International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4476
(02/2021)

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

OID-based resolution framework for transactions of a distributed ledger assigned to IoT resources

Recommendation ITU-T Y.4476

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.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–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.4476

OID-based resolution framework for transactions of a distributed ledger assigned to IoT resources

Summary

An object identifier (OID) is an identifier to name an object in a hierarchically assigned namespace. In the Internet of things (IoT), thousands of IoT resources will be intricately provided as fusion types of various services. For the thousands of IoT resources, object identifiers (OIDs) can provide a resolution framework with unlimited scalability. On the other hand, IoT resources need to secure their data, so the distributed ledger technology (DLT) can guarantee its integrity. In consequence, the convergence of DLT and OIDs provides a good solution for identifying secured data of IoT resources. Recommendation ITU-T Y.4476 therefore specifies a resolution framework for the transactions of a distributed ledger assigned to IoT resources. Recommendation ITU-T Y.4476 also describes the concepts, functional requirements, architecture and procedures of an OID-based resolution framework by using DLT.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4476	2021-02-06	20	11.1002/1000/14578

Keywords

Distributed ledger technology (DLT), Internet of things (IoT), OID, resolution framework.

[*] 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

1 Scope ... 1

2 References ... 1

3 Definitions ... 1

3.1 Terms defined elsewhere ... 1

3.2 Terms defined in this Recommendation ... 2

4 Abbreviations and acronyms ... 2

5 Conventions ... 2

6 Overview of a resolution framework for transaction assigned to IoT resources ... 2

7 Functional requirements for resolution framework using DLT ... 3

7.1 Support for interoperability with DLT ... 3

7.2 Support for identification of data handled by DLT ... 3

7.3 Support for data integrity of IoT resources ... 3

7.4 Support for data management of IoT resources ... 3

8 Architecture for OID-based resolution framework ... 4

8.1 General architecture ... 4

8.2 Functional entities ... 4

8.3 OID assignment ... 5

9 Procedures of the OID-based resolution framework ... 5

9.1 Registration ... 5

9.2 Resolution procedures ... 7

10 Security considerations ... 8

Bibliography ... 9

Recommendation ITU-T Y.4476

OID-based resolution framework for transactions of a distributed ledger assigned to IoT resources

1 Scope

The scope of this Recommendation includes:

- overview of resolution framework for transactions assigned to Internet of things (IoT) resources;
- functional requirements for the resolution framework;
- architecture and procedures of the resolution framework.

2 References

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

[ITU-T X.660]	Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree.*
[ITU-T X.672]	Recommendation ITU-T X.672 (2010) | ISO/IEC 29168-1:2011, *Information technology – Open systems interconnection – Object identifier resolution system (ORS).*
[ITU-T Y.4000]	Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

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

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

3.1.3 OID resolution process [ITU-T X.672]: Process which provides information associated with an OID.

3.1.4 OID resolution system (ORS) [ITU-T X.672]: Implementation of the OID resolution process in accordance with [ITU-T X.672].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DICOM	Digital Imaging and Communications in Medicine
DLT	Distributed Ledger Technology
ID	Identifier
IoT	Internet of Things
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
OID	Object Identifier
ORS	Object identifier Resolution System
RA	Registration Authority
RR	Resource Registry
RS-DLT	Resolution Server based on Distributed Ledger Technology
SNMP	Simple Network Management Protocol
SP	Service Provider
URI	Uniform Resource Identifier

5 Conventions

None.

6 Overview of a resolution framework for transaction assigned to IoT resources

An object identifier (OID) identifies a node in a hierarchically-assigned namespace, formally defined using [ITU-T X.660]. OIDs have been used for various implementations. For example, OIDs serve to name almost every object type in ITU-T X.509 certificates in computer security. They are used within ITU-T X.500 directory schemas and protocols, to uniquely name each attribute type and object class, and other elements of schema. Within lightweight directory access protocol (LDAP) schemas, each object class and each attribute type respectively have their unique OIDs. In communication networking, an OID, in the context of simple network management protocol (SNMP), consists of the object identifier for an object in a management information base (MIB). Health Level Seven International7 (HL7), digital imaging and communications in medicine (DICOM) and other healthcare related information interchange standards use OIDs for globally unique identifiers for both individual information objects as well as references to code systems and data element dictionaries.

