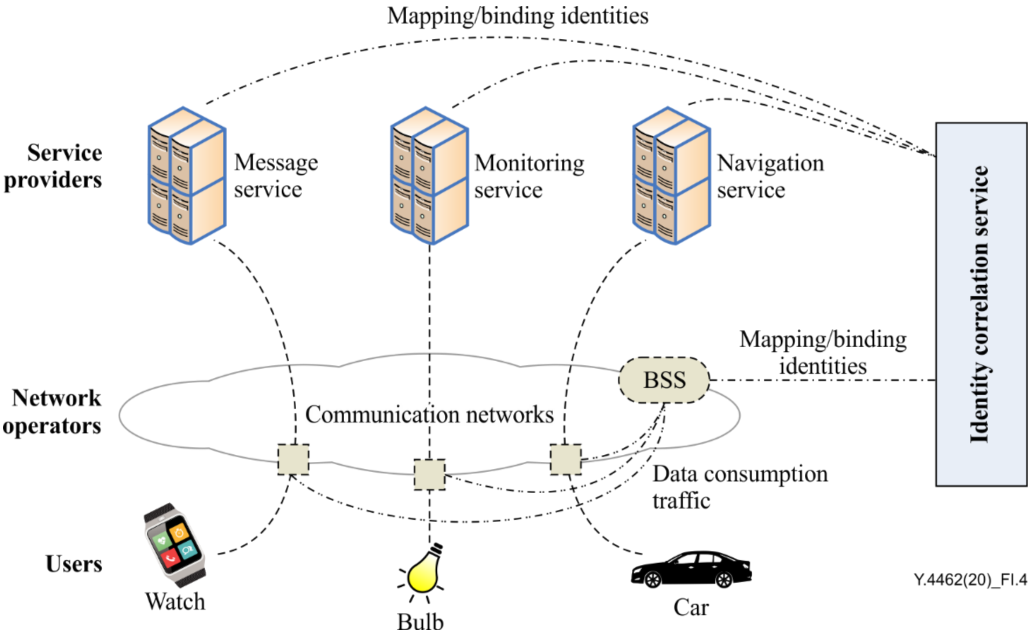


Figure I.4 – Promoting data package sharing between different services

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

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

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011), *Information technology – Security framework for ubiquitous sensor networks.*

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

[b-ITU-T Y.4050] Recommendation ITU-T Y.4050/Y.2069 (2012), *Terms and definitions for the Internet of Things.*

[b-ITU-T Y.4101] Recommendation ITU-T Y.4101/Y.2067 (2017), *Common requirements and capabilities of the gateway for Internet of things applications.*

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

[b-ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things.*

[b-ITU-T Y.4800] Recommendation ITU-T Y.4800/F.747.5 (2014), *Requirements and functional architecture of an automatic location identification system for ubiquitous sensor network applications and services.*

[b-ITU-T Y.4801] Recommendation ITU-T Y.4801/F.748.1 (2014), *Requirements and common characteristics of the IoT identifier for the IoT service*.

[b-ITU-T Y.4802] Recommendation ITU-T Y.4802/H.642.2 (2012), *Multimedia information access triggered by tag-based identification – Registration procedures for identifiers.*

[b-ITU-T Y.4803] Recommendation ITU-T Y.4803/H.642.3 (2012), *Information technology – Automatic identification and data capture technique – Identifier resolution protocol for multimedia information access triggered by tag-based identification.*

[b-ITU-T Y.4804] Recommendation ITU-T Y.4804/H.642.1 (2012), *Multimedia information access triggered by tag-based identification – Identification scheme.*

[b-FG-DPM TS D2.3] ITU-T Technical Report D2.3*, Web based data model for IoT and smart city.*

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts.*

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