In the Internet of things (IoT) [ITU-T Y.4000], thousands of IoT services based on heterogeneous IoT resources are provided. Each of the resources needs to be identified in IoT services. OIDs provide a solution to meet the requirements with an unlimited number of identifiers for the thousands of IoT resources.

Data integrity is an important security requirement. If the IoT resources provide private information (e.g., resource ID, sensing data, etc.), the data should be secured in order that only the authorized third parties can access the IoT data. The distributed ledger technology (DLT) with its inherent security features can provide a solution for data integrity of IoT resources.

Consequently, convergence of OIDs and DLT can be a good solution for data management of IoT resources.

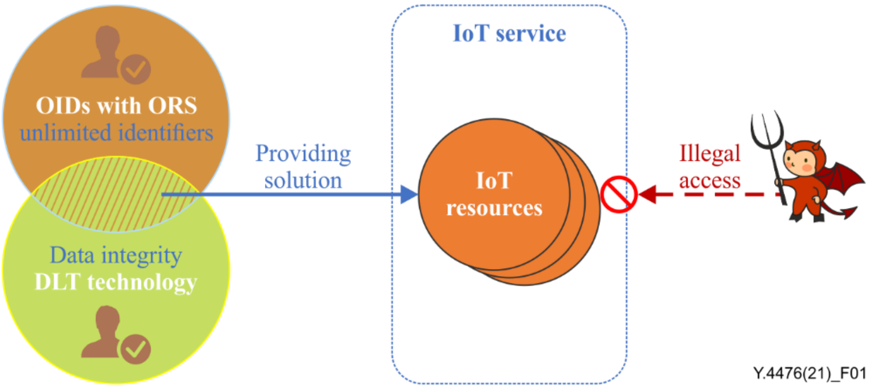

Figure 1 – Overview of OID-based resolution for IoT services

Figure 1 shows an overview of OID-based resolution for IoT services using DLT. OID is utilized to identify every IoT resource with the assistance of the object identifier resolution system (ORS). DLT secures information of IoT resources.

7 Functional requirements for resolution framework using DLT

7.1 Support for interoperability with DLT

The resolution framework handles data obtained from IoT resources and DLT in the resolution framework secures the integrity of the data. Therefore, resolution servers of the framework are recommended to support interoperability with DLT over the procedures.

7.2 Support for identification of data handled by DLT

The data of IoT resources are handled by DLT during the procedures of the resolution framework. The resolution framework is required to support identification for the data handled by DLT. The identification includes creation, assignment, and resolution of identifiers for the data handled by DLT.

7.3 Support for data integrity of IoT resources

Data, obtained from the IoT resources, is required to be handled in order not to damage the integrity of the data until the data has been processed. The resolution framework is recommended to support the integrity of the data by using DLT.

7.4 Support for data management of IoT resources

The resolution framework is required to support capabilities of resolution servers to manage and access data which has been secured in DLT. The data management includes obtaining data from IoT resources, storing, deleting, updating data and providing data to users.

8 Architecture for OID-based resolution framework

8.1 General architecture

Figure 2 presents a general architecture of an OID-based resolution framework for the transaction of distributed ledgers assigned to IoT resources. In Figure 2, there are three types of functional entities: object identifier resolution server (ORS), resolution server based on DLT (RS-DLT), and resource registries (RRs). The resource registries are operated by service providers. The key components of this framework are ORS and RS-DLT. The ORS is interconnected with the RS-DLTs, and the RS-DLTs are interconnected with resource registries of service providers to manage the information of IoT resources. The RS-DLTs are secured by DLT. Each resource registry manages the information of specific information of IoT resources provided by service providers.

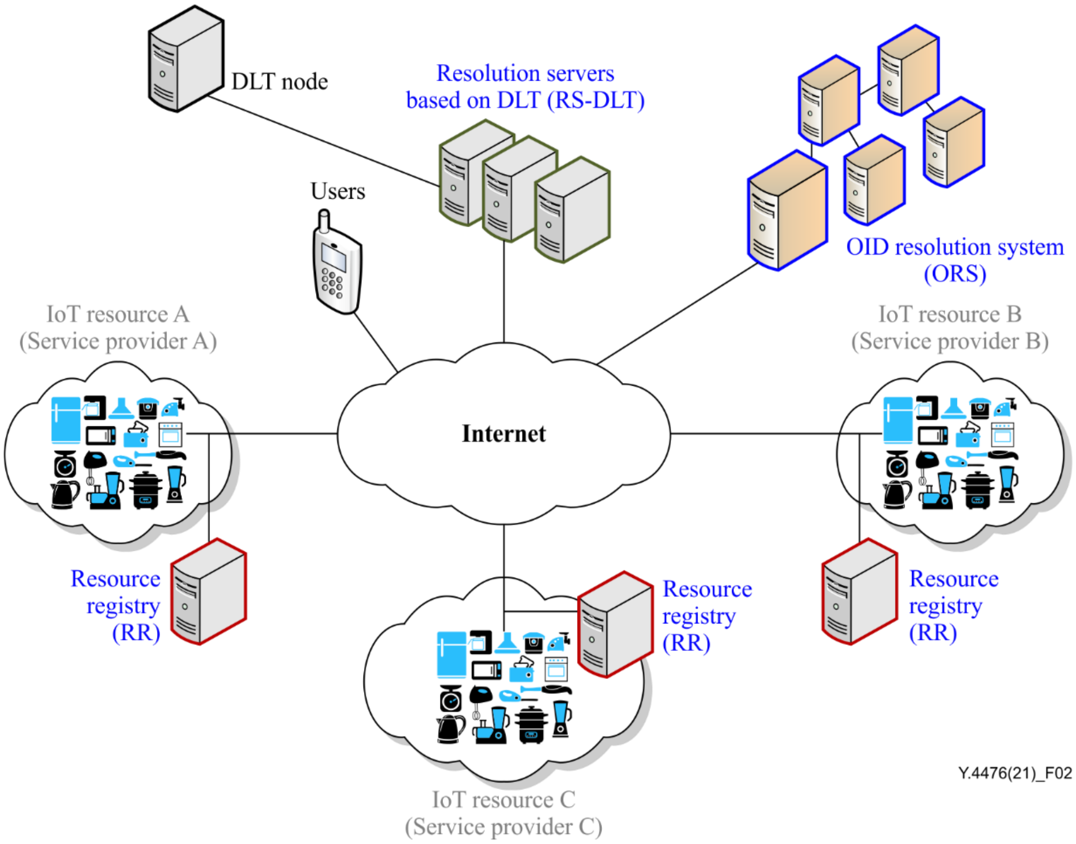
DLT node
Resolution servers based on DLT (RS-DLT)
Users
OID resolution system (ORS)
IoT resource A (Service provider A)
IoT resource B (Service provider B)
Internet
Resource registry (RR)
Resource registry (RR)
Resource registry (RR)
Y.4476(21)_F02
IoT resource C (Service provider C)

Figure 2 – General architecture of the OID-based resolution framework

8.2 Functional entities

8.2.1 Resolution server based on DLT

A resolution server based on DLT (RS-DLT) provides functions of information management for IoT resources and resource registries. RS-DLTs are secured by DLT. The RS-DLT has a database including OIDs and transaction ID for the look up of corresponding IDs of IoT resources and addresses of resource registries. An OID in the RS-DLT is also used as a parameter to identify IoT resources. With related requests, the RS-DLT can return the corresponding ID of IoT resources and an address of a resource registry.

The IoT resources and addresses of resource registries need to be managed as security information, so the database of RS-DLT is secured by DLT. When registration for a new IoT resource is requested from a resource registry, the RS-DLT creates a transaction including the information of IoT resources. The transaction is secured in blocks of DLT. The RS-DLT manages the ID of the transaction with its corresponding OID. When the RS-DLT receives a request for searching of the

OID, it returns the corresponding transaction ID with information of the IoT resource and resource registry.

8.2.2 Object identifier resolution system

An object identifier resolution system (ORS) [ITU-T X.672] plays the role of a centralized management and identification server for the RS-DLT. The ORS includes databases of OIDs and uniform resource identifiers (URIs) (based on UINF [ITU-T X.672]) of the RS-DLTs. OIDs are utilized as parameters to identify RS-DLTs. When a user sends an OID to the ORS, the ORS returns the URI of a corresponding RS-DLT.

8.2.3 Resource registry

A resource registry (RR) is a local resolution system to support IoT resources by a service provider (SP). A local SP has and manages one RR, and the RR manages a database of IDs of IoT resources and corresponding information. This database is used for the RR to search an ID for IoT resources, which have been provided by its SP. The ID schemes can be customized by SPs.

8.3 OID assignment

OIDs are predefined and have to be globally unique, and they are officially generated by registration authorities (RAs) and respectively assigned to all RS-DLTs. Each IoT resource can be identified by assigned OIDs. OIDs are used as well-known parameters in public-like port numbers of the transmission control protocol/Internet protocol (TCP/IP).

9 Procedures of the OID-based resolution framework

9.1 Registration

IoT resources are registered to RRs for management, furthermore, IoT resources are identified by OIDs. The OID-based resolution framework provides a two-level registration approach, including the first level registration for identification of IoT resources from service providers to RS-DLT and the second level registration for OID mapping from RS-DLT to ORS, as shown in Figure 3. In Figure 3, the OIDs (2.999.1.1, 2.999.1.2, 2.999.2.1) are shown as examples.

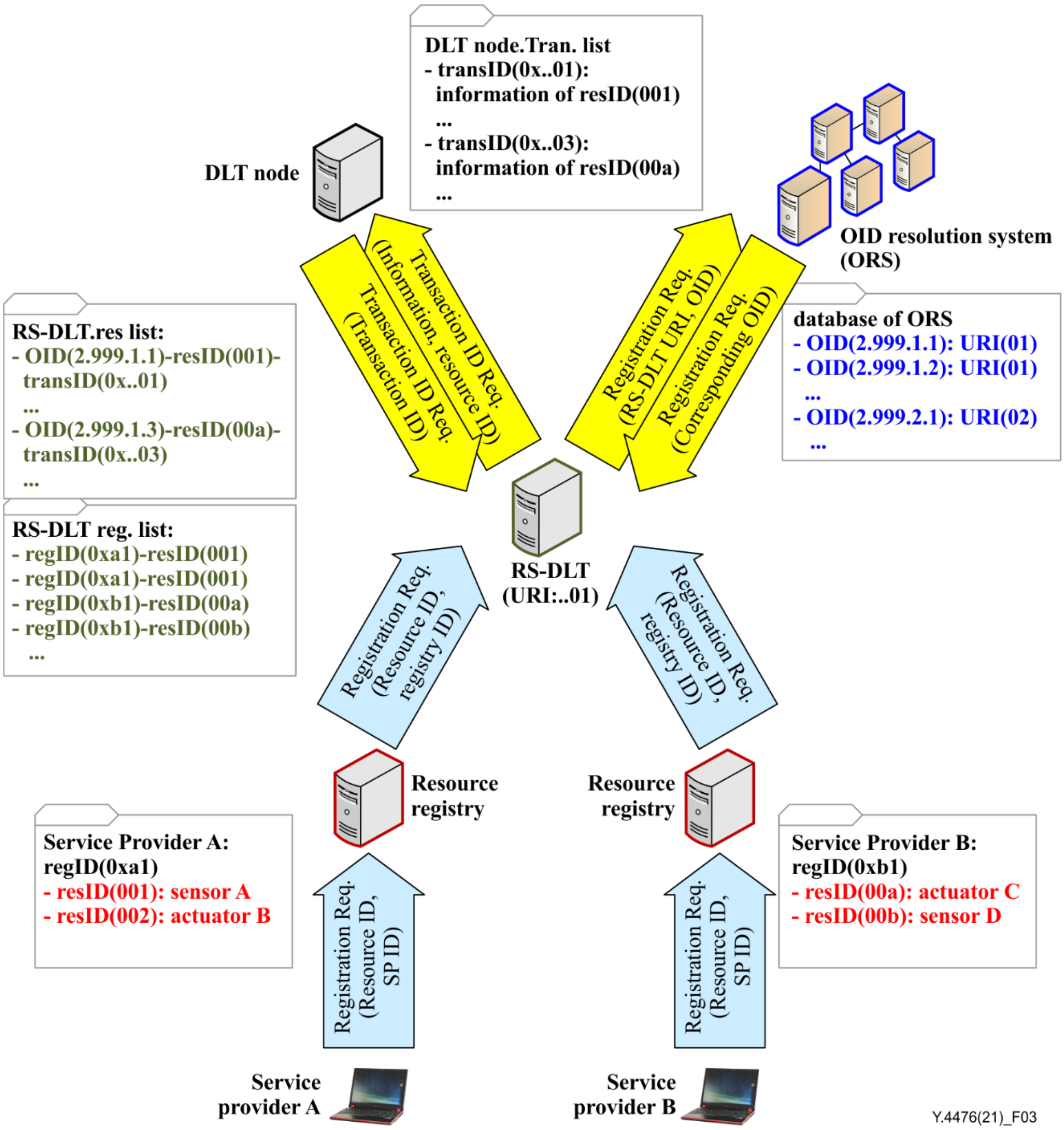

Figure 3 – OID registration procedures

9.1.1 Registration to RS-DLT

The first step for registration is allowing IoT resources to be registered by the SPs. The next step is when a new ID corresponding to an IoT resource is created, and the related pairing information (resource ID and resource information) is stored in the RR and managed by the RR. The resource IDs can be created by different generation mechanisms with different ID formats. The RS-DLT can provide functions for managing and identifying an RR as it can utilize related pairing information, such as an RR ID with its resource ID.

All the RRs are connected to the RS-DLTs. The RRs send their own IDs and resource IDs to the RS-DLTs. Then the RS-DLTs manage a database including related pairing information (i.e., RR ID and resource ID). In addition, the RS-DLTs manage another list including related pairing information (i.e., OID, resource ID, transaction ID). The OID, generated by the RA, is assigned to the RS-DLT for a new IoT resource and then registered into the ORS, and the transaction ID is created by a DLT node. The DLT node stores all the information for identifying IoT resources with a generated key parameter, transaction ID.

9.1.2 Registration to ORS

At the second level, when the ORS is requested for the registration of the OID and URI by the RS-DLT, the ORS creates a record including related pairing information (OID and URI). This record is utilized to identify and discover the RS-DLT. If the ORS gets an input OID, the ORS returns a URI of the corresponding RS-DLT.

9.2 Resolution procedures

This clause presents the resolution procedure of the OID-based resolution framework with the transaction of the distributed ledger assigned to IoT resources as shown in Figure 4. This procedure assumes that all the components are interconnected for networking through the Internet, and information for networking to the RS-DLT and the ORS is announced. In addition, Figure 4 shows the procedure when a user requests sensing data of the IoT resource (named as sensor A), through the service provider (named as SP A).

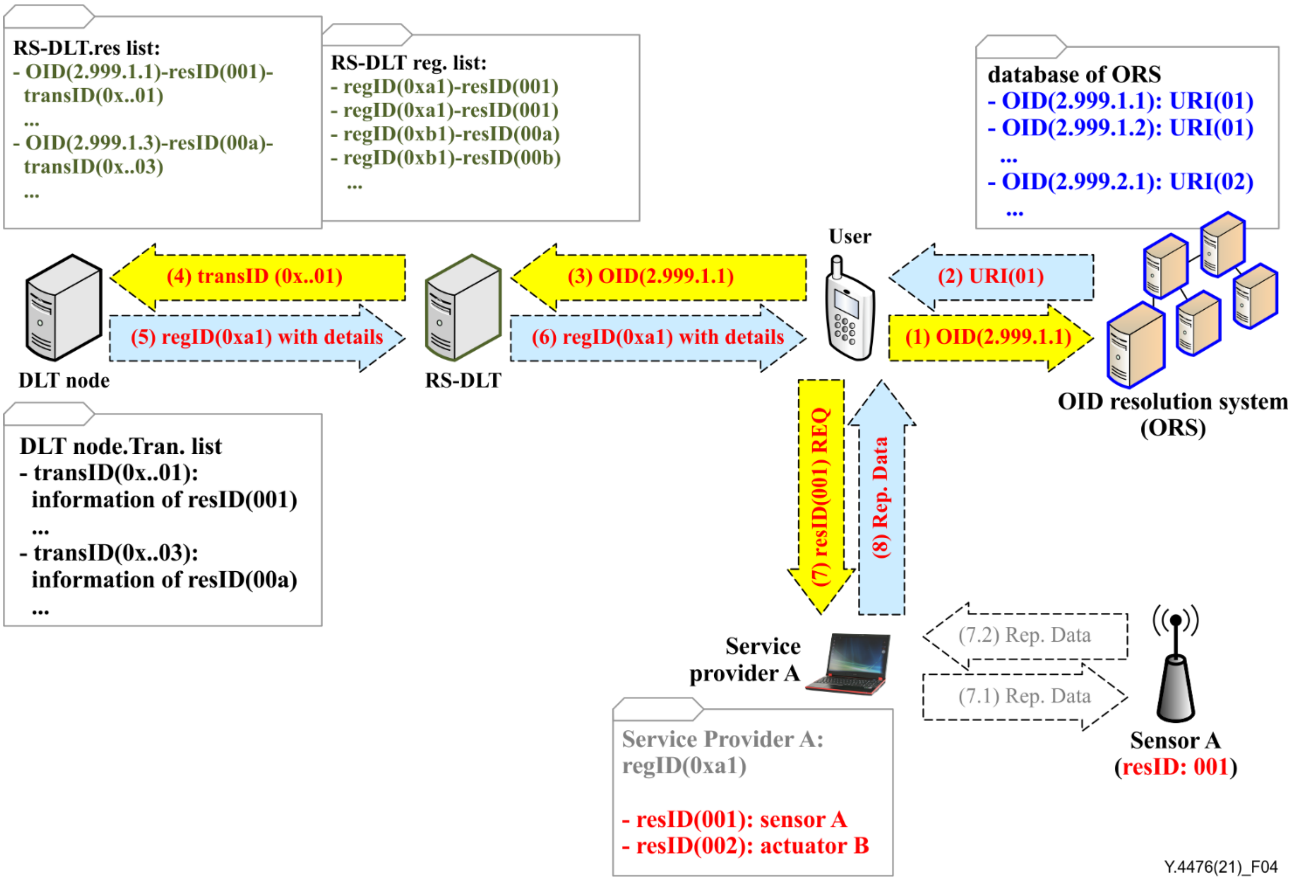

Figure 4 – Resolution procedures (requesting data to sensor A)

(1) The user sends the OID (e.g., 2.999.1.1) to the ORS.

The user requests sensing data from sensor A through the service provider A. The resource, sensor A, is assigned with an OID (2.999.1.1).

(2) The ORS retrieves a corresponding URI of the OID (2.999.1.1) from its database, and the corresponding URI (e.g., 01) of an RS-DLT is sent back from the ORS to the user's application.

(3) The user sends the OID (2.999.1.1) to the RS-DLT.

The user's application gets information for connection to the RS-DLT from the replied URI (01) information. The user's application sends the OID (2.999.1.1) to the RS-DLT for obtaining information about the IoT resource (sensor A).

(4) The RS-DLT resolves the OID (2.999.1.1) with a transaction ID (0x..01) for requesting detailed information of the resource (sensor A), and then the transaction ID is sent to the DLT node to get the information.

(5) The DLT node resolves the transaction ID (0x..01) with detailed information of the resource (sensor A), and then the information is sent back to the RS-DLT.

(6) The RS-DLT returns the information to the user.

The user gets all the information to connect to the IoT resource (sensor A).

(7) The user requests sensing data of the IoT resource (sensor A) to service provider A.

The service has connections with sensor A, and service provider A gets updated sensing data from sensor A.

(8) Service provider A returns the sensor data to the user.

NOTE – The interactions between service provider A and sensor A (step 1 and step 2) are not related to the OID resolution framework, so they are out of the scope of this Recommendation.

10 Security considerations

The data of IoT resources might be exposed to many security attacks, and third parties can exploit the data for illegal IoT services. To prevent these situations, the data should be secured during the interactions between users and service providers. The OID-based resolution framework guarantees the security of data during the resolution procedures from security threats (e.g., tampering of the communication, replay attack and denial of service (DoS)).

Bibliography

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

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, 2021